
Micro Focus Security

ArcSight ESM

CIP for NERC

Software Version: 6.00

Solutions Guide

Document Release Date: June, 2018

Software Release Date: June, 2018



Legal Notices

Warranty

The only warranties for products and services of Micro Focus and its affiliates and licensors ("Micro Focus") are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Micro Focus shall not be liable for technical or editorial errors or omissions contained herein. The information contained herein is subject to change without notice.

Restricted Rights Legend

Confidential computer software. Except as specifically indicated otherwise, a valid license from Micro Focus is required for possession, use or copying. Consistent with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items are licensed to the U.S. Government under vendor's standard commercial license.

Copyright Notice

© Copyright 2018 Micro Focus or one of its affiliates.

Trademark Notices

Adobe™ is a trademark of Adobe Systems Incorporated.

Microsoft® and Windows® are U.S. registered trademarks of Microsoft Corporation.

UNIX® is a registered trademark of The Open Group.

Support

Contact Information

Phone	A list of phone numbers is available on the Technical Support Page: https://softwaresupport.softwaregrp.com/support-contact-information
Support Web Site	https://softwaresupport.softwaregrp.com/
ArcSight Product Documentation	https://community.softwaregrp.com/t5/ArcSight-Product-Documentation/ctp/productdocs

Contents

Chapter 1: Solution for NERC CIP Overview and Architecture	5
ArcSight ESM CIP for NERC	5
NERC CIP Standards Addressed	6
Solution Architecture	6
Overview Dashboards	10
Notify, Investigate, Analyze, and Remediate	12
Notifications	12
Cases	12
Solution for NERC CIP Device Coverage	13
Chapter 2: Solution Installation and Configuration	14
Prepare for Installation	14
Prepare Environment	14
Verify Environment	15
Verify Supported Platforms	15
Install Solution for NERC CIP	16
Assign User Permissions	19
Configure Solution for NERC CIP	19
Model Assets (Assign Asset Categories)	22
CIP for NERC Categorization	22
Categorizing Assets and Zones	23
Configure Active Lists	30
Configure Active Lists Using Console Active List Editor	33
Configure Active Lists by Importing a CSV File	33
Configure My Filters	34
After Hours Filter	34
Intellectual Property Download Filter	35
Limit Regulation Filter	36
Deploy the Solution for NERC CIP Rules	37
Enable Data Monitors	39
Enable and Test Trends	39
Configure Cases	41
Configure Notifications	45
Configure Additional Resources	45

Build FlexConnector(s) for Physical Access Devices	45
Chapter 3: Solution for NERC CIP Resource Reference	48
Active Channels	48
Active Lists	54
Dashboards	56
Data Monitors	61
Field Sets	86
Filters	88
Focused Reports	115
Queries	116
Query Viewers	156
Reports	159
Rules	190
Trends	197
Use Cases	198
Appendix A: Supported Devices for Solution for NERC CIP v6.0 Reports	203
Appendix B: Mapping End User Resources to NERC CIPS	234
Appendix C: Compare, Backup, and Uninstall Packages	252
Generate a List of Resource Changes	252
Back Up the Solution Package	253
Uninstall the Solution for Solution for NERC CIP	253
Send Documentation Feedback	255

Chapter 1: Solution for NERC CIP Overview and Architecture

There has been an increased demand for regulations and enforceable reliability standards for the electric power industry, due to the following factors:

- Potential vulnerabilities in the North American electric utility systems to a cyber attack
- Potential for computer systems play a role in power disturbances
- Concern that a cyber attack or computer system failure could cause a wide spread power outage
- Increased public awareness about the risks

In response, the 2005 US Energy Policy Act (EPAct) legislated that an Electric Reliability Organization (ERO) be created to establish and enforce reliability standards for the bulk power system. In 2006, the Federal Energy Regulatory Commission approved the North American Electric Reliability Corporation (NERC) as the Electric Reliability Organization (ERO).

The mission of NERC is “to ensure the reliability of the bulk power system in North America”. To accomplish this mission, the North American Electric Reliability Corporation defines a set of Critical Infrastructure Protection (CIP) standards to help ensure the protection of electric utility operations and cyber assets.

ArcSight ESM CIP for NERC

The *Compliance Insight Package (CIP) for NERC v6.0*, coupled with ArcSight ESM, provides a security framework for monitoring, detecting, and responding to various cyberattacks and threats using the Defense Monitoring in Depth Model. This CIP also helps satisfy auditor expectations and to demonstrate compliance with the NERC standards.

The *Compliance Insight Package for NERC v.6.0* can assist you in complying with the NERC CIP Standards, by:

- Alerting and notifying when potentially hazardous events happen
- Providing real-time monitoring of risks and threats by correlating security events
- Monitoring actions, operations and processes on the network
- Displaying security events graphically which allows analysts to quickly analyze situations
- Generating reports that help show compliance to NERC CIP Standards
- Tracking potentially harmful users and machines
- Adhering to security policies and best practices

- Real-time monitoring, reporting of vulnerabilities, and configuration changes on critical BES Cyber assets

NERC CIP Standards Addressed

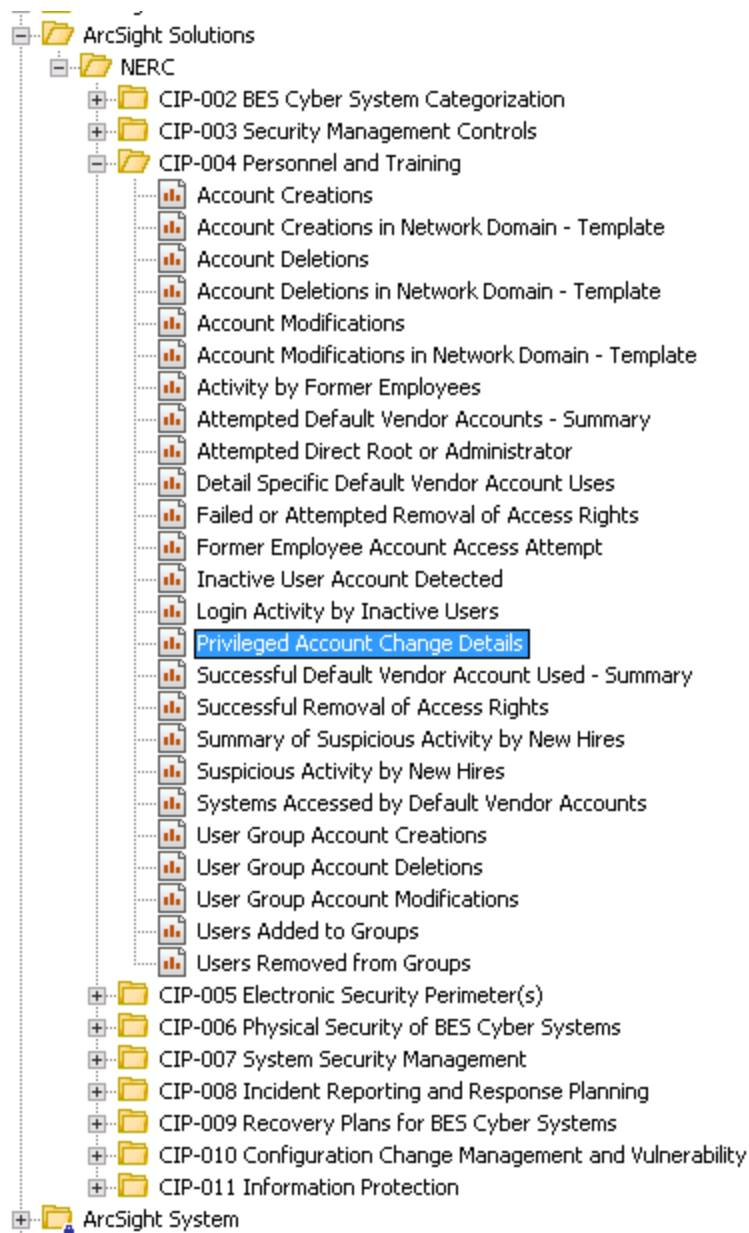
The ESM Compliance package for NERC addresses the following NERC Critical Infrastructure Protection standards:

CIP #	Title	CIP Version
002	Cyber Security : BES Cyber System Categorization	5.1
003	Cyber Security : Security Management Controls	6
004	Cyber Security : Personnel & Training	6
005	Cyber Security : Electronic Security Perimeter(s)	5
006	Cyber Security : Physical Security of BES Cyber Systems	6
007	Cyber Security : System Security Management	6
008	Cyber Security : Incident Reporting and Response Planning	5
009	Cyber Security : Recovery Plans for BES Cyber Systems	6
010	Cyber Security : Configuration Change Management and Vulnerability	2
011	Cyber Security : Information Protection	2

Resources for each CIP are discussed in detail in the following sections.

Solution Architecture

The *Solution for NERC CIP* provides ArcSight ESM resources that can assist with compliance to the NERC CIP Standards. Resources that help address a specific NERC CIP Standard are stored in the corresponding directory. For example, the Privileged Account Change Details report is provided to assist with compliance to NERC Standard CIP-004 and is stored in the CIP-004 Personnel and Training group as shown in the following figure.



In addition to the resources supplied to help address specific NERC CIP standards, there are a common set of filters and active lists that support the entire solution. These common resources are described in ["Solution Installation and Configuration" on page 14](#). These resources require configuration to tailor the content for your environment, such as privileged account names or the working hours in your organization. The following table describes each NERC CIP standard, the title of the CIP standard, and the purpose as defined by NERC. For all resources covered by Solution for NERC CIP, see ["Solution for NERC CIP Resource Reference" on page 48](#).

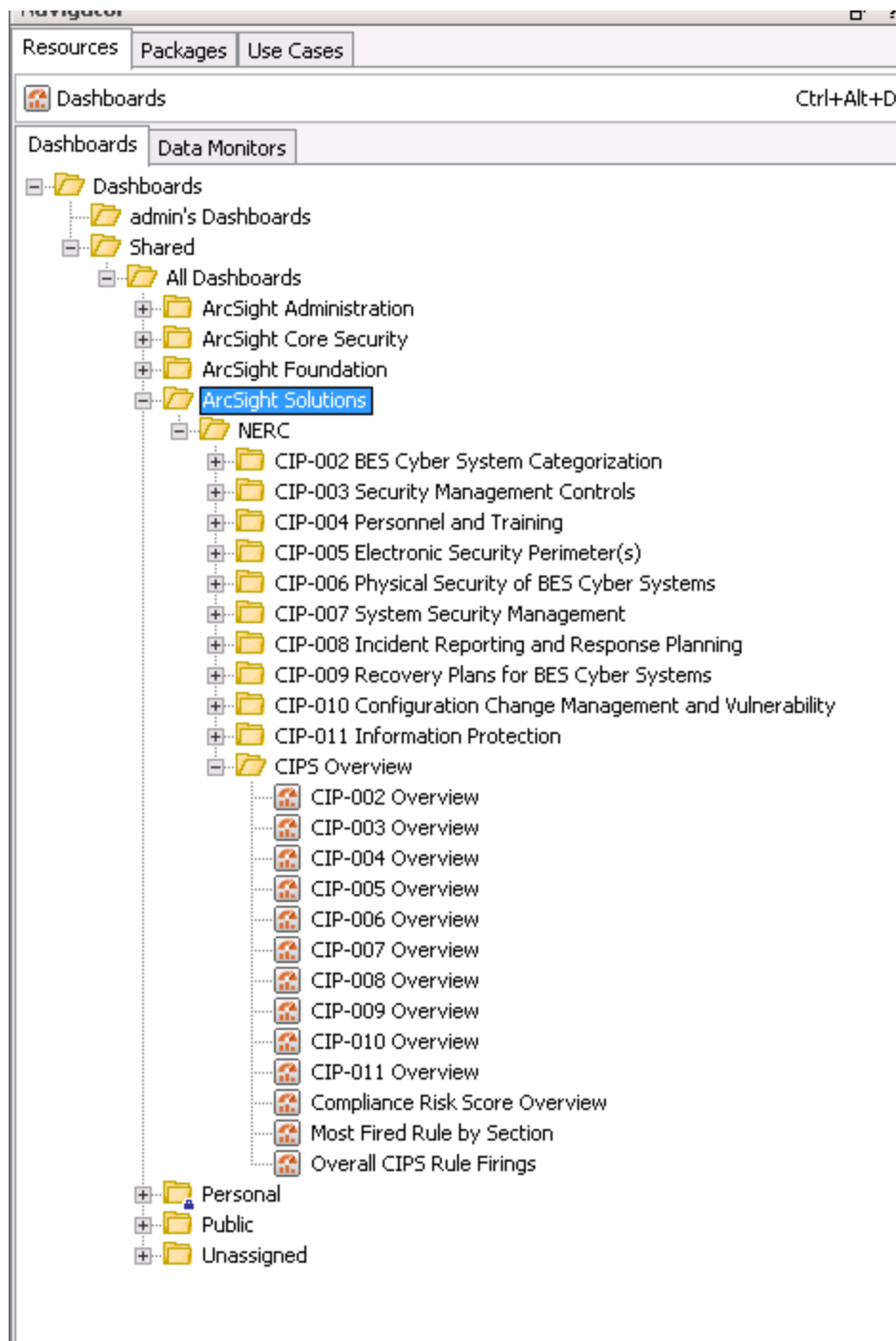
Number	Title	Purpose of NERC CIP Standard
CIP-002	Cyber Security - BES Cyber System Categorization	To identify and categorize BES Cyber Systems and their associated BES Cyber Assets for the application of cyber security requirements commensurate with the adverse impact that loss, compromise, or misuse of those BES Cyber Systems could have on the reliable operation of the BES. Identification and categorization of BES Cyber Systems support appropriate protection against compromises that could lead to misoperation or instability in the BES.
CIP-003	Cyber Security - Security Management Controls	To specify consistent and sustainable security management controls that establish responsibility and accountability to protect BES Cyber Systems against compromise that could lead to misoperation or instability in the Bulk Electric System (BES).
CIP-004	Cyber Security - Personnel and Training	To minimize the risk against compromise that could lead to misoperation or instability in the Bulk Electric System (BES) from individuals accessing BES Cyber Systems by requiring an appropriate level of personnel risk assessment, training, and security awareness in support of protecting BES Cyber Systems.
CIP-005	Cyber Security - Electronic Security Perimeter(s)	To manage electronic access to BES Cyber Systems by specifying a controlled Electronic Security Perimeter in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the BES.
CIP-006	Cyber Security - Physical Security of BES Cyber Systems	To manage physical access to Bulk Electric System (BES) Cyber Systems by specifying a physical security plan in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the BES.
CIP-007	Cyber Security - System Security Management	To manage system security by specifying select technical, operational, and procedural requirements in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the Bulk Electric System (BES).
CIP-008	Cyber Security - Incident Reporting and Response Planning	To mitigate the risk to the reliable operation of the BES as the result of a Cyber Security Incident by specifying incident response requirements.

Number	Title	Purpose of NERC CIP Standard
CIP-009	Cyber Security - Recovery Plans for BES Cyber Assets	To recover reliability functions performed by BES Cyber Systems by specifying recovery plan requirements in support of the continued stability, operability, and reliability of the BES.
CIP-010	Cyber Security - Configuration Change Management and Vulnerability Assessments	To prevent and detect unauthorized changes to BES Cyber Systems by specifying configuration change management and vulnerability assessment requirements in support of protecting BES Cyber Systems from compromise that could lead to misoperation or instability in the Bulk Electric System (BES).
CIP-011	Cyber Security - Information Protection	To prevent unauthorized access to BES Cyber System Information by specifying information protection requirements in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the Bulk Electric System (BES).

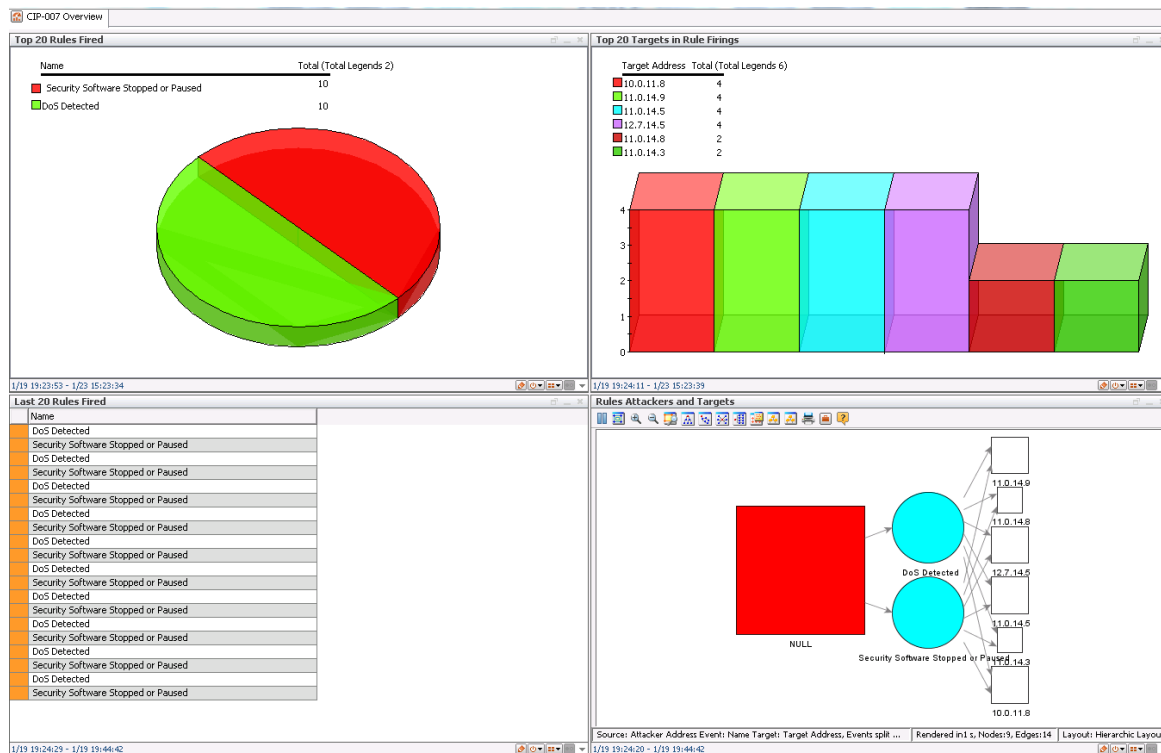
These Reliability Standards from the North American Electric Reliability Corporation website, which are being used by ArcSight for its software package entitled “*ArcSight* Compliance Insight Package for NERC v.6.0” (Solution for NERC CIP), are the property of the North American Electric Reliability Corporation and are available at <http://www.nerc.com/pa/Stand/Pages/CIPStandards.aspx>. This content may not be reproduced in whole or any part without the prior express written permission of the North American Electric Reliability Corporation. The Solution for NERC CIP is being provided for purposes of assisting end users in assessing compliance with certain rules, regulations and standards. Use of the Solution for NERC CIP does not guarantee compliance with the North American Electric Reliability Corporation Reliability Standards, rules, or regulations, and by accessing and using the Compliance Insight Package, the end user acknowledges and agrees that it is solely responsible for taking all steps necessary to achieve such compliance.

Overview Dashboards

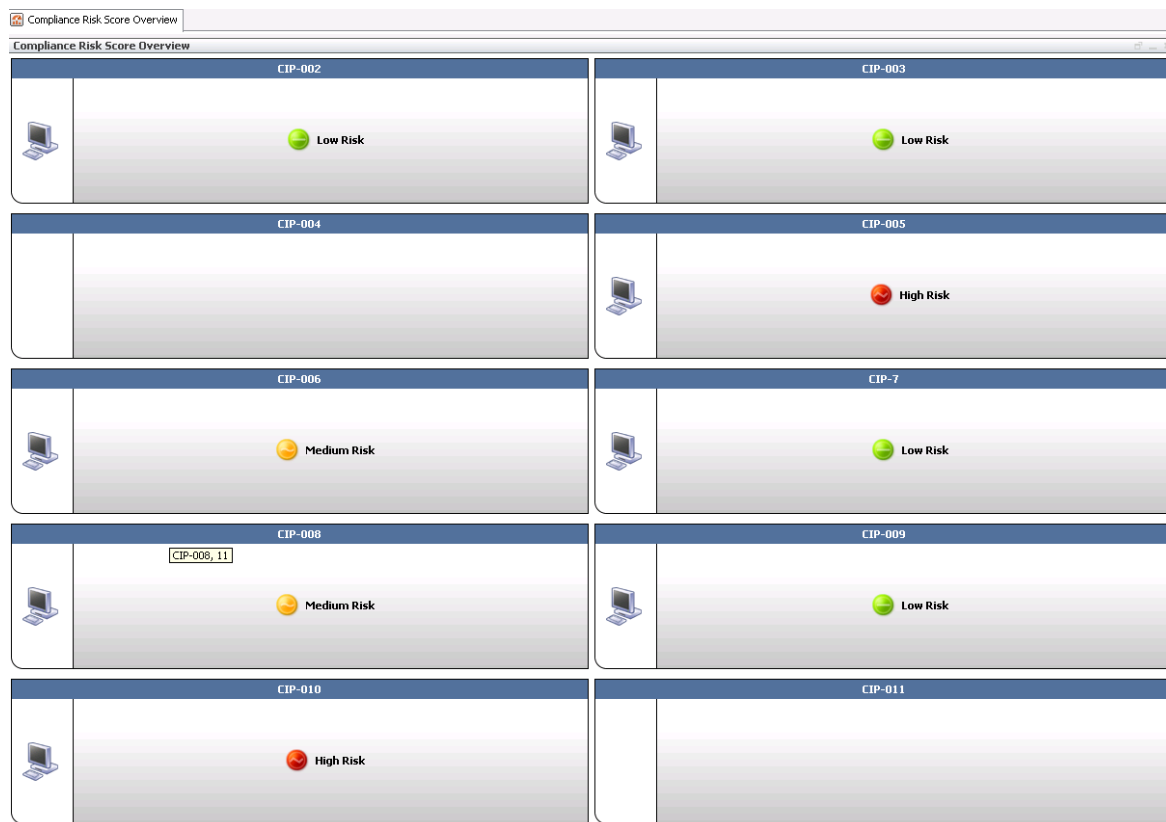
Overview dashboards are provided that summarize the compliance state determined by correlation rules for each NERC CIP Standard. The overview dashboards are available from the NERC/CIPS Overview group as shown in the following figure.



Each dashboard presents an event graph to show the relationships of the non-compliant systems with other systems on the network; a list of the last 20 triggered rules; a pie chart that breaks down the percentage of each triggered rule; and a bar chart that shows the top 20 targets of the triggered rules. The following figure shows the CIP-007 Overview dashboard.



The Compliance Risk Score Overview dashboard is a centralized heads-up display that shows the current state of compliance for each of the NERC CIP Standards by displaying the results of Compliance Risk Score Overview last-state data monitor. The dashboard summarizes your environment's overall state of compliance with the NERC CIPS as determined by correlation rules triggered for each family as shown in the following figure.



Notify, Investigate, Analyze, and Remediate

Once a security or compliance-related activity is identified, *Compliance Insight Package for NERC v.6.0* offers many ways to take action, investigate, and analyze.

Notifications



The first step in any escalation process is to notify the right people of a potential problem. You can configure the rules included in Solution for NERC CIP to activate your notification hierarchy in case of certain threats. You can configure this hierarchy to notify the right groups in the right situations. For more information, see ["Configure Notifications" on page 45](#).

Cases



Cases are ArcSight's built-in trouble-ticket system. When certain compliance-related conditions occur, the Solution for NERC CIP can be configured to open a case to track an issue so it can be investigated and properly remediated. For more information, see ["Configure Cases" on page 41](#).

Solution for NERC CIP Device Coverage

Solution for NERC CIP leverages event feeds from multiple sources. For a list of devices that are capable of generating events to populate the Solution for NERC CIP reports and other resources, see ["Supported Devices for Solution for NERC CIP v6.0 Reports" on page 203](#).

To gather events from physical access devices, such as badge readers, you must build FlexConnectors tailored to the type of physical access devices you use. For instructions about how to build and configure a FlexConnector for a physical access device, see ["Build FlexConnector\(s\) for Physical Access Devices" on page 45](#).

Chapter 2: Solution Installation and Configuration

This chapter contains information on installing and configuring the *Compliance Insight Package for NERC v.6.0* (Solution for NERC CIP).

Prepare for Installation

Before installing Solution for NERC CIP, complete the following preparation tasks:

1. ["Prepare Environment" below](#)
2. ["Verify Environment" on the next page](#)
3. ["Verify Supported Platforms" on the next page](#)

Prepare Environment

Before installing, prepare your environment for the Solution for NERC CIP:

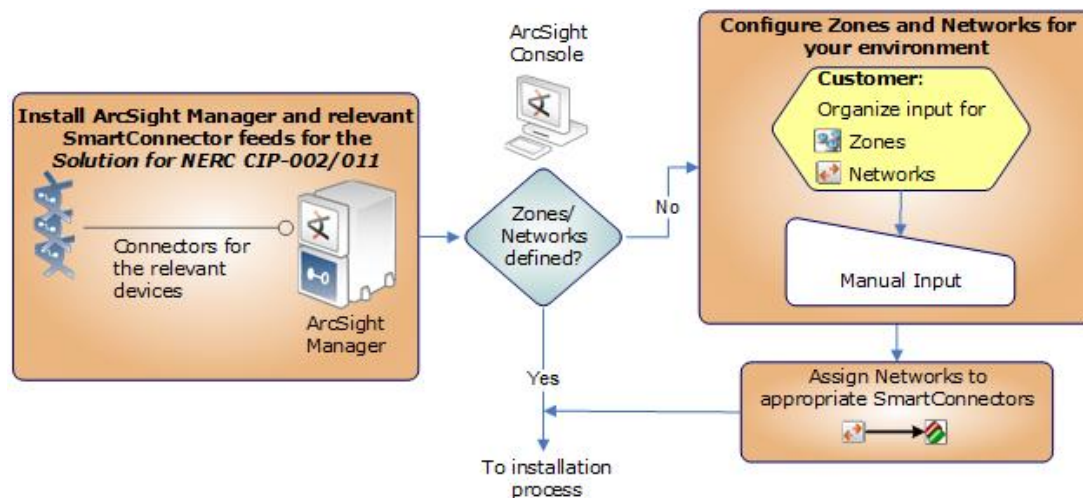
1. Install and configure the appropriate SmartConnectors for the devices found in your environment.

Note: The devices that provide events for the Solution for NERC CIP reports are listed in ["Supported Devices for Solution for NERC CIP v6.0 Reports" on page 203](#).

2. Model your network to include devices that supply events that help satisfy the NERC CIP standards. Verify that zones and networks are defined for your environment and that networks are assigned to the connectors reporting NERC CIP-relevant events into your ArcSight ESM Manager. Learn more about the ArcSight network modeling process in the *ArcSight ESM 101 Guide*. Find instructions for how to configure zones and networks in the *ArcSight Console online Help*, or the *ArcSight Console User's Guide*.

Note: RFC 1918 addresses(10.x.x.x, 192.168.x.x, 172.16-31.x.x) are automatically categorized as protected because their zones already are categorized as protected.

Prepare Your Environment



Verify Environment

Verify that your system has the ArcSight ESM Console connected to an ArcSight ESM Manager with this ESM product version installed and meets the prerequisite requirements.

Note: The Solution for NERC CIP is a self-contained solution that does not rely on any other ArcSight solution. You can install the Solution for NERC CIP with other solutions on the same Manager. Before installing new solutions, ArcSight recommends that you back up any existing solutions installed on the ESM Manager. For detailed instructions, see ["Compare, Backup, and Uninstall Packages" on page 252](#).

Updating from NERC CIP-002 to CIP-009 (Version 1.0) to NERC CIP-002 to CIP-011 (Version 6.0) requires :

1. Back up the old solution installed on the Manager, see ["Compare, Backup, and Uninstall Packages" on page 252](#).
2. Uninstall NERC CIP-002 to CIP-009 (Version 1.0).
3. Install NERC v6.0.

Verify Supported Platforms

Solution for NERC CIP operates on all supported Micro Focus ESM platforms 6.9.1 or higher, and is installed through the ArcSight ESM Console using the package import feature.

Install Solution for NERC CIP

Solution for NERC CIP is supplied in a single Micro Focus package bundle file called ArcSight-ComplianceInsightPackage-NERC.6.0<nnnn>.arb, where <nnnn> is the 4 character build number.

To install the Solution for NERC CIP package:

1. Using the log-in credentials supplied to you by Arcsight, download the Solution for NERC CIP package bundle from the Micro Focus software download site to the machine where you plan to launch the ArcSight ESM Console:

ArcSight-ComplianceInsightPackage-NERC.6.0.<nnnn>.arb

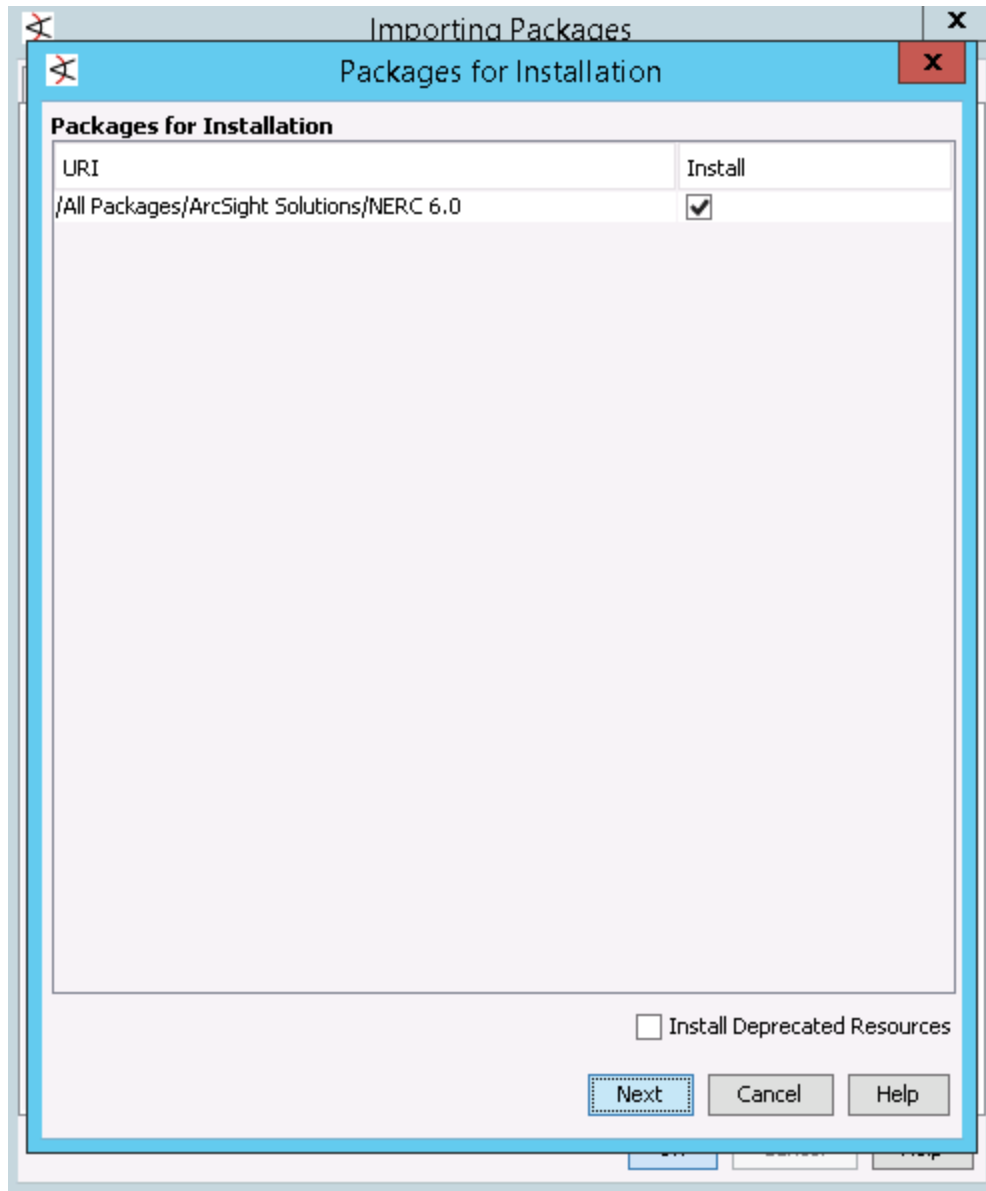
Where <nnnn> is the 4 character build number. (The exact build number is specified in the *ArcSight Compliance Insight Package for NERC v6.0 Release Notes*.)

Caution: If you use Internet Explorer to download the ARB file, it may convert the ARB file to a ZIP file. If this occurs, rename the ZIP file back to an ARB file before importing.

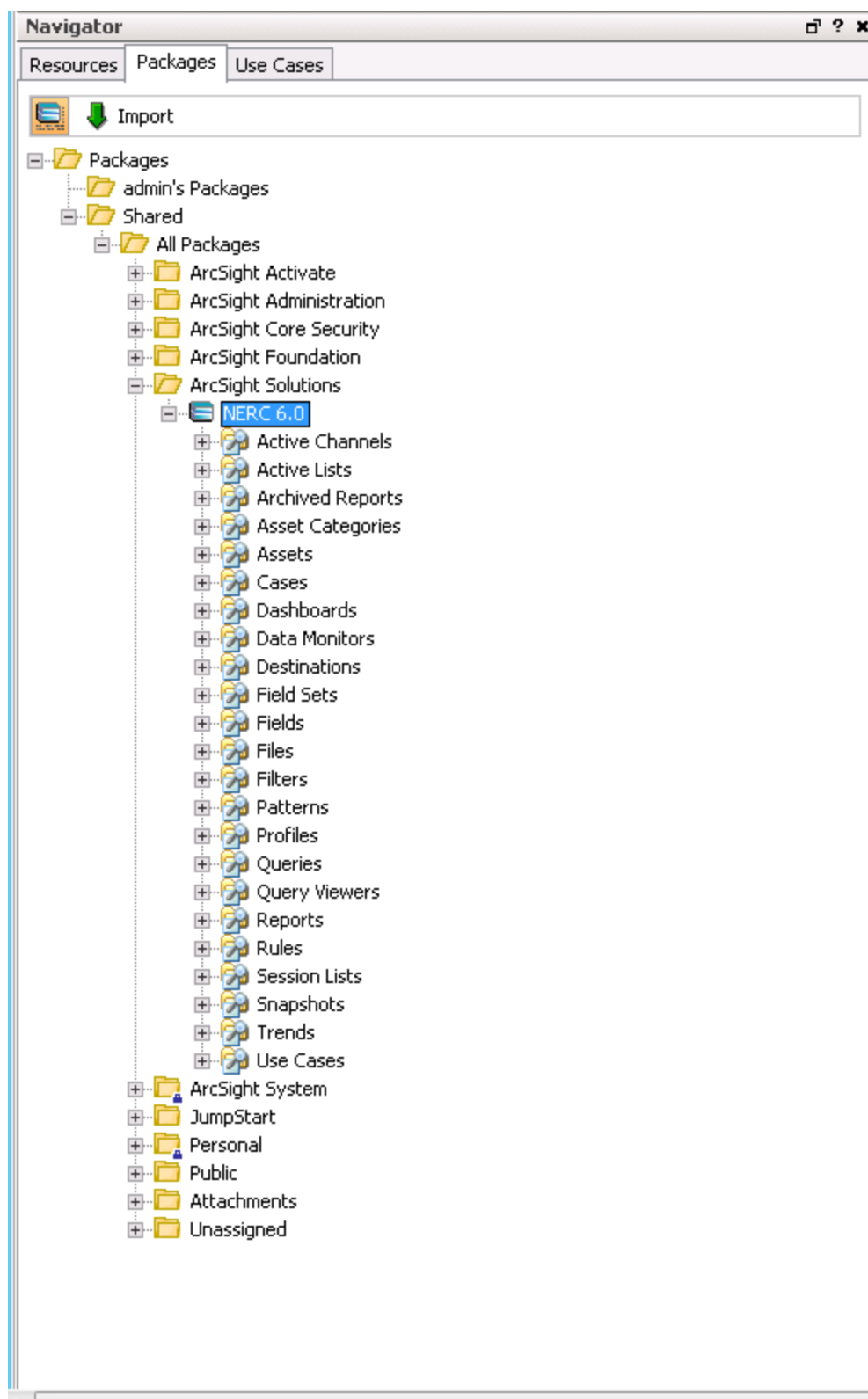
2. Log into the ArcSight ESM Console as a user with administrative privileges.
3. Click the **Packages** tab in the Navigator panel.
4. Click **Import** (↓).
5. In the Open dialog, browse and select the package bundle file and select **Open**.

The progress of the import of the package bundle is displayed in the Progress tab of the Importing Packages dialog.

When the import is complete, the Results tab of the Importing Packages dialog is displayed as well as the Packages for Installation dialog.



6. Leave the NERC 6.0 checkbox selected and in the Packages for Installation dialog, click **Next**.
The progress of the install is displayed in the Progress tab of the Installing Packages dialog. When the install is complete, the Results tab of the Installing Packages dialog displays the Summary Report.
7. In the Installing Packages dialog, click **OK**.
8. In the Importing Packages dialog, click **OK**.
9. To verify that the installation was successful and the content is accessible in the Navigator panel, expand the ArcSight Solutions/NERC 6.0 group.



Assign User Permissions

By default, users in the Default user group can view Solution for NERC CIP content, and users in the ArcSight Administrators and Analyzer Administrators user groups have read and write access to the solution content. Depending on how you have set up user access controls within your organization, you may need to adjust those controls to make sure the new content is accessible to the right users in your organization.

The following process assumes that you have user groups set up and users assigned to them.

In the following procedure, assign user permissions to all the following resource types:

- Active channels
- Active lists
- Cases
- Dashboards
- Data monitors
- Field Sets
- Filters
- Queries
- Reports
- Rules
- Session Lists
- Trends

To assign user permissions:

1. Log into the ArcSight ESM Console as a user with administrative privileges.
2. For all the resource types listed above, change the user permissions:
 - a. In the Navigator panel, go to the resource type and navigate to ArcSight Solutions/NERC.
 - b. Right-click the **NERC** group and select **Edit Access Control** to open the ACL editor in the Inspect/Edit panel.
 - c. In the ACL editor in the Inspect/Edit panel, select which user groups you want to have permissions to the Solution for NERC CIP resources and click **OK**.

Configure Solution for NERC CIP

Depending on the features you want to implement and how your network is set up, some configuration changes are required and some are optional. The list below shows all the configuration tasks involved

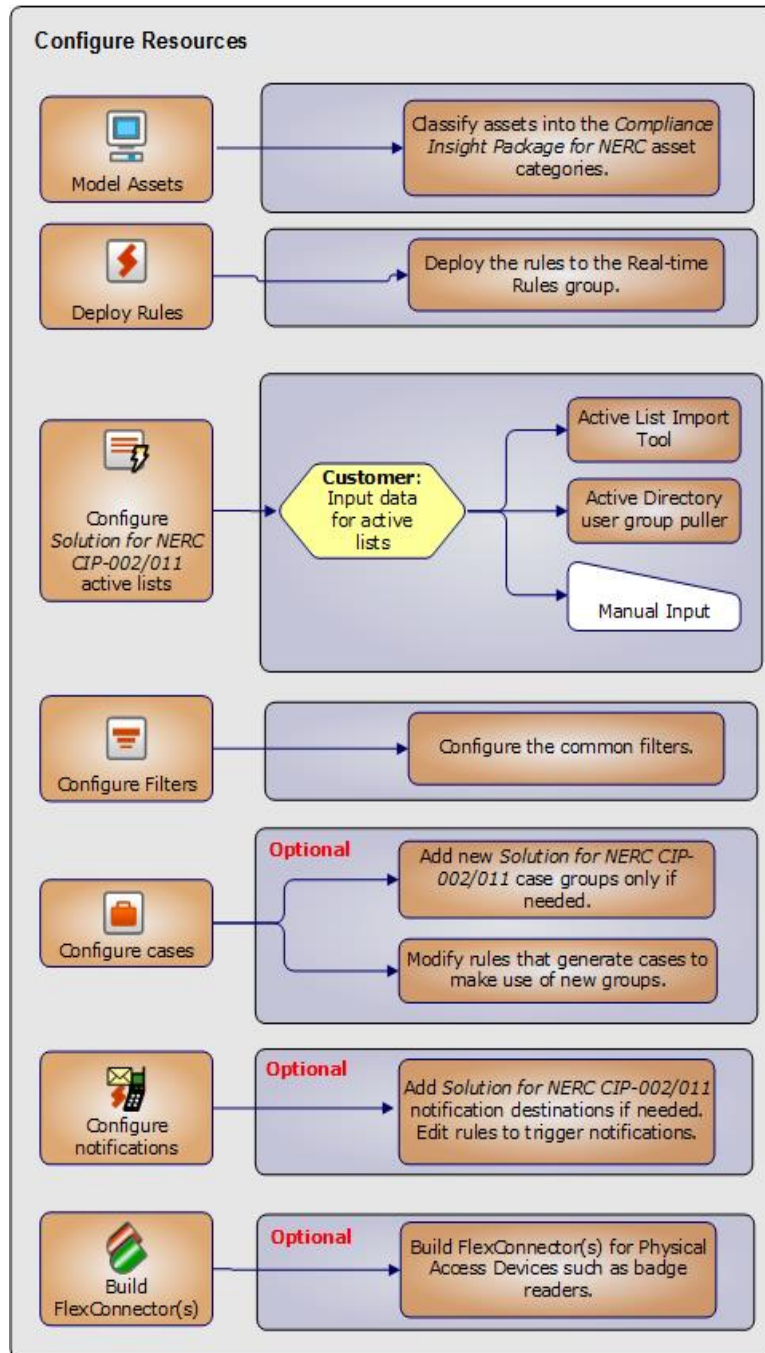
with the *Solution for NERC CIP* and where to find instructions for performing the configuration.

This section contains the instructions required to enable content for the *Solution for NERC CIP* and contains the following topics:

- ["Model Assets \(Assign Asset Categories\)" on page 22](#)
- ["Configure Active Lists" on page 30](#)
- ["Configure My Filters" on page 34](#)
- ["Deploy the Solution for NERC CIP Rules" on page 37](#)
- ["Configure Cases" on page 41](#)
- ["Configure Notifications " on page 45](#)
- ["Configure Additional Resources" on page 45](#)
- ["Build FlexConnector\(s\) for Physical Access Devices" on page 45](#)

The configuration processes outlined in this section (shown in the following figure) apply to resources that feed the *Solution for NERC CIP*.

Configure Resources

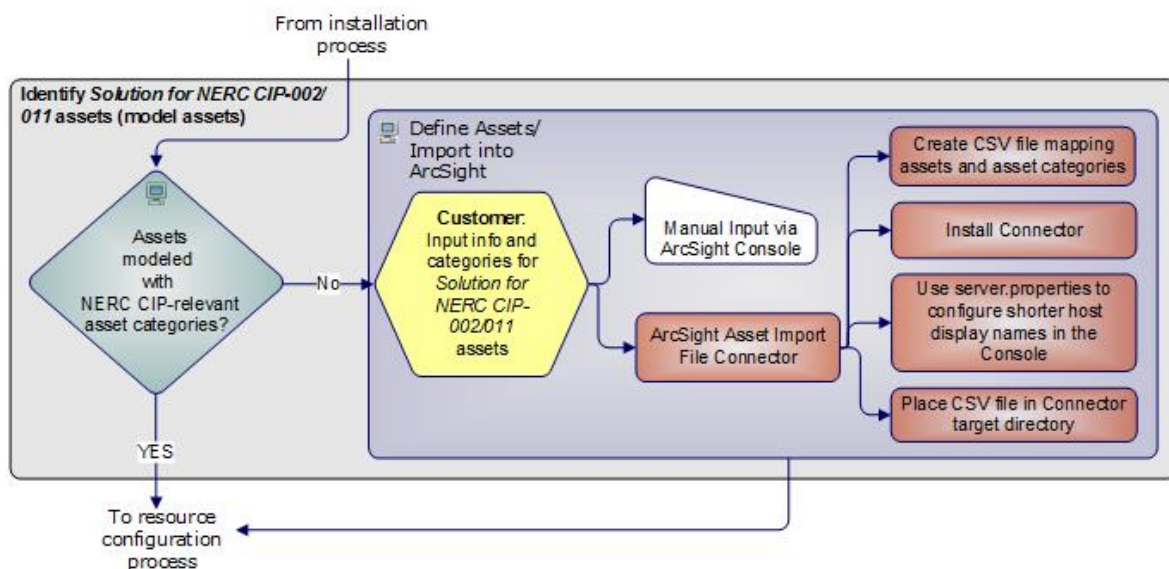


Model Assets (Assign Asset Categories)

Asset modeling is essential to enable *Solution for NERC CIP* content. Classifying assets in one or more of the solution asset categories is essential for the following reasons:

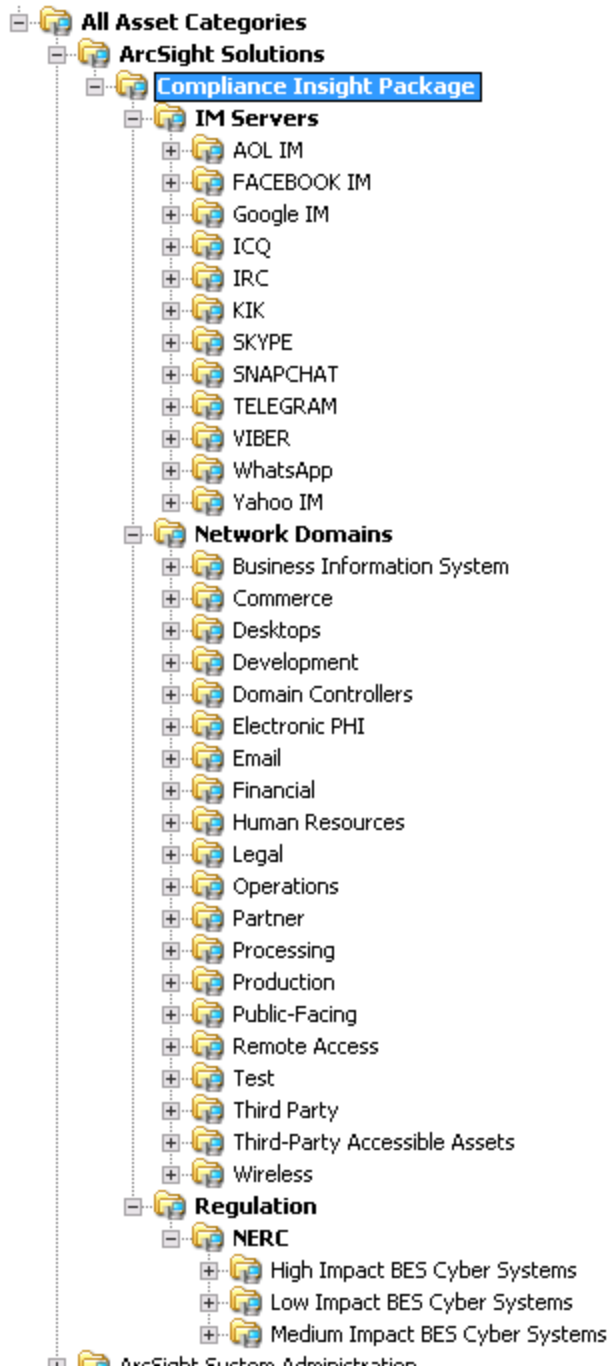
- Some of the *Solution for NERC CIP* content requires assets to be modeled in order to function correctly.
- In some cases, modeling assets adds valuable business context to the events evaluated by the *Solution for NERC CIP*.

Model Assets



CIP for NERC Categorization

CIP for NERC uses the asset categories under the /ArcSight Solutions/Compliance Insight Package/ group shown below.



Categorizing Assets and Zones

CIP for NERC relies on ArcSight asset and zone categorization to define your NERC environment. Certain content does not display unless assets or zones are categorized.

Below is a list of all asset and zone categorizations used and the filters which use those categorizations.

Filter	Asset Categorization	Zone Categorization
Target Asset is Wireless	/All Asset Categories/Arcsight Solutions/Compliance Insight Package/Network Domains/Wireless	/All Asset Categories/Arcsight Solutions/Compliance Insight Package/Network Domains/Wireless
Attacker Asset is Wireless	/All Asset Categories/Arcsight Solutions/Compliance Insight Package/Network Domains/Wireless	/All Asset Categories/Arcsight Solutions/Compliance Insight Package/Network Domains/Wireless
Database Target Host	/All Asset Categories/Site Asset Categories/Business Role/Service/Database /All Asset Categories/Arcsight System Administration/Databases	/All Asset Categories/Site Asset Categories/Business Role/Service/Database /All Asset Categories/Arcsight System Administration/Databases
Target Asset in High Impact BES Cyber Assets	/All Asset Categories/Arcsight Solutions/Compliance Insight Package/Regulation/High Impact BES Cyber Systems	/All Asset Categories/Arcsight Solutions/Compliance Insight Package/Regulation/High Impact BES Cyber Systems
Target Asset in Medium Impact BES Cyber Assets	/All Asset Categories/Arcsight Solutions/Compliance Insight Package/Regulation/Medium Impact BES Cyber Systems	/All Asset Categories/Arcsight Solutions/Compliance Insight Package/Regulation/Medium Impact BES Cyber Systems
Target Asset in Low Impact BES Cyber Assets	/All Asset Categories/Arcsight Solutions/Compliance Insight Package/Regulation/Low Impact BES Cyber Systems	/All Asset Categories/Arcsight Solutions/Compliance Insight Package/Regulation/Low Impact BES Cyber Systems
Attacker Asset in High Impact BES Cyber Assets	/All Asset Categories/Arcsight Solutions/Compliance Insight Package/Regulation/High Impact BES Cyber Systems	/All Asset Categories/Arcsight Solutions/Compliance Insight Package/Regulation/High Impact BES Cyber Systems
Attacker Asset in Medium Impact BES Cyber Assets	/All Asset Categories/Arcsight Solutions/Compliance Insight Package/Regulation/Medium Impact BES Cyber Systems	/All Asset Categories/Arcsight Solutions/Compliance Insight Package/Regulation/Medium Impact BES Cyber Systems
Attacker Asset in Low Impact BES Cyber Assets	/All Asset Categories/Arcsight Solutions/Compliance Insight Package/Regulation/Low Impact BES Cyber Systems	/All Asset Categories/Arcsight Solutions/Compliance Insight Package/Regulation/Low Impact BES Cyber Systems
Target Asset in Highly Critical Assets	/All Asset Categories/System Asset Categories/Criticality/Very High /All Asset Categories/System Asset Categories/Criticality/High	/All Asset Categories/System Asset Categories/Criticality/Very High /All Asset Categories/System Asset Categories/Criticality/High

Filter	Asset Categorization	Zone Categorization
Asset Categorized in Network Domains	/All Asset Categories/Arcsight Solutions/Compliance Insight Package/Network Domains/	
Internal Attackers	/All Asset Categories/Site Asset Categories/Address Spaces/Protected	/All Asset Categories/Site Asset Categories/Address Spaces/Protected
Internal Targets	/All Asset Categories/Site Asset Categories/Address Spaces/Protected	/All Asset Categories/Site Asset Categories/Address Spaces/Protected
Traffic from Higher to Lower Classification Level	/All Asset Categories/Site Asset Categories/Business Impact Analysis/Classification/Unclassified	/All Asset Categories/Site Asset Categories/Business Impact Analysis/Classification/Unclassified
	/All Asset Categories/Site Asset Categories/Business Impact Analysis/Classification/Secret	/All Asset Categories/Site Asset Categories/Business Impact Analysis/Classification/Secret
	/All Asset Categories/Site Asset Categories/Business Impact Analysis/Classification/Top Secret	/All Asset Categories/Site Asset Categories/Business Impact Analysis/Classification/Top Secret
Traffic from Lower to Higher Classification Level	/All Asset Categories/Site Asset Categories/Business Impact Analysis/Classification/Unclassified	/All Asset Categories/Site Asset Categories/Business Impact Analysis/Classification/Unclassified
	/All Asset Categories/Site Asset Categories/Business Impact Analysis/Classification/Secret	/All Asset Categories/Site Asset Categories/Business Impact Analysis/Classification/Secret
	/All Asset Categories/Site Asset Categories/Business Impact Analysis/Classification/Top Secret	/All Asset Categories/Site Asset Categories/Business Impact Analysis/Classification/Top Secret
Network IDS Configuration Modifications	/All Asset Categories/Site Asset Categories/Business Impact Analysis/Business Role/Security Devices/NIDS	/All Asset Categories/Site Asset Categories/Business Impact Analysis/Business Role/Security Devices/NIDS
Firewall Configuration Modifications	/All Asset Categories/Site Asset Categories/Business Impact Analysis/Business Role/Security Devices/Firewall	/All Asset Categories/Site Asset Categories/Business Impact Analysis/Business Role/Security Devices/Firewall

Filter	Asset Categorization	Zone Categorization
Successful User Logins from Third Party Systems	/All Asset Categories/Arcsight Solutions/Compliance Insight Package/Network Domains/Third Party	/All Asset Categories/Arcsight Solutions/Compliance Insight Package/Network Domains/Third Party
Unsuccessful User Logins from Third Party Systems	/All Asset Categories/Arcsight Solutions/Compliance Insight Package/Network Domains/Third Party	/All Asset Categories/Arcsight Solutions/Compliance Insight Package/Network Domains/Third Party
Successful User Logins to Third Party Systems	/All Asset Categories/Arcsight Solutions/Compliance Insight Package/Network Domains/Third Party	/All Asset Categories/Arcsight Solutions/Compliance Insight Package/Network Domains/Third Party
Unsuccessful User Logins to Third Party Systems	/All Asset Categories/Arcsight Solutions/Compliance Insight Package/Network Domains/Third Party	/All Asset Categories/Arcsight Solutions/Compliance Insight Package/Network Domains/Third Party
Successful Administrative Logins from Third Party Systems	/All Asset Categories/Arcsight Solutions/Compliance Insight Package/Network Domains/Third Party	/All Asset Categories/Arcsight Solutions/Compliance Insight Package/Network Domains/Third Party
Unsuccessful Administrative Logins from Third Party Systems	/All Asset Categories/Arcsight Solutions/Compliance Insight Package/Network Domains/Third Party	/All Asset Categories/Arcsight Solutions/Compliance Insight Package/Network Domains/Third Party
Successful Administrative Logins to Third Party Systems	/All Asset Categories/Arcsight Solutions/Compliance Insight Package/Network Domains/Third Party	/All Asset Categories/Arcsight Solutions/Compliance Insight Package/Network Domains/Third Party
Unsuccessful Administrative Logins to Third Party Systems	/All Asset Categories/Arcsight Solutions/Compliance Insight Package/Network Domains/Third Party	/All Asset Categories/Arcsight Solutions/Compliance Insight Package/Network Domains/Third Party
Communications between Test and Operations	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/Operations	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/Operations
	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/Test	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/Test

Filter	Asset Categorization	Zone Categorization
Communications between Development and Test	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/Development	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/Development
	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/Test	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/Test
Communications between Development and Operations	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/Development	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/Development
	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/Operations	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/Operations

Filter	Asset Categorization	Zone Categorization
IM Traffic	/ArcSight Solutions/Compliance Insight Package/IM Servers/Yahoo IM	/ArcSight Solutions/Compliance Insight Package/IM Servers/Yahoo IM
	/ArcSight Solutions/Compliance Insight Package/IM Servers/Google IM	/ArcSight Solutions/Compliance Insight Package/IM Servers/Google IM
	/ArcSight Solutions/Compliance Insight Package/IM Servers/AOL IM	/ArcSight Solutions/Compliance Insight Package/IM Servers/AOL IM
	/ArcSight Solutions/Compliance Insight Package/IM Servers/ICQ	/ArcSight Solutions/Compliance Insight Package/IM Servers/ICQ
	/ArcSight Solutions/Compliance Insight Package/IM Servers/IRC	/ArcSight Solutions/Compliance Insight Package/IM Servers/IRC
	/ArcSight Solutions/Compliance Insight Package/IM Servers/FACEBOOK IM	/ArcSight Solutions/Compliance Insight Package/IM Servers/FACEBOOK IM
	/ArcSight Solutions/Compliance Insight Package/IM Servers/KIK	/ArcSight Solutions/Compliance Insight Package/IM Servers/KIK
	/ArcSight Solutions/Compliance Insight Package/IM Servers/SKYPE	/ArcSight Solutions/Compliance Insight Package/IM Servers/SKYPE
	/ArcSight Solutions/Compliance Insight Package/IM Servers/SNAPCHAT	/ArcSight Solutions/Compliance Insight Package/IM Servers/SNAPCHAT
	/ArcSight Solutions/Compliance Insight Package/IM Servers/TELEGRAM	/ArcSight Solutions/Compliance Insight Package/IM Servers/TELEGRAM
	/ArcSight Solutions/Compliance Insight Package/IM Servers/VIBER	/ArcSight Solutions/Compliance Insight Package/IM Servers/VIBER
	/ArcSight Solutions/Compliance Insight Package/IM Servers/WhatsApp	/ArcSight Solutions/Compliance Insight Package/IM Servers/WhatsApp

Filter	Asset Categorization	Zone Categorization
Traffic from Dark Address Space	/All Asset Categories/Site Asset Categories/Address Spaces/Dark	/All Asset Categories/Site Asset Categories/Address Spaces/Dark
Traffic to Dark Address Space	/All Asset Categories/Site Asset Categories/Address Spaces/Dark	/All Asset Categories/Site Asset Categories/Address Spaces/Dark

You can assign the solution asset categories with the following methods:

One-by-one using the ArcSight Console

Use this method if you have only a few assets to categorize. One asset can be categorized in more than one asset category. To categorize your assets one-by-one:

1. In the Navigator panel, go to **Assets** and select the **Assets** tab.
2. On the **Asset** tab, expand the groups listed.
3. For each asset you want to classify with an asset category, repeat the following steps:
 - a. Right-click the asset you want to categorize and select **Edit Asset**.
 - b. In the Inspect/Edit panel, click the **Categories** tab. Click the add icon (+) at the top of the screen to select new resources.
 - c. In the Asset Categories Selector pop-up window, navigate to the appropriate network domain category and click **OK**.

After you assign your assets to the Compliance Insight Package asset categories, you can also assign them to other asset categories, either within the solution package or the general ArcSight categories, or those you have created yourself.

Using the Network Model Wizard

A Network Model wizard is provided on the ArcSight Console (menu option **Tools > Network Model**). The Network Model wizard enables you to quickly populate the ESM network model by batch loading asset and zone information from comma-separated value (CSV) files. For more information, see the ArcSight Console User's Guide.

Using the ArcSight Asset Import File Connector

If you have many assets that you want to track, you can configure them in a batch using the ArcSight Asset Import File Connector. This connector can also create new assets as part of the batch function. The ArcSight Asset Import File Connector is available as part of the ArcSight SmartConnector download. For instructions about how to use this connector to configure your assets for CIP for NERC see the ArcSight Asset Import File SmartConnector Configuration Guide.

Configure Active Lists

Solution for NERC CIP contains numerous active lists that retain specific data that is cross-referenced dynamically during run-time by Micro Focus resources that use conditions, such as filters, rules, and reports.

You can populate the *Solution for NERC CIP* active lists using any of the following processes:

- Add entries to active lists, one-by-one, using the Active List editor in the ArcSight ESM Console. For detailed instructions, see ["Configure Active Lists Using Console Active List Editor" on page 33](#). This method can be used to populate active lists with one, two, or more columns.
- Add entries in batch to active list from a comma separated value (CSV) file. For detailed instructions see ["Configure Active Lists by Importing a CSV File" on page 33](#). This method can be used to populate active lists with one, two, or more columns.

Some active lists are intended to be populated by rules and other required configurations. The following table defines all the active lists for the *Solution for NERC CIP* and their configuration requirements.

Active List	Description	Configuration Required	Expected Input Per Entry
Active Accounts	This active list stores user names who have successfully logged in within the last 30 days.	No	
Administrative Accounts List	<p>This active list should be populated with the usernames that have administrative privileges in your domain. Admins (those responsible for managing administrative users) populate this list manually whenever a new administrative user is added. Entries to this list are read by reports supplied in the content pack, but the list can also be added to or referenced in new content built around the provided infrastructure.</p> <p>This active list should be populated with the usernames that have administrative privileges in your domain. Entries in this list should be in all lower case. For example, the user Administrator should be added as "administrator".</p>	Yes	User name, in lowercase.


Active List	Description	Configuration Required	Expected Input Per Entry
Allowed Ports	<p>This active list contains all permissible destination ports (all permissible services). This active list should be populated according to your site policy.</p> <p>By default, all connection types and ports are allowed. To be considered a disallowed port, the connection type and port number must either be specified explicitly in the <code>Disallowed Ports</code> active list, or not specified in the <code>Allowed Ports</code> active list. If all ports are specified in the <code>Allowed Ports</code> active list (using the * character), the policy allows all ports (except those specified explicitly in the <code>Disallowed Ports</code> active list). Explicit (that is, not *) port entries in the <code>Disallowed Ports</code> active list always take precedence over entries in the <code>Allowed Ports</code> active list.</p>	Yes	Connection type and port number Where Connection type could be : Inbound, outbound or internal
Audit Log Cleared	This active list should be populated only by the rule Audit Log Cleared. It logs every time an audit log is cleared.	No	
Badged In	This list contains information about employees who are badged in.	No	
Badged Out	This active list contains the computer accounts of badged out employees.	No	
Badges to Accounts	This list contains the computer account and employee type for every physical device badge.	Yes	Badge ID, primary computer account for the badgeholder, and the employee type (in lowercase). Specifically, ensure that contractors are identified with the word "Contractor" (case insensitive) in the <code>employee type</code> field.
Compliance Score	This active list maintains the compliance risk score for each regulation section. The compliance risk score is calculated based on the triggered rules in the solution package. You can manually change the score as required. This change will be reflected in the Compliance Risk Score dashboard.	No	
Default Vendor Accounts	This active list contains the default user account names for various vendors. This list should be configured at set-up time with existing vendor user account names, and updated as necessary on an ongoing basis.	Yes	Default user account and vendor name, in lowercase.

Active List	Description	Configuration Required	Expected Input Per Entry
Disallowed Ports	<p>This active list contains all disallowed destination ports. This active list should be populated according to your site policy.</p> <p>By default, all connection types and ports are allowed. To be considered a disallowed port, the connection type and port number must either be specified explicitly in the Disallowed Ports active list, or not specified in the Allowed Ports active list. If all ports are specified in the Allowed Ports active list (using the * character), the policy allows all ports (except those specified explicitly in the Disallowed Ports active list). Explicit (that is, not *) port entries in the Disallowed Ports active list always take precedence over entries in the Allowed Ports active list.</p>	Yes	Connection type and port number Where Connection type could be : inbound, outbound or internal
Former Employees	This active list contains user accounts of former employees. User accounts in this active list are retained indefinitely. All the entries in this list need to be in lowercase.	Yes	User Name, in lowercase. This list should be maintained on a regular basis.
Insecure Ports	This active list includes ports related to unencrypted and thus insecure communication services.	Yes	Port number
Insecure Processes	This active list includes the names of processes that provide unencrypted and thus insecure communications.	Yes	Process name, in lowercase
Instant Messaging Domains	This active list contains all the DNS domains for public instant messaging servers. This list is used to detect when outbound traffic to these domains is detected, signifying a possible information leak. Note: All the domain names must be in lowercase.	Yes	Domain name of popular or known instant messaging server in lowercase
Internal Systems with Insecure Services	This list stores all internal systems with insecure services detected, populated only by the rule "Internal Insecure Service Provider Detected" .	No	
Internet Ports	This active list includes ports that are used for monitoring Internet (Web traffic) communication. By default it includes ports 80,443.	Yes	Port number
New Assets	This active list contains new assets and is automatically populated by the "New Host Detected" rule. New assets are retained for 7 days in the list.	No	
New Hire Accounts	This active list contains newly hired users and is automatically populated by the "New Hire Identification" rule. New users are retained for 7 days in the list.	Yes	User Name, in lowercase. This list should be maintained on a regular basis.

Active List	Description	Configuration Required	Expected Input Per Entry
Password Changes	This active is updated with the user and product information when a successful password change occurs.	No	
Stale Accounts	This active list is used to maintain user names that have not appeared in login events for the time specified by the Active Accounts active list TTL value.	No	
Suspicious Activities by New Hires	This active list stores events that were identified as attacks by new hires. The original event name is stored in the deviceCustomString1 field. By default, these events are stored for 60 days.	No	

Configure Active Lists Using Console Active List Editor

You can add entries to active lists, one-by-one, using the Active List editor of the ArcSight ESM Console.

1. In the Navigator panel, go to Lists and navigate to ArcSight/Solutions/NERC.
2. Right-click the active list you wish to populate and select **Show Entries**. The active list details are displayed in the Viewer panel.
3. For each entry you wish to add to the active list, repeat the following steps:
 - a. To add an entry to the list, click the add icon () in the active list header.
 - b. In the Active List Entry editor of the Inspect/Edit panel, enter values for each column in the list except for the dynamic columns listed in the following table and click **Add**.

Name	Value
Creation Time	This field is reserved for active lists that are populated dynamically by rule actions. Leave this field blank.
Last Seen Time	This field is reserved for active lists that are populated dynamically by rule actions. Leave this field blank.
Count	This field is reserved for active lists that are populated dynamically by rule actions. Leave this field unchanged.

Configure Active Lists by Importing a CSV File

Active lists can be populated in a single step, by importing entries from an existing CSV file. The number of columns in the active list must match the number of comma separated values in the CSV file. For example, if the active list has two columns of data, the imported CSV file must have two comma-separated fields. Do not include columns for Creation Time, Modification Time, or Count in the CSV file.

1. In the Active Lists resource tree of the ArcSight ESM Console, right-click an active list and choose **Import CSV File**.

A file browser displays.

2. Browse to find the CSV file you want to import, select it, and click **Open**. The Import Preview dialog displays the data from the CSV file to be imported into the active list.
3. To add the entries from the selected file into the active list, in the Import Preview dialog, click **OK**. The new entries from the file are appended to the existing entries in the active list.
4. To verify that your entries were imported as expected, right-click the active list you just populated with the CSV file and select **Show Entries**.

This displays the newly-added data from the CSV file in the Viewer panel as active list details.

Tip: By default, the active list displays 2000 entries at a time. To view entries outside the range shown, create an active list filter that specifies a different range (click **Filter** in the active list header).

Configure My Filters

Configure the following common filters stored in the My Filters group to reflect your organization:

- ["After Hours Filter" below](#)
- ["Intellectual Property Download Filter" on the next page](#)
- ["Limit Regulation Filter" on page 36](#)

After Hours Filter

The After Hours filter defines the time period which is considered to be after business hours. The default after hours time period is set to 8:00 p.m. to 6:00 a.m. on weekdays, and all day Saturday and Sunday.



The filter uses two variables:

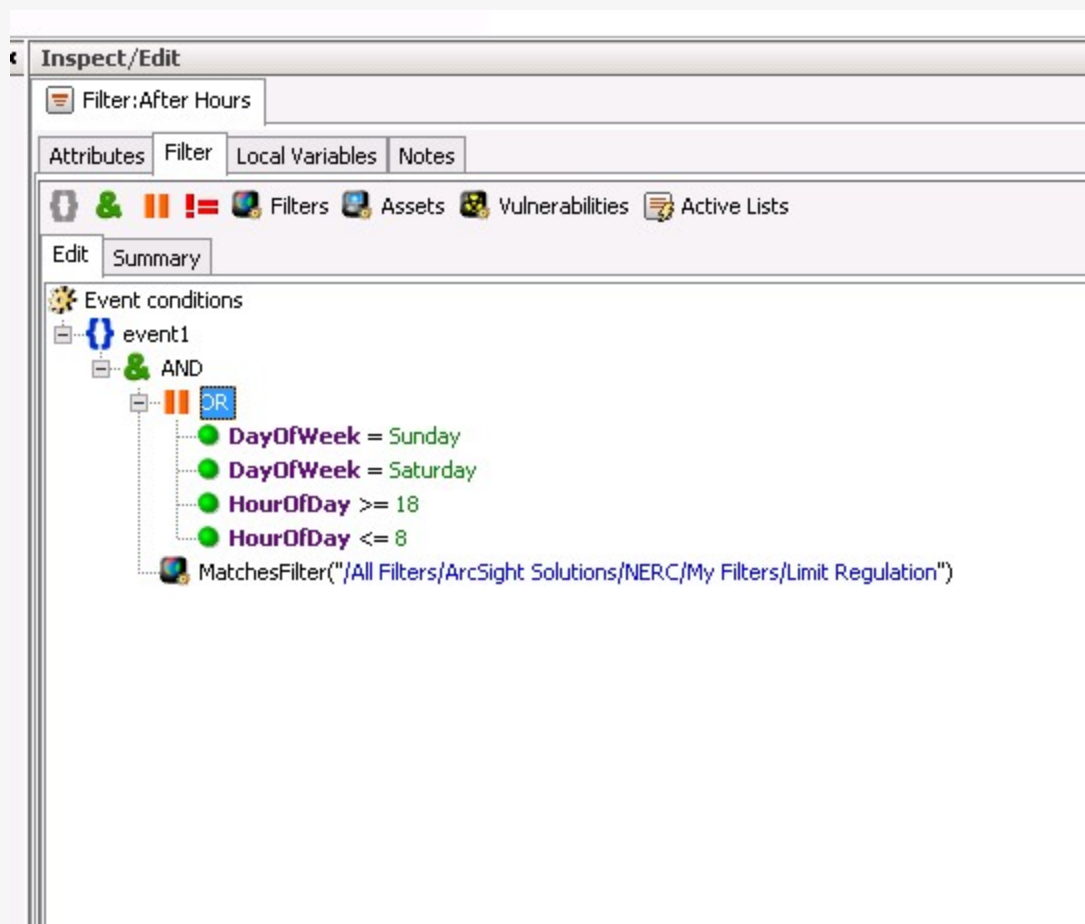
- DayOfWeek
- HourOfDay

You can change this filter to match what is considered to be after hours for your organization.

Tip: The DayOfWeek variable returns an integer value that is displayed on the ArcSight ESM Console as a string value of the current day: Saturday, Sunday, Monday, Tuesday, Wednesday, Thursday, or Friday. Since the DayOfWeek variable is an integer, you can specify a range of days such as (DayOfWeek >= Monday AND DayOfWeek <= Friday).

The HourOfDay variable returns a numerical value for the current hour in 24-hour format ranging from 12 AM = 0 to 11 PM = 23.

For example, to redefine the after business hours from 6:00 PM to 8:00 AM on all weekdays and all of Saturday and Sunday use the filter shown in the following figure.



Intellectual Property Download Filter

The Intellectual Property Download filter finds events that involve the download of possibly illegal intellectual property. By default, this filter is set to find a Snort signature that indicates video or audio download. Add the signatures for the content monitoring device(s) or NIDS you use that indicate intellectual property downloads, such as video streams, images, audio files, or possibly illegal intellectual property or copyrighted material.

Limit Regulation Filter

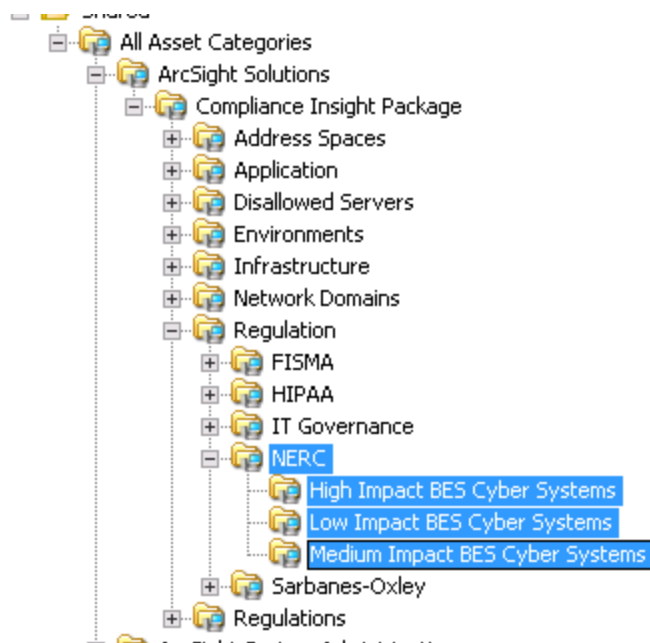
The purpose of the **Limit Regulation** filter limits event processing to only those events addressed by the NERC regulation. Customize it to reflect your environment. For example, you could configure it to specify the following conditions:

- The source machine is an asset under the NERC group
- The source machine's zone is categorized as NERC
- The destination machine is an asset categorized as NERC
- The destination machine is an asset under the NERC group
- The destination machine's zone is categorized as NERC
- The device machine is an asset categorized as NERC
- The device machine is an asset under the NERC group
- The device machine's zone is categorized as NERC

In addition you can configure it by using those filters as conditions:

- NERC/My Filters/Attacker Asset in High Impact BES Cyber Assets
- NERC/My Filters/Target Asset in High Impact BES Cyber Assets
- NERC/My Filters/Attacker Asset in Medium Impact BES Cyber Assets
- NERC/My Filters/Target Asset in Medium Impact BES Cyber Assets
- NERC/My Filters/Attacker Asset in Low Impact BES Cyber Assets
- NERC/My Filters/Target Asset in Low Impact BES Cyber Assets

To limit the regulation to the following assets categories:



By default, the CIP for NERC processes all incoming events.

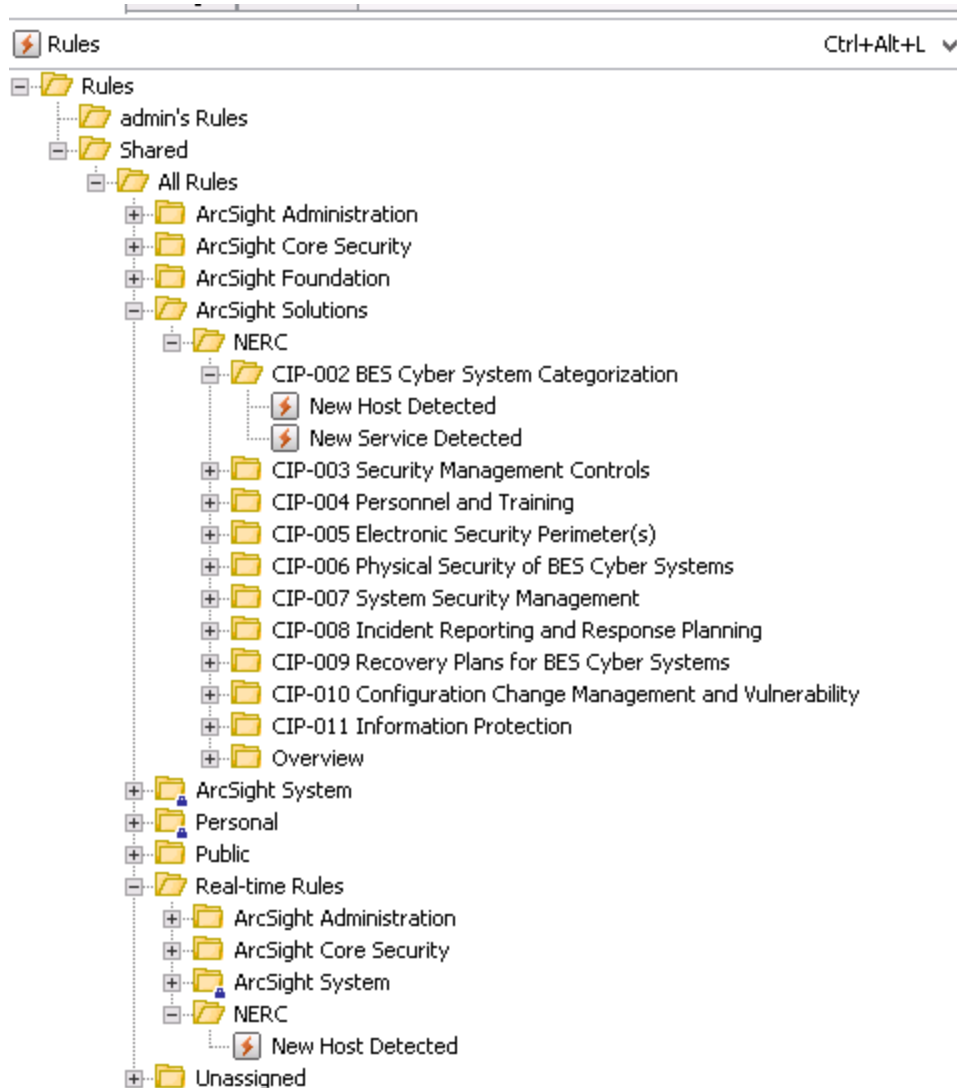
Deploy the Solution for NERC CIP Rules

In order for a CIP for NERC rule to process NERC-related events, the rule must be deployed to the **Real-time Rules** group. By default, CIP for NERC rules are not deployed in the **Real-time Rules** group, because deployed rules can have a performance impact. Only deploy a rule into the **Real-time Rules** group if you are interested in the associated use case and have device feeds configured in your environment that can trigger the rule.

To deploy a rule to the Real-time Rules group:

1. From the Resources tab in the Navigator panel, go to Rules and navigate to the ArcSight Solutions/NERC group.
2. Expand the CIP folder that contains the rule to deploy and select the Rule. For example, to select the New Host Detected rule, expand /ArcSight Solutions/NERC/ CIP-002 BES Cyber System Categorization.
3. Drag and drop the Rule from the appropriate /ArcSight Solutions/NERC group into the Real-time Rules/NERC group.
4. From the **Drag & Drop Options** dialog, select the **Link** option.

The rule is listed under the Real-time Rules/NERC group as shown in the following figure.



The rule in the Real-time Rules/NERC group is a link to the rule in the ArcSight Solutions/NERC group.

By default, the CIP for NERC rules are disabled. The rules do not trigger until they are deployed and enabled. After you have deployed the CIP for NERC rules to the Real-time Rules group, you can enable individual rules. Rules can place an additional load on the ArcSight Manager. Enable only the rules for the compliance scenarios you want to implement.

To enable a rule:

1. In the Navigator panel, go to **Rules** and navigate to the Real-time Rules/NERC group.
2. Navigate to the rule you want to enable.

3. Right-click the rule and select **Enable Rule**. To select multiple rules, press the **Ctrl** key and click each rule. To select a range of rules, press the **Ctrl** and **Shift** keys and click the first and last rule in the range.

Certain use cases in the CIP for NERC require that specific rule actions be enabled to trigger actions in the system, such as the creation of a new case. To enable a rule action, select an action below a trigger in the Actions tab of the Rule Editor and click **Enable Action**.

For more information about working with rules, see the Deploying Real-time Rules section in the ArcSight ESM Console Online Help.

Enable Data Monitors

All of the CIP's data monitors for NERC must be enabled to display data in the dashboards that use them.

To enable the data monitors:

1. In the Navigator panel, go to **Dashboards** and click the **Data Monitors** tab.
2. Navigate to the /All Data Monitors/ArcSight Solutions/NERC group.
3. Right-click the CIP group and select **Enable Data Monitor** to enable all the data monitors in the group.

Enable and Test Trends

By default, the Compliance Insight Package for NERC v.6.0 trends are not enabled. Some reports, query viewers, and dashboards require enabled trends to show data.

Below are the list of end user resources which requires enabling trends to show data:

End User Resource	Type	CIP	Required Trend
Count of Successful Administrative Logins in the Last 30 Days	Query Viewer	CIP-007	Count of Administrative Logins
Count of Unsuccessful Administrative Logins in the Last 30 Days	Query Viewer	CIP-007	Count of Administrative Logins
Anti-Virus Stopped or Paused in the Last Month	Report	CIP-007	Daily Trend of Anti-Virus Stopped or Paused Events

End User Resource	Type	CIP	Required Trend
Monthly Trend of Unsuccessful Administrative Logins	Report	CIP-007	Failed Administrative Logins - Long Term Trend
Number of Successful User Logins over the Past Week	Report	CIP-007	User Login Count
Number of Unsuccessful User Logins over the Past Month	Report	CIP-007	User Login Count
Number of Unsuccessful User Logins over the Past Week	Report	CIP-007	User Login Count
Attacks and Suspicious Activity Weekly Trend	Report	CIP-008	Attacks and Suspicious Activities Trend
Attacks and Suspicious Activity Monthly Trend	Report	CIP-008	Attacks and Suspicious Activities Trend
Average Time to Resolution - By Case Severity	Report	CIP-008	Case History
Average Time to Resolution - By Day	Report	CIP-008	Case History
Average Time to Resolution - By User	Report	CIP-008	Case History
DoS Attacks Weekly Trend	Report	CIP-008	DoS Attacks Trend
Top Critical Vulnerabilities	Query Viewer	CIP-010	Vulnerabilities
Top Vulnerable IP Addresses	Query Viewer	CIP-010	Vulnerabilities
Vulnerabilities	Query Viewer	CIP-010	Vulnerabilities
Vulnerability Events By Scanner	Query Viewer	CIP-010	Vulnerabilities
Vulnerability Scans	Query Viewer	CIP-010	Vulnerabilities

End User Resource	Type	CIP	Required Trend
Vulnerabilities by IP Address	Report	CIP-010	Vulnerabilities
Vulnerability Overview	Dashboard	CIP-010	Vulnerabilities
Weekly Trend - Configuration Modification Summary	Report	CIP-010	Configuration Changes

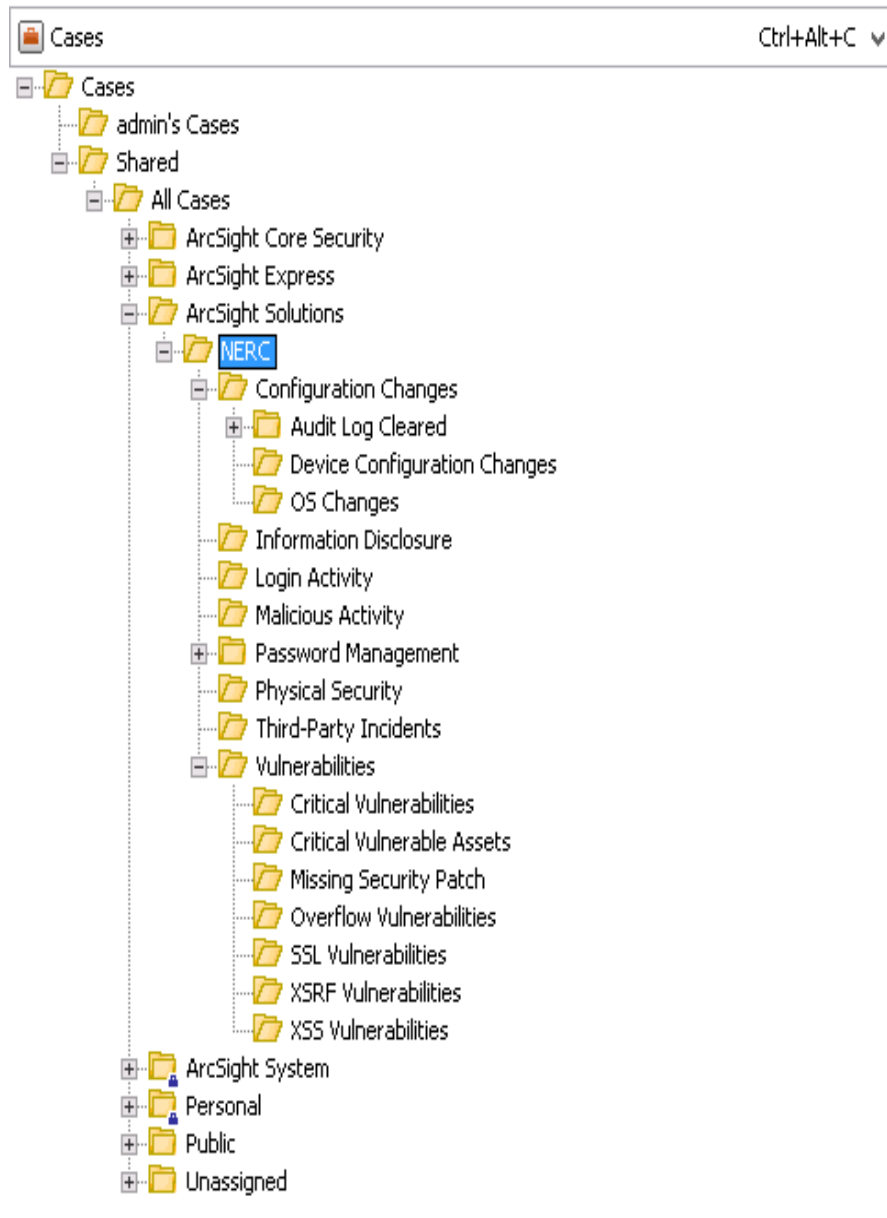
Before enabling a trend, verify that the trend captures data relevant for your environment as described in procedure below:

1. Generate or identify the required events and verify that they are being processed by ArcSight ESM
2. Navigate to the appropriate trend, right-click the trend, and then choose **Test**. If you see the events of interest in the test panel, the ArcSight ESM is processing events that can be captured by the trend. The test panel shows relevant events that can be captured by the trend in the last hour, up to 25 rows.

In addition, before enabling a trend, you can also customize its values like “The Partition Retention Period (in days), Scheduler Start Time, For general information about trends, see the ArcSight Console User’s Guide.

Configure Cases

Cases are ArcSight's trouble-ticket system that can be used as-is or in conjunction with a third-party trouble-ticket system. *Solution for NERC CIP* includes the ArcSight Solutions/NERC group, which holds the cases generated by some *Solution for NERC CIP* rules.



You can add more groups to the ArcSight Solutions/NERC group or your own group if you want to add more differentiations. If you do add more groups to the ArcSight Solutions/NERC group, modify the ESM rules that generate cases to use of your new case groups.

The rules listed below can generate cases by default in the NERC directory.

- Former Employee Account Activity
- Former Employee User Account Access Attempt
- Inactive User Account Detected
- Login Activity by a Stale Account
- Privileged Account Change
- Suspicious Activities by New Hires

The rules listed below can generate cases by default in the NERC/Malicious Activity directory.

- Disallowed Ports Access
- Possible Covert Channel
- Possible Email Attack
- Possible Information Interception
- Possible Redirection Attack
- Possible Traffic Anomaly
- DoS Detected
- Malware or Spyware Detected
- Potential Distributed DoS
- Suspicious Internal Trojan Detected
- Wireless Malicious Traffic Detected
- Worm Detected
- Severely Attacked System

The rules listed below can generate cases by default in the NERC/Physical Security directory.

- After Hours Building Access by Contractors
- Failed Building Access
- Local Logon from Badged Out Employee

The rules below can generate cases by default in the NERC/Login Activity directory:

- Consecutive Unsuccessful Logins to Administrative Account
- Successful Attack - Brute Force Login
- Unsuccessful Logins to Multiple Administrative Accounts

The rules below can generate cases by default in the NERC/Password Management directory:

- Password not Changed for Longer than Policy Standard
- Successful Password Change

The rules below can generate cases by default in the NERC/Configuration Changes/OS Changes directory:

- Information System Failures of Highly Critical Machine
- Resource Exhaustion of Highly Critical Machine
- Shutdown of Highly Critical Machine
- Critical Operating System Change Detected

The rule Audit Log Cleared can generate cases by default in the NERC/Configuration Changes/Audit Log Cleared directory.

The rule Critical Network Device Configuration Change Detected can generate cases by default in the NERC/Configuration Changes/Device Configuration Changes directory.

The rule Critical Vulnerability Detected can generate cases by default in the NERC/Vulnerabilities/Critical Vulnerabilities directory.

The rule Overflow Vulnerabilities can generate cases by default in the NERC/Vulnerabilities/Overflow Vulnerabilities directory.

The rule Security Patch Missing can generate cases by default in the NERC/Vulnerabilities/Missing Security Patch directory.

The rule SSL Vulnerabilities can generate cases by default in the NERC/Vulnerabilities/SSL Vulnerabilities directory.

The rule Vulnerabilities on Critical Machine can generate cases by default in the NERC/Vulnerabilities/Critical Vulnerable Assets directory.

The rule XSS Vulnerabilities can generate cases by default in the NERC/Vulnerabilities/XSS Vulnerabilities directory.

The rule XSRF Vulnerabilities can generate cases by default in the NERC/Vulnerabilities/XSRF Vulnerabilities directory.

The rules below can generate cases by default in the NERC/Information Disclosure directory:

- Organizational Data Information Leak
- Personal Information Leak

By default, the **Add to Existing Case** action for these rules are disabled. Enable the **Add to Existing Case** actions only for the rules that detect events are important to your organization and therefore should be tracked with cases.

To enable the **Add to Existing Case** action for a rule:

1. From the Resources tab in the Navigator panel, go to Rules and navigate to the ArcSight Solutions/NERC group.
2. Right-click a rule and select **Edit Rule**.
The rule displays in the Inspect/Edit panel.
3. Select the **Action** tab from the Inspect/Edit panel.
4. Right-click the **Add to Existing Case** action and select **Enable Action**.

After enabling the **Add to Existing Case** action, one of the following occurs when the rule fires:

- If a case with the same name does not exist, a new case is created.
- If a case with the same name does exist, the existing case is updated with additional events.

If you want to generate cases for additional activities, you can edit any rules in the ArcSight Solutions/NERC that trigger on that specific behavior and add actions those rules to create cases. For

example, if you want to create a case every time an account is locked out, edit the Account Lockout rule and add an action that creates a case.

Caution: Use caution when adding a **Create New Case** action to a rule. Every time a rule fires, a new case is created. If you expect the rule to fire repeatedly, consider using **Add to Existing Case** action instead.

If you are using the **Add to Existing Case** action and you choose to close the case, consider the following in order to detect new issues when the same circumstances occur:

1. Copy the case to another location.
2. Delete the case from the original directory.

Configure Notifications

When enabled, a notification action on a rule sends a notification when the rule fires. The following rules contain notification actions that are disabled by default:

- Successful Default Vendor Account Used
- Account Lockout
- Security Software Stopped or Paused
- Suspicious Internal Trojan Detected
- Multiple Cases Created on Short Period

You can enable the notification actions for these rules. You can add a rule action to other ArcSight Solutions/NERC rules. In addition, you can create notification destinations that receive the notifications when the rules fire. For more information including configuration information, see the *Notifications* topic in the *ArcSight Console online Help*. This configuration is optional.

Configure Additional Resources

Additional configuration may be required or desired for the individual resources provided to address a specific NERC CIP Standard. For more information (including information on asset categorization), see ["Solution for NERC CIP Resource Reference" on page 48](#).

Build FlexConnector(s) for Physical Access Devices

The Compliance Insight Package for NERC v.6.0 contains resources that make use of feeds from physical access systems, such as badge readers. This process is only required if you want to activate the Solution for NERC CIP content that leverages feeds from physical access systems. If you do not complete this process, the content that leverages feeds from physical access systems will remain dormant.

To enable these scenarios, develop a FlexConnector according to the instructions in the ArcSight FlexConnector Developer's Guide with the following field mappings to map the key event data into the ArcSight event schema:

ArcSight Field	Physical Access System Value
deviceEventClassId	Unique value for event type used for categorization
deviceReceiptTime	Access Time
destinationUserId	Users badge Id
deviceCustomString1	Location Accessed / Building

Use the following event categories for the following event types:

Event type	Object	Behavior	Technique	Device Group	Outcome	Significance
Successful building access	/Location	/Authentication/Verify		/Physical Access System	/Success	/Normal
Building access rejected	/Location	/Authentication/Verify		/Physical Access System	/Failure	/Information/Warning
Badge-out (Someone is leaving a building) [not all badge reader systems support this]	/Location	/Access/Stop		/Physical Access System	/Success	/Normal
Account created/deleted/modified - [Success assumed; in case of a failure, the Outcome needs to reflect that and the significance is /Informational/Error]	/Actor/User	/Authentication/[Add Delete Modify]		/Physical Access System	/Success	/Informational
Giving someone access to another room/building - [Success assumed; in case of a failure, the Outcome needs to reflect that and the significance is /Informational/Error]	/Actor/User	/Authorization/Modify		/Physical Access System	/Success	/Informational
Granting access to a room/building for an entire group of users	/Actor/Group	/Authorization/Modify		/Physical Access System	/Success	/Informational

You can add more user context to the events generated by your badge reader by creating a connector event mappings file.

Chapter 3: Solution for NERC CIP Resource Reference

This chapter lists all the Solution for NERC CIP resources by type:

- ["Active Channels" below](#)
- ["Active Lists" on page 54](#)
- ["Dashboards" on page 56](#)
- ["Data Monitors" on page 61](#)
- ["Field Sets" on page 86](#)
- ["Filters" on page 88](#)
- ["Focused Reports" on page 115](#)
- ["Queries" on page 116](#)
- ["Query Viewers" on page 156](#)
- ["Reports" on page 159](#)
- ["Rules" on page 190](#)
- ["Trends" on page 197](#)
- ["Use Cases" on page 198](#)

Active Channels

The following table lists all the active channels.

Active Channels Resources

Resource	Description	URI
Account Lockouts	This active channel shows events when a rule is fired to lock out a user ID.	/All Active Channels/ArcSight Solutions/NERC/CIP-007 System Security Management/
All Attacks and Suspicious Activity Events	This active channel shows all attack and suspicious activity events.	/All Active Channels/ArcSight Solutions/NERC/CIP-008 Incident Reporting and Response Planning/

Active Channels Resources, continued

Resource	Description	URI
All Information Leak Events	This active channel shows real-time feed of events reflecting information leakage.	/All Active Channels/ArcSight Solutions/NERC/CIP-011 Information Protection/
Asset Creation Deletion and Modifications	This active channel shows events related to asset creations, asset deletions, and asset modifications. The channel can be used to keep track of the asset inventory.	/All Active Channels/ArcSight Solutions/NERC/CIP-002 BES Cyber System Categorization/
Attacks and Suspicious Activity Targeting High Impact BES Cyber Systems	This active channel shows all attack and suspicious activity events where the target asset or zone is categorized in the High BES Cyber systems asset category.	/All Active Channels/ArcSight Solutions/NERC/CIP-008 Incident Reporting and Response Planning/
Attacks and Suspicious Activity Targeting Low Impact BES Cyber Systems	This active channel shows all attack and suspicious activity events where the target asset or zone is categorized in the Low Impact BES Cyber Systems asset category.	/All Active Channels/ArcSight Solutions/NERC/CIP-008 Incident Reporting and Response Planning/
Attacks and Suspicious Activity Targeting Medium Impact BES Cyber Systems	This active channel shows all attack and suspicious activity events where the target asset or zone is categorized in the Medium BES Cyber systems asset category.	/All Active Channels/ArcSight Solutions/NERC/CIP-008 Incident Reporting and Response Planning/
Attacks and Suspicious Activity Targeting Public Facing Resources	This active channel shows all events where the target asset or zone is categorized in the Public-Facing asset category.	/All Active Channels/ArcSight Solutions/NERC/CIP-008 Incident Reporting and Response Planning/
Attacks and Suspicious Activity Targeting Third Party Resources	This active channel shows all attack and suspicious activity events where the target is an asset from Third Party asset category.	/All Active Channels/ArcSight Solutions/NERC/CIP-008 Incident Reporting and Response Planning/
Attacks and Suspicious Activity from High Impact BES Cyber Systems	This active channel shows all attack and suspicious activity events where the source asset or zone is categorized in the High Impact BES Cyber Systems asset category.	/All Active Channels/ArcSight Solutions/NERC/CIP-008 Incident Reporting and Response Planning/

Active Channels Resources, continued

Resource	Description	URI
Attacks and Suspicious Activity from Low Impact BES Cyber Systems	This active channel shows all attack and suspicious activity events where the source asset or zone is categorized in the Low Impact BES Cyber Systems asset category.	/All Active Channels/ArcSight Solutions/NERC/CIP-008 Incident Reporting and Response Planning/
Attacks and Suspicious Activity from Medium Impact BES Cyber Systems	This active channel shows all attack and suspicious activity events where the source asset or zone is categorized in the Medium Impact BES Cyber Systems asset category.	/All Active Channels/ArcSight Solutions/NERC/CIP-008 Incident Reporting and Response Planning/
Attacks and Suspicious Activity from Public Facing Resources	This active channel shows all attack and suspicious activity events where the source asset or zone is categorized in the Public-Facing asset category.	/All Active Channels/ArcSight Solutions/NERC/CIP-008 Incident Reporting and Response Planning/
Attacks and Suspicious Activity from Third Party Resources	This active channel shows all attack and suspicious activity events where the attacker is an asset from Third Party asset category.	/All Active Channels/ArcSight Solutions/NERC/CIP-008 Incident Reporting and Response Planning/
Audit Log Cleared	This active channel looks for events that indicate an audit log is cleared .	/All Active Channels/ArcSight Solutions/NERC/CIP-010 Configuration Change Management and Vulnerability/
Configuration Changes	This active channel looks for events that indicate configuration changes occurring in NERC assets.	/All Active Channels/ArcSight Solutions/NERC/CIP-010 Configuration Change Management and Vulnerability/
Database Configuration Changes	This active channel looks for events that indicate database configuration changes occurring in NERC assets.	/All Active Channels/ArcSight Solutions/NERC/CIP-010 Configuration Change Management and Vulnerability/
Default Vendor Account Used	This active channel shows a 'live' feed of events reflecting the use vendor provided default credentials. This is based on the related rule firing. Manager Receipt Time is used as the time-stamp of choice to retain the real-time nature of the channel.	/All Active Channels/ArcSight Solutions/NERC/CIP-004 Personnel and Training/

Active Channels Resources, continued

Resource	Description	URI
DoS Attacks	This active channel shows events that are attributed to denial of service attacks.	/All Active Channels/ArcSight Solutions/NERC/CIP-008 Incident Reporting and Response Planning/
Firewall Configuration Changes	This active channel looks for events that indicate firewall configuration changes occurring in NERC assets.	/All Active Channels/ArcSight Solutions/NERC/CIP-010 Configuration Change Management and Vulnerability/
High Priority Events	This active channel shows high priority events which translate into high risk.	/All Active Channels/ArcSight Solutions/NERC/CIP-008 Incident Reporting and Response Planning/
Information System Failures	This active channel looks for information system failures.	/All Active Channels/ArcSight Solutions/NERC/CIP-009 Recovery Plans for BES Cyber Systems/
Intellectual Property Rights Violations	This active channel looks for intellectual property rights violations. To do so, it shows all the rule-firings that are indicating intellectual property rights violations.	/All Active Channels/ArcSight Solutions/NERC/CIP-003 Security Management Controls/
Internal Reconnaissance	This active channel shows reconnaissance events originating internal to the corporation.	/All Active Channels/ArcSight Solutions/NERC/CIP-008 Incident Reporting and Response Planning/
Invalid or Expired Certificate Events	This active channel shows a real-time feed of events which indicate that an invalid or expired certificate was detected.	/All Active Channels/ArcSight Solutions/NERC/CIP-011 Information Protection/
Login Attempts	This active channel shows a real-time feed of events where a login attempt was made.	/All Active Channels/ArcSight Solutions/NERC/CIP-007 System Security Management/
Logouts	This active channel shows a real-time feed of logout events.	/All Active Channels/ArcSight Solutions/NERC/CIP-007 System Security Management/

Active Channels Resources, continued

Resource	Description	URI
Network IDS Configuration Changes	This active channel looks for events that indicate NIDS configuration changes occurring in NERC assets.	/All Active Channels/ArcSight Solutions/NERC/CIP-010 Configuration Change Management and Vulnerability/
Network Routing Configuration Changes	This active channel looks for events that indicate network routing configuration changes occurring in NERC assets.	/All Active Channels/ArcSight Solutions/NERC/CIP-010 Configuration Change Management and Vulnerability/
New Hosts and Services	This active channel shows events related to new services and new hosts found on the network.	/All Active Channels/ArcSight Solutions/NERC/CIP-002 BES Cyber System Categorization/
Open Ports	This active channel shows all open ports events reported by vulnerability scanners.	/All Active Channels/ArcSight Solutions/NERC/CIP-007 System Security Management/
Operating System Configuration Changes	This active channel looks for events that indicate os configuration changes occurring in NERC assets.	/All Active Channels/ArcSight Solutions/NERC/CIP-010 Configuration Change Management and Vulnerability/
Personal and Organizational Records Information Leak	This active channel looks for leaks of personal and organizational records information.	/All Active Channels/ArcSight Solutions/NERC/CIP-011 Information Protection/
Physical Security	This active channel shows all physical access related activities.	/All Active Channels/ArcSight Solutions/NERC/CIP-006 Physical Security of BES Cyber Systems/
Policy Breaches	This active channel looks for policy violations in the past.	/All Active Channels/ArcSight Solutions/NERC/CIP-003 Security Management Controls/

Active Channels Resources, continued

Resource	Description	URI
Possible Availability Impacts	This active channel shows events which could have an impact on the availability of information systems, such as DoS attacks.	/All Active Channels/ArcSight Solutions/NERC/CIP-009 Recovery Plans for BES Cyber Systems/
Privileged Account Changed	This active channel shows a 'live' feed of events reflecting alteration of privileges. This is based on the related rule firing. Manager Receipt Time is used as the time-stamp of choice to retain the real-time nature of the channel.	/All Active Channels/ArcSight Solutions/NERC/CIP-004 Personnel and Training/
Removal of Access Rights	This active channel shows a live feed of events reflecting a removal of a user's access privileges.	/All Active Channels/ArcSight Solutions/NERC/CIP-004 Personnel and Training/
Software Changes	This active channel looks for events that indicate software changes occurring in NERC assets.	/All Active Channels/ArcSight Solutions/NERC/CIP-010 Configuration Change Management and Vulnerability/
System Startup and Shutdown	This active channel shows system startup and shutdown events .	/All Active Channels/ArcSight Solutions/NERC/CIP-009 Recovery Plans for BES Cyber Systems/
Technical Compliance Check Failures	This active channel looks for events which indicate that a technical compliance check failed, meaning that an either misconfigured or vulnerable system was found.	/All Active Channels/ArcSight Solutions/NERC/CIP-002 BES Cyber System Categorization/
VPN Configuration Changes	This active channel looks for events that indicate vpn configuration changes occurring in NERC assets.	/All Active Channels/ArcSight Solutions/NERC/CIP-010 Configuration Change Management and Vulnerability/
Vulnerability Events	This active channel looks for events that indicate the existence of vulnerabilities in NERC assets.	/All Active Channels/ArcSight Solutions/NERC/CIP-010 Configuration Change Management and Vulnerability/

Active Lists

The following table lists all the active lists.

Active Lists Resources

Resource	Description	URI
Active Accounts	This active list stores user names who have successfully logged in within the last 30 days.	/All Active Lists/ArcSight Solutions/NERC/
Administrative Accounts List	<p>This active list should be populated with the usernames that have administrative privileges in your domain. Admins (those responsible for managing administrative users) populate this list manually whenever a new administrative user is added. Entries to this list are read by reports supplied in the content pack, but the list can also be added to or referenced in new content built around the provided infrastructure.</p> <p>This active list should be populated with the usernames that have administrative privileges in your domain. Entries in this list should be in all lower case.</p> <p>For example, the user Administrator should be added as "administrator".</p>	/All Active Lists/ArcSight Solutions/NERC/
Allowed Ports	This active list contains all permissible destination ports (all permissible services). This active list should be populated according to your site policy.	/All Active Lists/ArcSight Solutions/NERC/
Audit Log Cleared	This active list should be populated only by the rule Audit Log Cleared. It logs every time an audit log is cleared.	/All Active Lists/ArcSight Solutions/NERC/
Badged In	This list contains information about employees who are badged in.	/All Active Lists/ArcSight Solutions/NERC/
Badged Out	This active list contains the computer accounts of badged out employees.	/All Active Lists/ArcSight Solutions/NERC/
Badges to Accounts	This list contains the computer account and employee type for every physical device badge.	/All Active Lists/ArcSight Solutions/NERC/
Compliance Score	This active list maintains the compliance risk score for each regulation section. The compliance risk score is calculated based on the triggered rules in the solution package. You can manually change the score as required. This change will be reflected in the Compliance Risk Score dashboard.	/All Active Lists/ArcSight Solutions/NERC/
Default Vendor Accounts	<p>This active list contains the default user account names for various vendors.</p> <p>This list should be configured at set-up time with existing vendor user account names, and updated as necessary on an ongoing basis.</p>	/All Active Lists/ArcSight Solutions/NERC/

Active Lists Resources, continued

Resource	Description	URI
Disallowed Ports	This active list contains all disallowed destination ports. This active list should be populated according to your site policy.	/All Active Lists/ArcSight Solutions/NERC/
Former Employees	This active list contains user accounts of former employees. User accounts in this active list are retained indefinitely. All the entries in this list need to be in lowercase.	/All Active Lists/ArcSight Solutions/NERC/
Insecure Ports	This active list includes ports related to unencrypted and thus insecure communication services.	/All Active Lists/ArcSight Solutions/NERC/
Insecure Processes	This active list includes the names of processes that provide unencrypted and thus insecure communications.	/All Active Lists/ArcSight Solutions/NERC/
Instant Messaging Domains	This active list contains all the DNS domains for public Instant messaging servers. This list is used to detect when outbound traffic to these domains is detected signifying a possible information leak. Note: All the domain names must be in lowercase.	/All Active Lists/ArcSight Solutions/NERC/
Internal Systems with Insecure Services	This list stores all internal systems with insecure services detected.	/All Active Lists/ArcSight Solutions/NERC/
Internet Ports	This active list includes ports that are used for Internet communication.	/All Active Lists/ArcSight Solutions/NERC/
New Assets	This active list contains new assets and is automatically populated by the "New Host Detected" rule. New assets are retained for 7 days in the list.	/All Active Lists/ArcSight Solutions/NERC/
New Hire Accounts	This active list contains newly hired users and is automatically populated by the "New Hire Identification" rule. New users are retained for 7 days in the list.	/All Active Lists/ArcSight Solutions/NERC/
Password Changes	This active is updated with the user and product information when a successful password change occurs.	/All Active Lists/ArcSight Solutions/NERC/
Stale Accounts	This active list is used to maintain user names that have not appeared in login events for the time specified by the Active Accounts active list TTL value.	/All Active Lists/ArcSight Solutions/NERC/
Suspicious Activities by New Hires	This active list stores events that were identified as attacks by new hires. The original event name is stored in the deviceCustomString1 field. By default, these events are stored for 60 days.	/All Active Lists/ArcSight Solutions/NERC/

Dashboards

The following table lists all the dashboards.

Dashboards Resources

Resource	Description	URI
Account Activity	This dashboard shows information related to user account activity.	/All Dashboards/ArcSight Solutions/NERC/CIP-004 Personnel and Training/
Account Lockouts	This dashboard displays information about account lockouts.	/All Dashboards/ArcSight Solutions/NERC/CIP-007 System Security Management/
Administrative Logins and Logouts	This dashboard shows an overview of the administrative login and logouts activity on the organization.	/All Dashboards/ArcSight Solutions/NERC/CIP-007 System Security Management/
Anti-Virus Activity	This dashboard shows an overview of the anti-virus activity on the organization.	/All Dashboards/ArcSight Solutions/NERC/CIP-007 System Security Management/
Asset Activity	This dashboard displays asset creation, deletion, and modification activities.	/All Dashboards/ArcSight Solutions/NERC/CIP-002 BES Cyber System Categorization/
Attacks and Suspicious Activity	This dashboard displays information about attacks and suspicious activity events.	/All Dashboards/ArcSight Solutions/NERC/CIP-008 Incident Reporting and Response Planning/
Attacks and Suspicious Activity to and from High Impact BES Cyber Systems	This dashboard displays information about attacks and suspicious activity events to and from high impact BES cyber systems.	/All Dashboards/ArcSight Solutions/NERC/CIP-008 Incident Reporting and Response Planning/
Attacks and Suspicious Activity to and from Low Impact BES Cyber Systems	This dashboard displays information about attacks and suspicious activity events to and from low impact BES cyber systems.	/All Dashboards/ArcSight Solutions/NERC/CIP-008 Incident Reporting and Response Planning/
Attacks and Suspicious Activity to and from Medium Impact BES Cyber Systems	This dashboard displays information about attacks and suspicious activity events to and from medium impact BES cyber systems.	/All Dashboards/ArcSight Solutions/NERC/CIP-008 Incident Reporting and Response Planning/
Attacks and Suspicious Activity to and from Third Party Resources	This dashboard displays information about third party assets involved in attacks and suspicious behavior.	/All Dashboards/ArcSight Solutions/NERC/CIP-008 Incident Reporting and Response Planning/

Dashboards Resources, continued

Resource	Description	URI
Audit Log Cleared	This dashboard displays Audit Log Cleared compliant status.	/All Dashboards/ArcSight Solutions/NERC/CIP-010 Configuration Change Management and Vulnerability/
Blocked Traffic Activity	This dashboard shows information related to blocked traffic activity .	/All Dashboards/ArcSight Solutions/NERC/CIP-005 Electronic Security Perimeter(s)/
CIP-002 Overview	This dashboard shows high-level information around NERC standard CIP-002.	/All Dashboards/ArcSight Solutions/NERC/CIPS Overview/
CIP-003 Overview	This dashboard shows high-level information around NERC standard CIP-003.	/All Dashboards/ArcSight Solutions/NERC/CIPS Overview/
CIP-004 Overview	This dashboard shows high-level information around NERC standard CIP-004.	/All Dashboards/ArcSight Solutions/NERC/CIPS Overview/
CIP-005 Overview	This dashboard shows high-level information around NERC standard CIP-005.	/All Dashboards/ArcSight Solutions/NERC/CIPS Overview/
CIP-006 Overview	This dashboard shows high-level information around NERC standard CIP-006.	/All Dashboards/ArcSight Solutions/NERC/CIPS Overview/
CIP-007 Overview	This dashboard shows high-level information around NERC standard CIP-007.	/All Dashboards/ArcSight Solutions/NERC/CIPS Overview/
CIP-008 Overview	This dashboard shows high-level information around NERC standard CIP-008.	/All Dashboards/ArcSight Solutions/NERC/CIPS Overview/
CIP-009 Overview	This dashboard shows high-level information around NERC standard CIP-009.	/All Dashboards/ArcSight Solutions/NERC/CIPS Overview/
CIP-010 Overview	This dashboard shows high-level information around NERC standard CIP-009.	/All Dashboards/ArcSight Solutions/NERC/CIPS Overview/
CIP-011 Overview	This dashboard shows high-level information around NERC standard CIP-009.	/All Dashboards/ArcSight Solutions/NERC/CIPS Overview/
Compliance Risk Score Overview	This dashboard displays information about the compliance risk score for each regulation section.	/All Dashboards/ArcSight Solutions/NERC/CIPS Overview/

Dashboards Resources, continued

Resource	Description	URI
Configuration Modifications Overview	This dashboard displays information about configuration changes.	/All Dashboards/ArcSight Solutions/NERC/CIP-010 Configuration Change Management and Vulnerability/
Default Vendor Account Activity	This dashboard shows the uses of default vendor accounts.	/All Dashboards/ArcSight Solutions/NERC/CIP-004 Personnel and Training/
Disallowed Ports Communications	This dashboard displays information around events to disallowed ports.	/All Dashboards/ArcSight Solutions/NERC/CIP-005 Electronic Security Perimeter(s)/
DoS Activity	This dashboard provides an overview of events associated with denial of service and availability attacks.	/All Dashboards/ArcSight Solutions/NERC/CIP-008 Incident Reporting and Response Planning/
Firewall Configuration Modifications Overview	This dashboard displays information about firewall configuration changes.	/All Dashboards/ArcSight Solutions/NERC/CIP-010 Configuration Change Management and Vulnerability/
Former Employee Activity	This dashboard shows information related to activity by former employees.	/All Dashboards/ArcSight Solutions/NERC/CIP-004 Personnel and Training/
General User Login Attempts	This dashboard shows an overview of user login attempts on the organization.	/All Dashboards/ArcSight Solutions/NERC/CIP-007 System Security Management/
High Impact BES Systems Blocked Traffic	This dashboard shows information related to blocked traffic activity on high impact BES cyber systems.	/All Dashboards/ArcSight Solutions/NERC/CIP-005 Electronic Security Perimeter(s)/
Information Interception	This dashboard displays information about interception events.	/All Dashboards/ArcSight Solutions/NERC/CIP-005 Electronic Security Perimeter(s)/
Information Leaks	This dashboard displays information around information leakage.	/All Dashboards/ArcSight Solutions/NERC/CIP-011 Information Protection/
Intellectual Property Rights Violations	This dashboard displays information around violations and violators of IPR.	/All Dashboards/ArcSight Solutions/NERC/CIP-003 Security Management Controls/
Internal External Communications	This dashboard shows information related to internal -external communications.	/All Dashboards/ArcSight Solutions/NERC/CIP-005 Electronic Security Perimeter(s)/
Internal Reconnaissance	This dashboard displays information about internal reconnaissance events and sources.	/All Dashboards/ArcSight Solutions/NERC/CIP-008 Incident Reporting and Response Planning/

Dashboards Resources, continued

Resource	Description	URI
Last 20 Vulnerabilities - by Type	This Dashboard provides an overview of the latest vulnerabilities by types vulnerability types included SSL,XSS,Overflow,XSRF .	/All Dashboards/ArcSight Solutions/NERC/CIP-010 Configuration Change Management and Vulnerability/
Last State External Devices Overview	This Dashboard provides Real-time display of the last 20 external device activities and their status.	/All Dashboards/ArcSight Solutions/NERC/CIP-010 Configuration Change Management and Vulnerability/
Last State Vulnerability Overview	This Dashboard provides Real-time compliance status of the last 20 vulnerabilities. Compliance Status is determined using the following : Agent-Severity =High or Very-High -> Violation Agent-Severity =Medium -> Possible Violation Agent-Severity =Low -> Compliant	/All Dashboards/ArcSight Solutions/NERC/CIP-010 Configuration Change Management and Vulnerability/
Latest Vulnerabilities	This Dashboard provides overview of the latest vulnerabilities.	/All Dashboards/ArcSight Solutions/NERC/CIP-010 Configuration Change Management and Vulnerability/
Low Impact BES Systems Blocked Traffic	This dashboard shows information related to blocked traffic activity on low impact BES cyber systems.	/All Dashboards/ArcSight Solutions/NERC/CIP-005 Electronic Security Perimeter(s)/
Malicious Code Activity	This dashboard shows an overview of the malicious code activity on the organization.	/All Dashboards/ArcSight Solutions/NERC/CIP-007 System Security Management/
Medium Impact BES Systems Blocked Traffic	This dashboard shows information related to blocked traffic activity on medium impact BES cyber systems.	/All Dashboards/ArcSight Solutions/NERC/CIP-005 Electronic Security Perimeter(s)/
Most Fired Rule by Section	For every NERC CIP, this dashboard shows the most fired rule.	/All Dashboards/ArcSight Solutions/NERC/CIPS Overview/
Network Controls	This dashboard displays information about logging devices and firewall open ports.	/All Dashboards/ArcSight Solutions/NERC/CIP-005 Electronic Security Perimeter(s)/
Network Devices Configuration Changes Overview	This dashboard displays information about network devices equipments (such as router, switch, NIDS) configuration changes.	/All Dashboards/ArcSight Solutions/NERC/CIP-010 Configuration Change Management and Vulnerability/

Dashboards Resources, continued

Resource	Description	URI
New Hires Activity	This dashboard shows information related to activity by new hire employees.	/All Dashboards/ArcSight Solutions/NERC/CIP-004 Personnel and Training/
Operating Systems Configuration Modifications Overview	This dashboard displays information about os configuration changes.	/All Dashboards/ArcSight Solutions/NERC/CIP-010 Configuration Change Management and Vulnerability/
Overall CIPS Rule Firings	This dashboard shows the number of rules fired for every NERC CIP standard.	/All Dashboards/ArcSight Solutions/NERC/CIPS Overview/
Physical Security Overview	This dashboard displays information around physical access.	/All Dashboards/ArcSight Solutions/NERC/CIP-006 Physical Security of BES Cyber Systems/
Policy Breaches	This dashboard displays information about policy violations and violators.	/All Dashboards/ArcSight Solutions/NERC/CIP-003 Security Management Controls/
Port Activity	This dashboard shows an overview of port activity on the organization.	/All Dashboards/ArcSight Solutions/NERC/CIP-007 System Security Management/
Technical Compliance Checking	This dashboard displays different views of failed compliance checks.	/All Dashboards/ArcSight Solutions/NERC/CIP-002 BES Cyber System Categorization/
Top 10 Vulnerable Assets	This Dashboard provides an overview of the top vulnerable assets.	/All Dashboards/ArcSight Solutions/NERC/CIP-010 Configuration Change Management and Vulnerability/
Traffic Anomaly	This dashboard displays information about traffic anomaly events.	/All Dashboards/ArcSight Solutions/NERC/CIP-005 Electronic Security Perimeter(s)/
Traffic Between Network Domains	This dashboard displays information about traffic between network domains.	/All Dashboards/ArcSight Solutions/NERC/CIP-005 Electronic Security Perimeter(s)/
Unsuccessful Administrative Logins	This dashboard shows an overview of unsuccessful administrative logins activity on the organization.	/All Dashboards/ArcSight Solutions/NERC/CIP-007 System Security Management/
Unsuccessful User Logins	This dashboard shows an overview of unsuccessful user activity on the organization.	/All Dashboards/ArcSight Solutions/NERC/CIP-007 System Security Management/
Up Down Status of Highly Critical Assets	This dashboard shows whether the highly critical assets in your environment are either up or down.	/All Dashboards/ArcSight Solutions/NERC/CIP-009 Recovery Plans for BES Cyber Systems/

Dashboards Resources, continued

Resource	Description	URI
User Group Activity	This dashboard shows information related to user group activity.	/All Dashboards/ArcSight Solutions/NERC/CIP-004 Personnel and Training/
User Logins and Logouts	This dashboard shows an overview of the user login and logouts activity on the organization.	/All Dashboards/ArcSight Solutions/NERC/CIP-007 System Security Management/
Vulnerability Overview	This Dashboard provides overview of NERC vulnerability events for the last 14 days.	/All Dashboards/ArcSight Solutions/NERC/CIP-010 Configuration Change Management and Vulnerability/

Data Monitors

The following table lists all the data monitors.

Data Monitors Resources

Resource	Description	URI
Account Lockouts	This data monitor displays events when an account has been locked out; triggered by a related rule firing.	/All Data Monitors/ArcSight Solutions/NERC/CIP-007 System Security Management/
Anti-Virus Stopped or Paused	This data monitor shows the Last State of systems that have had Anti-Virus services stopped or paused.	/All Data Monitors/ArcSight Solutions/NERC/CIP-007 System Security Management/
Attacks and Suspicious Activity Event Names - Event Graph	This data monitor shows connections between source and destination machines and event names as they appear in attack and suspicious activity events.	/All Data Monitors/ArcSight Solutions/NERC/CIP-008 Incident Reporting and Response Planning/
Attacks and Suspicious Activity Event Ports - Event Graph	This data monitor shows connection between source and destination machines and ports as they appear in attack and suspicious activity events.	/All Data Monitors/ArcSight Solutions/NERC/CIP-008 Incident Reporting and Response Planning/

Data Monitors Resources, continued

Resource	Description	URI
Attacks and Suspicious Activity Events in the High Impact BES Cyber Systems - Event Graph	This data monitor shows connection between source and destination machines and ports as they appear in attack and suspicious activity events in the High Impact BES Cyber Systems .	/All Data Monitors/ArcSight Solutions/NERC/CIP-008 Incident Reporting and Response Planning/
Attacks and Suspicious Activity Events in the Low Impact BES Cyber Systems - Event Graph	This data monitor shows connection between source and destination machines and ports as they appear in attack and suspicious activity events in the Low Impact BES Cyber Systems .	/All Data Monitors/ArcSight Solutions/NERC/CIP-008 Incident Reporting and Response Planning/
Attacks and Suspicious Activity Events in the Medium Impact BES Cyber Systems - Event Graph	This data monitor shows connection between source and destination machines and ports as they appear in attack and suspicious activity events in the Medium Impact BES Cyber Systems .	/All Data Monitors/ArcSight Solutions/NERC/CIP-008 Incident Reporting and Response Planning/
Attacks and Suspicious Activity Events in the Third Party Network Domain - Event Graph	This data monitor shows connection between source and destination machines and ports as they appear in attack and suspicious activity events in the Third Party Network Domain.	/All Data Monitors/ArcSight Solutions/NERC/CIP-008 Incident Reporting and Response Planning/
Audit Log Cleared Status	This data monitor reports violation suspected status when an audit log cleared event is present.	/All Data Monitors/ArcSight Solutions/NERC/CIP-010 Configuration Change Management and Vulnerability/
Blocked Traffic	This data monitor presenting blocked traffic in event graph chart .	/All Data Monitors/ArcSight Solutions/NERC/CIP-005 Electronic Security Perimeter(s)/
Building Access - Event Graph	This data monitor is used to show the hour of day that users are accessing buildings.	/All Data Monitors/ArcSight Solutions/NERC/CIP-006 Physical Security of BES Cyber Systems/

Data Monitors Resources, continued

Resource	Description	URI
CIP-002 Most Fired Rule	This data monitor shows the rule that fired most in CIP-002 in the last hour.	/All Data Monitors/ArcSight Solutions/NERC/CIPS Overview/CIP-002 Overview/
CIP-003 Most Fired Rule	This data monitor shows the rule that fired most in CIP-003 in the last hour.	/All Data Monitors/ArcSight Solutions/NERC/CIPS Overview/CIP-003 Overview/
CIP-004 Most Fired Rule	This data monitor shows the rule that fired most in CIP-004 in the last hour.	/All Data Monitors/ArcSight Solutions/NERC/CIPS Overview/CIP-004 Overview/
CIP-005 Most Fired Rule	This data monitor shows the rule that fired most in CIP-005 in the last hour.	/All Data Monitors/ArcSight Solutions/NERC/CIPS Overview/CIP-005 Overview/
CIP-006 Most Fired Rule	This data monitor shows the rule that fired most in CIP-006 in the last hour.	/All Data Monitors/ArcSight Solutions/NERC/CIPS Overview/CIP-006 Overview/
CIP-007 Most Fired Rule	This data monitor shows the rule that fired most in CIP-007 in the last hour.	/All Data Monitors/ArcSight Solutions/NERC/CIPS Overview/CIP-007 Overview/
CIP-008 Most Fired Rule	This data monitor shows the rule that fired most in CIP-008 in the last hour.	/All Data Monitors/ArcSight Solutions/NERC/CIPS Overview/CIP-008 Overview/
CIP-009 Most Fired Rule	This data monitor shows the rule that fired most in CIP-009 in the last hour.	/All Data Monitors/ArcSight Solutions/NERC/CIPS Overview/CIP-009 Overview/
CIP-010 Most Fired Rule	This data monitor shows the rule that fired most in CIP-010 in the last hour.	/All Data Monitors/ArcSight Solutions/NERC/CIPS Overview/CIP-010 Overview/

Data Monitors Resources, continued

Resource	Description	URI
CIP-011 Most Fired Rule	This data monitor shows the rule that fired most in CIP-011 in the last hour.	/All Data Monitors/ArcSight Solutions/NERC/CIPS Overview/CIP-011 Overview/
Compliance Risk Score Overview	This data monitor displays an icon indicating the compliance risk score for each regulation section. The compliance score is maintained in the Compliance Score active list, and is calculated based on the severity of the rules that were triggered in the solution package.	/All Data Monitors/ArcSight Solutions/NERC/CIPS Overview/
Contractor Access After Hours	This data monitor shows the top contractors accesses after hours.	/All Data Monitors/ArcSight Solutions/NERC/CIP-006 Physical Security of BES Cyber Systems/
Disallowed Ports by Policy	This data monitor provides the distribution of disallowed ports by policies.	/All Data Monitors/ArcSight Solutions/NERC/CIP-005 Electronic Security Perimeter(s)/
DoS Attacks Event Names - Event Graph	This data monitor shows connections between attacker and target machines and event names as they appear in denial of service attack events	/All Data Monitors/ArcSight Solutions/NERC/CIP-008 Incident Reporting and Response Planning/
DoS Attacks Event Ports - Event Graph	This data monitor shows connection between attacker and target machines and ports as they appear in denial of service attack events.	/All Data Monitors/ArcSight Solutions/NERC/CIP-008 Incident Reporting and Response Planning/
Firewall Open Ports	This data monitor is used to determine which ports a particular firewall is allowing traffic on.	/All Data Monitors/ArcSight Solutions/NERC/CIP-005 Electronic Security Perimeter(s)/
Internal Inter-Domain Traffic by Attacker Domain	This data monitor shows the internal inter-domain traffic by attacker domain.	/All Data Monitors/ArcSight Solutions/NERC/CIP-005 Electronic Security Perimeter(s)/

Data Monitors Resources, continued

Resource	Description	URI
Internal Inter-Domain Traffic by Target Domain	This data monitor shows the internal inter-domain traffic by target domain.	/All Data Monitors/ArcSight Solutions/NERC/CIP-005 Electronic Security Perimeter(s)/
Internal Reconnaissance	This Event Graph data monitor shows all internal reconnaissance activity.	/All Data Monitors/ArcSight Solutions/NERC/CIP-008 Incident Reporting and Response Planning/
Internet Activity by New Hires	This data monitor shows Internet activity per reporting device per new hire over a day's period.	/All Data Monitors/ArcSight Solutions/NERC/CIP-004 Personnel and Training/
Last 10 Anti-Virus Service Stopped or Paused Events	This data monitor shows the last 10 Anti-Virus service stopped paused or disabled events.	/All Data Monitors/ArcSight Solutions/NERC/CIP-007 System Security Management/
Last 10 Asset Creations	This data monitor provides a list of the last 10 assets created.	/All Data Monitors/ArcSight Solutions/NERC/CIP-002 BES Cyber System Categorization/
Last 10 Asset Deletions	This data monitor provides a list of the last 10 assets deleted.	/All Data Monitors/ArcSight Solutions/NERC/CIP-002 BES Cyber System Categorization/
Last 10 Blocked Traffic Events	This data monitor shows the last 10 blocked traffic events.	/All Data Monitors/ArcSight Solutions/NERC/CIP-005 Electronic Security Perimeter(s)/
Last 10 Blocked Traffic from High Impact BES Systems	This data monitor shows the last 10 blocked traffic events from high impact BES systems.	/All Data Monitors/ArcSight Solutions/NERC/CIP-005 Electronic Security Perimeter(s)/
Last 10 Blocked Traffic from Low Impact BES Systems	This data monitor shows the last 10 blocked traffic events from low impact BES systems.	/All Data Monitors/ArcSight Solutions/NERC/CIP-005 Electronic Security Perimeter(s)/

Data Monitors Resources, continued

Resource	Description	URI
Last 10 Blocked Traffic from Medium Impact BES Systems	This data monitor shows the last 10 blocked traffic events from medium impact BES systems.	/All Data Monitors/ArcSight Solutions/NERC/CIP-005 Electronic Security Perimeter(s)/
Last 10 Blocked Traffic to High Impact BES Systems	This data monitor shows the last 10 blocked traffic events to high impact BES systems.	/All Data Monitors/ArcSight Solutions/NERC/CIP-005 Electronic Security Perimeter(s)/
Last 10 Blocked Traffic to Low Impact BES Systems	This data monitor shows the last 10 blocked traffic events to low impact BES systems.	/All Data Monitors/ArcSight Solutions/NERC/CIP-005 Electronic Security Perimeter(s)/
Last 10 Blocked Traffic to Medium Impact BES Systems	This data monitor shows the last 10 blocked traffic events to medium impact BES systems.	/All Data Monitors/ArcSight Solutions/NERC/CIP-005 Electronic Security Perimeter(s)/
Last 10 Configuration Modifications	This data monitor tracks the most recent system configuration modifications.	/All Data Monitors/ArcSight Solutions/NERC/CIP-010 Configuration Change Management and Vulnerability/
Last 10 External to Internal Communications	This data monitor displays the last 10 communications originates from an external network segment and the target is in an internal network segment.	/All Data Monitors/ArcSight Solutions/NERC/CIP-005 Electronic Security Perimeter(s)/
Last 10 Failed Anti-Virus Updates	This data monitor shows the last 20 Anti-Virus service stopped paused or disabled events.	/All Data Monitors/ArcSight Solutions/NERC/CIP-007 System Security Management/
Last 10 Firewall Configuration Modifications	This data monitor tracks the most recent firewall configuration modifications.	/All Data Monitors/ArcSight Solutions/NERC/CIP-010 Configuration Change Management and Vulnerability/

Data Monitors Resources, continued

Resource	Description	URI
Last 10 Former Employee Activity	This data monitor shows former employee activity.	/All Data Monitors/ArcSight Solutions/NERC/CIP-004 Personnel and Training/
Last 10 Information Interception Events	This data monitor shows the last 10 Information Interception events.	/All Data Monitors/ArcSight Solutions/NERC/CIP-005 Electronic Security Perimeter(s)/
Last 10 Internal Reconnaissance Events	This data monitor displays in real-time the last 10 Internal Reconnaissance Events.	/All Data Monitors/ArcSight Solutions/NERC/CIP-008 Incident Reporting and Response Planning/
Last 10 Internal to External Communications	This data monitor displays the last 10 communications originates from an internal network segment and the target is in an external network segment.	/All Data Monitors/ArcSight Solutions/NERC/CIP-005 Electronic Security Perimeter(s)/
Last 10 Malware Activity	This data monitor shows the last 10 Malware Activity	/All Data Monitors/ArcSight Solutions/NERC/CIP-007 System Security Management/
Last 10 Network Devices Configuration Modifications	This data monitor tracks the most recent network devices configuration modifications.	/All Data Monitors/ArcSight Solutions/NERC/CIP-010 Configuration Change Management and Vulnerability/
Last 10 Network IDSs Configuration Modifications	This data monitor tracks the most recent NIDSs configuration modifications.	/All Data Monitors/ArcSight Solutions/NERC/CIP-010 Configuration Change Management and Vulnerability/
Last 10 Network Routing Configuration Modifications	This data monitor tracks the most recent network routing configuration modifications.	/All Data Monitors/ArcSight Solutions/NERC/CIP-010 Configuration Change Management and Vulnerability/

Data Monitors Resources, continued

Resource	Description	URI
Last 10 Operating Systems Configuration Modifications	This data monitor tracks the most recent os configuration modifications.	/All Data Monitors/ArcSight Solutions/NERC/CIP-010 Configuration Change Management and Vulnerability/
Last 10 Security Patch Missing Events	Real-time display of the last 20 vulnerabilities related to NERC assets.	/All Data Monitors/ArcSight Solutions/NERC/CIP-010 Configuration Change Management and Vulnerability/
Last 10 Shutdowns of Highly Critical Assets	This data monitor displays the last 10 Shutdowns of Highly Critical Assets .	/All Data Monitors/ArcSight Solutions/NERC/CIP-009 Recovery Plans for BES Cyber Systems/
Last 10 Successful Administrative Logins	This data monitor provides a list of the last 10 successful administrative logins across your assets categorized in Network Domains.	/All Data Monitors/ArcSight Solutions/NERC/CIP-007 System Security Management/
Last 10 Successful Administrative Logouts	This data monitor provides a list of the last 10 administrative logouts across your assets categorized in Network Domains.	/All Data Monitors/ArcSight Solutions/NERC/CIP-007 System Security Management/
Last 10 Successful User Logins	This data monitor provides a list of the last 10 successful logins by non-administrative users across your assets categorized in Network Domains.	/All Data Monitors/ArcSight Solutions/NERC/CIP-007 System Security Management/
Last 10 Successful User Logouts	This data monitor provides a list of the last 10 successful non-administrative user logouts across your assets categorized in Network Domains.	/All Data Monitors/ArcSight Solutions/NERC/CIP-007 System Security Management/
Last 10 Traffic Anomaly Events	This data monitor shows the last 10 Traffic Anomaly events.	/All Data Monitors/ArcSight Solutions/NERC/CIP-005 Electronic Security Perimeter(s)/

Data Monitors Resources, continued

Resource	Description	URI
Last 20 Asset Modifications	This data monitor provides a list of the last 20 asset modifications done to assets.	/All Data Monitors/ArcSight Solutions/NERC/CIP-002 BES Cyber System Categorization/
Last 20 Attacks and Suspicious Activity Events	This data monitor displays the last 20 attack and suspicious activity events.	/All Data Monitors/ArcSight Solutions/NERC/CIP-008 Incident Reporting and Response Planning/
Last 20 Attacks and Suspicious Activity Events Targeting High Impact BES Cyber Systems	This data monitor displays the last 20 attack and suspicious activity events where the traffic is destined for a High Impact BES Cyber Systems asset or zone.	/All Data Monitors/ArcSight Solutions/NERC/CIP-008 Incident Reporting and Response Planning/
Last 20 Attacks and Suspicious Activity Events Targeting Low Impact BES Cyber Systems	This data monitor displays the last 20 attack and suspicious activity events where the traffic is destined for a Low Impact BES Cyber Systems asset or zone.	/All Data Monitors/ArcSight Solutions/NERC/CIP-008 Incident Reporting and Response Planning/
Last 20 Attacks and Suspicious Activity Events Targeting Medium Impact BES Cyber Systems	This data monitor displays the last 20 attack and suspicious activity events where the traffic is destined for a Medium Impact BES Cyber Systems asset or zone.	/All Data Monitors/ArcSight Solutions/NERC/CIP-008 Incident Reporting and Response Planning/
Last 20 Attacks and Suspicious Activity Events Targeting Third Party Resources	This data monitor displays the last 20 attack and suspicious activity events where the traffic is destined for a Third Party asset or zone.	/All Data Monitors/ArcSight Solutions/NERC/CIP-008 Incident Reporting and Response Planning/
Last 20 Attacks and Suspicious Activity Events from High Impact BES Cyber Systems	This data monitor displays the last 20 attack and suspicious activity events where the traffic originated from a High Impact BES Cyber Systems asset or zone.	/All Data Monitors/ArcSight Solutions/NERC/CIP-008 Incident Reporting and Response Planning/
Last 20 Attacks and Suspicious Activity Events from Low Impact BES Cyber Systems	This data monitor displays the last 20 attack and suspicious activity events where the traffic originated from a Low Impact BES Cyber Systems asset or zone.	/All Data Monitors/ArcSight Solutions/NERC/CIP-008 Incident Reporting and Response Planning/

Data Monitors Resources, continued

Resource	Description	URI
Last 20 Attacks and Suspicious Activity Events from Medium Impact BES Cyber Systems	This data monitor displays the last 20 attack and suspicious activity events where the traffic originated from a Medium Impact BES Cyber Systems asset or zone.	/All Data Monitors/ArcSight Solutions/NERC/CIP-008 Incident Reporting and Response Planning/
Last 20 Attacks and Suspicious Activity Events from Third Party Resources	This data monitor displays the last 20 attack and suspicious activity events where the traffic originated from a Third Party asset or zone.	/All Data Monitors/ArcSight Solutions/NERC/CIP-008 Incident Reporting and Response Planning/
Last 20 Audit Log Cleared Events	This data monitor reports the last 10 audit log cleared events.	/All Data Monitors/ArcSight Solutions/NERC/CIP-010 Configuration Change Management and Vulnerability/
Last 20 Building Access Events	This data monitor shows the last 20 physical access events.	/All Data Monitors/ArcSight Solutions/NERC/CIP-006 Physical Security of BES Cyber Systems/
Last 20 DoS Attack Events	This data monitor displays the last 20 denial of service attack events.	/All Data Monitors/ArcSight Solutions/NERC/CIP-008 Incident Reporting and Response Planning/
Last 20 Failed Technical Compliance Checks	This data monitor shows the last 10 events indicating failed technical compliance checks.	/All Data Monitors/ArcSight Solutions/NERC/CIP-002 BES Cyber System Categorization/
Last 20 Information System Accounts Created	This data monitor displays the last 20 account creations.	/All Data Monitors/ArcSight Solutions/NERC/CIP-004 Personnel and Training/
Last 20 Information System Accounts Deleted	This data monitor displays the last 20 account deletions.	/All Data Monitors/ArcSight Solutions/NERC/CIP-004 Personnel and Training/
Last 20 Information System Accounts Modified	This data monitor displays the last 20 account modifications.	/All Data Monitors/ArcSight Solutions/NERC/CIP-004 Personnel and Training/

Data Monitors Resources, continued

Resource	Description	URI
Last 20 Machines Failing Technical Compliance Checks	This data monitor reports the last 20 machines that were reported to have failed technical compliance check.	/All Data Monitors/ArcSight Solutions/NERC/CIP-002 BES Cyber System Categorization/
Last 20 Overflow Vulnerabilities	This Data Monitor provides Real-time display of the last 20 overflow vulnerabilities related to NERC assets.	/All Data Monitors/ArcSight Solutions/NERC/CIP-010 Configuration Change Management and Vulnerability/
Last 20 Rules Fired	This data monitor shows a graphic distribution of the last 20 correlation rules fired from this section.	/All Data Monitors/ArcSight Solutions/NERC/CIPS Overview/CIP-002 Overview/
Last 20 Rules Fired	This data monitor displays a graphic distribution of the last 20 correlation rules fired from this section.	/All Data Monitors/ArcSight Solutions/NERC/CIPS Overview/CIP-003 Overview/
Last 20 Rules Fired	This data monitor displays a graphic distribution of the last 20 correlation rules fired from this section.	/All Data Monitors/ArcSight Solutions/NERC/CIPS Overview/CIP-004 Overview/
Last 20 Rules Fired	This data monitor displays a graphic distribution of the last 20 correlation rules fired from this section.	/All Data Monitors/ArcSight Solutions/NERC/CIPS Overview/CIP-005 Overview/
Last 20 Rules Fired	This data monitor displays a graphic distribution of the last 20 correlation rules fired from this section.	/All Data Monitors/ArcSight Solutions/NERC/CIPS Overview/CIP-006 Overview/
Last 20 Rules Fired	This data monitor displays a graphic distribution of the last 20 correlation rules fired from this section.	/All Data Monitors/ArcSight Solutions/NERC/CIPS Overview/CIP-007 Overview/

Data Monitors Resources, continued

Resource	Description	URI
Last 20 Rules Fired	This data monitor displays a graphic distribution of the last 20 correlation rules fired from this section.	/All Data Monitors/ArcSight Solutions/NERC/CIPS Overview/CIP-008 Overview/
Last 20 Rules Fired	This data monitor displays a graphic distribution of the last 20 correlation rules fired from this section.	/All Data Monitors/ArcSight Solutions/NERC/CIPS Overview/CIP-009 Overview/
Last 20 Rules Fired	This data monitor displays a graphic distribution of the last 20 correlation rules fired from this section.	/All Data Monitors/ArcSight Solutions/NERC/CIPS Overview/CIP-010 Overview/
Last 20 Rules Fired	This data monitor displays a graphic distribution of the last 20 correlation rules fired from this section.	/All Data Monitors/ArcSight Solutions/NERC/CIPS Overview/CIP-011 Overview/
Last 20 SSL Vulnerabilities	This Data Monitor provides Real-time Real-time display of the last 20 SSL vulnerabilities related to NERC assets.	/All Data Monitors/ArcSight Solutions/NERC/CIP-010 Configuration Change Management and Vulnerability/
Last 20 Unsuccessful Administrative Logins	This data monitor provides a list of the last 20 unsuccessful administrative logins across your assets categorized in Network Domains.	/All Data Monitors/ArcSight Solutions/NERC/CIP-007 System Security Management/
Last 20 Unsuccessful User Logins	This data monitor provides a list of the last 20 unsuccessful non-administrative user logins across your assets categorized in Network Domains.	/All Data Monitors/ArcSight Solutions/NERC/CIP-007 System Security Management/
Last 20 User Group Created	This data monitor displays the last 20 user group creations.	/All Data Monitors/ArcSight Solutions/NERC/CIP-004 Personnel and Training/
Last 20 User Group Deleted	This data monitor displays the last 20 user group deletions.	/All Data Monitors/ArcSight Solutions/NERC/CIP-004 Personnel and Training/

Data Monitors Resources, continued

Resource	Description	URI
Last 20 User Group Modified	This data monitor displays the last 20 user group modifications.	/All Data Monitors/ArcSight Solutions/NERC/CIP-004 Personnel and Training/
Last 20 User Login Attempts	This data monitor shows in real-time the last 20 login attempts for non-administrative users across your assets categorized in Network Domains.	/All Data Monitors/ArcSight Solutions/NERC/CIP-007 System Security Management/
Last 20 Vulnerabilities	Real-time display of the last 20 vulnerabilities related to NERC assets .	/All Data Monitors/ArcSight Solutions/NERC/CIP-010 Configuration Change Management and Vulnerability/
Last 20 Vulnerabilities with High CVSS	Real-time display of the last 20 vulnerabilities with CVSS equal or higher than 8 and related to NERC assets.	/All Data Monitors/ArcSight Solutions/NERC/CIP-010 Configuration Change Management and Vulnerability/
Last 20 XSRF Vulnerabilities	This Data Monitor provides Real-time display of the last 20 XSRF vulnerabilities related to NERC assets .	/All Data Monitors/ArcSight Solutions/NERC/CIP-010 Configuration Change Management and Vulnerability/
Last 20 XSS Vulnerabilities	This Data Monitor provides Real-time display of the last 20 XSS vulnerabilities related to NERC assets.	/All Data Monitors/ArcSight Solutions/NERC/CIP-010 Configuration Change Management and Vulnerability/
Last Connections to Disallowed Ports	This data monitors shows the last 10 connections to disallowed ports to or from the network.	/All Data Monitors/ArcSight Solutions/NERC/CIP-005 Electronic Security Perimeter(s)/
Last Default Vendor Account Credentials Observed	This data monitor displays login events where user has attempted to login to a system with vendor-supplied default User ID.	/All Data Monitors/ArcSight Solutions/NERC/CIP-004 Personnel and Training/

Data Monitors Resources, continued

Resource	Description	URI
Last State External Device Overview	Real-time display of the last 20 external device activity and their status.	/All Data Monitors/ArcSight Solutions/NERC/CIP-010 Configuration Change Management and Vulnerability/
Last State Vulnerability Overview	Real-time display of the last 20 vulnerabilities related to assets and their compliance status.	/All Data Monitors/ArcSight Solutions/NERC/CIP-010 Configuration Change Management and Vulnerability/
Logging Devices	This data monitor shows all devices other than ArcSight that are sending their logs.	/All Data Monitors/ArcSight Solutions/NERC/CIP-005 Electronic Security Perimeter(s)/
Malicious Code Activity	This Event Graph data monitor shows the malicious code activity between Attacker-Target pairs.	/All Data Monitors/ArcSight Solutions/NERC/CIP-007 System Security Management/
New Hires Logins	This data monitor shows the new hire user logins.	/All Data Monitors/ArcSight Solutions/NERC/CIP-004 Personnel and Training/
Organizational Records Leak	This data monitor displays a graph with events which pertain to information leaks of organizational records.	/All Data Monitors/ArcSight Solutions/NERC/CIP-011 Information Protection/
Overall CIPS Rule Firings	This data monitor shows a count of the rules that were fired per section across all sections of the ITGov3.0 solution in the last hour.	/All Data Monitors/ArcSight Solutions/NERC/CIPS Overview/
Personal Information Leak	This data monitor shows communications pertaining to personal information leaks.	/All Data Monitors/ArcSight Solutions/NERC/CIP-011 Information Protection/
Ports Used in Attacks and Suspicious Activity Events	This data monitor shows the ports used in attack and suspicious activity events. By default the data monitor shows data from the last 5 minutes.	/All Data Monitors/ArcSight Solutions/NERC/CIP-008 Incident Reporting and Response Planning/

Data Monitors Resources, continued

Resource	Description	URI
Ports Used in Attacks and Suspicious Activity Events Targeting High Impact BES Cyber Systems	This data monitor shows the ports used in attack and suspicious activity events that targeted High Impact BES Cyber Systems assets or zones. By default the data monitor shows data from the last 5 minutes.	/All Data Monitors/ArcSight Solutions/NERC/CIP-008 Incident Reporting and Response Planning/
Ports Used in Attacks and Suspicious Activity Events Targeting Low Impact BES Cyber Systems	This data monitor shows the ports used in attack and suspicious activity events that targeted Low Impact BES Cyber Systems assets or zones. By default the data monitor shows data from the last 5 minutes.	/All Data Monitors/ArcSight Solutions/NERC/CIP-008 Incident Reporting and Response Planning/
Ports Used in Attacks and Suspicious Activity Events Targeting Medium Impact BES Cyber Systems	This data monitor shows the ports used in attack and suspicious activity events that targeted Medium Impact BES Cyber Systems assets or zones. By default the data monitor shows data from the last 5 minutes.	/All Data Monitors/ArcSight Solutions/NERC/CIP-008 Incident Reporting and Response Planning/
Ports Used in Attacks and Suspicious Activity Events Targeting Third Party Resources	This data monitor shows the ports used in attack and suspicious activity events that targeted Third Party assets or zones. By default the data monitor shows data from the last 5 minutes.	/All Data Monitors/ArcSight Solutions/NERC/CIP-008 Incident Reporting and Response Planning/
Ports Used in Attacks and Suspicious Activity Events from High Impact BES Cyber Systems	This data monitor shows the ports used in attack and suspicious activity events that originated from High Impact BES Cyber Systems assets or zones. By default the data monitor shows data from the last 5 minutes.	/All Data Monitors/ArcSight Solutions/NERC/CIP-008 Incident Reporting and Response Planning/
Ports Used in Attacks and Suspicious Activity Events from Low Impact BES Cyber Systems	This data monitor shows the ports used in attack and suspicious activity events that originated from Low Impact BES Cyber Systems assets or zones. By default the data monitor shows data from the last 5 minutes.	/All Data Monitors/ArcSight Solutions/NERC/CIP-008 Incident Reporting and Response Planning/
Ports Used in Attacks and Suspicious Activity Events from Medium Impact BES Cyber Systems	This data monitor shows the ports used in attack and suspicious activity events that originated from Medium Impact BES Cyber Systems assets or zones. By default the data monitor shows data from the last 5 minutes.	/All Data Monitors/ArcSight Solutions/NERC/CIP-008 Incident Reporting and Response Planning/
Ports Used in Attacks and Suspicious Activity Events from Third Party Resources	This data monitor shows the ports used in attack and suspicious activity events that originated from Third Party assets or zones. By default the data monitor shows data from the last 5 minutes.	/All Data Monitors/ArcSight Solutions/NERC/CIP-008 Incident Reporting and Response Planning/

Data Monitors Resources, continued

Resource	Description	URI
Rules Attackers and Targets	Event graph to show attacker-target pair relationship for the various rule firings from this section.	/All Data Monitors/ArcSight Solutions/NERC/CIPS Overview/CIP-002 Overview/
Rules Attackers and Targets	Event graph to show attacker-target pair relationship for the various rule firings from this section.	/All Data Monitors/ArcSight Solutions/NERC/CIPS Overview/CIP-003 Overview/
Rules Attackers and Targets	Event graph to show attacker-target pair relationship for the various rule firings from this section.	/All Data Monitors/ArcSight Solutions/NERC/CIPS Overview/CIP-004 Overview/
Rules Attackers and Targets	Event graph to show attacker-target pair relationship for the various rule firings from this section.	/All Data Monitors/ArcSight Solutions/NERC/CIPS Overview/CIP-005 Overview/
Rules Attackers and Targets	Event graph to show attacker-target pair relationship for the various rule firings from this section.	/All Data Monitors/ArcSight Solutions/NERC/CIPS Overview/CIP-006 Overview/
Rules Attackers and Targets	Event graph to show attacker-target pair relationship for the various rule firings from this section.	/All Data Monitors/ArcSight Solutions/NERC/CIPS Overview/CIP-007 Overview/
Rules Attackers and Targets	Event graph to show attacker-target pair relationship for the various rule firings from this section.	/All Data Monitors/ArcSight Solutions/NERC/CIPS Overview/CIP-008 Overview/
Rules Attackers and Targets	Event graph to show attacker-target pair relationship for the various rule firings from this section.	/All Data Monitors/ArcSight Solutions/NERC/CIPS Overview/CIP-009 Overview/
Rules Attackers and Targets	Event graph to show attacker-target pair relationship for the various rule firings from this section.	/All Data Monitors/ArcSight Solutions/NERC/CIPS Overview/CIP-010 Overview/

Data Monitors Resources, continued

Resource	Description	URI
Rules Attackers and Targets	Event graph to show attacker-target pair relationship for the various rule firings from this section.	/All Data Monitors/ArcSight Solutions/NERC/CIPS Overview/CIP-011 Overview/
Suspicious Activity by New Hires	This data monitor shows the new hires suspicious activity count. Suspicious activity is counted for 7 days (as long as the user is defined new, see New Hire Accounts active list).	/All Data Monitors/ArcSight Solutions/NERC/CIP-004 Personnel and Training/
Top 10 Administrative Users with Successful Logins	This data monitor provides a list of the administrative attacker and target user name pairs with most successful logins	/All Data Monitors/ArcSight Solutions/NERC/CIP-007 System Security Management/
Top 10 Administrative Users with Unsuccessful Logins	This data monitor provides a list of the administrative attacker and target user name pairs with most failed logins	/All Data Monitors/ArcSight Solutions/NERC/CIP-007 System Security Management/
Top 10 Asset Network Domains with Account Creation Deletion and Modification	This data monitor displays the Network Domains asset categories in which the most accounts have been created, modified or deleted.	/All Data Monitors/ArcSight Solutions/NERC/CIP-004 Personnel and Training/
Top 10 Assets missing Security Patches	Real-time display of the top 10 assets with security patches missing.	/All Data Monitors/ArcSight Solutions/NERC/CIP-010 Configuration Change Management and Vulnerability/
Top 10 Assets with Critical Vulnerabilities	Real-time display of the top 10 assets with critical vulnerability events.	/All Data Monitors/ArcSight Solutions/NERC/CIP-010 Configuration Change Management and Vulnerability/
Top 10 Configuration Modifications Events	This data monitor tracks the top 10 system configuration modifications.	/All Data Monitors/ArcSight Solutions/NERC/CIP-010 Configuration Change Management and Vulnerability/

Data Monitors Resources, continued

Resource	Description	URI
Top 10 Devices with Configuration Modifications	This data monitor provides a list of the assets that have their configurations changed frequently.	/All Data Monitors/ArcSight Solutions/NERC/CIP-010 Configuration Change Management and Vulnerability/
Top 10 DoS Attackers	This data monitor shows the top 10 DoS Attackers.	/All Data Monitors/ArcSight Solutions/NERC/CIP-008 Incident Reporting and Response Planning/
Top 10 DoS Targets	This data monitor shows the top 10 DoS targets.	/All Data Monitors/ArcSight Solutions/NERC/CIP-008 Incident Reporting and Response Planning/
Top 10 Failed Technical Compliance Checks	This data monitor shows the top ten events indicating failed technical compliance checks.	/All Data Monitors/ArcSight Solutions/NERC/CIP-002 BES Cyber System Categorization/
Top 10 Firewall Configuration Modifications Events	This data monitor tracks the top 10 firewall configuration modifications.	/All Data Monitors/ArcSight Solutions/NERC/CIP-010 Configuration Change Management and Vulnerability/
Top 10 Firewalls with Configuration Modifications	This data monitor provides a list of the Firewalls that have their configurations changed frequently.	/All Data Monitors/ArcSight Solutions/NERC/CIP-010 Configuration Change Management and Vulnerability/
Top 10 Hosts with Dynamic Open Ports	This data monitor provides top list of hosts that have dynamic open ports.	/All Data Monitors/ArcSight Solutions/NERC/CIP-007 System Security Management/
Top 10 Hosts with Open Ports	This data monitor provides top list of hosts that have open ports.	/All Data Monitors/ArcSight Solutions/NERC/CIP-007 System Security Management/

Data Monitors Resources, continued

Resource	Description	URI
Top 10 Hosts with Successful Administrative Logins	This data monitor provides a list of the hosts with most successful administrative logins.	/All Data Monitors/ArcSight Solutions/NERC/CIP-007 System Security Management/
Top 10 Hosts with Unsecured Open Ports	This data monitor provides top list of hosts that have unsecured open ports.	/All Data Monitors/ArcSight Solutions/NERC/CIP-007 System Security Management/
Top 10 Hosts with Unsuccessful Administrative Logins	This data monitor provides a list of the hosts with most unsuccessful administrative logins.	/All Data Monitors/ArcSight Solutions/NERC/CIP-007 System Security Management/
Top 10 Hosts with Unsuccessful User Logins	This data monitor provides an ordered list of hosts that most frequently have login failures for non-administrative users.	/All Data Monitors/ArcSight Solutions/NERC/CIP-007 System Security Management/
Top 10 Intellectual Property Rights Violations	This data monitor shows the top 10 violations concerning intellectual property by looking for the rule-firing in this use-case.	/All Data Monitors/ArcSight Solutions/NERC/CIP-003 Security Management Controls/
Top 10 Intellectual Property Rights Violators	This data monitor shows the top 10 violators downloading intellectual property by looking for the rule-firing in this use-case.	/All Data Monitors/ArcSight Solutions/NERC/CIP-003 Security Management Controls/
Top 10 Machines Failing Technical Compliance Checks	This data monitor shows the top 10 machines with failed compliance checks.	/All Data Monitors/ArcSight Solutions/NERC/CIP-002 BES Cyber System Categorization/
Top 10 Malwares	This data monitor provides a list of the top 10 malware activity.	/All Data Monitors/ArcSight Solutions/NERC/CIP-007 System Security Management/

Data Monitors Resources, continued

Resource	Description	URI
Top 10 Network Devices with Configuration Modifications	This data monitor provides a list of the network devices that have their configurations changed frequently.	/All Data Monitors/ArcSight Solutions/NERC/CIP-010 Configuration Change Management and Vulnerability/
Top 10 Network Domains with Successful Administrative Logins	This data monitor provides an ordered list of the Network Domains that with most successful administrative logins.	/All Data Monitors/ArcSight Solutions/NERC/CIP-007 System Security Management/
Top 10 Network Domains with Unsuccessful User Logins	This data monitor provides an ordered list of the Network Domains that most frequently have non-administrative user login failures.	/All Data Monitors/ArcSight Solutions/NERC/CIP-007 System Security Management/
Top 10 Network IDSs with Configuration Modifications	This data monitor provides a list of the NIDSs that have their configurations changed frequently.	/All Data Monitors/ArcSight Solutions/NERC/CIP-010 Configuration Change Management and Vulnerability/
Top 10 Network Routings with Configuration Modifications	This data monitor provides a list of the network routings equipments that have their configurations changed frequently.	/All Data Monitors/ArcSight Solutions/NERC/CIP-010 Configuration Change Management and Vulnerability/
Top 10 Operating Systems Configuration Modifications Events	This data monitor tracks the top 10 OS configuration modifications.	/All Data Monitors/ArcSight Solutions/NERC/CIP-010 Configuration Change Management and Vulnerability/
Top 10 Operating Systems with Configuration Modifications	This data monitor provides a list of the Firewalls that have their configurations changed frequently.	/All Data Monitors/ArcSight Solutions/NERC/CIP-010 Configuration Change Management and Vulnerability/
Top 10 Policy Violations	This data monitor shows the top 10 policy breach events.	/All Data Monitors/ArcSight Solutions/NERC/CIP-003 Security Management Controls/

Data Monitors Resources, continued

Resource	Description	URI
Top 10 Policy Violators	This data monitor shows the top 10 policy violators.	/All Data Monitors/ArcSight Solutions/NERC/CIP-003 Security Management Controls/
Top 10 Shutdowns of Highly Critical Assets	This data monitor shows the 10 highly critical assets with top shutdowns .	/All Data Monitors/ArcSight Solutions/NERC/CIP-009 Recovery Plans for BES Cyber Systems/
Top 10 Unsecured Open Ports	This data monitor provides top list of hosts that have unsecured open ports.	/All Data Monitors/ArcSight Solutions/NERC/CIP-007 System Security Management/
Top 10 Users with Unsuccessful User Logins	This data monitor provides an ordered list of non-administrative users who most frequently have failed logins.	/All Data Monitors/ArcSight Solutions/NERC/CIP-007 System Security Management/
Top 10 Vulnerable Assets	Real-time display of the top 10 assets with vulnerability events.	/All Data Monitors/ArcSight Solutions/NERC/CIP-010 Configuration Change Management and Vulnerability/
Top 20 Rules Fired	This data monitor displays a graphic distribution of the 20 most frequently firing correlation rules of this section.	/All Data Monitors/ArcSight Solutions/NERC/CIPS Overview/CIP-002 Overview/
Top 20 Rules Fired	This data monitor displays a graphic distribution of the 20 most frequently firing correlation rules of this section.	/All Data Monitors/ArcSight Solutions/NERC/CIPS Overview/CIP-003 Overview/
Top 20 Rules Fired	This data monitor displays a graphic distribution of the 20 most frequently firing correlation rules of this section.	/All Data Monitors/ArcSight Solutions/NERC/CIPS Overview/CIP-004 Overview/

Data Monitors Resources, continued

Resource	Description	URI
Top 20 Rules Fired	This data monitor displays a graphic distribution of the 20 most frequently firing correlation rules of this section.	/All Data Monitors/ArcSight Solutions/NERC/CIPS Overview/CIP-005 Overview/
Top 20 Rules Fired	This data monitor displays a graphic distribution of the 20 most frequently firing correlation rules of this section.	/All Data Monitors/ArcSight Solutions/NERC/CIPS Overview/CIP-006 Overview/
Top 20 Rules Fired	This data monitor displays a graphic distribution of the 20 most frequently firing correlation rules of this section.	/All Data Monitors/ArcSight Solutions/NERC/CIPS Overview/CIP-007 Overview/
Top 20 Rules Fired	This data monitor displays a graphic distribution of the 20 most frequently firing correlation rules of this section.	/All Data Monitors/ArcSight Solutions/NERC/CIPS Overview/CIP-008 Overview/
Top 20 Rules Fired	This data monitor displays a graphic distribution of the 20 most frequently firing correlation rules of this section.	/All Data Monitors/ArcSight Solutions/NERC/CIPS Overview/CIP-009 Overview/
Top 20 Rules Fired	This data monitor displays a graphic distribution of the 20 most frequently firing correlation rules of this section.	/All Data Monitors/ArcSight Solutions/NERC/CIPS Overview/CIP-010 Overview/
Top 20 Rules Fired	This data monitor displays a graphic distribution of the 20 most frequently firing correlation rules of this section.	/All Data Monitors/ArcSight Solutions/NERC/CIPS Overview/CIP-011 Overview/
Top 20 Targets in Rule Firings	This data monitor shows which targets are most frequently involved in rule firings for that section. This may reveal a trend about certain targets.	/All Data Monitors/ArcSight Solutions/NERC/CIPS Overview/CIP-002 Overview/
Top 20 Targets in Rule Firings	This data monitor shows which targets are most frequently involved in rule firings for that section. This may reveal a trend about certain targets.	/All Data Monitors/ArcSight Solutions/NERC/CIPS Overview/CIP-003 Overview/

Data Monitors Resources, continued

Resource	Description	URI
Top 20 Targets in Rule Firings	This data monitor shows which targets are most frequently involved in rule firings for that section. This may reveal a trend about certain targets.	/All Data Monitors/ArcSight Solutions/NERC/CIPS Overview/CIP-004 Overview/
Top 20 Targets in Rule Firings	This data monitor shows which targets are most frequently involved in rule firings for that section. This may reveal a trend about certain targets.	/All Data Monitors/ArcSight Solutions/NERC/CIPS Overview/CIP-005 Overview/
Top 20 Targets in Rule Firings	This data monitor shows which targets are most frequently involved in rule firings for that section. This may reveal a trend about certain targets.	/All Data Monitors/ArcSight Solutions/NERC/CIPS Overview/CIP-006 Overview/
Top 20 Targets in Rule Firings	This data monitor shows which targets are most frequently involved in rule firings for that section. This may reveal a trend about certain targets.	/All Data Monitors/ArcSight Solutions/NERC/CIPS Overview/CIP-007 Overview/
Top 20 Targets in Rule Firings	This data monitor shows which targets are most frequently involved in rule firings for that section. This may reveal a trend about certain targets.	/All Data Monitors/ArcSight Solutions/NERC/CIPS Overview/CIP-008 Overview/
Top 20 Targets in Rule Firings	This data monitor shows which targets are most frequently involved in rule firings for that section. This may reveal a trend about certain targets.	/All Data Monitors/ArcSight Solutions/NERC/CIPS Overview/CIP-009 Overview/
Top 20 Targets in Rule Firings	This data monitor shows which targets are most frequently involved in rule firings for that section. This may reveal a trend about certain targets.	/All Data Monitors/ArcSight Solutions/NERC/CIPS Overview/CIP-010 Overview/
Top 20 Targets in Rule Firings	This data monitor shows which targets are most frequently involved in rule firings for that section. This may reveal a trend about certain targets.	/All Data Monitors/ArcSight Solutions/NERC/CIPS Overview/CIP-011 Overview/
Top Blocked Traffic Attackers	This data monitor displays a bar chart of the top attacker addresses of blocked traffic.	/All Data Monitors/ArcSight Solutions/NERC/CIP-005 Electronic Security Perimeter(s)/

Data Monitors Resources, continued

Resource	Description	URI
Top Blocked Traffic Attackers to High Impact BES Systems	This data monitor displays a bar chart of the top attacker addresses of blocked traffic to High Impact BES Systems.	/All Data Monitors/ArcSight Solutions/NERC/CIP-005 Electronic Security Perimeter(s)/
Top Blocked Traffic Attackers to Low Impact BES Systems	This data monitor displays a bar chart of the top attacker addresses of blocked traffic to Low Impact BES Systems.	/All Data Monitors/ArcSight Solutions/NERC/CIP-005 Electronic Security Perimeter(s)/
Top Blocked Traffic Attackers to Medium Impact BES Systems	This data monitor displays a bar chart of the top attacker addresses of blocked traffic to Medium Impact BES Systems.	/All Data Monitors/ArcSight Solutions/NERC/CIP-005 Electronic Security Perimeter(s)/
Top Default Vendor Accounts Observed	This data monitor displays top vendor-supplied default account observed.	/All Data Monitors/ArcSight Solutions/NERC/CIP-004 Personnel and Training/
Top Disallowed Ports	This data monitor provides a list of the top 10 disallowed ports.	/All Data Monitors/ArcSight Solutions/NERC/CIP-005 Electronic Security Perimeter(s)/
Top External to Internal Communications	This data monitor displays a bar chart of the top traffic originates from an external network segment and the target is in an internal network segment.	/All Data Monitors/ArcSight Solutions/NERC/CIP-005 Electronic Security Perimeter(s)/
Top Information Interception Attackers	This data monitor displays a bar chart of the attacker addresses and priorities for information interception events.	/All Data Monitors/ArcSight Solutions/NERC/CIP-005 Electronic Security Perimeter(s)/
Top Internal Hosts to Disallowed Ports	This data monitor provides a list of the top 10 internal hosts that accessed disallowed ports.	/All Data Monitors/ArcSight Solutions/NERC/CIP-005 Electronic Security Perimeter(s)/
Top Internal Inter-Domain Communications	This data monitor shows the top attacker and target domain pairs with most traffic.	/All Data Monitors/ArcSight Solutions/NERC/CIP-005 Electronic Security Perimeter(s)/

Data Monitors Resources, continued

Resource	Description	URI
Top Internal Providers of Disallowed Ports	This data monitor provides a list of the top 10 internal providers of disallowed ports.	/All Data Monitors/ArcSight Solutions/NERC/CIP-005 Electronic Security Perimeter(s)/
Top Internal Reconnaissance Sources	This data monitor shows the top internal reconnaissance sources identified by the rule in this section.	/All Data Monitors/ArcSight Solutions/NERC/CIP-008 Incident Reporting and Response Planning/
Top Internal Reconnaissance Targets	This data monitor shows the top internal reconnaissance targets identified by the rule in this section.	/All Data Monitors/ArcSight Solutions/NERC/CIP-008 Incident Reporting and Response Planning/
Top Internal to External Communications	This data monitor displays a bar chart of the top traffic originates from an internal network segment and the target is in an external network segment.	/All Data Monitors/ArcSight Solutions/NERC/CIP-005 Electronic Security Perimeter(s)/
Top Targets with Default Vendor Accounts	This data monitor displays login events where user has attempted to login to a system with vendor-supplied default account.	/All Data Monitors/ArcSight Solutions/NERC/CIP-004 Personnel and Training/
Top Traffic Anomaly Attackers	This data monitor provides a list of the top 10 anomaly traffic per Attacker and Target Addresses addresses .	/All Data Monitors/ArcSight Solutions/NERC/CIP-005 Electronic Security Perimeter(s)/
Top User Login Activity	This data monitor shows the top 20 non-administrative users attempting to login to a system.	/All Data Monitors/ArcSight Solutions/NERC/CIP-007 System Security Management/
Top Users Accessing Buildings	This data monitor shows the top 10 users accessing buildings.	/All Data Monitors/ArcSight Solutions/NERC/CIP-006 Physical Security of BES Cyber Systems/
Traffic Anomaly	This data monitor presenting traffic anomaly in event graph chart .	/All Data Monitors/ArcSight Solutions/NERC/CIP-005 Electronic Security Perimeter(s)/

Data Monitors Resources, continued

Resource	Description	URI
Traffic Anomaly by Protocol	This data monitor provides the distribution of traffic anomaly by protocol.	/All Data Monitors/ArcSight Solutions/NERC/CIP-005 Electronic Security Perimeter(s)/
Traffic Between Zones	This data monitor shows the target ports between zones.	/All Data Monitors/ArcSight Solutions/NERC/CIP-005 Electronic Security Perimeter(s)/
Unsuccessful User Logins	This data monitor reports on a moving average of the number of unsuccessful user logins.	/All Data Monitors/ArcSight Solutions/NERC/CIP-007 System Security Management/
Up Down Status of Highly Critical Assets	This Last State data monitor shows the state of highly critical assets and whether they are up or down.	/All Data Monitors/ArcSight Solutions/NERC/CIP-009 Recovery Plans for BES Cyber Systems/
User Logins	This data monitor reports on a moving average of the number of user logins.	/All Data Monitors/ArcSight Solutions/NERC/CIP-007 System Security Management/
Users Changing Accounts	This data monitor shown the users that added, deleted and modified accounts.	/All Data Monitors/ArcSight Solutions/NERC/CIP-004 Personnel and Training/

Field Sets

The following table lists all the field sets.

Field Sets Resources

Resource	Description	URI
Asset Inventory	This field set shows event fields relevant to asset inventory type of events.	/All Field Sets/ArcSight Solutions/NERC/
Audit Tool Logins	This field set shows logins from remote machines to the audit tool.	/All Field Sets/ArcSight Solutions/NERC/

Field Sets Resources, continued

Resource	Description	URI
Device Configuration Changes	Includes device fields.	/All Field Sets/ArcSight Solutions/NERC/
Event with Attacker Data	This field set shows the attacker fields.	/All Field Sets/ArcSight Solutions/NERC/
Events with Attacker Assets	This field set shows events which are related to attacker assets.	/All Field Sets/ArcSight Solutions/NERC/
Events with Target Assets	This field set shows events which are related to target assets.	/All Field Sets/ArcSight Solutions/NERC/
Internet Activity - Machine based	This field set shows machine based internet activity.	/All Field Sets/ArcSight Solutions/NERC/
Internet Activity - User based	This field set shows machine based internet activity.	/All Field Sets/ArcSight Solutions/NERC/
New Services and New Hosts	This field set shows events with target host and service information.	/All Field Sets/ArcSight Solutions/NERC/
OS Events	Includes OS events fields.	/All Field Sets/ArcSight Solutions/NERC/
Open Ports	Includes open ports events fields.	/All Field Sets/ArcSight Solutions/NERC/
Physical Security	A field set that can be used to show the relevant fields for physical security events.	/All Field Sets/ArcSight Solutions/NERC/
Service Fields	Includes service events fields.	/All Field Sets/ArcSight Solutions/NERC/
Third Party Events	This field set shows events involving 3rd parties.	/All Field Sets/ArcSight Solutions/NERC/

Field Sets Resources, continued

Resource	Description	URI
Traffic with Target Asset Criticality	This field set shows the assets involved in a communication along with the target assets' criticality assignment.	/All Field Sets/ArcSight Solutions/NERC/
User Authentication	This field set is used by an active channel to display all user authentication related events.	/All Field Sets/ArcSight Solutions/NERC/
Vulnerability Fields	Includes the vulnerability fields.	/All Field Sets/ArcSight Solutions/NERC/

Filters

The following table lists all the filters.

Filters Resources

Resource	Description	URI
Account Creation	This filter identifies account creation events.	/All Filters/ArcSight Solutions/NERC/CIP-004 Personnel and Training/
Account Creations, Modifications and Deletions	This purpose of this filter is to identify all account management events.	/All Filters/ArcSight Solutions/NERC/CIP-004 Personnel and Training/
Account Deletion	This filter identifies account deletion events.	/All Filters/ArcSight Solutions/NERC/CIP-004 Personnel and Training/
Account Lockouts	This filter is used to identify account lockouts. By default it will recognize lockouts on Microsoft Windows and Unix systems.	/All Filters/ArcSight Solutions/NERC/CIP-007 System Security Management/
Account Modification	The purpose of this filter is to identify account modification events.	/All Filters/ArcSight Solutions/NERC/CIP-004 Personnel and Training/
Administrative Login Attempts	The purpose of this filter is to identify login attempts by administrative users. Administrative accounts should be defined in all-lower case in the Administrative Accounts active list.	/All Filters/ArcSight Solutions/NERC/General Filters/Authentication/
Administrative User	The purpose of this filter is identify events with administrative users. These events are defined as such in which either the source or destination users are administrative users. Administrative accounts have to be defined *in all lower case* in the active list Administrative Accounts.	/All Filters/ArcSight Solutions/NERC/General Filters/Authentication/

Filters Resources, continued

Resource	Description	URI
After Hours	This filter defines the time period of 'after hours'. Change this filter to adjust the default settings.	/All Filters/ArcSight Solutions/NERC/General Filters/
After Hours	This filter is used to define the time period of 'after hours'. Change this filter to adjust the default settings.	/All Filters/ArcSight Solutions/NERC/My Filters/
AirDefense Events	This filter identifies events from an AirDefense device.	/All Filters/ArcSight Solutions/NERC/CIP-005 Electronic Security Perimeter(s)/
AirMagnet Events	This filter identifies events from an AirMagnet device.	/All Filters/ArcSight Solutions/NERC/CIP-005 Electronic Security Perimeter(s)/
AirPatrol Events	This filter identifies events from an AirPatrol device.	/All Filters/ArcSight Solutions/NERC/CIP-005 Electronic Security Perimeter(s)/
All Brute Force Login Attempts	This filter identifies all types of Brute Force Login Attempts.	/All Filters/ArcSight Solutions/NERC/CIP-007 System Security Management/
All Information Leak Events	This filter selects events that reflect information leakage.	/All Filters/ArcSight Solutions/NERC/CIP-011 Information Protection/
Anti-Virus Clean or Quarantine Attempt	This filter looks for anti-virus events that indicate a quarantine or cleaning attempt of a detected malware instance.	/All Filters/ArcSight Solutions/NERC/CIP-007 System Security Management/
Anti-Virus Service Stopped or Paused	This filter selects events where any of the named security services are stopped on any system. Refer to the Filter tab for the list of such services.	/All Filters/ArcSight Solutions/NERC/CIP-007 System Security Management/
Anti-Virus Service Stopped or Paused in Windows	This filter selects windows events where any of the named security services are stopped on any system. Refer to the Filter tab for the list of such services.	/All Filters/ArcSight Solutions/NERC/CIP-007 System Security Management/
Application Brute Force Login Attempts	This filter identifies all application brute force login attempt events.	/All Filters/ArcSight Solutions/NERC/CIP-007 System Security Management/

Filters Resources, continued

Resource	Description	URI
Asset Categorized in Network Domains	This filter checks whether the target asset is categorized under the Network Domains category.	/All Filters/ArcSight Solutions/NERC/General Filters/
Asset Creation	Select events indicating the creation of a new asset.	/All Filters/ArcSight Solutions/NERC/CIP-002 BES Cyber System Categorization/
Asset Deletion	Select events indicating the deletion of an asset.	/All Filters/ArcSight Solutions/NERC/CIP-002 BES Cyber System Categorization/
Asset Modification	Select events indicating the modification of an asset.	/All Filters/ArcSight Solutions/NERC/CIP-002 BES Cyber System Categorization/
Attacker Asset in High Impact BES Cyber Assets	This filter looks for events originated from High Impact BES Cyber Assets.	/All Filters/ArcSight Solutions/NERC/My Filters/
Attacker Asset in Highly Critical Assets	This filter identifies all events that originate from highly critical assets.	/All Filters/ArcSight Solutions/NERC/My Filters/
Attacker Asset in Low Impact BES Cyber Assets	This filter looks for events originated from Low Impact BES Cyber Assets	/All Filters/ArcSight Solutions/NERC/My Filters/
Attacker Asset in Medium Impact BES Cyber Assets	This filter looks for events originated from Medium Impact BES Cyber Assets.	/All Filters/ArcSight Solutions/NERC/My Filters/
Attacker Asset is Wireless	This filter looks for events originated from wireless devices .	/All Filters/ArcSight Solutions/NERC/My Filters/
Attacker Host or Address Present	This filter identifies events that have either the Attacker Host Name or Attacker Address event fields populated.	/All Filters/ArcSight Solutions/NERC/General Filters/
Attacker User Is Administrator	This filter checks whether the attacker user is an administrator.	/All Filters/ArcSight Solutions/NERC/General Filters/

Filters Resources, continued

Resource	Description	URI
Attacker User Present	This filter identifies events that have the Attacker User Name event fields populated.	/All Filters/ArcSight Solutions/NERC/General Filters/
Attacker or Target User Present	This filter identifies events that have either the Attacker User Name or Target User Name event fields populated.	/All Filters/ArcSight Solutions/NERC/General Filters/
Attacks and Suspicious Activity	This filter identifies events which indicate compromise, reconnaissance, hostile, or suspicious activity.	/All Filters/ArcSight Solutions/NERC/CIP-008 Incident Reporting and Response Planning/
Attacks and Suspicious Activity	Filtering in events which indicate Compromise, Reconnaissance, Hostile, or Suspicious activity.	/All Filters/ArcSight Solutions/NERC/General Filters/
Attacks and Suspicious Activity Targeting High Impact BES Cyber Systems	This filter identifies attack and suspicious activity events targeting assets or zones that are categorized in the High Impact BES Cyber Systems asset category.	/All Filters/ArcSight Solutions/NERC/CIP-008 Incident Reporting and Response Planning/
Attacks and Suspicious Activity Targeting Low Impact BES Cyber Systems	This filter identifies attack and suspicious activity events targeting assets or zones that are categorized in the Low Impact BES Cyber Systems asset category.	/All Filters/ArcSight Solutions/NERC/CIP-008 Incident Reporting and Response Planning/
Attacks and Suspicious Activity Targeting Medium Impact BES Cyber Systems	This filter identifies attack and suspicious activity events targeting assets or zones that are categorized in the Medium Impact BES Cyber Systems asset category.	/All Filters/ArcSight Solutions/NERC/CIP-008 Incident Reporting and Response Planning/
Attacks and Suspicious Activity Targeting Public Facing Resources	This filter identifies attack and suspicious activity events that target assets or zones categorized in the Public-Facing asset category.	/All Filters/ArcSight Solutions/NERC/CIP-008 Incident Reporting and Response Planning/

Filters Resources, continued

Resource	Description	URI
Attacks and Suspicious Activity Targeting Third Party Resources	This filter identifies attack and suspicious activity events targeting assets or zones categorized in the Third Party asset category.	/All Filters/ArcSight Solutions/NERC/CIP-008 Incident Reporting and Response Planning/
Attacks and Suspicious Activity from High Impact BES Cyber Systems	This filter identifies attack and suspicious activity events from assets or zones that are categorized in the High Impact BES Cyber Systems asset category.	/All Filters/ArcSight Solutions/NERC/CIP-008 Incident Reporting and Response Planning/
Attacks and Suspicious Activity from Low Impact BES Cyber Systems	This filter identifies attack and suspicious activity events from assets or zones that are categorized in the Low Impact BES Cyber Systems asset category.	/All Filters/ArcSight Solutions/NERC/CIP-008 Incident Reporting and Response Planning/
Attacks and Suspicious Activity from Medium Impact BES Cyber Systems	This filter identifies attack and suspicious activity events from assets or zones that are categorized in the Medium Impact BES Cyber Systems asset category.	/All Filters/ArcSight Solutions/NERC/CIP-008 Incident Reporting and Response Planning/
Attacks and Suspicious Activity from Public Facing Resources	This filter identifies attack and suspicious activity events from assets or zones that are categorized in the Public-Facing asset category.	/All Filters/ArcSight Solutions/NERC/CIP-008 Incident Reporting and Response Planning/
Attacks and Suspicious Activity from Third Party Resources	This filter identifies attack and suspicious activity events that are generated by assets categorized in the Third Party asset category.	/All Filters/ArcSight Solutions/NERC/CIP-008 Incident Reporting and Response Planning/
Attacks and Suspicious Activity to and from High Impact BES Cyber Systems	This filter identifies attack and suspicious activity events targeting or originating from assets or zones categorized in the High Impact BES Cyber Systems asset category.	/All Filters/ArcSight Solutions/NERC/CIP-008 Incident Reporting and Response Planning/

Filters Resources, continued

Resource	Description	URI
Attacks and Suspicious Activity to and from Low Impact BES Cyber Systems	This filter identifies attack and suspicious activity events targeting or originating from assets or zones categorized in the Low Impact BES Cyber Systems asset category.	/All Filters/ArcSight Solutions/NERC/CIP-008 Incident Reporting and Response Planning/
Attacks and Suspicious Activity to and from Medium Impact BES Cyber Systems	This filter identifies attack and suspicious activity events targeting or originating from assets or zones categorized in the Medium Impact BES Cyber Systems asset category.	/All Filters/ArcSight Solutions/NERC/CIP-008 Incident Reporting and Response Planning/
Attacks and Suspicious Activity to and from Third Party Resources	This filter identifies attack and suspicious activity events targeting or originating from assets or zones categorized in the Third Party asset category.	/All Filters/ArcSight Solutions/NERC/CIP-008 Incident Reporting and Response Planning/
Audit Log Cleared	This filter selects all events where an audit log was cleared from a host. By default it will recognize events on Microsoft Windows and Symantec HostID systems, modify this filter to include events from other devices.	/All Filters/ArcSight Solutions/NERC/CIP-010 Configuration Change Management and Vulnerability/
Audit Log Cleared Rule Fired	This filter detects correlated events the rule Audit Log Cleared generates	/All Filters/ArcSight Solutions/NERC/CIP-010 Configuration Change Management and Vulnerability/
Badge Out	This filter identifies badge out in event.	/All Filters/ArcSight Solutions/NERC/CIP-006 Physical Security of BES Cyber Systems/
Blocked Traffic from High Impact BES Systems	This filter identifies blocked traffic from High Impact BES Systems .	/All Filters/ArcSight Solutions/NERC/CIP-005 Electronic Security Perimeter(s)/
Blocked Traffic from Low Impact BES Systems	This filter identifies blocked traffic from Low Impact BES Systems .	/All Filters/ArcSight Solutions/NERC/CIP-005 Electronic Security Perimeter(s)/
Blocked Traffic from Medium Impact BES Systems	This filter identifies blocked traffic from Medium Impact BES Systems .	/All Filters/ArcSight Solutions/NERC/CIP-005 Electronic Security Perimeter(s)/

Filters Resources, continued

Resource	Description	URI
Blocked Traffic to High Impact BES Systems	This filter identifies blocked traffic to High Impact BES Systems .	/All Filters/ArcSight Solutions/NERC/CIP-005 Electronic Security Perimeter(s)/
Blocked Traffic to Low Impact BES Systems	This filter identifies blocked traffic to Low Impact BES Systems .	/All Filters/ArcSight Solutions/NERC/CIP-005 Electronic Security Perimeter(s)/
Blocked Traffic to Medium Impact BES Systems	This filter identifies blocked traffic to Medium Impact BES Systems .	/All Filters/ArcSight Solutions/NERC/CIP-005 Electronic Security Perimeter(s)/
Building Access	This filter selects all building access events.	/All Filters/ArcSight Solutions/NERC/CIP-006 Physical Security of BES Cyber Systems/
CIP-002 Rules Firing	A generic filter to select events generated by any rule firing in this section.	/All Filters/ArcSight Solutions/NERC/General Filters/Section Overview/
CIP-003 Rules Firing	A generic filter to select events generated by any rule firing in this section.	/All Filters/ArcSight Solutions/NERC/General Filters/Section Overview/
CIP-004 Rules Firing	A generic filter to select events generated by any rule firing in this section.	/All Filters/ArcSight Solutions/NERC/General Filters/Section Overview/
CIP-005 Rules Firing	A generic filter to select events generated by any rule firing in this section.	/All Filters/ArcSight Solutions/NERC/General Filters/Section Overview/
CIP-006 Rules Firing	A generic filter to select events generated by any rule firing in this section.	/All Filters/ArcSight Solutions/NERC/General Filters/Section Overview/
CIP-007 Rules Firing	A generic filter to select events generated by any rule firing in this section.	/All Filters/ArcSight Solutions/NERC/General Filters/Section Overview/

Filters Resources, continued

Resource	Description	URI
CIP-008 Rules Firing	A generic filter to select events generated by any rule firing in this section.	/All Filters/ArcSight Solutions/NERC/General Filters/Section Overview/
CIP-009 Rules Firing	A generic filter to select events generated by any rule firing in this section.	/All Filters/ArcSight Solutions/NERC/General Filters/Section Overview/
CIP-010 Rules Firing	A generic filter to select events generated by any rule firing in this section.	/All Filters/ArcSight Solutions/NERC/General Filters/Section Overview/
CIP-011 Rules Firing	A generic filter to select events generated by any rule firing in this section.	/All Filters/ArcSight Solutions/NERC/General Filters/Section Overview/
CIPS Rule Firing	This filter selects all rule firing events, where the rule is a part of the compliance content. This filter is used by the overview last-state data monitors. Also, the filter contains an exclusion list for the rules that should not contribute to the overall state as intended to be shown by the overview data monitor.	/All Filters/ArcSight Solutions/NERC/General Filters/Section Overview/
Case Updated	This filter is used to identify events in which a case under the NERC group has been updated.	/All Filters/ArcSight Solutions/NERC/General Filters/
Communications between Development and Operations	This filter identifies traffic between Development and Operations domains.	/All Filters/ArcSight Solutions/NERC/CIP-005 Electronic Security Perimeter(s)/
Communications between Development and Test	This filter identifies traffic between Development and Test domains.	/All Filters/ArcSight Solutions/NERC/CIP-005 Electronic Security Perimeter(s)/
Communications between High Impact and Low Impact BES Systems	This filter identifies traffic between high Impact and low impact BES cyber systems .	/All Filters/ArcSight Solutions/NERC/CIP-005 Electronic Security Perimeter(s)/
Communications between High Impact and Medium Impact BES Systems	This filter identifies traffic between high Impact and medium impact BES cyber systems .	/All Filters/ArcSight Solutions/NERC/CIP-005 Electronic Security Perimeter(s)/

Filters Resources, continued

Resource	Description	URI
Communications between Medium Impact and Low Impact BES Systems	This filter identifies traffic between medium Impact and low impact BES cyber systems .	/All Filters/ArcSight Solutions/NERC/CIP-005 Electronic Security Perimeter(s)/
Communications between Test and Operations	This filter identifies traffic between Test and Operations domains.	/All Filters/ArcSight Solutions/NERC/CIP-005 Electronic Security Perimeter(s)/
Compliance Score Rules	This filter identifies the rules associated with the Compliance Score use case.	/All Filters/ArcSight Solutions/NERC/General Filters/Section Overview/
Compliance Score Updates	This filter identifies events that are generated when values in the Compliance Score active list are changed.	/All Filters/ArcSight Solutions/NERC/General Filters/Section Overview/
Configuration Modifications	This filter detects configuration modifications.	/All Filters/ArcSight Solutions/NERC/CIP-010 Configuration Change Management and Vulnerability/
Contractor Access After Hours	This filter identifies contractors accessing buildings after hours.	/All Filters/ArcSight Solutions/NERC/CIP-006 Physical Security of BES Cyber Systems/
Covert Channel	This filter detects events indicating a covert channel is being used.	/All Filters/ArcSight Solutions/NERC/CIP-005 Electronic Security Perimeter(s)/
Critical Vulnerability Detected	Selects events indicating that a critical vulnerability was detected .	/All Filters/ArcSight Solutions/NERC/CIP-010 Configuration Change Management and Vulnerability/
Database Configuration Modification	This filter defines database configuration modifications.	/All Filters/ArcSight Solutions/NERC/CIP-010 Configuration Change Management and Vulnerability/
Database Target Host	This filter selects events targeting database hosts.	/All Filters/ArcSight Solutions/NERC/My Filters/

Filters Resources, continued

Resource	Description	URI
Default Vendor Account Access Attempted	This filter identifies events where system access with vendor-supplied accounts is attempted.	/All Filters/ArcSight Solutions/NERC/CIP-004 Personnel and Training/
Default Vendor Account Credential Observed	This filter identifies events where system access with vendor-supplied accounts is observed.	/All Filters/ArcSight Solutions/NERC/CIP-004 Personnel and Training/
Direct Root or Administrator Credential Observed	This filter identifies events where system access with root or administrator credential is observed.	/All Filters/ArcSight Solutions/NERC/CIP-004 Personnel and Training/
Disallowed Ports Access	This filter tracks all connections to disallowed ports.	/All Filters/ArcSight Solutions/NERC/CIP-005 Electronic Security Perimeter(s)/
Disallowed Ports Access from Internal Hosts	This filter tracks all connections to disallowed ports from internal hosts.	/All Filters/ArcSight Solutions/NERC/CIP-005 Electronic Security Perimeter(s)/
Disallowed Ports Access to Internal Hosts	This filter tracks all connections to disallowed ports hosted by internal hosts.	/All Filters/ArcSight Solutions/NERC/CIP-005 Electronic Security Perimeter(s)/
DoS Attacks	This filter identifies denial of service attacks.	/All Filters/ArcSight Solutions/NERC/CIP-007 System Security Management/
Dynamic Ports Events	This filter identifies dynamic open ports events reported by vulnerability scanners .	/All Filters/ArcSight Solutions/NERC/CIP-007 System Security Management/
Email Attacks	This filter detects events indicating an email attack occurred.	/All Filters/ArcSight Solutions/NERC/CIP-005 Electronic Security Perimeter(s)/
Event Limit	The purpose of this filter is to limit events processed and reported by the solution pack to only the events that are relevant to the regulation. This is achieved by including this filter in the conditions of all other resources in the package such as rules, queries, and filters etc either directly or indirectly. You can change the events processed and reported by this package by editing this filter.	/All Filters/ArcSight Solutions/NERC/General Filters/

Filters Resources, continued

Resource	Description	URI
External to High Impact BES Cyber Systems Traffic	This filter selects events where the traffic originates from external network segment and the target is in high impact BES cyber system assets.	/All Filters/ArcSight Solutions/NERC/CIP-005 Electronic Security Perimeter(s)/
External to Internal Traffic	This filter selects events where the traffic originates from external network segment and the target is in an internal network segment.	/All Filters/ArcSight Solutions/NERC/CIP-005 Electronic Security Perimeter(s)/
External to Low Impact BES Cyber Systems Traffic	This filter selects events where the traffic originates from external network segment and the target is in low impact BES cyber system assets.	/All Filters/ArcSight Solutions/NERC/CIP-005 Electronic Security Perimeter(s)/
External to Medium Impact BES Cyber Systems Traffic	This filter selects events where the traffic originates from external network segment and the target is in medium impact BES cyber system assets.	/All Filters/ArcSight Solutions/NERC/CIP-005 Electronic Security Perimeter(s)/
Failed Anti-Virus Updates	This filter looks for events when an attempt to update a virus signature on a host failed.	/All Filters/ArcSight Solutions/NERC/CIP-007 System Security Management/
Failed Password Change	This filter identifies unsuccessful password change events.	/All Filters/ArcSight Solutions/NERC/CIP-007 System Security Management/
Failed Technical Compliance Check	This filter looks for events which indicate a compliance check failure.	/All Filters/ArcSight Solutions/NERC/CIP-002 BES Cyber System Categorization/
Failed Virus Removal Attempt	This filter looks for events when an attempt to remove/quarantine a virus on a host failed.	/All Filters/ArcSight Solutions/NERC/CIP-007 System Security Management/
File Creations	This filter identifies all fiile creations .	/All Filters/ArcSight Solutions/NERC/CIP-010 Configuration Change Management and Vulnerability/
File Deletions	This filter identifies all fiile deletions .	/All Filters/ArcSight Solutions/NERC/CIP-010 Configuration Change Management and Vulnerability/

Filters Resources, continued

Resource	Description	URI
File Modifications	This filter identifies all file changes.	/All Filters/ArcSight Solutions/NERC/CIP-010 Configuration Change Management and Vulnerability/
Firewall Accepts	This filter selects all events where a firewall granted passage to traffic.	/All Filters/ArcSight Solutions/NERC/CIP-005 Electronic Security Perimeter(s)/
Firewall Accepts	Filter to select all events where a firewall granted passage to traffic.	/All Filters/ArcSight Solutions/NERC/General Filters/Firewall/
Firewall Configuration Modifications	This filter tracks events when the configuration of a firewall is changed.	/All Filters/ArcSight Solutions/NERC/CIP-010 Configuration Change Management and Vulnerability/
Firewall Deny	This filter selects events where a firewall denied passage to traffic.	/All Filters/ArcSight Solutions/NERC/CIP-005 Electronic Security Perimeter(s)/
Firewall Deny	Filter to select events where a firewall denied passage to traffic.	/All Filters/ArcSight Solutions/NERC/General Filters/Firewall/
Firewall Events	Filter to select events where a firewall has detected traffic attempting to pass through it. This filter does not look for the outcome of the attempt.	/All Filters/ArcSight Solutions/NERC/General Filters/Firewall/
Former Employee Account Detected	This filter selects events that identify a former employee account. This filter may need additional configuration.	/All Filters/ArcSight Solutions/NERC/CIP-004 Personnel and Training/
Former Employee Activity	This filter identifies base events associated with users who are known to be terminated according to the Former Employees active list.	/All Filters/ArcSight Solutions/NERC/CIP-004 Personnel and Training/
High Impact BES Cyber Systems to External Traffic	This filter selects events where the traffic originated from high impact BES cyber systems and the target is in an external network segment.	/All Filters/ArcSight Solutions/NERC/CIP-005 Electronic Security Perimeter(s)/
High Priority Events	This filter shows events in which the Priority field is 10.	/All Filters/ArcSight Solutions/NERC/CIP-008 Incident Reporting and Response Planning/

Filters Resources, continued

Resource	Description	URI
IDS Detected Brute Force Login Attempts	This filter shows events sent by Intrusion Detection Systems that indicate brute force login attempts.	/All Filters/ArcSight Solutions/NERC/CIP-007 System Security Management/
IDS Detected Successful Brute Force Logins	This filter selects events from Intrusion Detection Systems that indicate a successful brute force login has occurred.	/All Filters/ArcSight Solutions/NERC/CIP-007 System Security Management/
IM Traffic	This filter identifies all instant messaging traffic that are not supposed to be allowed.	/All Filters/ArcSight Solutions/NERC/CIP-005 Electronic Security Perimeter(s)/
Inbound	This filter can be used to filter for inbound traffic.	/All Filters/ArcSight Solutions/NERC/General Filters/
Inbound Events	This filter looks for events coming from outside the organization network targeting internal networks .	/All Filters/ArcSight Solutions/NERC/CIP-007 System Security Management/
Information Interception	This filter detects events indicating an information interception is being used.	/All Filters/ArcSight Solutions/NERC/CIP-005 Electronic Security Perimeter(s)/
Information Security Incidents	This filter identifies various kinds of information security incidents such as malicious code activities, denial of service attacks and policy violations.	/All Filters/ArcSight Solutions/NERC/CIP-008 Incident Reporting and Response Planning/
Information System Failures	This filter identifies information system failures.	/All Filters/ArcSight Solutions/NERC/CIP-009 Recovery Plans for BES Cyber Systems/
Insecure Cryptographic Storage Detected	Selects events indicating that Insecure cryptographic storage has been detected.	/All Filters/ArcSight Solutions/NERC/CIP-011 Information Protection/
Insecure Services	This filter selects events based on inherently insecure services.	/All Filters/ArcSight Solutions/NERC/CIP-005 Electronic Security Perimeter(s)/
Insignificant Events	This filter is used to identify events with no or little value. Preferably, these events should be filtered out by the connector.	/All Filters/ArcSight Solutions/NERC/General Filters/

Filters Resources, continued

Resource	Description	URI
Intellectual Property Download	<p>This filter is used to define events which talk about the download of possibly illegal intellectual property. Videos, Images, and Audio files can fall into this category.</p> <p>This filter should be configured to catch all the events in the environment which indicate the download of possibly illegal intellectual property. Do not include content that looks for peer to peer protocols. That is handled in a separate filter.</p>	/All Filters/ArcSight Solutions/NERC/My Filters/
Intellectual Property Rights Violations	This filter looks for violations of intellectual property rights by looking at the rule for this use-case.	/All Filters/ArcSight Solutions/NERC/CIP-003 Security Management Controls/
Internal Attackers	This filter looks for events coming from systems inside the organization network.	/All Filters/ArcSight Solutions/NERC/General Filters/
Internal Connection	This filter is looking for connections within the network.	/All Filters/ArcSight Solutions/NERC/General Filters/
Internal Inter-Domain Traffic	This filter identifies internal inter-domain traffic.	/All Filters/ArcSight Solutions/NERC/CIP-005 Electronic Security Perimeter(s)/
Internal Recon	This filter identifies reconnaissance events that originated internal to the organization. This could indicate that someone is trying to scan the network which is a policy violation.	/All Filters/ArcSight Solutions/NERC/CIP-008 Incident Reporting and Response Planning/
Internal Targets	This filter looks for events targeting systems inside the organization network.	/All Filters/ArcSight Solutions/NERC/General Filters/
Internal to External Traffic	This filter selects events where the traffic originates from an internal network segment and the target is in an external network segment.	/All Filters/ArcSight Solutions/NERC/CIP-005 Electronic Security Perimeter(s)/
Invalid or Expired Certificate	This filter selects events which indicate that an invalid or expired certificate was detected.	/All Filters/ArcSight Solutions/NERC/CIP-011 Information Protection/

Filters Resources, continued

Resource	Description	URI
Limit Regulation	<p>The purpose of this filter is to limit events processed and reported by this package only to the ones that are relevant to the NERC regulation.</p> <p>This is achieved by including this filter in the conditions of every other resource (Rules, Queries, Filters, etc.) in the Compliance Insight Package for NERC (in addition to the other conditions of the resource).</p> <p>You can control the events processed and reported by this package by editing this filter. For example, to process and report on all events that are sent to ESM, change the condition of this filter to "True".</p> <p>The default value of this filter will ensure that the Compliance Insight Package for NERC will only process and report on events in which one of the following is true:</p> <ol style="list-style-type: none"> 1. The source address is an asset categorized under /All Asset Categories/ArcSight Solutions/Compliance Insight Package/Regulation/NERC 2. The destination address is an asset categorized under the above asset category. 3. The device address is an asset categorized under the above asset category. 4. The source zone is categorized under the above asset category. 5. The destination zone is categorized under the above asset category. 6. The reporting device's zone is categorized under the above asset category. 7. The source address is an asset under the /All Assets/ArcSight Solutions/NERC group. 8. The destination address is an asset under the /All Assets/ArcSight Solutions/NERC group 9. The device address is an asset under the /All Assets/ArcSight Solutions/NERC group 	/All Filters/ArcSight Solutions/NERC/My Filters/
Local Logins	This filter identifies local login events to a MS Windows or UNIX system.	/All Filters/ArcSight Solutions/NERC/General Filters/Authentication/
Login Activity by Stale User Accounts	This filter identifies login activities by accounts that are on the Stale Accounts active list.	/All Filters/ArcSight Solutions/NERC/CIP-004 Personnel and Training/

Filters Resources, continued

Resource	Description	URI
Login Attempts	This filter selects any attempts at logging into systems. It excludes machine logins into Microsoft Windows systems.	/All Filters/ArcSight Solutions/NERC/General Filters/Authentication/
Logouts	This filter identifies all logout events. Change the conditions in this filter to match logout events from non-Windows systems.	/All Filters/ArcSight Solutions/NERC/General Filters/Authentication/
Low Impact BES Cyber Systems to External Traffic	This filter selects events where the traffic originated from low impact BES cyber systems and the target is in an external network segment.	/All Filters/ArcSight Solutions/NERC/CIP-005 Electronic Security Perimeter(s)/
Malicious Code Activity	This filter selects events where malicious code activity is detected.	/All Filters/ArcSight Solutions/NERC/CIP-007 System Security Management/
Malware Activity	This filter identifies virus and other malware activities reported by either an Intrusion Detection System (IDS) or an anti-virus application.	/All Filters/ArcSight Solutions/NERC/CIP-007 System Security Management/
Medium Impact BES Cyber Systems to External Traffic	This filter selects events where the traffic originated from medium impact BES cyber systems and the target is in an external network segment.	/All Filters/ArcSight Solutions/NERC/CIP-005 Electronic Security Perimeter(s)/
NERC Case Created	This filter identifies events where a new case is created.	/All Filters/ArcSight Solutions/NERC/CIP-008 Incident Reporting and Response Planning/
Network Device Configuration Modifications	This filter tracks events when the configuration of an infrastructural equipment (router, switch) is changed.	/All Filters/ArcSight Solutions/NERC/CIP-010 Configuration Change Management and Vulnerability/
Network IDS Configuration Modifications	This filter tracks events when the configuration of NIDS equipment is changed.	/All Filters/ArcSight Solutions/NERC/CIP-010 Configuration Change Management and Vulnerability/
Network Routing Configuration Modifications	This filter tracks events when a modification to the routing table of an infrastructural equipment (router, switch) is made.	/All Filters/ArcSight Solutions/NERC/CIP-010 Configuration Change Management and Vulnerability/

Filters Resources, continued

Resource	Description	URI
New Hire Based Internet Outbound Activity	This filter identifies the outbound internet activity of new hire users. Internet activity is defined as a successful connection to external addresses on ports 80, 443, 21 or 20.	/All Filters/ArcSight Solutions/NERC/CIP-004 Personnel and Training/
New Hire Identification	This filter identifies newly created accounts.	/All Filters/ArcSight Solutions/NERC/CIP-004 Personnel and Training/
New Hire Suspicious Activities	This filter identifies suspicious activity by new hires.	/All Filters/ArcSight Solutions/NERC/CIP-004 Personnel and Training/
New Hires Successful Logins	This filter identified successful logins by new hire users .	/All Filters/ArcSight Solutions/NERC/CIP-004 Personnel and Training/
New Host Detected	Filter to capture events which indicate that new hosts were detected on the network. Normally reported by network based anomaly detection systems (NBAD).	/All Filters/ArcSight Solutions/NERC/CIP-002 BES Cyber System Categorization/
New Service Detected	Filter to capture events which indicate that new services were detected on a host. Normally reported by network based anomaly detection systems (NBAD) or by operating systems .	/All Filters/ArcSight Solutions/NERC/CIP-002 BES Cyber System Categorization/
Non Administrative User	The purpose of this filter is identify events associated with non-administrative users. These events are defined as such in which neither the source nor destination users are administrative users.	/All Filters/ArcSight Solutions/NERC/General Filters/Authentication/
Open Port Events	This filter identifies open ports events reported by vulnerability scanners .	/All Filters/ArcSight Solutions/NERC/CIP-007 System Security Management/
Organizational Records Information Leak	This filter identifies information leaks with regard to company information.	/All Filters/ArcSight Solutions/NERC/CIP-011 Information Protection/
Outbound	This filter can be used to filter outbound traffic.	/All Filters/ArcSight Solutions/NERC/General Filters/
Outbound Events	This filter looks for events coming from inside the organization network targeting the public network.	/All Filters/ArcSight Solutions/NERC/CIP-007 System Security Management/

Filters Resources, continued

Resource	Description	URI
Outbound Internet Activity	This filter detects all outbound internet activity related events.	/All Filters/ArcSight Solutions/NERC/CIP-007 System Security Management/
Overflow Vulnerability Detected	Selects events indicating that an overflow vulnerability detected.	/All Filters/ArcSight Solutions/NERC/CIP-010 Configuration Change Management and Vulnerability/
Password Change Attempts	This filter identifies password change attempts. By default it only identifies these events on Microsoft Windows systems. Configure this filter to identify password change events from other systems as necessary.	/All Filters/ArcSight Solutions/NERC/CIP-007 System Security Management/
Personal Information Leak	This filter selects events which indicate a personal information leak.	/All Filters/ArcSight Solutions/NERC/CIP-011 Information Protection/
Physical Access Events	This filter selects all events sent to ArcSight by physical security systems.	/All Filters/ArcSight Solutions/NERC/CIP-006 Physical Security of BES Cyber Systems/
Policy Violations	Filter in events with breach of policy.	/All Filters/ArcSight Solutions/NERC/CIP-003 Security Management Controls/
Port Detected	Selects events indicating that port is detected	/All Filters/ArcSight Solutions/NERC/CIP-011 Information Protection/
Potential Trojan Inside Network	This filter selects events where a trojan is likely to be present inside the company network.	/All Filters/ArcSight Solutions/NERC/CIP-007 System Security Management/
Privileged Access on a Remote Connection	This filter selects events where a connection is reported by a VPN device, and the user name belongs to a privileged account.	/All Filters/ArcSight Solutions/NERC/CIP-005 Electronic Security Perimeter(s)/
Privileged Account Change	This filter selects events where an privileged account (as defined by the referenced active list) is attempted to be changed.	/All Filters/ArcSight Solutions/NERC/CIP-004 Personnel and Training/
Redirection Attacks	This filter detects events indicating a redirection attack occurred.	/All Filters/ArcSight Solutions/NERC/CIP-005 Electronic Security Perimeter(s)/

Filters Resources, continued

Resource	Description	URI
Removable Media Detected	This query selects events indicating that a removable device is detected.	/All Filters/ArcSight Solutions/NERC/CIP-010 Configuration Change Management and Vulnerability/
Removal of Access Rights	This filter identifies events indicating a user access right is removed. Removal could mean that either the user was removed from the system, or the privileges related to that ID were modified.	/All Filters/ArcSight Solutions/NERC/CIP-004 Personnel and Training/
Resource Exhaustion	This query shows resources reaching their upper end of utilization (for capacity management and planning purposes).	/All Filters/ArcSight Solutions/NERC/CIP-009 Recovery Plans for BES Cyber Systems/
SSL Vulnerability Detected	Selects events indicating that an SSL vulnerability was detected.	/All Filters/ArcSight Solutions/NERC/CIP-010 Configuration Change Management and Vulnerability/
Security Patch Missing	Selects events indicating that a security patch is missing.	/All Filters/ArcSight Solutions/NERC/CIP-010 Configuration Change Management and Vulnerability/
Software Changes	This filter detects all changes to any software installed .	/All Filters/ArcSight Solutions/NERC/CIP-010 Configuration Change Management and Vulnerability/
Spyware Activity	This filter identifies spyware activity reported by either an Intrusion Detection System (IDS) or an anti-virus application.	/All Filters/ArcSight Solutions/NERC/CIP-007 System Security Management/
Startup and Shutdown of Highly Critical Assets	This filter identifies startups and shutdowns of highly critical machines.	/All Filters/ArcSight Solutions/NERC/CIP-009 Recovery Plans for BES Cyber Systems/
Successful Administrative Login	This filter identifies successful logins by administrators.	/All Filters/ArcSight Solutions/NERC/General Filters/Authentication/
Successful Administrative Logins from Third Party Systems	The purpose of this filter is to identify successful logins with an administrative account from third party systems. Third party systems have to be modeled as assets in ESM and be categorizes as Third Party. Administrative accounts should be defined in all-lower case in the Administrative Accounts active list.	/All Filters/ArcSight Solutions/NERC/CIP-007 System Security Management/

Filters Resources, continued

Resource	Description	URI
Successful Administrative Logins to High Impact BES Cyber Systems	The purpose of this filter is to identify successful logins with an administrative account to High Impact BES Cyber Systems. High Impact BES Cyber Systems have to be modeled as assets in ESM and be categorizes as High Impact BES Cyber Systems , Administrative accounts should be defined in all-lower case in the Administrative Accounts active list.	/All Filters/ArcSight Solutions/NERC/CIP-007 System Security Management/
Successful Administrative Logins to Low Impact BES Cyber Systems	The purpose of this filter is to identify successful logins with an administrative account to Low Impact BES Cyber Systems. Low Impact BES Cyber System have to be modeled as assets in ESM and be categorizes as Low Impact BES Cyber Systems . Administrative accounts should be defined in all-lower case in the Administrative Accounts active list.	/All Filters/ArcSight Solutions/NERC/CIP-007 System Security Management/
Successful Administrative Logins to Medium Impact BES Cyber Systems	The purpose of this filter is to identify successful logins with an administrative account to Medium Impact BES Cyber System. Medium Impact BES Cyber systems have to be modeled as assets in ESM and be categorizes as Medium Impact BES Cyber Systems . Administrative accounts should be defined in all-lower case in the Administrative Accounts active list.	/All Filters/ArcSight Solutions/NERC/CIP-007 System Security Management/
Successful Administrative Logins to Third Party Systems	The purpose of this filter is to identify successful logins with an administrative account to third party systems. Third party systems have to be modeled as assets in ESM and be categorizes as Third Party. Administrative accounts should be defined in all-lower case in the Administrative Accounts active list.	/All Filters/ArcSight Solutions/NERC/CIP-007 System Security Management/
Successful Administrative Logout	This filter identifies events that indicate successful administrative logouts from assets categorized in one of your Network Domains.	/All Filters/ArcSight Solutions/NERC/General Filters/Authentication/
Successful After Hours Building Access	This filter selects all events indicating successful occurrences of physical access after hours. The actual time definition is defined in the After Hours filter.	/All Filters/ArcSight Solutions/NERC/CIP-006 Physical Security of BES Cyber Systems/
Successful Badge In	This filter identifies a successful badge in event.	/All Filters/ArcSight Solutions/NERC/CIP-006 Physical Security of BES Cyber Systems/
Successful Brute Force Logins	This filter identifies events generated by the Probable Successful Brute Force rule that involve assets categorized in one of your Network Domains.	/All Filters/ArcSight Solutions/NERC/CIP-007 System Security Management/

Filters Resources, continued

Resource	Description	URI
Successful Configuration Modifications	This filter identifies successful configuration modifications.	/All Filters/ArcSight Solutions/NERC/CIP-010 Configuration Change Management and Vulnerability/
Successful Logins	This filter identified successful logins by both administrative and non-administrative users.	/All Filters/ArcSight Solutions/NERC/General Filters/Authentication/
Successful Logouts	This filter identifies successful logouts by both administrative and non-administrative users.	/All Filters/ArcSight Solutions/NERC/General Filters/Authentication/
Successful Modifications to Operating Systems	This filter identifies successful configuration modifications to operating systems.	/All Filters/ArcSight Solutions/NERC/CIP-010 Configuration Change Management and Vulnerability/
Successful Password Change	This filter identifies successful password change events.	/All Filters/ArcSight Solutions/NERC/CIP-007 System Security Management/
Successful User Login	This filter identifies successful logins by non-administrative users.	/All Filters/ArcSight Solutions/NERC/General Filters/Authentication/
Successful User Logins from Third Party Systems	The purpose of this filter is to identify successful non-administrative logins from third party systems. Third party systems have to be modeled as assets in ESM and be categorizes as Third Party.	/All Filters/ArcSight Solutions/NERC/CIP-007 System Security Management/
Successful User Logins to High Impact BES Cyber Systems	The purpose of this filter is to identify successful non-administrative logins to High Impact BES Cyber Systems. High Impact BES Cyber Systems have to be modeled as assets in ESM and be categorizes as High Impact BES Cyber Systems.	/All Filters/ArcSight Solutions/NERC/CIP-007 System Security Management/
Successful User Logins to Low Impact BES Cyber System	The purpose of this filter is to identify successful non-administrative logins to Low Impact BES Cyber Systems. Low Impact BES Cyber Systems have to be modeled as assets in ESM and be categorizes as Low Impact BES Cyber Systems.	/All Filters/ArcSight Solutions/NERC/CIP-007 System Security Management/
Successful User Logins to Medium Impact BES Cyber Systems	The purpose of this filter is to identify successful non-administrative logins to Medium Impact BES Cyber Systems. Medium Impact BES Cyber Systems have to be modeled as assets in ESM and be categorizes as Medium Impact BES Cyber Systems.	/All Filters/ArcSight Solutions/NERC/CIP-007 System Security Management/

Filters Resources, continued

Resource	Description	URI
Successful User Logins to Third Party Systems	The purpose of this filter is to identify successful non-administrative logins to third party systems. Third party systems have to be modeled as assets in ESM and be categorized as Third Party.	/All Filters/ArcSight Solutions/NERC/CIP-007 System Security Management/
Successful User Logout	This filter identifies events that indicate successful logouts by non-administrative users.	/All Filters/ArcSight Solutions/NERC/General Filters/Authentication/
System Shutdown	This filter identifies system shut downs.	/All Filters/ArcSight Solutions/NERC/CIP-009 Recovery Plans for BES Cyber Systems/
System Shutdown of Highly Critical Assets	This filter identifies system shut downs of highly critical assets.	/All Filters/ArcSight Solutions/NERC/CIP-009 Recovery Plans for BES Cyber Systems/
System Startup	This filter identifies system startups.	/All Filters/ArcSight Solutions/NERC/CIP-009 Recovery Plans for BES Cyber Systems/
Target Asset in High Impact BES Cyber Assets	This filter looks for events targeting High Impact BES Cyber Assets	/All Filters/ArcSight Solutions/NERC/My Filters/
Target Asset in Highly Critical Assets	This filter identifies events that are targeting highly critical assets.	/All Filters/ArcSight Solutions/NERC/My Filters/
Target Asset in Low Impact BES Cyber Assets	This filter looks for events targeting Low Impact BES Cyber Assets	/All Filters/ArcSight Solutions/NERC/My Filters/
Target Asset in Medium Impact BES Cyber Assets	This filter looks for events targeting Medium Impact BES Cyber Assets	/All Filters/ArcSight Solutions/NERC/My Filters/
Target Asset is Wireless	This filter looks for events targeting wireless devices .	/All Filters/ArcSight Solutions/NERC/My Filters/
Target Host or Address Present	This filter identifies events that have either the Target Host Name or Target Address event fields populated.	/All Filters/ArcSight Solutions/NERC/General Filters/

Filters Resources, continued

Resource	Description	URI
Target MAC Address Present	This filter identifies events that have the Target MAC Address event fields populated.	/All Filters/ArcSight Solutions/NERC/General Filters/
Target User Present	This filter checks whether the Target User Name field is populated.	/All Filters/ArcSight Solutions/NERC/General Filters/
Traffic Anomaly	This filter detects events indicating a traffic anomaly.	/All Filters/ArcSight Solutions/NERC/CIP-005 Electronic Security Perimeter(s)/
Traffic Anomaly on Application Layer	This filter detects events indicating a traffic anomaly on application layer	/All Filters/ArcSight Solutions/NERC/CIP-005 Electronic Security Perimeter(s)/
Traffic Anomaly on Network Layer	This filter detects events indicating traffic anomaly on network layer.	/All Filters/ArcSight Solutions/NERC/CIP-005 Electronic Security Perimeter(s)/
Traffic Anomaly on Transport Layer	This filter detects events indicating traffic anomaly in transport layer .	/All Filters/ArcSight Solutions/NERC/CIP-005 Electronic Security Perimeter(s)/
Traffic Between Network Zones	This filter detects events in which the attacker zone is different than the target zone.	/All Filters/ArcSight Solutions/NERC/CIP-005 Electronic Security Perimeter(s)/
Traffic from Dark Address Space	This filter detects events that are coming from the Dark Address Space.	/All Filters/ArcSight Solutions/NERC/CIP-005 Electronic Security Perimeter(s)/
Traffic from Higher to Lower Classification Level	This filter identifies events going from an asset in a higher classification level to an asset in a lower classification level.	/All Filters/ArcSight Solutions/NERC/CIP-011 Information Protection/
Traffic from Lower to Higher Classification Level	This filter identifies events going from an asset in a lower classification level to an asset in a higher classification level.	/All Filters/ArcSight Solutions/NERC/CIP-011 Information Protection/
Traffic to Dark Address Space	This filter detects events that are targeting the Dark Address Space.	/All Filters/ArcSight Solutions/NERC/CIP-005 Electronic Security Perimeter(s)/

Filters Resources, continued

Resource	Description	URI
Trojan Activity	This filter selects events where trojan activity is detected.	/All Filters/ArcSight Solutions/NERC/CIP-007 System Security Management/
Unsecured Open Port Events	This filter identifies unsecured open ports events reported by vulnerability scanners . for the list of the unsecured ports refer to the filter description.	/All Filters/ArcSight Solutions/NERC/CIP-007 System Security Management/
Unsecured Port Detected	Selects events indicating that an unsecured port is detected.	/All Filters/ArcSight Solutions/NERC/CIP-011 Information Protection/
Unsuccessful Administrative Login	This filter identifies events that indicate unsuccessful administrative login attempts to an asset categorized in one of your Network Domains.	/All Filters/ArcSight Solutions/NERC/General Filters/Authentication/
Unsuccessful Administrative Logins from Third Party Systems	The purpose of this filter is to identify failed logins using an administrative account from third party systems. Third party systems have to be modeled as assets in ESM and be categorizes as Third Party. Administrative accounts should be defined in all-lower case in the Administrative Accounts active list.	/All Filters/ArcSight Solutions/NERC/CIP-007 System Security Management/
Unsuccessful Administrative Logins to High Impact BES Cyber Systems	The purpose of this filter is to identify failed administrative logins to High Impact BES Cyber Systems. High Impact BES Cyber Systems have to be modeled as assets in ESM and be categorizes as High Impact BES Cyber Systems. Administrative accounts should be defined in all-lower case in the Administrative Accounts active list.	/All Filters/ArcSight Solutions/NERC/CIP-007 System Security Management/
Unsuccessful Administrative Logins to Low Impact BES Cyber System	The purpose of this filter is to identify failed administrative logins to Low Impact BES Cyber System. Low Impact BES Cyber System have to be modeled as assets in ESM and be categorizes as Low Impact BES Cyber System. Administrative accounts should be defined in all-lower case in the Administrative Accounts active list.	/All Filters/ArcSight Solutions/NERC/CIP-007 System Security Management/
Unsuccessful Administrative Logins to Medium Impact BES Cyber Systems	The purpose of this filter is to identify failed administrative logins to Medium Impact BES Cyber Systems. Medium Impact BES Cyber Systems have to be modeled as assets in ESM and be categorizes as Medium Impact BES Cyber Systems. Administrative accounts should be defined in all-lower case in the Administrative Accounts active list.	/All Filters/ArcSight Solutions/NERC/CIP-007 System Security Management/
Unsuccessful Administrative Logins to Third Party Systems	The purpose of this filter is to identify failed administrative logins to Third Party Assets.Third Party systems have to be modeled as assets in ESM and be categorizes as Third Party. Administrative accounts should be defined in all-lower case in the Administrative Accounts active list.	/All Filters/ArcSight Solutions/NERC/CIP-007 System Security Management/

Filters Resources, continued

Resource	Description	URI
Unsuccessful After Hours Building Access	This filter selects all events indicating successful occurrences of physical access after hours. The actual time definition is defined in the After Hours filter.	/All Filters/ArcSight Solutions/NERC/CIP-006 Physical Security of BES Cyber Systems/
Unsuccessful Changes to Operating Systems	This filter identifies unsuccessful change attempts to operating systems.	/All Filters/ArcSight Solutions/NERC/CIP-010 Configuration Change Management and Vulnerability/
Unsuccessful Configuration Modifications	This filter identifies unsuccessful configuration modifications.	/All Filters/ArcSight Solutions/NERC/CIP-010 Configuration Change Management and Vulnerability/
Unsuccessful Logins	This filter identified failed logins by both administrative and non-administrative users.	/All Filters/ArcSight Solutions/NERC/General Filters/Authentication/
Unsuccessful User Login	This filter identifies failed logins by non-administrative users.	/All Filters/ArcSight Solutions/NERC/General Filters/Authentication/
Unsuccessful User Logins from Third Party Systems	The purpose of this filter is to identify failed non-administrative logins from third party systems. Third party systems have to be modeled as assets in ESM and be categorizes as Third Party.	/All Filters/ArcSight Solutions/NERC/CIP-007 System Security Management/
Unsuccessful User Logins to High Impact BES Cyber Systems	The purpose of this filter is to identify failed non-administrative logins to High Impact BES Cyber Systems. High Impact BES Cyber Systems have to be modeled as assets in ESM and be categorizes as High Impact BES Cyber Systems.	/All Filters/ArcSight Solutions/NERC/CIP-007 System Security Management/
Unsuccessful User Logins to Low Impact BES Cyber System	The purpose of this filter is to identify failed non-administrative logins to Low Impact BES Cyber Systems. Low Impact BES Cyber Systems have to be modeled as assets in ESM and be categorizes as Low Impact BES Cyber Systems.	/All Filters/ArcSight Solutions/NERC/CIP-007 System Security Management/
Unsuccessful User Logins to Medium Impact BES Cyber Systems	The purpose of this filter is to identify failed non-administrative logins to Medium Impact BES Cyber Systems. Medium Impact BES Cyber Systems have to be modeled as assets in ESM and be categorizes as Medium Impact BES Cyber Systems.	/All Filters/ArcSight Solutions/NERC/CIP-007 System Security Management/
Unsuccessful User Logins to Third Party Systems	The purpose of this filter is to identify failed non-administrative logins to third party systems. Third party systems have to be modeled as assets in ESM and be categorizes as Third Party.	/All Filters/ArcSight Solutions/NERC/CIP-007 System Security Management/

Filters Resources, continued

Resource	Description	URI
Unsuccessful VPN Access	This filter identifies failed VPN access attempts.	/All Filters/ArcSight Solutions/NERC/CIP-005 Electronic Security Perimeter(s)/
Unsuccessful Badge In	This filter identifies an unsuccessful badge in event.	/All Filters/ArcSight Solutions/NERC/CIP-006 Physical Security of BES Cyber Systems/
User Added to Group	This filter identifies when a user added to group.	/All Filters/ArcSight Solutions/NERC/CIP-004 Personnel and Training/
User Group Creation	This filter identifies user group creation events.	/All Filters/ArcSight Solutions/NERC/CIP-004 Personnel and Training/
User Group Deletion	This filter identifies user group deletion events.	/All Filters/ArcSight Solutions/NERC/CIP-004 Personnel and Training/
User Group Modification	This filter identifies user group modification events.	/All Filters/ArcSight Solutions/NERC/CIP-004 Personnel and Training/
User Login Attempts	This filter selects any attempts at logging into systems by non-administrative users. It excludes machine logins into Microsoft Windows systems.	/All Filters/ArcSight Solutions/NERC/General Filters/Authentication/
User Removed from Group	This filter identifies when a user removed from group.	/All Filters/ArcSight Solutions/NERC/CIP-004 Personnel and Training/
VPN Access Attempt	This filter identifies VPN access attempts.	/All Filters/ArcSight Solutions/NERC/CIP-005 Electronic Security Perimeter(s)/
VPN Configuration Modifications	Selects events indicating that a VPN configuration change has occurred.	/All Filters/ArcSight Solutions/NERC/CIP-010 Configuration Change Management and Vulnerability/
Virus Activity	This filter identifies virus activities reported by either an Intrusion Detection System (IDS) or an anti-virus application.	/All Filters/ArcSight Solutions/NERC/CIP-007 System Security Management/
Vulnerability Events by Non-Scanners	This filter identifies vulnerability events reported by non-scanner devices.	/All Filters/ArcSight Solutions/NERC/General Filters/Vulnerabilities/

Filters Resources, continued

Resource	Description	URI
Vulnerability Scanner Events	This filter identifies scanner-generated events.	/All Filters/ArcSight Solutions/NERC/General Filters/Vulnerabilities/
Windows Domain Policy Changed	Selects events indicating that a Windows domain policy was changed.	/All Filters/ArcSight Solutions/NERC/CIP-010 Configuration Change Management and Vulnerability/
Windows Events with a Non-Machine User	This filters identified Microsoft Windows events that have a non machine/system user either in the attacker or the target fields.	/All Filters/ArcSight Solutions/NERC/General Filters/
Windows Group Policy Changed	Selects events indicating that a windows group policy was changed.	/All Filters/ArcSight Solutions/NERC/CIP-010 Configuration Change Management and Vulnerability/
Wireless Intrusion Detection Systems	This filter identifies events reported by a wireless Intrusion Detection System (IDS).	/All Filters/ArcSight Solutions/NERC/CIP-005 Electronic Security Perimeter(s)/
Wireless Malicious Traffic Detected	This filter identifies events where malicious wireless traffic is observed.	/All Filters/ArcSight Solutions/NERC/CIP-005 Electronic Security Perimeter(s)/
Worm Activity	This filter identifies worm activities reported by either an Intrusion Detection System (IDS) or an anti-virus application.	/All Filters/ArcSight Solutions/NERC/CIP-007 System Security Management/
XSRF Vulnerability Detected	Selects events indicating that an XSRF vulnerability was detected.	/All Filters/ArcSight Solutions/NERC/CIP-010 Configuration Change Management and Vulnerability/
XSS Vulnerability Detected	Selects events indicating that an XSS vulnerability was detected.	/All Filters/ArcSight Solutions/NERC/CIP-010 Configuration Change Management and Vulnerability/

Focused Reports

The following table lists all the focused reports.

Focused Reports Resources

Resource	Description	URI
Assets in High Impact BES Cyber Systems	This report provides the listing of all the assets for the high impact BES cyber systems , sorted by creation time.	/All Reports/ArcSight Solutions/NERC/CIP-002 BES Cyber System Categorization/
Assets in Low Impact BES Cyber Systems	This report provides the listing of all the assets for the low impact BES cyber systems , sorted by creation time.	/All Reports/ArcSight Solutions/NERC/CIP-002 BES Cyber System Categorization/
Assets in Medium Impact BES Cyber Systems	This report provides the listing of all the assets for the medium impact BES cyber systems , sorted by creation time.	/All Reports/ArcSight Solutions/NERC/CIP-002 BES Cyber System Categorization/
Assets in the Development Network Domain	This report provides the listing of all the assets for the Development Network Domain.	/All Reports/ArcSight Solutions/NERC/CIP-002 BES Cyber System Categorization/
Assets in the Development Network Domain (Creation-Time Sorted)	This report provides the listing of all the assets for the Development Network Domain, sorted by creation time.	/All Reports/ArcSight Solutions/NERC/CIP-002 BES Cyber System Categorization/
Assets in the Public-Facing Network Domain	This report provides the listing of all the assets for the Public-Facing Network Domain.	/All Reports/ArcSight Solutions/NERC/CIP-002 BES Cyber System Categorization/
Assets in the Public-Facing Network Domain (Creation-Time Sorted)	This report provides the listing of all the assets for the Public-Facing Network Domain, sorted by creation time.	/All Reports/ArcSight Solutions/NERC/CIP-002 BES Cyber System Categorization/
Policy Violations In High Impact BES Cyber Assets	This report provides a listing of events categorized by ArcSight as policy violations which target high impact BES cyber assets .	/All Reports/ArcSight Solutions/NERC/CIP-003 Security Management Controls/
Policy Violations In Low Impact BES Cyber Assets	This report provides a listing of events categorized by ArcSight as policy violations which target low impact BES cyber assets .	/All Reports/ArcSight Solutions/NERC/CIP-003 Security Management Controls/
Policy Violations In Medium Impact BES Cyber Assets	This report provides a listing of events categorized by ArcSight as policy violations which target medium impact BES cyber assets .	/All Reports/ArcSight Solutions/NERC/CIP-003 Security Management Controls/

Queries

The following table lists all the queries.

Queries Resources

Resource	Description	URI
Account Creations	This query provides a listing of all Information System accounts that were created.	/All Queries/ArcSight Solutions/NERC/CIP-004 Personnel and Training/
Account Creations in Network Domain - Template	This query provides a listing of Information System accounts that were deleted in a specific network domain. By default, the Development network domain is used. Assets have to be modeled in ESM and categorized with one or more Asset Categories under the /All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains group.	/All Queries/ArcSight Solutions/NERC/CIP-004 Personnel and Training/
Account Deletions	This query provides a listing of all Information System accounts that were deleted.	/All Queries/ArcSight Solutions/NERC/CIP-004 Personnel and Training/
Account Deletions in Network Domain - Template	This query provides a listing of Information System accounts that were deleted in a specific network domain. By default, the Development network domain is used. Assets have to be modeled in ESM and categorized with one or more Asset Categories under the /All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains group.	/All Queries/ArcSight Solutions/NERC/CIP-004 Personnel and Training/
Account Lockouts	This query retrieves all information about account lockouts.	/All Queries/ArcSight Solutions/NERC/CIP-007 System Security Management/
Account Lockouts per System	This query retrieves a count of all the account lockouts per system during the last 24 hours.	/All Queries/ArcSight Solutions/NERC/CIP-007 System Security Management/
Account Lockouts per User and System	This query counts account lockouts per user and system.	/All Queries/ArcSight Solutions/NERC/CIP-007 System Security Management/

Queries Resources, continued

Resource	Description	URI
Account Modifications	This query provides a listing of all Information System accounts that were modified.	/All Queries/ArcSight Solutions/NERC/CIP-004 Personnel and Training/
Account Modifications in Network Domain - Template	This query provides a listing of Information System accounts that were modified in a specific network domain. By default, the Development network domain is used. Assets have to be modeled in ESM and categorized with one or more Asset Categories under the /All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains group.	/All Queries/ArcSight Solutions/NERC/CIP-004 Personnel and Training/
Activity by Former Employees	This query shows any activity performed by users who are known to be terminated.	/All Queries/ArcSight Solutions/NERC/CIP-004 Personnel and Training/
Administrative Logins and Logouts per User	This query provides a listing of administrative logins and logouts per user name.	/All Queries/ArcSight Solutions/NERC/CIP-007 System Security Management/
All Events by New Hires	This query shows all events by new hires.	/All Queries/ArcSight Solutions/NERC/CIP-004 Personnel and Training/
All File Related Activity on High Impact BES cyber Systems	This query shows a count of all file activity on high impact BES cyber systems.	/All Queries/ArcSight Solutions/NERC/CIP-010 Configuration Change Management and Vulnerability/
All File Related Activity on Low Impact BES cyber Systems	This query shows a count of all file activity on low impact BES cyber systems.	/All Queries/ArcSight Solutions/NERC/CIP-010 Configuration Change Management and Vulnerability/
All File Related Activity on Medium Impact BES cyber Systems	This query shows a count of all file activity on medium impact BES cyber systems.	/All Queries/ArcSight Solutions/NERC/CIP-010 Configuration Change Management and Vulnerability/

Queries Resources, continued

Resource	Description	URI
All File Related Activity on Third Party Accessible Systems	This query shows a count of all file activity on assets accessible to third parties.	/All Queries/ArcSight Solutions/NERC/CIP-010 Configuration Change Management and Vulnerability/
All Information Leaks	This query shows all activity flagged as information leakage.	/All Queries/ArcSight Solutions/NERC/CIP-011 Information Protection/
All Information Leaks from High Impact BES Cyber Systems	This query shows all activity flagged as information leakage on high impact BES cyber systems .	/All Queries/ArcSight Solutions/NERC/CIP-011 Information Protection/
All Information Leaks from Low Impact BES Cyber Systems	This query shows all activity flagged as information leakage on low impact BES cyber systems	/All Queries/ArcSight Solutions/NERC/CIP-011 Information Protection/
All Information Leaks from Medium Impact BES Cyber Systems	This query shows all activity flagged as information leakage on medium impact BES cyber systems .	/All Queries/ArcSight Solutions/NERC/CIP-011 Information Protection/
All Password Change Events	This query provides a list of all password change events and their outcome.	/All Queries/ArcSight Solutions/NERC/CIP-007 System Security Management/
All Suspicious Events by New Hires	This query shows all suspicious events by new hires based on the event table.	/All Queries/ArcSight Solutions/NERC/CIP-004 Personnel and Training/
All User Logins per User	This query provides a listing of user logins per user name.	/All Queries/ArcSight Solutions/NERC/CIP-007 System Security Management/

Queries Resources, continued

Resource	Description	URI
Anti-Virus Stopped or Paused in the Last Month	This query shows all events when a anti-virus service is stopped or paused in the last month.	/All Queries/ArcSight Solutions/NERC/CIP- 007 System Security Management/
Application Brute Force Login Attempts	This query shows application brute force login attempts.	/All Queries/ArcSight Solutions/NERC/CIP- 007 System Security Management/
Application Configuration Modifications	This query shows any configuration modifications of any application on a system. Default time window: Last 24 hours.	/All Queries/ArcSight Solutions/NERC/CIP- 010 Configuration Change Management and Vulnerability/
Asset Creation by Location	This query provides a listing of newly created assets.	/All Queries/ArcSight Solutions/NERC/CIP- 002 BES Cyber System Categorization/
Asset Deletion by Location	This query provides a listing of deleted assets.	/All Queries/ArcSight Solutions/NERC/CIP- 002 BES Cyber System Categorization/
Asset Identification Report	This query shows all assets and their respective network domain.	/All Queries/ArcSight Solutions/NERC/CIP- 002 BES Cyber System Categorization/
Asset Modification by Location	This query provides a listing of modified assets.	/All Queries/ArcSight Solutions/NERC/CIP- 002 BES Cyber System Categorization/

Queries Resources, continued

Resource	Description	URI
Assets Available to Third Parties by Domain	This query shows the assets that are available to third parties as defined by the assets available to 3rd parties asset category. This query is organized by network domain.	/All Queries/ArcSight Solutions/NERC/CIP-002 BES Cyber System Categorization/
Assets Available to Third-Parties by Criticality	This query shows the assets that are available to third parties as defined by the assets available to 3rd parties asset category. This query is organized by asset criticality.	/All Queries/ArcSight Solutions/NERC/CIP-002 BES Cyber System Categorization/
Assets by Network Domain (Creation Time) - Template	This query provides the listing of all the assets for the various Network Domains. This query may (and should) be focused based on the Network Domain of interest. Sorted by Creation time.	/All Queries/ArcSight Solutions/NERC/CIP-002 BES Cyber System Categorization/
Assets by Network Domain - Template	This query provides the listing of all the assets for the various Network Domains. This query may (and should) be focused based on the Network Domain of interest.	/All Queries/ArcSight Solutions/NERC/CIP-002 BES Cyber System Categorization/
Assets that Failed Technical Compliance Check	This query finds assets which failed the technical compliance check.	/All Queries/ArcSight Solutions/NERC/CIP-002 BES Cyber System Categorization/
Attacks and Suspicious Activities - All	This query provides a listing of all hostile or suspicious events sorted by the event's end time.	/All Queries/ArcSight Solutions/NERC/CIP-008 Incident Reporting and Response Planning/
Attacks and Suspicious Activities Trend	This query summarizes the number of attacks and suspicious activities for long term reporting.	/All Queries/ArcSight Solutions/NERC/CIP-008 Incident Reporting and Response Planning/

Queries Resources, continued

Resource	Description	URI
Attacks and Suspicious Activities on High Impact BES Cyber Systems	This query provides a listing of all hostile or suspicious events on High Impact BES Cyber Systems sorted by the event's end time.	/All Queries/ArcSight Solutions/NERC/CIP- 008 Incident Reporting and Response Planning/
Attacks and Suspicious Activities on Low Impact BES Cyber Systems	This query provides a listing of all hostile or suspicious events on Low Impact BES Cyber Systems sorted by the event's end time.	/All Queries/ArcSight Solutions/NERC/CIP- 008 Incident Reporting and Response Planning/
Attacks and Suspicious Activities on Medium Impact BES Cyber Systems	This query provides a listing of all hostile or suspicious events on Medium Impact BES Cyber Systems sorted by the event's end time.	/All Queries/ArcSight Solutions/NERC/CIP- 008 Incident Reporting and Response Planning/
Audit Log Cleared	This query shows all events where an audit log was cleared from a host.	/All Queries/ArcSight Solutions/NERC/CIP- 010 Configuration Change Management and Vulnerability/
Audit Log Cleared per Attacker User Name	This query shows the number of times an audit log was cleared by an attacker user name.	/All Queries/ArcSight Solutions/NERC/CIP- 010 Configuration Change Management and Vulnerability/
Audit Log Cleared per Attacker and Target	This query shows the number of times audit logs were cleared from a host by an attacker	/All Queries/ArcSight Solutions/NERC/CIP- 010 Configuration Change Management and Vulnerability/
Audit Log Cleared per Target User Name	This query shows the number of times an audit log was cleared by a target user name.	/All Queries/ArcSight Solutions/NERC/CIP- 010 Configuration Change Management and Vulnerability/

Queries Resources, continued

Resource	Description	URI
Average Time to Resolution - By Case Severity	This query shows the Average Time to Resolution by Case Severity. It should be run once a week and reported to management.	/All Queries/ArcSight Solutions/NERC/CIP-008 Incident Reporting and Response Planning/
Average Time to Resolution - By Day	This query shows the average time to resolution of all the closed cases by day. This query should be run once a week and reported to management.	/All Queries/ArcSight Solutions/NERC/CIP-008 Incident Reporting and Response Planning/
Average Time to Resolution - By User	This query shows how long it takes individuals to close their cases. This query should be run once a week and reported to management.	/All Queries/ArcSight Solutions/NERC/CIP-008 Incident Reporting and Response Planning/
Blocked Firewall Traffic from Assets - Template	This query provides a listing of the blocked outbound firewall traffic originating from assets in the indicated Network Domain of interest.	/All Queries/ArcSight Solutions/NERC/CIP-005 Electronic Security Perimeter (s)/
Blocked Firewall Traffic to Assets - Template	This query provides a listing of the blocked inbound firewall traffic directed at assets in the indicated Network Domain of interest.	/All Queries/ArcSight Solutions/NERC/CIP-005 Electronic Security Perimeter (s)/
CIP-002 Case Overview	This query shows the number of open cases per stage for cases that have been created as a result of NERC CIP-002 rule actions.	/All Queries/ArcSight Solutions/NERC/CIP-008 Incident Reporting and Response Planning/
CIP-003 Case Overview	This query shows the number of open cases per stage for cases that have been created as a result of NERC CIP-003 rule actions.	/All Queries/ArcSight Solutions/NERC/CIP-008 Incident Reporting and Response Planning/

Queries Resources, continued

Resource	Description	URI
CIP-004 Case Overview	This query shows the number of open cases per stage for cases that have been created as a result of NERC CIP-004 rule actions.	/All Queries/ArcSight Solutions/NERC/CIP- 008 Incident Reporting and Response Planning/
CIP-005 Case Overview	This query shows the number of open cases per stage for cases that have been created as a result of nerc NERC CIP-005 rule actions.	/All Queries/ArcSight Solutions/NERC/CIP- 008 Incident Reporting and Response Planning/
CIP-006 Case Overview	This query shows the number of open cases per stage for cases that have been created as a result of NERC CIP-006 rule actions.	/All Queries/ArcSight Solutions/NERC/CIP- 008 Incident Reporting and Response Planning/
CIP-007 Case Overview	This query shows the number of open cases per stage for cases that have been created as a result of NERC CIP-007 rule actions.	/All Queries/ArcSight Solutions/NERC/CIP- 008 Incident Reporting and Response Planning/
CIP-008 Case Overview	This query shows the number of open cases per stage for cases that have been created as a result of NERC CIP-008 rule actions.	/All Queries/ArcSight Solutions/NERC/CIP- 008 Incident Reporting and Response Planning/
CIP-009 Case Overview	This query shows the number of open cases per stage for cases that have been created as a result of NERC CIP-009 rule actions.	/All Queries/ArcSight Solutions/NERC/CIP- 008 Incident Reporting and Response Planning/
CIP-010 Case Overview	This query shows the number of open cases per stage for cases that have been created as a result of NERC CIP-010 rule actions.	/All Queries/ArcSight Solutions/NERC/CIP- 008 Incident Reporting and Response Planning/

Queries Resources, continued

Resource	Description	URI
CIP-011 Case Overview	This query shows the number of open cases per stage for cases that have been created as a result of NERC CIP-011 rule actions.	/All Queries/ArcSight Solutions/NERC/CIP- 008 Incident Reporting and Response Planning/
CVSS Score Greater than or Equal to 8	Shows vulnerabilities with CVSS >=8.	/All Queries/ArcSight Solutions/NERC/CIP- 010 Configuration Change Management and Vulnerability/
Case Audit Events - Trend Base	This query collects Time to Resolution (TTR) information from case audit events and stores them in a trend for case history reporting.	/All Queries/ArcSight Solutions/NERC/CIP- 008 Incident Reporting and Response Planning/
Case Status by Owner	This query provides a breakdown by owner of all cases.	/All Queries/ArcSight Solutions/NERC/CIP- 008 Incident Reporting and Response Planning/
Cases by Stage	This query provides an overview of all cases in their current stages.	/All Queries/ArcSight Solutions/NERC/CIP- 008 Incident Reporting and Response Planning/
Classification of Assets	This query will show the asset classifications sorted by network domain.	/All Queries/ArcSight Solutions/NERC/CIP- 002 BES Cyber System Categorization/
Configuration Changes - Trend Base	Retrieves all configuration changes for the last hour and used as trend base query for the Configuration Changes trend.	/All Queries/ArcSight Solutions/NERC/CIP- 010 Configuration Change Management and Vulnerability/

Queries Resources, continued

Resource	Description	URI
Count of Administrative Logins	This query shows details of all successful administrative logins within the last 30 days.	/All Queries/ArcSight Solutions/NERC/CIP- 007 System Security Management/
Count of Attacks and Suspicious Activities Per Attacker Machine	This query provides a count of attacker addresses appearing in of hostile or suspicious events.	/All Queries/ArcSight Solutions/NERC/CIP- 008 Incident Reporting and Response Planning/
Count of Attacks and Suspicious Activities Per Target Machine	This query provides a count of target addresses appearing in of hostile or suspicious events.	/All Queries/ArcSight Solutions/NERC/CIP- 008 Incident Reporting and Response Planning/
Count of Attacks and Suspicious Activity Event Names	This report counts the names of attack and suspicious activity events.	/All Queries/ArcSight Solutions/NERC/CIP- 008 Incident Reporting and Response Planning/
Count of Attacks and Suspicious Activity Per Day	This query counts the total number of weekly attack and suspicious activity events.	/All Queries/ArcSight Solutions/NERC/CIP- 008 Incident Reporting and Response Planning/
Count of DoS Attacks per Day	This query counts the total number of weekly denial of service attack events.	/All Queries/ArcSight Solutions/NERC/CIP- 008 Incident Reporting and Response Planning/
Count of Successful Administrative Logins in the Last 30 days	This query shows a count of successful administrative logins within the last 30 days.	/All Queries/ArcSight Solutions/NERC/CIP- 007 System Security Management/
Count of Unsuccessful Administrative Logins in the Last 30 days	This query shows a count of unsuccessful administrative logins within the last 30 days.	/All Queries/ArcSight Solutions/NERC/CIP- 007 System Security Management/

Queries Resources, continued

Resource	Description	URI
Covert Channel Activity	This query shows all covert channel activity.	/All Queries/ArcSight Solutions/NERC/CIP- 005 Electronic Security Perimeter (s)/
Critical Assets	This query lists all the critical assets. It can be used to gather the key assets to implement the business continuity process.	/All Queries/ArcSight Solutions/NERC/CIP- 002 BES Cyber System Categorization/
Critical Assets	This query lists all the critical assets which have been categorized with a criticality of high or very-high. It can be used to identify key assets to implement the business continuity process.	/All Queries/ArcSight Solutions/NERC/CIP- 009 Recovery Plans for BES Cyber Systems/
Criticality of Assets	This query will show the asset criticality sorted by their criticality and network domain.	/All Queries/ArcSight Solutions/NERC/CIP- 002 BES Cyber System Categorization/
Daily Anti-Virus Stopped or Paused - Base	This query shows all events when a anti-virus service is stopped or paused on systems.	/All Queries/ArcSight Solutions/NERC/CIP- 007 System Security Management/
Daily Count of Successful User Logins	This query gets information about the number of successful non-administrative user logins every day over the past week.	/All Queries/ArcSight Solutions/NERC/CIP- 007 System Security Management/
Daily Count of Unsuccessful User Logins	This query counts the number of unsuccessful daily user logins.	/All Queries/ArcSight Solutions/NERC/CIP- 007 System Security Management/
Daily Successful Administrative Logins per Hour	This query shows the hourly number of successful administrative logins.	/All Queries/ArcSight Solutions/NERC/CIP- 007 System Security Management/

Queries Resources, continued

Resource	Description	URI
Daily Unsuccessful Administrative Logins per Hour	This query shows the hourly number of unsuccessful administrative logins.	/All Queries/ArcSight Solutions/NERC/CIP-007 System Security Management/
Detail Default Vendor Account Used	This query shows if a vendor supplied user account without password is being used to login.	/All Queries/ArcSight Solutions/NERC/CIP-004 Personnel and Training/
Detected Malware Summary by Hosts	This query shows a summary of malware detected on systems sorted by host.	/All Queries/ArcSight Solutions/NERC/CIP-007 System Security Management/
Development and Test Cross-Talk	This query provides the cross-talk in the last 24 hours between assets in Development category and assets in Test category.	/All Queries/ArcSight Solutions/NERC/CIP-005 Electronic Security Perimeter (s)/
Disallowed Ports	This query shows traffic that should not be seen per the Allowed Ports active list.	/All Queries/ArcSight Solutions/NERC/CIP-005 Electronic Security Perimeter (s)/
Disallowed Ports by Connection Types	This query shows the top disallowed ports grouped by connection types.	/All Queries/ArcSight Solutions/NERC/CIP-005 Electronic Security Perimeter (s)/
DoS Attacks Trend	This query summarizes the number of DoS attacks for long term reporting.	/All Queries/ArcSight Solutions/NERC/CIP-008 Incident Reporting and Response Planning/
DoS Attacks by Attacker	This query provides a weekly count of attacker addresses appearing in DoS attack events.	/All Queries/ArcSight Solutions/NERC/CIP-008 Incident Reporting and Response Planning/

Queries Resources, continued

Resource	Description	URI
DoS Attacks by Target	This query provides a weekly count of target addresses appearing in DoS attack events.	/All Queries/ArcSight Solutions/NERC/CIP- 008 Incident Reporting and Response Planning/
Dynamic Open Ports Events	This query list all dynamic open port events reported by vulnerability scanners.	/All Queries/ArcSight Solutions/NERC/CIP- 007 System Security Management/
Email Attacks	This query shows all email attacks.	/All Queries/ArcSight Solutions/NERC/CIP- 005 Electronic Security Perimeter (s)/
External Hosts Receiving Most IM Traffic	This query shows top external hosts receiving most Instant Messaging traffic.	/All Queries/ArcSight Solutions/NERC/CIP- 005 Electronic Security Perimeter (s)/
External to High Impact BES Cyber Systems Traffic	This query counts all events from external to high impact BES cyber system sources per device and source-target pair. The query runs over the last 24 hours.	/All Queries/ArcSight Solutions/NERC/CIP- 005 Electronic Security Perimeter (s)/
External to Internal Traffic	This query counts all events from external to internal sources per device and source-target pair. The query runs over the last 24 hours.	/All Queries/ArcSight Solutions/NERC/CIP- 005 Electronic Security Perimeter (s)/
External to Low Impact BES Cyber Systems Traffic	This query counts all events from external to low impact BES cyber system sources per device and source-target pair. The query runs over the last 24 hours.	/All Queries/ArcSight Solutions/NERC/CIP- 005 Electronic Security Perimeter (s)/

Queries Resources, continued

Resource	Description	URI
External to Medium Impact BES Cyber Systems Traffic	This query counts all events from external to medium impact BES cyber system sources per device and source-target pair. The query runs over the last 24 hours.	/All Queries/ArcSight Solutions/NERC/CIP- 005 Electronic Security Perimeter (s)/
Failed After Hours Building Accesses	This query shows the failed physical access of a building after business hours, regardless of whether the access was granted, or not. Actual time values are defined in the filter referenced in the 'Conditions' pane.	/All Queries/ArcSight Solutions/NERC/CIP- 006 Physical Security of BES Cyber Systems/
Failed Anti-Virus Updates	This query shows all the failed Anti-Virus updates on systems.	/All Queries/ArcSight Solutions/NERC/CIP- 007 System Security Management/
Failed Building Access Events	This query shows failed attempts to enter a building at any time.	/All Queries/ArcSight Solutions/NERC/CIP- 006 Physical Security of BES Cyber Systems/
Failed Password Changes	This query retrieves failed password change events, ordered by target user name.	/All Queries/ArcSight Solutions/NERC/CIP- 007 System Security Management/
Failed or Attempted Removal of Access Rights	This query shows all failed or attempted removal of access rights from a host resource.	/All Queries/ArcSight Solutions/NERC/CIP- 004 Personnel and Training/
Fault Logs	This query shows events indicating a process has failed to execute in the expected way.	/All Queries/ArcSight Solutions/NERC/CIP- 009 Recovery Plans for BES Cyber Systems/
File Creations on Third Party Accessible Systems	This query shows a count of all file creations on assets accessible to third parties.	/All Queries/ArcSight Solutions/NERC/CIP- 010 Configuration Change Management and Vulnerability/

Queries Resources, continued

Resource	Description	URI
File Deletions on Third Party Accessible Systems	This query shows a count of all file deletions on assets accessible to third parties.	/All Queries/ArcSight Solutions/NERC/CIP- 010 Configuration Change Management and Vulnerability/
File Modifications on Third Party Accessible Systems	This query shows a count of all file modifications on assets accessible to third parties.	/All Queries/ArcSight Solutions/NERC/CIP- 010 Configuration Change Management and Vulnerability/
Firewall Configuration Modifications	This query shows any configuration modifications of any firewall. Default time window: Last 24 hours.	/All Queries/ArcSight Solutions/NERC/CIP- 010 Configuration Change Management and Vulnerability/
Firewall Configuration Modifications by Name	This query shows the top configuration modifications of any firewall.	/All Queries/ArcSight Solutions/NERC/CIP- 010 Configuration Change Management and Vulnerability/
Former Employee Account Access Attempt	This query lists all log-in activity from a former employee.	/All Queries/ArcSight Solutions/NERC/CIP- 004 Personnel and Training/
Former Employee Accounts in Use	This query identifies all former employee user names and reporting device details associated with recent events.	/All Queries/ArcSight Solutions/NERC/CIP- 004 Personnel and Training/
Frequent Unsuccessful Logins by User Name	This query identifies all user names for which there are a continuous set of unsuccessful login attempts.	/All Queries/ArcSight Solutions/NERC/CIP- 007 System Security Management/
Frequent Unsuccessful Logins from Attacker Host	This query identifies all attacker hosts from which a continuous set of unsuccessful login attempts have been occurring.	/All Queries/ArcSight Solutions/NERC/CIP- 007 System Security Management/

Queries Resources, continued

Resource	Description	URI
Frequent Unsuccessful Logins to Target Host	This query identifies all target hosts which have received a continuous set of unsuccessful login attempts.	/All Queries/ArcSight Solutions/NERC/CIP-007 System Security Management/
High Impact BES Cyber Systems to External Traffic	This query counts all events from internal high impact BES cyber systems to external sources per device and source-target pair. The query runs over the last 24 hours.	/All Queries/ArcSight Solutions/NERC/CIP-005 Electronic Security Perimeter (s)/
High Priority Events	This query shows events in which the Priority is 10.	/All Queries/ArcSight Solutions/NERC/CIP-008 Incident Reporting and Response Planning/
High Priority Events on High Impact BES Cyber Systems	This query shows events in which the Priority field is 10 where the attacker or the target are in High Impact BES Cyber Systems .	/All Queries/ArcSight Solutions/NERC/CIP-008 Incident Reporting and Response Planning/
High Priority Events on Low Impact BES Cyber Systems	This query shows events in which the Priority field is 10 where the attacker or the target are in Low Impact BES Cyber Systems .	/All Queries/ArcSight Solutions/NERC/CIP-008 Incident Reporting and Response Planning/
High Priority Events on Medium Impact BES Cyber Systems	This query shows events in which the Priority field is 10 where the attacker or the target are in Medium Impact BES Cyber Systems .	/All Queries/ArcSight Solutions/NERC/CIP-008 Incident Reporting and Response Planning/
High and Medium Impact BES Cyber Systems Cross-Talk	This query provides the cross-talk in the last 24 hours between assets in High Impact BES Cyber Systems category and assets in Medium Impact BES Cyber Systems category.	/All Queries/ArcSight Solutions/NERC/CIP-005 Electronic Security Perimeter (s)/

Queries Resources, continued

Resource	Description	URI
High to Low Classified Asset Communication	This query shows all the assets which are classified in a higher classification level which are communicating with a lower-classified asset.	/All Queries/ArcSight Solutions/NERC/CIP- 011 Information Protection/
Inactive User Accounts	This query shows all user names that are in the Stale Accounts active list.	/All Queries/ArcSight Solutions/NERC/CIP- 004 Personnel and Training/
Inbound Insecure Transmissions	This query lists all traffic deemed as inherently insecure. All such traffic is listed in the referenced filter.	/All Queries/ArcSight Solutions/NERC/CIP- 005 Electronic Security Perimeter (s)/
Information Interception Activity	This query shows all covert channel activity.	/All Queries/ArcSight Solutions/NERC/CIP- 005 Electronic Security Perimeter (s)/
Information System Failures by Hosts	This query shows the information system which generated error log entries.	/All Queries/ArcSight Solutions/NERC/CIP- 009 Recovery Plans for BES Cyber Systems/
Insecure Cryptographic Storage	This query selects events indicating that insecure cryptographic storage has been detected.	/All Queries/ArcSight Solutions/NERC/CIP- 011 Information Protection/
Insecure Transmissions	This query lists all traffic deemed as inherently insecure. All such traffic is listed in the referenced filter.	/All Queries/ArcSight Solutions/NERC/CIP- 005 Electronic Security Perimeter (s)/
Intellectual Property Rights Violations	This query shows the various intellectual property rights violations.	/All Queries/ArcSight Solutions/NERC/CIP- 003 Security Management Controls/

Queries Resources, continued

Resource	Description	URI
Intellectual Property Rights Violators	This query shows all the assets which violated intellectual property rights.	/All Queries/ArcSight Solutions/NERC/CIP- 003 Security Management Controls/
Internal IM Sender	This query shows internal hosts with outgoing (not necessarily outbound) Instant Messaging traffic.	/All Queries/ArcSight Solutions/NERC/CIP- 005 Electronic Security Perimeter (s)/
Internal Insecure Service Providers	This query returns the internal providers of insecure services.	/All Queries/ArcSight Solutions/NERC/CIP- 005 Electronic Security Perimeter (s)/
Internal Reconnaissance Events	This query shows the top events executed for internal reconnaissance.	/All Queries/ArcSight Solutions/NERC/CIP- 008 Incident Reporting and Response Planning/
Internal Reconnaissance Sources	This query shows the top sources conducting internal reconnaissance.	/All Queries/ArcSight Solutions/NERC/CIP- 008 Incident Reporting and Response Planning/
Internal Reconnaissance Targets	This query shows the top targets accessed by internal reconnaissance activity.	/All Queries/ArcSight Solutions/NERC/CIP- 008 Incident Reporting and Response Planning/
Internal to External Traffic	This query counts all events from internal to external sources per device and source-target pair. The query runs over the last 24 hours.	/All Queries/ArcSight Solutions/NERC/CIP- 005 Electronic Security Perimeter (s)/

Queries Resources, continued

Resource	Description	URI
Invalid or Expired Certificate	This query shows incidents which indicate that an invalid or expired certificate was detected.	/All Queries/ArcSight Solutions/NERC/CIP- 011 Information Protection/
Login Activity by Stale User Accounts	This query shows stale user accounts from which login activity was attempted.	/All Queries/ArcSight Solutions/NERC/CIP- 004 Personnel and Training/
Low Impact BES Cyber Systems to External Traffic	This query counts all events from internal low impact BES cyber systems to external sources per device and source-target pair. The query runs over the last 24 hours.	/All Queries/ArcSight Solutions/NERC/CIP- 005 Electronic Security Perimeter (s)/
Low and High Impact BES Cyber Systems Cross-Talk	This query provides the cross-talk in the last 24 hours between assets in High Impact BES Cyber Systems category and assets in Low Impact BES Cyber Systems category.	/All Queries/ArcSight Solutions/NERC/CIP- 005 Electronic Security Perimeter (s)/
Low and Medium Impact BES Cyber Systems Cross-Talk	This query provides the cross-talk in the last 24 hours between assets in Low Impact BES Cyber Systems category and assets in Medium Impact BES Cyber Systems category.	/All Queries/ArcSight Solutions/NERC/CIP- 005 Electronic Security Perimeter (s)/
Low to High Classified Asset Communication	This query shows all the assets which are classified in a lower classification level which are communicating with a higher-classified asset.	/All Queries/ArcSight Solutions/NERC/CIP- 011 Information Protection/
Machines Conducting Policy Breaches	This query shows machines which were involved in policy breaches.	/All Queries/ArcSight Solutions/NERC/CIP- 003 Security Management Controls/
Malicious Code Activities from Internal Sources	This query shows all malicious code activities from internal sources.	/All Queries/ArcSight Solutions/NERC/CIP- 007 System Security Management/

Queries Resources, continued

Resource	Description	URI
Medium Impact BES Cyber Systems to External Traffic	This query counts all events from internal medium impact BES cyber systems to external sources per device and source-target pair. The query runs over the last 24 hours.	/All Queries/ArcSight Solutions/NERC/CIP- 005 Electronic Security Perimeter (s)/
Most Popular IM Traffic Ports	This query shows the most common Instant Messaging target ports.	/All Queries/ArcSight Solutions/NERC/CIP- 005 Electronic Security Perimeter (s)/
Most Popular IM Traffic Services	This query shows the most common Instant Messaging services.	/All Queries/ArcSight Solutions/NERC/CIP- 005 Electronic Security Perimeter (s)/
Network Device Configuration Modifications	This query shows any configuration modifications of any network equipment.	/All Queries/ArcSight Solutions/NERC/CIP- 010 Configuration Change Management and Vulnerability/
Network Device Configuration Modifications by Name	This query shows the top configuration modifications of network equipment.	/All Queries/ArcSight Solutions/NERC/CIP- 010 Configuration Change Management and Vulnerability/
Network Routing Changes	This query shows all router configuration modifications.	/All Queries/ArcSight Solutions/NERC/CIP- 010 Configuration Change Management and Vulnerability/
Network Routing Changes by Name	This query shows the top router configuration modifications.	/All Queries/ArcSight Solutions/NERC/CIP- 010 Configuration Change Management and Vulnerability/

Queries Resources, continued

Resource	Description	URI
Number of Daily User Logins	This query captures the number of logins per user and outcome over the entire day.	/All Queries/ArcSight Solutions/NERC/CIP- 007 System Security Management/
Number of Successful Administrative Logins by User and Host Information	This query provides a listing of administrative users with successful logins grouped by user and host information. The administrative users are sorted by the number of attempts in a decreasing order. This query may (and should) be focused based on the Network Domain of interest.	/All Queries/ArcSight Solutions/NERC/CIP- 007 System Security Management/
Number of Unsuccessful Administrative Logins by User and Host Information	This query provides a listing of administrative users with unsuccessful login attempts, grouped by user and host information. The administrative users are sorted by the number of attempts in a decreasing order. This query may be focused based on the Network Domain of interest.	/All Queries/ArcSight Solutions/NERC/CIP- 007 System Security Management/
Number of VPN Access Attempts	This query provides an overview of the number of VPN access attempts by non-administrative users.	/All Queries/ArcSight Solutions/NERC/CIP- 005 Electronic Security Perimeter (s)/
Open Cases	This query shows all currently open cases.	/All Queries/ArcSight Solutions/NERC/CIP- 008 Incident Reporting and Response Planning/
Open Cases by CIP	This query shows all currently open cases by cips .	/All Queries/ArcSight Solutions/NERC/CIP- 008 Incident Reporting and Response Planning/
Open Cases by CIP and Severity	This query shows a breakdown of open cases by severity for each regulation section.	/All Queries/ArcSight Solutions/NERC/CIP- 008 Incident Reporting and Response Planning/

Queries Resources, continued

Resource	Description	URI
Open Cases by Severity	This query shows the number of open cases by severity.	/All Queries/ArcSight Solutions/NERC/CIP- 008 Incident Reporting and Response Planning/
Open Firewall Port Details	This query gives details of all the ports that are allowed to pass through various firewalls.	/All Queries/ArcSight Solutions/NERC/CIP- 005 Electronic Security Perimeter (s)/
Open Firewall Port Summary	This query gives a summary of all the ports that are allowed to pass through firewalls.	/All Queries/ArcSight Solutions/NERC/CIP- 005 Electronic Security Perimeter (s)/
Open Ports Events	This query list all open port events reported by vulnerability scanners.	/All Queries/ArcSight Solutions/NERC/CIP- 007 System Security Management/
Operating System Configuration Modifications by Name	This query shows the top configuration modifications of any firewall.	/All Queries/ArcSight Solutions/NERC/CIP- 010 Configuration Change Management and Vulnerability/
Operations and Development Cross-Talk	This query provides all cross-talk in the last 24 hours between assets in Operations category and assets in Development category.	/All Queries/ArcSight Solutions/NERC/CIP- 005 Electronic Security Perimeter (s)/
Operations and Test Cross-Talk	This query provides all cross-talk in the last 24 hours between assets in Operations category and assets in Test category.	/All Queries/ArcSight Solutions/NERC/CIP- 005 Electronic Security Perimeter (s)/

Queries Resources, continued

Resource	Description	URI
Organizational Records Information Leaks	This query shows communications which were classified as information leaks of organizational records.	/All Queries/ArcSight Solutions/NERC/CIP- 011 Information Protection/
Passwords not Changed for Longer than Policy Standard	This query lists accounts for which the password was not changed for longer than the policy standard permits.	/All Queries/ArcSight Solutions/NERC/CIP- 007 System Security Management/
Personal Information Leaks	This query shows events which indicate a personal information leak.	/All Queries/ArcSight Solutions/NERC/CIP- 011 Information Protection/
Policy Violations - Template	This query provides a listing of events categorized by ArcSight as policy violations which target the various Network Domains by Asset. This query may (and should) be focused based on the Network Domain of interest.	/All Queries/ArcSight Solutions/NERC/CIP- 003 Security Management Controls/
Policy Violations from Third-Party Assets	This query provides a listing of events categorized by ArcSight as policy violations coming from assets categorized as Third-Party.	/All Queries/ArcSight Solutions/NERC/CIP- 003 Security Management Controls/
Privileged Account Change Details	This query lists details of events when an privileged account was attempted to be changed.	/All Queries/ArcSight Solutions/NERC/CIP- 004 Personnel and Training/
Privileged VPN Remote Access Attempts	This query shows all connections reported by a VPN device, where the user name belongs to a privileged account.	/All Queries/ArcSight Solutions/NERC/CIP- 005 Electronic Security Perimeter (s)/
Redirection Attacks	This query shows all redirection attacks.	/All Queries/ArcSight Solutions/NERC/CIP- 005 Electronic Security Perimeter (s)/

Queries Resources, continued

Resource	Description	URI
Removable Media Activity	Shows all the removable media activity for the last 24 hours.	/All Queries/ArcSight Solutions/NERC/CIP- 010 Configuration Change Management and Vulnerability/
Resource Exhaustion Detected	This query shows resources reaching their upper end of utilization (for capacity management and planning purposes).	/All Queries/ArcSight Solutions/NERC/CIP- 009 Recovery Plans for BES Cyber Systems/
Services by Asset - Template	This query will show all successful access attempts.	/All Queries/ArcSight Solutions/NERC/CIP- 002 BES Cyber System Categorization/
Shutdown of Critical Machines	This query shows all shutdown events of machines categorized as critical or highly critical.	/All Queries/ArcSight Solutions/NERC/CIP- 009 Recovery Plans for BES Cyber Systems/
Shutdown of Machines	This query shows all machine shutdown events.	/All Queries/ArcSight Solutions/NERC/CIP- 009 Recovery Plans for BES Cyber Systems/
Software Changes in High Impact BES Cyber Systems	This query shows all changes to any software installed in high impact BES cyber systems .	/All Queries/ArcSight Solutions/NERC/CIP- 010 Configuration Change Management and Vulnerability/
Software Changes in Low Impact BES Cyber Systems	This query shows all changes to any software installed in low impact BES cyber systems .	/All Queries/ArcSight Solutions/NERC/CIP- 010 Configuration Change Management and Vulnerability/

Queries Resources, continued

Resource	Description	URI
Software Changes in Medium Impact BES Cyber Systems	This query shows all changes to any software installed in medium impact BES cyber systems .	/All Queries/ArcSight Solutions/NERC/CIP-010 Configuration Change Management and Vulnerability/
Software Changes in Operations	This query shows all changes to any software installed in the operations network segment.	/All Queries/ArcSight Solutions/NERC/CIP-010 Configuration Change Management and Vulnerability/
Successful Administrative Logins	This query shows details of all successful Administrative logins within the last day.	/All Queries/ArcSight Solutions/NERC/CIP-007 System Security Management/
Successful Administrative Logins from Third Party Systems	This query retrieves successful logins with an administrator account from assets categorized as Third Party.	/All Queries/ArcSight Solutions/NERC/CIP-007 System Security Management/
Successful Administrative Logins to High Impact BES Cyber Systems	This query identifies successful logins with an administrative account to high impact BES Cyber systems .	/All Queries/ArcSight Solutions/NERC/CIP-007 System Security Management/
Successful Administrative Logins to Low Impact BES Cyber Systems	This query identifies successful logins with an administrative account to Low impact BES Cyber systems .	/All Queries/ArcSight Solutions/NERC/CIP-007 System Security Management/
Successful Administrative Logins to Medium Impact BES Cyber Systems	This query identifies successful logins with an administrative account to Medium impact BES Cyber systems .	/All Queries/ArcSight Solutions/NERC/CIP-007 System Security Management/
Successful Administrative Logins to Third Party Systems	This query identifies successful logins with an administrative account to third party systems.	/All Queries/ArcSight Solutions/NERC/CIP-007 System Security Management/

Queries Resources, continued

Resource	Description	URI
Successful After Hours Building Accesses	This query shows the successful physical access of a building after business hours, regardless of whether the access was granted, or not. Actual time values are defined in the filter referenced in the 'Conditions' pane.	/All Queries/ArcSight Solutions/NERC/CIP- 006 Physical Security of BES Cyber Systems/
Successful Brute Force Logins	This query provides a listing of events categorized by ArcSight as probable successful brute-force login attempts. This query may (and should) be focused based on the Network Domain of interest.	/All Queries/ArcSight Solutions/NERC/CIP- 007 System Security Management/
Successful Building Access Events	This query shows successful building access events at all times.	/All Queries/ArcSight Solutions/NERC/CIP- 006 Physical Security of BES Cyber Systems/
Successful Changes to Operating Systems	This query shows the number of times changes were made to operating systems.	/All Queries/ArcSight Solutions/NERC/CIP- 010 Configuration Change Management and Vulnerability/
Successful Configuration Changes to High Impact BES Cyber Systems	This query lists a count of successful configuration changes made to high impact BES cyber systems.	/All Queries/ArcSight Solutions/NERC/CIP- 010 Configuration Change Management and Vulnerability/
Successful Configuration Changes to Low Impact BES Cyber Systems	This query lists a count of successful configuration changes made to low impact BES cyber systems .	/All Queries/ArcSight Solutions/NERC/CIP- 010 Configuration Change Management and Vulnerability/
Successful Configuration Changes to Medium Impact BES Cyber Systems	This query lists a count of successful configuration changes made to medium impact BES cyber systems.	/All Queries/ArcSight Solutions/NERC/CIP- 010 Configuration Change Management and Vulnerability/

Queries Resources, continued

Resource	Description	URI
Successful Configuration Changes to Third Party Machines	This query lists a count of successful configuration changes made to third party systems.	/All Queries/ArcSight Solutions/NERC/CIP- 010 Configuration Change Management and Vulnerability/
Successful Database Configuration Modification	This query shows all events on database configuration modifications.	/All Queries/ArcSight Solutions/NERC/CIP- 010 Configuration Change Management and Vulnerability/
Successful High or Critical Configuration Changes	This query shows all successful non ArcSight internal high or critical configuration modifications.	/All Queries/ArcSight Solutions/NERC/CIP- 010 Configuration Change Management and Vulnerability/
Successful Password Changes	This query lists successful password change events, ordered by target user name.	/All Queries/ArcSight Solutions/NERC/CIP- 007 System Security Management/
Successful Removal of Access Rights	This query shows all the removal of access rights from a host resource. Removal could mean that either the user was removed from the system, or the privileges related to that ID were modified.	/All Queries/ArcSight Solutions/NERC/CIP- 004 Personnel and Training/
Successful User Logins	This query shows details of all successful user logins within the last day.	/All Queries/ArcSight Solutions/NERC/CIP- 007 System Security Management/
Successful User Logins by Hour	This query gets the number of non-administrative successful user logins per hour.	/All Queries/ArcSight Solutions/NERC/CIP- 007 System Security Management/
Successful User Logins from Third Party Systems	This query retrieves successful logins using a non-administrative account, from assets categorized as Third Party.	/All Queries/ArcSight Solutions/NERC/CIP- 007 System Security Management/

Queries Resources, continued

Resource	Description	URI
Successful User Logins to High Impact BES Cyber Systems	This query retrieves successful logins using a non-administrative account, to assets categorized as High Impact BES Cyber Systems	/All Queries/ArcSight Solutions/NERC/CIP- 007 System Security Management/
Successful User Logins to Low Impact BES Cyber Systems	This query retrieves successful logins using a non-administrative account, to assets categorized as Low Impact BES Cyber Systems	/All Queries/ArcSight Solutions/NERC/CIP- 007 System Security Management/
Successful User Logins to Medium Impact BES Cyber Systems	This query retrieves successful logins using a non-administrative account, to assets categorized as Medium Impact BES Cyber Systems	/All Queries/ArcSight Solutions/NERC/CIP- 007 System Security Management/
Successful User Logins to Third Party Systems	This query retrieves successful logins using a non-administrative account, to assets categorized as Third Party.	/All Queries/ArcSight Solutions/NERC/CIP- 007 System Security Management/
Summary of Suspicious Activity by New Hires	This query displays the number of suspicious events per new hire.	/All Queries/ArcSight Solutions/NERC/CIP- 004 Personnel and Training/
Suspicious Activity by New Hires	This query displays all the identified suspicious activity performed by new users.	/All Queries/ArcSight Solutions/NERC/CIP- 004 Personnel and Training/
Systems Accessed by Default Vendor Accounts	This query shows all systems that users have tried to access directly as root or administrator.	/All Queries/ArcSight Solutions/NERC/CIP- 004 Personnel and Training/
Third-Party Access	This query shows all access attempts to third party assets.	/All Queries/ArcSight Solutions/NERC/CIP- 005 Electronic Security Perimeter (s)/

Queries Resources, continued

Resource	Description	URI
Top 10 Hosts with Most Unsuccessful Administrative Logins	This query returns the top 10 hosts with most unsuccessful login attempts within the last 2 hours. This query may (and should) be focused based on the Network Domain of interest.	/All Queries/ArcSight Solutions/NERC/CIP- 007 System Security Management/
Top 10 Vulnerabilities	Shows the top 10 vulnerabilities on NERC assets.	/All Queries/ArcSight Solutions/NERC/CIP- 010 Configuration Change Management and Vulnerability/
Top 10 Vulnerabilities - High Impact BES Cyber Systems	This query provides a listing of the 10 most vulnerable High Impact BES Cyber Assets.	/All Queries/ArcSight Solutions/NERC/CIP- 010 Configuration Change Management and Vulnerability/
Top 10 Vulnerabilities - Low Impact BES Cyber Systems	This query provides a listing of the 10 most vulnerable Low Impact BES Cyber Assets.	/All Queries/ArcSight Solutions/NERC/CIP- 010 Configuration Change Management and Vulnerability/
Top 10 Vulnerabilities - Medium Impact BES Cyber Systems	This query provides a listing of the 10 most vulnerable Medium Impact BES Cyber Assets.	/All Queries/ArcSight Solutions/NERC/CIP- 010 Configuration Change Management and Vulnerability/
Top 10 Vulnerable Assets	Shows the top 10 vulnerable NERC assets.	/All Queries/ArcSight Solutions/NERC/CIP- 010 Configuration Change Management and Vulnerability/
Top 10 Vulnerable Assets - High Impact BES Cyber Systems	This query provides a listing of the 10 most vulnerable high impact BES cyber systems.	/All Queries/ArcSight Solutions/NERC/CIP- 010 Configuration Change Management and Vulnerability/

Queries Resources, continued

Resource	Description	URI
Top 10 Vulnerable Assets - Low Impact BES Cyber Systems	This query provides a listing of the 10 most vulnerable low impact BES cyber systems.	/All Queries/ArcSight Solutions/NERC/CIP- 010 Configuration Change Management and Vulnerability/
Top 10 Vulnerable Assets - Medium Impact BES Cyber Systems	This query provides a listing of the 10 most vulnerable medium impact BES cyber systems.	/All Queries/ArcSight Solutions/NERC/CIP- 010 Configuration Change Management and Vulnerability/
Top 10 Vulnerable Assets - Public Facing	This query provides a listing of the 10 most vulnerable Assets in your Public Facing Network Domains.	/All Queries/ArcSight Solutions/NERC/CIP- 010 Configuration Change Management and Vulnerability/
Top 10 Vulnerable Assets - Third Party	This query provides a listing of the 10 most vulnerable Third Party Assets.	/All Queries/ArcSight Solutions/NERC/CIP- 010 Configuration Change Management and Vulnerability/
Top 20 Policy Breach Events	This query shows the top 20 policy breach events.	/All Queries/ArcSight Solutions/NERC/CIP- 003 Security Management Controls/
Top Attackers Attempted Default Vendor Accounts	This query shows the top hosts from which attackers most attempted default vendor account.	/All Queries/ArcSight Solutions/NERC/CIP- 004 Personnel and Training/
Top Attackers Using Default Vendor Account	This query shows the top attackers successfully used a vendor supplied user account.	/All Queries/ArcSight Solutions/NERC/CIP- 004 Personnel and Training/
Top Attackers Using Direct Root or Administrator Account	This query shows the top attackers attempting direct root or administrator credential.	/All Queries/ArcSight Solutions/NERC/CIP- 004 Personnel and Training/

Queries Resources, continued

Resource	Description	URI
Top Critical Vulnerabilities - on Trend	This query retrieves the top 20 critical vulnerabilities for the last 14 days.	/All Queries/ArcSight Solutions/NERC/CIP- 010 Configuration Change Management and Vulnerability/
Top Default Vendor Accounts Attempted	This query shows the top vendor supplied user account still being used to login.	/All Queries/ArcSight Solutions/NERC/CIP- 004 Personnel and Training/
Top Default Vendor Accounts Used	This query shows the top vendor supplied user account still being used to login.	/All Queries/ArcSight Solutions/NERC/CIP- 004 Personnel and Training/
Top Disallowed Ports	This query shows the top disallowed ports.	/All Queries/ArcSight Solutions/NERC/CIP- 005 Electronic Security Perimeter (s)/
Top DoS Attackers	This query shows the top attackers responsible for initiating denial of service attacks.	/All Queries/ArcSight Solutions/NERC/CIP- 008 Incident Reporting and Response Planning/
Top DoS Targets	This query shows hosts which were targeted the most with denial of service attacks.	/All Queries/ArcSight Solutions/NERC/CIP- 008 Incident Reporting and Response Planning/
Top External Sources with Malicious Code Activities	This query shows the top external sources with most malicious code activities.	/All Queries/ArcSight Solutions/NERC/CIP- 007 System Security Management/
Top Firewalls with Most Successful Configuration Modifications	This query shows the top firewalls with most successful configuration modifications.	/All Queries/ArcSight Solutions/NERC/CIP- 010 Configuration Change Management and Vulnerability/

Queries Resources, continued

Resource	Description	URI
Top Hosts with Most Malware Activities	This query finds the top 10 systems with the most malware activities (routine maintenance and remediation events).	/All Queries/ArcSight Solutions/NERC/CIP- 007 System Security Management/
Top Hosts with Most Spyware Activities	This query finds the top 10 systems with most spyware activities (routine maintenance and remediation events).	/All Queries/ArcSight Solutions/NERC/CIP- 007 System Security Management/
Top Hosts with Most Virus Activities	This query shows the top hosts with most virus activities detected on systems.	/All Queries/ArcSight Solutions/NERC/CIP- 007 System Security Management/
Top Internal Hosts Accessed Disallowed Ports	This query shows the top internal hosts that accessed most disallowed ports.	/All Queries/ArcSight Solutions/NERC/CIP- 005 Electronic Security Perimeter (s)/
Top Internal Hosts Provided Disallowed Ports	This query shows the top internal hosts that provided most disallowed ports.	/All Queries/ArcSight Solutions/NERC/CIP- 005 Electronic Security Perimeter (s)/
Top Internal Sources with Malicious Code Activities	This query shows the top internal sources with most malicious code activities.	/All Queries/ArcSight Solutions/NERC/CIP- 007 System Security Management/
Top Malware Instances	This query provides the names of the top 10 detected malware instances.	/All Queries/ArcSight Solutions/NERC/CIP- 007 System Security Management/
Top Network Devices with Most Successful Configuration Modifications	This query shows the top network devices with most successful configuration modifications.	/All Queries/ArcSight Solutions/NERC/CIP- 010 Configuration Change Management and Vulnerability/

Queries Resources, continued

Resource	Description	URI
Top Network Devices with Most Successful Network Routing Changes	This query shows top routers/switches with most successful routing configuration modifications.	/All Queries/ArcSight Solutions/NERC/CIP-010 Configuration Change Management and Vulnerability/
Top Operating System with Most Successful Configuration Modifications	This query shows the top firewalls with most successful configuration modifications.	/All Queries/ArcSight Solutions/NERC/CIP-010 Configuration Change Management and Vulnerability/
Top Spyware Instances	This query provides the names of the top 10 detected spyware instances.	/All Queries/ArcSight Solutions/NERC/CIP-007 System Security Management/
Top Target Hosts Where Default Vendor Account Attempted	This query shows the top hosts where a vendor supplied user account still being used to login.	/All Queries/ArcSight Solutions/NERC/CIP-004 Personnel and Training/
Top Target Hosts Where Default Vendor Account Used	This query shows the top hosts where a vendor supplied user account still being used to login.	/All Queries/ArcSight Solutions/NERC/CIP-004 Personnel and Training/
Top Target Hosts Where Direct Root or Administrator Account Observed	This query shows the top hosts where direct root or administrator account is attempted.	/All Queries/ArcSight Solutions/NERC/CIP-004 Personnel and Training/
Top Users with Most Successful Firewall Modifications	This query shows the top users who made most successful configuration modifications.	/All Queries/ArcSight Solutions/NERC/CIP-010 Configuration Change Management and Vulnerability/

Queries Resources, continued

Resource	Description	URI
Top Users with Most Successful Network Devices Configuration Modifications	This query shows the top users with most successful configuration modifications.	/All Queries/ArcSight Solutions/NERC/CIP- 010 Configuration Change Management and Vulnerability/
Top Users with Most Successful Operating System Modifications	This query shows the top users with most successful configuration modifications.	/All Queries/ArcSight Solutions/NERC/CIP- 010 Configuration Change Management and Vulnerability/
Top Virus Instances	This query shows a summary of virus activities detected on systems sorted by virus.	/All Queries/ArcSight Solutions/NERC/CIP- 007 System Security Management/
Top Vulnerable IP Addresses	This query retrieves the top 10 vulnerable IP Addresses for the last 14 days.	/All Queries/ArcSight Solutions/NERC/CIP- 010 Configuration Change Management and Vulnerability/
Traffic Anomaly on Application Layer	This query shows traffic anomaly on application layer.	/All Queries/ArcSight Solutions/NERC/CIP- 005 Electronic Security Perimeter (s)/
Traffic Anomaly on Network Layer	This query shows traffic anomaly on network layer.	/All Queries/ArcSight Solutions/NERC/CIP- 005 Electronic Security Perimeter (s)/
Traffic Anomaly on Transport Layer	This query shows traffic anomaly on transport layer.	/All Queries/ArcSight Solutions/NERC/CIP- 005 Electronic Security Perimeter (s)/

Queries Resources, continued

Resource	Description	URI
Traffic Between Zones	This query shows the target ports between zones.	/All Queries/ArcSight Solutions/NERC/CIP- 005 Electronic Security Perimeter (s)/
Traffic from Dark Address Space	This query shows all traffic from a dark address range targeting systems. This should be considered very suspicious.	/All Queries/ArcSight Solutions/NERC/CIP- 005 Electronic Security Perimeter (s)/
Traffic to Dark Address Space	This query shows all traffic directed to a dark address range. This should be considered very suspicious.	/All Queries/ArcSight Solutions/NERC/CIP- 005 Electronic Security Perimeter (s)/
Trend of Attacks and Suspicious Activities By Attacker Address	This query provides a weekly count of attacker addresses appearing in hostile or suspicious events.	/All Queries/ArcSight Solutions/NERC/CIP- 008 Incident Reporting and Response Planning/
Trend of Attacks and Suspicious Activities By Target Address	This query provides a weekly count of target addresses appearing in hostile or suspicious events.	/All Queries/ArcSight Solutions/NERC/CIP- 008 Incident Reporting and Response Planning/
Trend of Unsuccessful Administrative Logins	This query shows the trend of unsuccessful administrative logins over long term.	/All Queries/ArcSight Solutions/NERC/CIP- 007 System Security Management/
Unencrypted Services by Host Name	Returns all unencrypted services by a particular host name identified in the last 24 hours.	/All Queries/ArcSight Solutions/NERC/CIP- 011 Information Protection/
Unsecured Open Ports Events	This query list unsecured open port events reported by vulnerability scanners.	/All Queries/ArcSight Solutions/NERC/CIP- 007 System Security Management/

Queries Resources, continued

Resource	Description	URI
Unsuccessful Administrative Logins	This query shows details of all unsuccessful administrative logins within the last day.	/All Queries/ArcSight Solutions/NERC/CIP- 007 System Security Management/
Unsuccessful Administrative Logins - Long Term Trend	This query counts the number of failed administrative logins per attacker user name, target user name and target address per month.	/All Queries/ArcSight Solutions/NERC/CIP- 007 System Security Management/
Unsuccessful Administrative Logins from Third Party Systems	This query retrieves failed logins using an administrative account, from assets categorized as Third Party.	/All Queries/ArcSight Solutions/NERC/CIP- 007 System Security Management/
Unsuccessful Administrative Logins in the Last 2 Hours	This query shows details of all unsuccessful administrative logins within the last 2 hours.	/All Queries/ArcSight Solutions/NERC/CIP- 007 System Security Management/
Unsuccessful Administrative Logins in the Last Day	This query shows details of all unsuccessful administrative logins within the last day.	/All Queries/ArcSight Solutions/NERC/CIP- 007 System Security Management/
Unsuccessful Administrative Logins to Medium Impact BES Cyber Systems	This query retrieves failed logins using an administrative account, to assets categorized as Medium Impact BES Cyber Systems.	/All Queries/ArcSight Solutions/NERC/CIP- 007 System Security Management/
Unsuccessful Administrative Logins to High Impact BES Cyber Systems	This query retrieves failed logins using an administrative account, to assets categorized as High Impact BES Cyber Systems.	/All Queries/ArcSight Solutions/NERC/CIP- 007 System Security Management/
Unsuccessful Administrative Logins to Low Impact BES Cyber Systems	This query retrieves failed logins using an administrative account, to assets categorized as Low Impact BES Cyber Systems.	/All Queries/ArcSight Solutions/NERC/CIP- 007 System Security Management/

Queries Resources, continued

Resource	Description	URI
Unsuccessful Administrative Logins to Third Party Systems	This query retrieves failed logins using an administrative account, to assets categorized as Third Party.	/All Queries/ArcSight Solutions/NERC/CIP- 007 System Security Management/
Unsuccessful Changes to Operating Systems	This query lists unsuccessful changes made to operating systems.	/All Queries/ArcSight Solutions/NERC/CIP- 010 Configuration Change Management and Vulnerability/
Unsuccessful User Logins	This query shows details of all unsuccessful user logins within the last day.	/All Queries/ArcSight Solutions/NERC/CIP- 007 System Security Management/
Unsuccessful User Logins by Hour	This query gets the number of non-administrative successful user logins per hour.	/All Queries/ArcSight Solutions/NERC/CIP- 007 System Security Management/
Unsuccessful User Logins from Third Party Systems	This query retrieves failed logins using a non-administrative account, from assets categorized as Third Party.	/All Queries/ArcSight Solutions/NERC/CIP- 007 System Security Management/
Unsuccessful User Logins to High Impact BES Cyber Systems	This query retrieves failed logins with a non-administrator account to assets categorized as High Impact BES Cyber Systems.	/All Queries/ArcSight Solutions/NERC/CIP- 007 System Security Management/
Unsuccessful User Logins to Low Impact BES Cyber Systems	This query retrieves failed logins with a non-administrator account to assets categorized as Low Impact BES Cyber Systems.	/All Queries/ArcSight Solutions/NERC/CIP- 007 System Security Management/
Unsuccessful User Logins to Medium Impact BES Cyber Systems	This query retrieves failed logins with a non-administrator account to assets categorized as Medium Impact BES Cyber Systems.	/All Queries/ArcSight Solutions/NERC/CIP- 007 System Security Management/

Queries Resources, continued

Resource	Description	URI
Unsuccessful User Logins to Third Party Systems	This query retrieves failed logins with a non-administrator account to assets categorized as Third Party.	/All Queries/ArcSight Solutions/NERC/CIP- 007 System Security Management/
Unsuccessful VPN Access	This query lists all failed VPN access attempts.	/All Queries/ArcSight Solutions/NERC/CIP- 005 Electronic Security Perimeter (s)/
Unsuccessful High or Critical Configuration Changes	This query shows all unsuccessful non ArcSight internal high or critical configuration modifications.	/All Queries/ArcSight Solutions/NERC/CIP- 010 Configuration Change Management and Vulnerability/
User Group Creations	This query provides a listing of all Information User Groups that were created.	/All Queries/ArcSight Solutions/NERC/CIP- 004 Personnel and Training/
User Group Deletions	This query provides a listing of all Information User Groups that were deleted.	/All Queries/ArcSight Solutions/NERC/CIP- 004 Personnel and Training/
User Group Modifications	This query provides a listing of all Information User Groups that were modified.	/All Queries/ArcSight Solutions/NERC/CIP- 004 Personnel and Training/
Users Added to Groups	This query provides a listing of all Information of Users which added to Groups.	/All Queries/ArcSight Solutions/NERC/CIP- 004 Personnel and Training/
Users Removed from Groups	This query provides a listing of all Information of Users which removed from Groups.	/All Queries/ArcSight Solutions/NERC/CIP- 004 Personnel and Training/

Queries Resources, continued

Resource	Description	URI
Vulnerabilities - Trend Base	Retrieves all the vulnerabilities for the last hour. Used as trend base query for the vulnerabilities trend.	/All Queries/ArcSight Solutions/NERC/CIP- 010 Configuration Change Management and Vulnerability/
Vulnerabilities - on Trend	This query retrieves all the vulnerabilities for the last 14 days.	/All Queries/ArcSight Solutions/NERC/CIP- 010 Configuration Change Management and Vulnerability/
Vulnerabilities Summary	Provides overview of the vulnerability summary on NERC assets.	/All Queries/ArcSight Solutions/NERC/CIP- 010 Configuration Change Management and Vulnerability/
Vulnerabilities by IP Address	This report shows vulnerability overview by IP Address for the last 14 days	/All Queries/ArcSight Solutions/NERC/CIP- 010 Configuration Change Management and Vulnerability/
Vulnerabilities on New Assets	Retrieves all the vulnerabilities on new NERC assets.	/All Queries/ArcSight Solutions/NERC/CIP- 010 Configuration Change Management and Vulnerability/
Vulnerability Events By Scanner - on Trend	This Query shows vulnerability count per scanner for the last 14 days.	/All Queries/ArcSight Solutions/NERC/CIP- 010 Configuration Change Management and Vulnerability/
Vulnerability Scans - on Trend	This Query shows all the vulnerability scans for the last 14 days.	/All Queries/ArcSight Solutions/NERC/CIP- 010 Configuration Change Management and Vulnerability/

Queries Resources, continued

Resource	Description	URI
Weekly Trend - Configuration Changes by Address	This query shows the top configuration modifications by ip address	/All Queries/ArcSight Solutions/NERC/CIP- 010 Configuration Change Management and Vulnerability/
Weekly Trend - Configuration Changes by Name	This query shows the top configuration modifications.	/All Queries/ArcSight Solutions/NERC/CIP- 010 Configuration Change Management and Vulnerability/
Weekly Trend - Configuration Changes by User	This query shows the top configuration modifications .	/All Queries/ArcSight Solutions/NERC/CIP- 010 Configuration Change Management and Vulnerability/
Windows Domain Policy Changes	This query lists all the changes to Microsoft Domain Policy.	/All Queries/ArcSight Solutions/NERC/CIP- 010 Configuration Change Management and Vulnerability/
Windows Group Policy Changes	This query lists all the changes to Microsoft Active Directory.	/All Queries/ArcSight Solutions/NERC/CIP- 010 Configuration Change Management and Vulnerability/
Worm Activity	This query shows all worm activity.	/All Queries/ArcSight Solutions/NERC/CIP- 007 System Security Management/

Query Viewers

The following table lists all the query viewers.

Query Viewers Resources

Resource	Description	URI
Account Lockouts	This query viewer shows all account lockout events in the last hour. You can drill down on either the host address or the user name for more focused results.	/All Query Viewers/ArcSight Solutions/NERC/CIP-007 System Security Management/
All Events by New Hires	This query viewer shows all events by new hires.	/All Query Viewers/ArcSight Solutions/NERC/CIP-004 Personnel and Training/
CIP-002 Case Overview	This query viewer shows the number of open cases per stage for cases that have been created as a result of NERC CIP-002 rule actions.	/All Query Viewers/ArcSight Solutions/NERC/CIP-008 Incident Reporting and Response Planning/
CIP-003 Case Overview	This query viewer shows the number of open cases per stage for cases that have been created as a result of NERC CIP-003 rule actions.	/All Query Viewers/ArcSight Solutions/NERC/CIP-008 Incident Reporting and Response Planning/
CIP-004 Case Overview	This query viewer shows the number of open cases per stage for cases that have been created as a result of NERC CIP-004 rule actions.	/All Query Viewers/ArcSight Solutions/NERC/CIP-008 Incident Reporting and Response Planning/
CIP-005 Case Overview	This query viewer shows the number of open cases per stage for cases that have been created as a result of NERC CIP-005 rule actions.	/All Query Viewers/ArcSight Solutions/NERC/CIP-008 Incident Reporting and Response Planning/
CIP-006 Case Overview	This query viewer shows the number of open cases per stage for cases that have been created as a result of NERC CIP-006 rule actions.	/All Query Viewers/ArcSight Solutions/NERC/CIP-008 Incident Reporting and Response Planning/
CIP-007 Case Overview	This query viewer shows the number of open cases per stage for cases that have been created as a result of NERC CIP-007 rule actions.	/All Query Viewers/ArcSight Solutions/NERC/CIP-008 Incident Reporting and Response Planning/
CIP-008 Case Overview	This query viewer shows the number of open cases per stage for cases that have been created as a result of NERC CIP-008 rule actions.	/All Query Viewers/ArcSight Solutions/NERC/CIP-008 Incident Reporting and Response Planning/

Query Viewers Resources, continued

Resource	Description	URI
CIP-009 Case Overview	This query viewer shows the number of open cases per stage for cases that have been created as a result of NERC CIP-009 rule actions.	/All Query Viewers/ArcSight Solutions/NERC/CIP-008 Incident Reporting and Response Planning/
CIP-010 Case Overview	This query viewer shows the number of open cases per stage for cases that have been created as a result of NERC CIP-010 rule actions.	/All Query Viewers/ArcSight Solutions/NERC/CIP-008 Incident Reporting and Response Planning/
CIP-011 Case Overview	This query viewer shows the number of open cases per stage for cases that have been created as a result of NERC CIP-011 rule actions.	/All Query Viewers/ArcSight Solutions/NERC/CIP-008 Incident Reporting and Response Planning/
Count of Successful Administrative Logins in the Last 30 Days	This query viewer shows a count of successful administrative logins in the last 30 days, ordered by the most occurring logins.	/All Query Viewers/ArcSight Solutions/NERC/CIP-007 System Security Management/
Count of Unsuccessful Administrative Logins in the Last 30 Days	This query viewer shows a count of unsuccessful administrative logins in the last 30 days, ordered by the most occurring failures.	/All Query Viewers/ArcSight Solutions/NERC/CIP-007 System Security Management/
Dynamic Open Ports	This Query Viewer lists all dynamic open port events reported by vulnerability scanners.	/All Query Viewers/ArcSight Solutions/NERC/CIP-007 System Security Management/
Former Employee Accounts in Use	This query identifies all former employee user names and reporting device details associated with recent events.	/All Query Viewers/ArcSight Solutions/NERC/CIP-004 Personnel and Training/
Open Firewall Port Summary	This query viewer gives a summary of all the ports that are allowed to pass through various firewalls.	/All Query Viewers/ArcSight Solutions/NERC/CIP-005 Electronic Security Perimeter(s)/
Open Ports	This Query Viewer lists all open port events reported by vulnerability scanners.	/All Query Viewers/ArcSight Solutions/NERC/CIP-007 System Security Management/
Password Changes	This query viewer shows all password change events.	/All Query Viewers/ArcSight Solutions/NERC/CIP-007 System Security Management/
Suspicious Activities by New Hires	This query viewer shows all suspicious events by new hires in the last 2 hours.	/All Query Viewers/ArcSight Solutions/NERC/CIP-004 Personnel and Training/

Query Viewers Resources, continued

Resource	Description	URI
Top 10 Hosts with Most Unsuccessful Administrative Logins in the Last 2 Hours	This query viewer shows top 10 hosts with most unsuccessful administrative logins in the last 2 hours. It provides drill-downs by host name to detailed info about host's unsuccessful administrative logins .	/All Query Viewers/ArcSight Solutions/NERC/CIP-007 System Security Management/
Top Critical Vulnerabilities	This Query Viewer shows summary of top critical vulnerabilities , where the user can drill down to detailed information about those vulnerabilities.	/All Query Viewers/ArcSight Solutions/NERC/CIP-010 Configuration Change Management and Vulnerability/
Top Vulnerable IP Addresses	This query Shows top vulnerable IP addresses in bar chart format.	/All Query Viewers/ArcSight Solutions/NERC/CIP-010 Configuration Change Management and Vulnerability/
Unsecured Open Ports	This Query Viewer lists unsecure open port events reported by vulnerability scanners.	/All Query Viewers/ArcSight Solutions/NERC/CIP-007 System Security Management/
Unsuccessful Administrative Logins in the Last 2 Hours	This query viewer shows details of all unsuccessful administrative logins in the last 2 hours. It provides drill-downs into various fields.	/All Query Viewers/ArcSight Solutions/NERC/CIP-007 System Security Management/
Vulnerabilities	This Query Viewer shows all the vulnerabilities on NERC assets.	/All Query Viewers/ArcSight Solutions/NERC/CIP-010 Configuration Change Management and Vulnerability/
Vulnerability Events By Scanner	This Query Viewer shows vulnerability events count for each scanner.	/All Query Viewers/ArcSight Solutions/NERC/CIP-010 Configuration Change Management and Vulnerability/
Vulnerability Scans	This Query Viewer shows all the vulnerability scans for the last 14 days, where the user can drill down to all the vulnerabilities which pertains to specific scan .	/All Query Viewers/ArcSight Solutions/NERC/CIP-010 Configuration Change Management and Vulnerability/

Reports

The following table lists all the reports.

Reports Resources

Resource	Description	URI
Account Creations	This reports shows all account creations.	/All Reports/ArcSight Solutions/NERC/CIP-004 Personnel and Training/
Account Creations in Network Domain - Template	This report provides a listing of Information System accounts that were created in a specific network domain. The network domain has to be specified at report runtime. Assets have to be modeled in ESM and categorized with one or more Asset Categories under the /All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains group.	/All Reports/ArcSight Solutions/NERC/CIP-004 Personnel and Training/
Account Deletions	This reports shows all account deletions.	/All Reports/ArcSight Solutions/NERC/CIP-004 Personnel and Training/
Account Deletions in Network Domain - Template	This report provides a listing of Information System accounts that were deleted in a specific network domain. The network domain has to be specified at report runtime. Assets have to be modeled in ESM and categorized with one or more Asset Categories under the /All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains group.	/All Reports/ArcSight Solutions/NERC/CIP-004 Personnel and Training/
Account Lockouts per System	This report shows a count of account lockouts per system. It also shows the number of distinct user names that contributed to the total number of lockouts.	/All Reports/ArcSight Solutions/NERC/CIP-007 System Security Management/
Account Lockouts per User and System	This report shows a counts of account lockouts per user and system, and a chart of the total number of lockouts per user.	/All Reports/ArcSight Solutions/NERC/CIP-007 System Security Management/
Account Modifications	This reports shows all account modifications.	/All Reports/ArcSight Solutions/NERC/CIP-004 Personnel and Training/

Reports Resources, continued

Resource	Description	URI
Account Modifications in Network Domain - Template	This report provides a listing of Information System accounts that were modified in a specific network domain. The network domain has to be specified at report runtime. Assets have to be modeled in ESM and categorized with one or more Asset Categories under the /All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains group.	/All Reports/ArcSight Solutions/NERC/CIP-004 Personnel and Training/
Activity by Former Employees	This report shows any activity performed by users who are known to be terminated.	/All Reports/ArcSight Solutions/NERC/CIP-004 Personnel and Training/
Administrative Logins and Logouts per User	This report provides a listing of administrative logins and logouts per target or attacker user name.	/All Reports/ArcSight Solutions/NERC/CIP-007 System Security Management/
All Information Leaks	This report shows all activity that was flagged as information leakage.	/All Reports/ArcSight Solutions/NERC/CIP-011 Information Protection/
All Information Leaks from High Impact BES Cyber Systems	This report shows all activity that was flagged as information leakage on high impact BES cyber systems.	/All Reports/ArcSight Solutions/NERC/CIP-011 Information Protection/
All Information Leaks from Low Impact BES Cyber Systems	This report shows all activity that was flagged as information leakage on low impact BES cyber systems.	/All Reports/ArcSight Solutions/NERC/CIP-011 Information Protection/
All Information Leaks from Medium Impact BES Cyber Systems	This report shows all activity that was flagged as information leakage on medium impact BES cyber systems.	/All Reports/ArcSight Solutions/NERC/CIP-011 Information Protection/
All Password Change Events	This report provides a list of all password change events, ordered by the time in which they occurred.	/All Reports/ArcSight Solutions/NERC/CIP-007 System Security Management/

Reports Resources, continued

Resource	Description	URI
All User Logins per User	This report provides a listing of all logins for a particular user.	/All Reports/ArcSight Solutions/NERC/CIP- 007 System Security Management/
All VPN Access Attempts	This report lists all VPN access attempts.	/All Reports/ArcSight Solutions/NERC/CIP- 005 Electronic Security Perimeter (s)/
Anti-Virus Stopped or Paused in the Last Month	This report shows all events when a Anti-Virus is stopped or paused in the last month.	/All Reports/ArcSight Solutions/NERC/CIP- 007 System Security Management/
Application Brute Force Login Attempts	This report shows application brute force login attempts.	/All Reports/ArcSight Solutions/NERC/CIP- 007 System Security Management/
Application Configuration Modifications	This report shows any configuration modifications of any application on a system. Default time window: Last 24 hours.	/All Reports/ArcSight Solutions/NERC/CIP- 010 Configuration Change Management and Vulnerability/
Asset Creation by Location	This report provides a listing of newly created assets.	/All Reports/ArcSight Solutions/NERC/CIP- 002 BES Cyber System Categorization/
Asset Deletion by Location	This report provides a listing of deleted assets.	/All Reports/ArcSight Solutions/NERC/CIP- 002 BES Cyber System Categorization/
Asset Identification Report	This report shows all assets and their respective network domain.	/All Reports/ArcSight Solutions/NERC/CIP- 002 BES Cyber System Categorization/

Reports Resources, continued

Resource	Description	URI
Asset Modification by Location	This report provides a listing of modified assets.	/All Reports/ArcSight Solutions/NERC/CIP-002 BES Cyber System Categorization/
Assets Available to Third Parties by Domain	This report shows the assets that are available to third parties as defined by the assets available to 3rd parties asset category. This report is organized by network domain.	/All Reports/ArcSight Solutions/NERC/CIP-002 BES Cyber System Categorization/
Assets Available to Third-Parties by Criticality	This report shows the assets that are available to third parties as defined by the assets available to 3rd parties asset category. This report is organized by asset criticality.	/All Reports/ArcSight Solutions/NERC/CIP-002 BES Cyber System Categorization/
Assets by Network Domain (Creation Time) - Template	This report provides the listing of all the assets for the various Network Domains. This report may (and should) be focused based on the Network Domain of interest. Sorted by Creation time.	/All Reports/ArcSight Solutions/NERC/CIP-002 BES Cyber System Categorization/
Assets by Network Domain - Template	This report provides the listing of all the assets for the various Network Domains. This report may (and should) be focused based on the Network Domain of interest.	/All Reports/ArcSight Solutions/NERC/CIP-002 BES Cyber System Categorization/
Assets that Failed Technical Compliance Check	This report finds assets which failed the technical compliance check.	/All Reports/ArcSight Solutions/NERC/CIP-002 BES Cyber System Categorization/
Attacks and Suspicious Activities	This report shows a list of all attack and suspicious activity events.	/All Reports/ArcSight Solutions/NERC/CIP-008 Incident Reporting and Response Planning/

Reports Resources, continued

Resource	Description	URI
Attacks and Suspicious Activities on High Impact BES Cyber Systems	This report shows a list of all attack and suspicious activity events on high impact BES cyber systems.	/All Reports/ArcSight Solutions/NERC/CIP-008 Incident Reporting and Response Planning/
Attacks and Suspicious Activities on Low Impact BES Cyber Systems	This report shows a list of all attack and suspicious activity events on low impact BES cyber systems.	/All Reports/ArcSight Solutions/NERC/CIP-008 Incident Reporting and Response Planning/
Attacks and Suspicious Activities on Medium Impact BES Cyber Systems	This report shows a list of all attack and suspicious activity events on medium impact BES cyber systems.	/All Reports/ArcSight Solutions/NERC/CIP-008 Incident Reporting and Response Planning/
Attacks and Suspicious Activity Monthly Trend	This report displays a monthly overview of attack and suspicious activity events.	/All Reports/ArcSight Solutions/NERC/CIP-008 Incident Reporting and Response Planning/
Attacks and Suspicious Activity Weekly Trend	This report displays a weekly overview of attack and suspicious activity events.	/All Reports/ArcSight Solutions/NERC/CIP-008 Incident Reporting and Response Planning/
Attempted Default Vendor Accounts - Summary	This report shows summary views of events and systems when a vendor supplied user account is attempted by a user to login.	/All Reports/ArcSight Solutions/NERC/CIP-004 Personnel and Training/
Attempted Direct Root or Administrator	This report shows events and systems when direct root or administrator account is attempted by a user to login.	/All Reports/ArcSight Solutions/NERC/CIP-004 Personnel and Training/

Reports Resources, continued

Resource	Description	URI
Audit Log Cleared	This report shows all events where an audit log was cleared from a host.	/All Reports/ArcSight Solutions/NERC/CIP-010 Configuration Change Management and Vulnerability/
Audit Log Cleared per Attacker User Name	This report shows all events where an audit log was cleared by an attacker user name.	/All Reports/ArcSight Solutions/NERC/CIP-010 Configuration Change Management and Vulnerability/
Audit Log Cleared per Attacker and Target	This report shows all events where audit logs were cleared from a host by an attacker	/All Reports/ArcSight Solutions/NERC/CIP-010 Configuration Change Management and Vulnerability/
Audit Log Cleared per Target User Name	This report shows all events where an audit log was cleared by a target user name.	/All Reports/ArcSight Solutions/NERC/CIP-010 Configuration Change Management and Vulnerability/
Average Time to Resolution - By Case Severity	This report will show the Average Time to Resolution by Case Severity. It should be run once a week and reported to management.	/All Reports/ArcSight Solutions/NERC/CIP-008 Incident Reporting and Response Planning/
Average Time to Resolution - By Day	This report shows the average time to resolution of all the closed cases by day. This report should be run once a week and reported to management.	/All Reports/ArcSight Solutions/NERC/CIP-008 Incident Reporting and Response Planning/
Average Time to Resolution - By User	This report shows how long it is taking individuals to close their cases. This report should be run once a week and reported to management.	/All Reports/ArcSight Solutions/NERC/CIP-008 Incident Reporting and Response Planning/

Reports Resources, continued

Resource	Description	URI
Blocked Firewall Traffic from Assets in Network Domain - Template	This report provides a listing of the blocked outbound firewall traffic originating from assets in the indicated Network Domain of interest.	/A11 Reports/ArcSight Solutions/NERC/CIP-005 Electronic Security Perimeter (s)/
Blocked Firewall Traffic to Assets in Network Domain - Template	This report provides a listing of the blocked inbound firewall traffic directed at assets in the indicated Network Domain of interest.	/A11 Reports/ArcSight Solutions/NERC/CIP-005 Electronic Security Perimeter (s)/
CVSS Score Greater than or Equal to 8 Overview	This report provides overview of vulnerabilities with CVSS >=8 on the last 24 hours.	/A11 Reports/ArcSight Solutions/NERC/CIP-010 Configuration Change Management and Vulnerability/
Cases by Stage	This report provides an overview of all cases and their current stages.	/A11 Reports/ArcSight Solutions/NERC/CIP-008 Incident Reporting and Response Planning/
Classification of Assets	This report will show the asset classifications sorted by network domain.	/A11 Reports/ArcSight Solutions/NERC/CIP-002 BES Cyber System Categorization/
Configuration Changes to High Impact BES Cyber Systems	This report lists a count of successful configuration changes made to High Impact BES Cyber Systems .	/A11 Reports/ArcSight Solutions/NERC/CIP-010 Configuration Change Management and Vulnerability/
Configuration Changes to Low Impact BES Cyber Systems	This report lists a count of successful configuration changes made to low Impact BES Cyber Systems .	/A11 Reports/ArcSight Solutions/NERC/CIP-010 Configuration Change Management and Vulnerability/

Reports Resources, continued

Resource	Description	URI
Configuration Changes to Medium Impact BES Cyber Systems	This report lists a count of successful configuration changes made to Medium Impact BES Cyber Systems .	/All Reports/ArcSight Solutions/NERC/CIP-010 Configuration Change Management and Vulnerability/
Configuration Changes to Third Party Machines	This report lists a count of successful configuration changes made to third party systems.	/All Reports/ArcSight Solutions/NERC/CIP-010 Configuration Change Management and Vulnerability/
Count of Attacks and Suspicious Activities per Attacker Machine	This reports shows a count of attack and suspicious activity events per attacker machine.	/All Reports/ArcSight Solutions/NERC/CIP-008 Incident Reporting and Response Planning/
Count of Attacks and Suspicious Activities per Target Machine	This reports shows a count of attack and suspicious activity events per target machine.	/All Reports/ArcSight Solutions/NERC/CIP-008 Incident Reporting and Response Planning/
Count of Attacks and Suspicious Activity Event Names	This report displays a count of the event names of attack and suspicious activity events sorted by the most common events. It also displays the number of unique target machines that were affected by the event.	/All Reports/ArcSight Solutions/NERC/CIP-008 Incident Reporting and Response Planning/
Covert Channel Activity	This report shows all covert channel activity.	/All Reports/ArcSight Solutions/NERC/CIP-005 Electronic Security Perimeter (s)/
Critical Assets	This report lists all the critical assets. It can be used to gather the key assets to implement the business continuity process.	/All Reports/ArcSight Solutions/NERC/CIP-002 BES Cyber System Categorization/

Reports Resources, continued

Resource	Description	URI
Critical Assets	This report lists all the critical assets which have been categorized with a criticality of high or very-high. It can be used to identify key assets to implement the business continuity process.	/A11 Reports/ArcSight Solutions/NERC/CIP-009 Recovery Plans for BES Cyber Systems/
Criticality of Assets	This report will show the asset criticality sorted by their criticality and network domain.	/A11 Reports/ArcSight Solutions/NERC/CIP-002 BES Cyber System Categorization/
Detail Daily Unsuccessful Administrative Logins	This report shows a chart of top 20 unsuccessful administrative user names and a full listing of unsuccessful administrative login attempts in the last day.	/A11 Reports/ArcSight Solutions/NERC/CIP-007 System Security Management/
Detail Disallowed Port Access	This report shows traffic that should not be seen per the Allowed Ports/Disallowed Ports active list.	/A11 Reports/ArcSight Solutions/NERC/CIP-005 Electronic Security Perimeter (s)/
Detail Specific Default Vendor Account Uses	This report shows all logins using a specific vendor supplied user account.	/A11 Reports/ArcSight Solutions/NERC/CIP-004 Personnel and Training/
Development and Test Cross-Talk	This report shows all cross-talk in the last 24 hours between assets in Development category and assets in Test category.	/A11 Reports/ArcSight Solutions/NERC/CIP-005 Electronic Security Perimeter (s)/
Disallowed Port Access Summary	This report shows several summary aspects of traffic to disallowed ports.	/A11 Reports/ArcSight Solutions/NERC/CIP-005 Electronic Security Perimeter (s)/

Reports Resources, continued

Resource	Description	URI
DoS Attacks Weekly Trend	This report displays a weekly overview of DoS attack events.	/All Reports/ArcSight Solutions/NERC/CIP-008 Incident Reporting and Response Planning/
Dynamic Open Ports	This Report lists all dynamic open port events reported by vulnerability scanners.	/All Reports/ArcSight Solutions/NERC/CIP-007 System Security Management/
Email Attacks	This report shows all email attacks	/All Reports/ArcSight Solutions/NERC/CIP-005 Electronic Security Perimeter (s)/
Failed After Hours Building Accesses	This report shows the failed physical access of a building after business hours, regardless of whether the access was granted, or not. Actual time values are defined in the filter referenced in the 'Conditions' pane.	/All Reports/ArcSight Solutions/NERC/CIP-006 Physical Security of BES Cyber Systems/
Failed Anti-Virus Updates	This report shows all the failed Anti-Virus updates.	/All Reports/ArcSight Solutions/NERC/CIP-007 System Security Management/
Failed Building Access Events	This report shows failed attempts to enter a building at any time.	/All Reports/ArcSight Solutions/NERC/CIP-006 Physical Security of BES Cyber Systems/
Failed Password Changes	This report displays failed password change events.	/All Reports/ArcSight Solutions/NERC/CIP-007 System Security Management/
Failed or Attempted Removal of Access Rights	This report shows all the attempts or failed removal of access rights from a host resource. Removal could mean that either the user was removed from the system, or the privileges related to that ID were modified.	/All Reports/ArcSight Solutions/NERC/CIP-004 Personnel and Training/

Reports Resources, continued

Resource	Description	URI
Fault Logs	This report shows events indicating a process has failed to execute in the expected way.	/All Reports/ArcSight Solutions/NERC/CIP- 009 Recovery Plans for BES Cyber Systems/
File Creations on Third Party Accessible Systems	This report shows a count of all file creations on assets accessible to third parties.	/All Reports/ArcSight Solutions/NERC/CIP- 010 Configuration Change Management and Vulnerability/
File Deletions on Third Party Accessible Systems	This report shows a count of all file deletions on assets accessible to third parties.	/All Reports/ArcSight Solutions/NERC/CIP- 010 Configuration Change Management and Vulnerability/
File Modifications on Third Party Accessible Systems	This report shows a count of all file modifications on assets accessible to third parties.	/All Reports/ArcSight Solutions/NERC/CIP- 010 Configuration Change Management and Vulnerability/
File Related Activity on High Impact BES Cyber Systems	This report shows a count of all file activity on high impact BES cyber systems.	/All Reports/ArcSight Solutions/NERC/CIP- 010 Configuration Change Management and Vulnerability/
File Related Activity on Low Impact BES Cyber Systems	This report shows a count of all file activity on low impact BES cyber systems.	/All Reports/ArcSight Solutions/NERC/CIP- 010 Configuration Change Management and Vulnerability/
File Related Activity on Medium Impact BES Cyber Systems	This report shows a count of all file activity on medium impact BES cyber systems.	/All Reports/ArcSight Solutions/NERC/CIP- 010 Configuration Change Management and Vulnerability/

Reports Resources, continued

Resource	Description	URI
File Related Activity on Third Party Accessible Systems	This report shows a count of all file activity on assets accessible to third parties.	/All Reports/ArcSight Solutions/NERC/CIP-010 Configuration Change Management and Vulnerability/
Firewall Configuration Modification Summary	This report shows several top-level views related to firewall configuration modifications.	/All Reports/ArcSight Solutions/NERC/CIP-010 Configuration Change Management and Vulnerability/
Former Employee Account Access Attempt	This report lists all log-in activity from a former employee.	/All Reports/ArcSight Solutions/NERC/CIP-004 Personnel and Training/
Frequent Unsuccessful Logins by User Name	This report displays all user names for which there are a continuous set of unsuccessful login attempts.	/All Reports/ArcSight Solutions/NERC/CIP-007 System Security Management/
Frequent Unsuccessful Logins from Attacker Host	This report displays all attacker hosts from which a continuous set of unsuccessful login attempts have been occurring.	/All Reports/ArcSight Solutions/NERC/CIP-007 System Security Management/
Frequent Unsuccessful Logins to Target Host	This report lists all target hosts which have received a continuous set of unsuccessful login attempts.	/All Reports/ArcSight Solutions/NERC/CIP-007 System Security Management/
High Priority Events	This report shows events in which the Priority field is 10.	/All Reports/ArcSight Solutions/NERC/CIP-008 Incident Reporting and Response Planning/
High Priority Events on High Impact BES Cyber Systems	This report shows events in which the Priority field is 10 where the attacker or the target are in High Impact BES Cyber Systems .	/All Reports/ArcSight Solutions/NERC/CIP-008 Incident Reporting and Response Planning/

Reports Resources, continued

Resource	Description	URI
High Priority Events on Low Impact BES Cyber Systems	This report shows events in which the Priority field is 10 where the attacker or the target are in Low Impact BES Cyber Systems .	/A11 Reports/ArcSight Solutions/NERC/CIP-008 Incident Reporting and Response Planning/
High Priority Events on Medium Impact BES Cyber Systems	This report shows events in which the Priority field is 10 where the attacker or the target are in Medium Impact BES Cyber Systems .	/A11 Reports/ArcSight Solutions/NERC/CIP-008 Incident Reporting and Response Planning/
High to Low Classified Asset Communication	This report shows all the assets which are classified in a higher classification level which are communicating with a lower-classified asset.	/A11 Reports/ArcSight Solutions/NERC/CIP-011 Information Protection/
IM Traffic Summary	This report shows several high-level views of Instant Messaging traffic.	/A11 Reports/ArcSight Solutions/NERC/CIP-005 Electronic Security Perimeter (s)/
Inactive User Account Detected	This report shows all user names that are in the Stale Accounts active list.	/A11 Reports/ArcSight Solutions/NERC/CIP-004 Personnel and Training/
Inbound Insecure Transmissions	This report lists all inbound traffic deemed as inherently insecure. All such traffic is listed in the referenced filter.	/A11 Reports/ArcSight Solutions/NERC/CIP-005 Electronic Security Perimeter (s)/
Information Interception Activity	This report shows all information interception activity.	/A11 Reports/ArcSight Solutions/NERC/CIP-005 Electronic Security Perimeter (s)/

Reports Resources, continued

Resource	Description	URI
Information System Failures by Hosts	This report shows the information system which generated error log entries.	/A11 Reports/ArcSight Solutions/NERC/CIP-009 Recovery Plans for BES Cyber Systems/
Insecure Cryptographic Storage	This report shows all insecure cryptographic assets events identified in the last 24 hours.	/A11 Reports/ArcSight Solutions/NERC/CIP-011 Information Protection/
Insecure Transmissions	This report lists all traffic deemed as inherently insecure. All such traffic is listed in the referenced filter.	/A11 Reports/ArcSight Solutions/NERC/CIP-005 Electronic Security Perimeter (s)/
Intellectual Property Rights Violations	This report shows the different intellectual property rights violations.	/A11 Reports/ArcSight Solutions/NERC/CIP-003 Security Management Controls/
Intellectual Property Rights Violators	This report shows all the assets which violated intellectual property rights.	/A11 Reports/ArcSight Solutions/NERC/CIP-003 Security Management Controls/
Internal IM Senders	This report shows several high-level views of internal Instant Messaging senders.	/A11 Reports/ArcSight Solutions/NERC/CIP-005 Electronic Security Perimeter (s)/
Internal Insecure Service Providers	This report lists all internal providers of insecure services.	/A11 Reports/ArcSight Solutions/NERC/CIP-005 Electronic Security Perimeter (s)/

Reports Resources, continued

Resource	Description	URI
Internal Reconnaissance Sources	This report shows the top sources conducting internal reconnaissance.	/All Reports/ArcSight Solutions/NERC/CIP-008 Incident Reporting and Response Planning/
Internal Reconnaissance Top Events	This report shows the top events executed for internal reconnaissance.	/All Reports/ArcSight Solutions/NERC/CIP-008 Incident Reporting and Response Planning/
Internal Reconnaissance Top Targets	This report shows the top targets accessed by internal reconnaissance activity.	/All Reports/ArcSight Solutions/NERC/CIP-008 Incident Reporting and Response Planning/
Invalid or Expired Certificate	This report shows incidents which indicate that an invalid or expired certificate was detected.	/All Reports/ArcSight Solutions/NERC/CIP-011 Information Protection/
List of Firewall Configuration Modifications	This report shows any configuration modifications of any firewall.	/All Reports/ArcSight Solutions/NERC/CIP-010 Configuration Change Management and Vulnerability/
List of Network Device Configuration Modifications	This report shows any configuration modifications of any network equipment. Default time window: Last 24 hours.	/All Reports/ArcSight Solutions/NERC/CIP-010 Configuration Change Management and Vulnerability/
List of Network Routing Modifications	This report shows all router configuration modifications.	/All Reports/ArcSight Solutions/NERC/CIP-010 Configuration Change Management and Vulnerability/

Reports Resources, continued

Resource	Description	URI
Login Activity by Inactive Users	This report shows login activity by users that are on the Stale Accounts Active List. The report is ordered by the outcome of the login event.	/All Reports/ArcSight Solutions/NERC/CIP-004 Personnel and Training/
Low and High Impact BES Cyber Systems Cross-Talk	This report shows all cross-talk in the last 24 hours between assets in Low Impact BES Cyber Systems category and assets in High Impact BES Cyber Systems category.	/All Reports/ArcSight Solutions/NERC/CIP-005 Electronic Security Perimeter (s)/
Low and Medium Impact BES Cyber Systems Cross-Talk	This report shows all cross-talk in the last 24 hours between assets in Low Impact BES Cyber Systems category and assets in Medium Impact BES Cyber Systems category.	/All Reports/ArcSight Solutions/NERC/CIP-005 Electronic Security Perimeter (s)/
Low to High Classified Asset Communication	This report shows all the assets which are classified in a lower classification level which are communicating with a higher-classified asset.	/All Reports/ArcSight Solutions/NERC/CIP-011 Information Protection/
Machines Conducting Policy Breaches	This report shows machines which were involved in policy breaches.	/All Reports/ArcSight Solutions/NERC/CIP-003 Security Management Controls/
Malicious Code Sources	This report shows the internal sources of malicious code activities.	/All Reports/ArcSight Solutions/NERC/CIP-007 System Security Management/
Malware Activities	This report shows an overview of malware activities (including remediation).	/All Reports/ArcSight Solutions/NERC/CIP-007 System Security Management/
Malware Activity Summary	This report shows a summary of virus activities detected on systems, sorted by host.	/All Reports/ArcSight Solutions/NERC/CIP-007 System Security Management/

Reports Resources, continued

Resource	Description	URI
Medium and High Impact BES Cyber Systems Cross-Talk	This report shows all cross-talk in the last 24 hours between assets in High Impact BES Cyber Systems category and assets in Medium Impact BES Cyber Systems category.	/A11 Reports/ArcSight Solutions/NERC/CIP-005 Electronic Security Perimeter (s)/
Monthly Trend of Unsuccessful Administrative Logins	This report shows different aspects of the trend of unsuccessful administrative logins in the last 16 weeks.	/A11 Reports/ArcSight Solutions/NERC/CIP-007 System Security Management/
Network Device Configuration Modification Summary	This report shows several top-level views of configuration modifications of any network equipment.	/A11 Reports/ArcSight Solutions/NERC/CIP-010 Configuration Change Management and Vulnerability/
Network Routing Modification Summary	This report shows the top routers with routing configuration modifications, and top routing modifications.	/A11 Reports/ArcSight Solutions/NERC/CIP-010 Configuration Change Management and Vulnerability/
Number of Successful Administrative Logins by User and Host	This report shows the hourly number of successful administrative logins and a list of those logins, grouped by user and host information.	/A11 Reports/ArcSight Solutions/NERC/CIP-007 System Security Management/
Number of Successful User Logins over the Past Week	This report shows the number of successful user logins every day over the past week.	/A11 Reports/ArcSight Solutions/NERC/CIP-007 System Security Management/
Number of Successful User Logins per Hour over the Past Day	This report shows the number of successful user logins per hour.	/A11 Reports/ArcSight Solutions/NERC/CIP-007 System Security Management/
Number of Unsuccessful Administrative Logins by User and Host	This report shows the hourly number of unsuccessful administrative logins, and a listing of those attempts, grouped by user and host information.	/A11 Reports/ArcSight Solutions/NERC/CIP-007 System Security Management/

Reports Resources, continued

Resource	Description	URI
Number of Unsuccessful User Logins over the Past Month	This report shows the number of unsuccessful user logins every day over the past month.	/All Reports/ArcSight Solutions/NERC/CIP-007 System Security Management/
Number of Unsuccessful User Logins over the Past Week	This report shows the number of unsuccessful user logins every day over the past week.	/All Reports/ArcSight Solutions/NERC/CIP-007 System Security Management/
Number of Unsuccessful User Logins per Hour over the Past Day	This report shows the number of unsuccessful user logins every hour over the past day.	/All Reports/ArcSight Solutions/NERC/CIP-007 System Security Management/
Open Cases by CIP	This report shows all currently open cases by CIP.	/All Reports/ArcSight Solutions/NERC/CIP-008 Incident Reporting and Response Planning/
Open Cases by CIP and Severity	This report shows all currently open cases by CIP and Severity.	/All Reports/ArcSight Solutions/NERC/CIP-008 Incident Reporting and Response Planning/
Open Cases by Owner	This report provides a breakdown by owner of all open cases.	/All Reports/ArcSight Solutions/NERC/CIP-008 Incident Reporting and Response Planning/
Open Cases by Severity	This report shows all currently open cases by severity.	/All Reports/ArcSight Solutions/NERC/CIP-008 Incident Reporting and Response Planning/

Reports Resources, continued

Resource	Description	URI
Open Firewall Port Details	This report gives details of all the ports that are allowed to pass through various firewalls.	/All Reports/ArcSight Solutions/NERC/CIP-005 Electronic Security Perimeter (s)/
Open Ports	This report lists all open port events reported by vulnerability scanners.	/All Reports/ArcSight Solutions/NERC/CIP-007 System Security Management/
Operation System Modification Summary	This report shows several top-level views related to firewall configuration modifications.	/All Reports/ArcSight Solutions/NERC/CIP-010 Configuration Change Management and Vulnerability/
Operations and Development Cross-Talk	This report shows all cross-talk in the last 24 hours between assets in Operations category and assets in Development category.	/All Reports/ArcSight Solutions/NERC/CIP-005 Electronic Security Perimeter (s)/
Organizational Records Information Leaks	This report shows the communications which were classified as information leaks of organizational records.	/All Reports/ArcSight Solutions/NERC/CIP-011 Information Protection/
Passwords not Changed for Longer than Policy Standard	This report lists passwords that were not changed for longer than the policy standard.	/All Reports/ArcSight Solutions/NERC/CIP-007 System Security Management/
Personal Information Leaks	This report shows events which indicate a personal information leak.	/All Reports/ArcSight Solutions/NERC/CIP-011 Information Protection/
Policy Violations - Template	This report provides a listing of events categorized by ArcSight as policy violations which target the various Network Domains by Asset. This report may (and should) be focused based on the Network Domain of interest.	/All Reports/ArcSight Solutions/NERC/CIP-003 Security Management Controls/

Reports Resources, continued

Resource	Description	URI
Policy Violations from Third-Party Assets	This report provides a listing of events categorized by ArcSight as policy violations coming from assets categorized as Third-Party.	/All Reports/ArcSight Solutions/NERC/CIP-003 Security Management Controls/
Potential Vulnerabilities on New Assets	Shows vulnerabilities on new assets.	/All Reports/ArcSight Solutions/NERC/CIP-010 Configuration Change Management and Vulnerability/
Privileged Account Change Details	This report lists details of events when an Privileged account was attempted to be changed.	/All Reports/ArcSight Solutions/NERC/CIP-004 Personnel and Training/
Privileged VPN Remote Access Attempts	This report shows remote VPN connections attempts by an administrative account. The report is ordered by the connection outcome so you can easily distinguish the successful connections from the unsuccessful ones.	/All Reports/ArcSight Solutions/NERC/CIP-005 Electronic Security Perimeter (s)/
Redirection Attacks	This report shows all redirection attacks	/All Reports/ArcSight Solutions/NERC/CIP-005 Electronic Security Perimeter (s)/
Removable Media Activity	This report shows all the removable media activity for the last 24 hours using windows events .	/All Reports/ArcSight Solutions/NERC/CIP-010 Configuration Change Management and Vulnerability/
Resource Exhaustion Detected	This report shows the resources reaching their upper end of utilization (for capacity management and planning purposes).	/All Reports/ArcSight Solutions/NERC/CIP-009 Recovery Plans for BES Cyber Systems/

Reports Resources, continued

Resource	Description	URI
Services by Asset - Template	This report will show all successful access attempts.	/All Reports/ArcSight Solutions/NERC/CIP-002 BES Cyber System Categorization/
Shutdown of Critical Machines	This report shows all shutdown events of machines categorized as critical or highly critical.	/All Reports/ArcSight Solutions/NERC/CIP-009 Recovery Plans for BES Cyber Systems/
Shutdown of Machines	This report shows all machine shutdown events.	/All Reports/ArcSight Solutions/NERC/CIP-009 Recovery Plans for BES Cyber Systems/
Software Changes in High Impact BES Cyber Systems	This report shows all changes to any software installed in high impact BES cyber systems.	/All Reports/ArcSight Solutions/NERC/CIP-010 Configuration Change Management and Vulnerability/
Software Changes in Low Impact BES Cyber Systems	This report shows all changes to any software installed in low impact BES cyber Systems.	/All Reports/ArcSight Solutions/NERC/CIP-010 Configuration Change Management and Vulnerability/
Software Changes in Medium Impact BES Cyber Systems	This report shows all changes to any software installed in medium impact BES cyber systems.	/All Reports/ArcSight Solutions/NERC/CIP-010 Configuration Change Management and Vulnerability/
Software Changes in Operations	This report shows all changes to any software installed in the operations segment.	/All Reports/ArcSight Solutions/NERC/CIP-010 Configuration Change Management and Vulnerability/

Reports Resources, continued

Resource	Description	URI
Spyware Activities	This report shows an overview of spyware activities.	/All Reports/ArcSight Solutions/NERC/CIP- 007 System Security Management/
Successful Database Configuration Modification	This report shows all events on database configuration modification.	/All Reports/ArcSight Solutions/NERC/CIP- 010 Configuration Change Management and Vulnerability/
Successful Administrative Logins	This report provides a listing of successful administrative login attempts.	/All Reports/ArcSight Solutions/NERC/CIP- 007 System Security Management/
Successful Administrative Logins from Third Party Systems	This report displays all successful administrative logins from assets categorized as Third Party.	/All Reports/ArcSight Solutions/NERC/CIP- 007 System Security Management/
Successful Administrative Logins to High Impact BES Cyber Systems	This report displays all successful logins to assets categorized as High Impact BES Cyber Systems, that were done with an administrator account.	/All Reports/ArcSight Solutions/NERC/CIP- 007 System Security Management/
Successful Administrative Logins to Low Impact BES Cyber Systems	This report displays all successful logins to assets categorized as Low Impact BES Cyber Systems, that were done with an administrator account.	/All Reports/ArcSight Solutions/NERC/CIP- 007 System Security Management/
Successful Administrative Logins to Medium Impact BES Cyber Systems	This report displays all successful logins to assets categorized as Medium Impact BES Cyber Systems, that were done with an administrator account.	/All Reports/ArcSight Solutions/NERC/CIP- 007 System Security Management/
Successful Administrative Logins to Third Party Systems	This report displays all successful logins to assets categorized as Third Party, that were done with an administrator account.	/All Reports/ArcSight Solutions/NERC/CIP- 007 System Security Management/

Reports Resources, continued

Resource	Description	URI
Successful After Hours Building Accesses	This report shows the successful physical access of a building after business hours, regardless of whether the access was granted, or not. Actual time values are defined in the filter referenced in the 'Conditions' pane.	/All Reports/ArcSight Solutions/NERC/CIP-006 Physical Security of BES Cyber Systems/
Successful Brute Force Logins	This report provides a listing of events categorized by ArcSight as probable successful brute force login attempts. This report may (and should) be focused based on the Network Domain of interest.	/All Reports/ArcSight Solutions/NERC/CIP-007 System Security Management/
Successful Building Access Events	This report shows successful building access events at all times.	/All Reports/ArcSight Solutions/NERC/CIP-006 Physical Security of BES Cyber Systems/
Successful Changes to Operating Systems	This report displays the number of times changes were made to operating systems.	/All Reports/ArcSight Solutions/NERC/CIP-010 Configuration Change Management and Vulnerability/
Successful Default Vendor Account Used - Summary	This report shows high level summary views of events when a vendor-supplied user account is used to login.	/All Reports/ArcSight Solutions/NERC/CIP-004 Personnel and Training/
Successful High or Critical Configuration Changes	This report shows all successful non ArcSight internal high or critical configuration modifications.	/All Reports/ArcSight Solutions/NERC/CIP-010 Configuration Change Management and Vulnerability/
Successful Password Changes	This report displays successful password change events.	/All Reports/ArcSight Solutions/NERC/CIP-007 System Security Management/
Successful Removal of Access Rights	This report shows the removal of access rights from a host resource. Removal could mean that either the user was removed from the system, or the privileges related to that ID were modified.	/All Reports/ArcSight Solutions/NERC/CIP-004 Personnel and Training/

Reports Resources, continued

Resource	Description	URI
Successful User Logins	This report provides a listing of successful user login attempts.	/A11 Reports/ArcSight Solutions/NERC/CIP- 007 System Security Management/
Successful User Logins from Third Party Systems	This report displays all successful non-administrative logins from assets categorized as Third Party.	/A11 Reports/ArcSight Solutions/NERC/CIP- 007 System Security Management/
Successful User Logins to High Impact BES Cyber Systems	This report displays all successful non-administrative logins to assets categorized as High Impact BES Cyber Systems.	/A11 Reports/ArcSight Solutions/NERC/CIP- 007 System Security Management/
Successful User Logins to Low Impact BES Cyber Systems	This report displays all successful non-administrative logins to assets categorized as Low Impact BES Cyber Systems.	/A11 Reports/ArcSight Solutions/NERC/CIP- 007 System Security Management/
Successful User Logins to Medium Impact BES Cyber Systems	This report displays all successful non-administrative logins to assets categorized as Medium Impact BES Cyber Systems.	/A11 Reports/ArcSight Solutions/NERC/CIP- 007 System Security Management/
Successful User Logins to Third Party Systems	This report displays all successful non-administrative logins to assets categorized as Third Party.	/A11 Reports/ArcSight Solutions/NERC/CIP- 007 System Security Management/
Summary of Suspicious Activity by New Hires	This report shows a summary of attacks and suspicious events by new hires.	/A11 Reports/ArcSight Solutions/NERC/CIP- 004 Personnel and Training/
Suspicious Activity by New Hires	This report displays all the identified suspicious activity performed by new users.	/A11 Reports/ArcSight Solutions/NERC/CIP- 004 Personnel and Training/

Reports Resources, continued

Resource	Description	URI
Systems Accessed by Default Vendor Accounts	This report shows all systems that users have tried to access as a default vendor account.	/A11 Reports/ArcSight Solutions/NERC/CIP-004 Personnel and Training/
Test and Operations Cross-Talk	This report shows all cross-talk in the last 24 hours between assets in Test category and assets in Operations category.	/A11 Reports/ArcSight Solutions/NERC/CIP-005 Electronic Security Perimeter (s)/
Third-Party Access	This report shows all access attempts to third party assets.	/A11 Reports/ArcSight Solutions/NERC/CIP-005 Electronic Security Perimeter (s)/
Top 10 Vulnerabilities	Shows the top 10 vulnerabilities on NERC assets.	/A11 Reports/ArcSight Solutions/NERC/CIP-010 Configuration Change Management and Vulnerability/
Top 10 Vulnerabilities - High Impact BES Cyber Systems	This report shows the top 10 vulnerabilities on High Impact NERC assets.	/A11 Reports/ArcSight Solutions/NERC/CIP-010 Configuration Change Management and Vulnerability/
Top 10 Vulnerabilities - Low Impact BES Cyber Systems	This report shows the top 10 vulnerabilities on Low Impact NERC assets.	/A11 Reports/ArcSight Solutions/NERC/CIP-010 Configuration Change Management and Vulnerability/
Top 10 Vulnerabilities - Medium Impact BES Cyber Systems	This report shows the top 10 vulnerabilities on Medium Impact NERC assets.	/A11 Reports/ArcSight Solutions/NERC/CIP-010 Configuration Change Management and Vulnerability/

Reports Resources, continued

Resource	Description	URI
Top 10 Vulnerable Assets	Shows the top 10 vulnerable systems.	/All Reports/ArcSight Solutions/NERC/CIP-010 Configuration Change Management and Vulnerability/
Top 10 Vulnerable Assets - High Impact BES Cyber Systems	This report shows the top 10 vulnerable systems on high impact BES cyber assets .	/All Reports/ArcSight Solutions/NERC/CIP-010 Configuration Change Management and Vulnerability/
Top 10 Vulnerable Assets - Low Impact BES Cyber Systems	This report shows the top 10 vulnerable systems on low impact BES cyber assets .	/All Reports/ArcSight Solutions/NERC/CIP-010 Configuration Change Management and Vulnerability/
Top 10 Vulnerable Assets - Medium Impact BES Cyber Systems	This report shows the top 10 vulnerable systems on medium impact BES cyber assets .	/All Reports/ArcSight Solutions/NERC/CIP-010 Configuration Change Management and Vulnerability/
Top 10 Vulnerable Assets - Public Facing	This report shows the top 10 vulnerable systems on public facing assets.	/All Reports/ArcSight Solutions/NERC/CIP-010 Configuration Change Management and Vulnerability/
Top 10 Vulnerable Assets - Third Party	This report shows the top 10 vulnerable systems on third party assets.	/All Reports/ArcSight Solutions/NERC/CIP-010 Configuration Change Management and Vulnerability/
Top 20 Policy Breach Events	This report shows the top 20 policy breach events.	/All Reports/ArcSight Solutions/NERC/CIP-003 Security Management Controls/

Reports Resources, continued

Resource	Description	URI
Top DoS Attackers	This report shows a list of top attackers responsible for initiating denial of service attacks.	/All Reports/ArcSight Solutions/NERC/CIP-008 Incident Reporting and Response Planning/
Top DoS Targets	This report shows hosts which were targeted the most with a denial of service attack.	/All Reports/ArcSight Solutions/NERC/CIP-008 Incident Reporting and Response Planning/
Traffic Anomaly on Application Layer	This report shows traffic anomaly on application layer.	/All Reports/ArcSight Solutions/NERC/CIP-005 Electronic Security Perimeter (s)/
Traffic Anomaly on Network Layer	This report shows traffic anomaly on network layer.	/All Reports/ArcSight Solutions/NERC/CIP-005 Electronic Security Perimeter (s)/
Traffic Anomaly on Transport Layer	This report shows traffic anomaly on transport layer.	/All Reports/ArcSight Solutions/NERC/CIP-005 Electronic Security Perimeter (s)/
Traffic Between High Impact BES Systems and External	This report shows two tables. The first showing a count of events representing traffic from high impact BES cyber systems to external sources. The second table shows a count of events representing traffic from external to high impact BES cyber system. The count is shown for each source-destination pair and for each device.	/All Reports/ArcSight Solutions/NERC/CIP-005 Electronic Security Perimeter (s)/
Traffic Between Internal and External Sources - All	This report shows two tables. The first showing a count of events representing traffic from internal to external sources. The second table shows a count of events representing traffic from external to internal sources. The count is shown for each source-destination pair and for each device.	/All Reports/ArcSight Solutions/NERC/CIP-005 Electronic Security Perimeter (s)/

Reports Resources, continued

Resource	Description	URI
Traffic Between Low Impact BES Systems and External	This report shows two tables. The first showing a count of events representing traffic from low impact BES cyber systems to external sources. The second table shows a count of events representing traffic from external to low impact BES cyber system. The count is shown for each source-destination pair and for each device.	/A11 Reports/ArcSight Solutions/NERC/CIP-005 Electronic Security Perimeter (s)/
Traffic Between Medium Impact BES Systems and External	This report shows two tables. The first showing a count of events representing traffic from medium impact BES cyber systems to external sources. The second table shows a count of events representing traffic from external to medium impact BES cyber system. The count is shown for each source-destination pair and for each device.	/A11 Reports/ArcSight Solutions/NERC/CIP-005 Electronic Security Perimeter (s)/
Traffic Between Zones	This report shows the target ports between zones.	/A11 Reports/ArcSight Solutions/NERC/CIP-005 Electronic Security Perimeter (s)/
Traffic Coming from Dark Address Space	This report shows all traffic from a dark address range targeting systems. This should be considered very suspicious.	/A11 Reports/ArcSight Solutions/NERC/CIP-005 Electronic Security Perimeter (s)/
Traffic to Dark Address Space	This report shows all traffic directed to a dark address range. This should be considered very suspicious.	/A11 Reports/ArcSight Solutions/NERC/CIP-005 Electronic Security Perimeter (s)/
Unencrypted Services by Host Name	Returns all unencrypted services by a particular host name identified in the last 24 hours.	/A11 Reports/ArcSight Solutions/NERC/CIP-011 Information Protection/
Unsecured Open Ports	This report lists unsecured open port events reported by vulnerability scanners.	/A11 Reports/ArcSight Solutions/NERC/CIP-007 System Security Management/
Unsuccessful Administrative Logins	This report provides a listing of unsuccessful administrative login attempts.	/A11 Reports/ArcSight Solutions/NERC/CIP-007 System Security Management/

Reports Resources, continued

Resource	Description	URI
Unsuccessful Administrative Logins from Third Party Systems	This report displays all failed logins with an administrative account from assets categorized as Third Party.	/All Reports/ArcSight Solutions/NERC/CIP-007 System Security Management/
Unsuccessful Administrative Logins to High Impact BES Cyber Systems	This report displays all failed logins with an administrative account to assets categorized as High Impact BES Cyber Systems.	/All Reports/ArcSight Solutions/NERC/CIP-007 System Security Management/
Unsuccessful Administrative Logins to Low Impact BES Cyber Systems	This report displays all failed logins with an administrative account to assets categorized as Low Impact BES Cyber Systems.	/All Reports/ArcSight Solutions/NERC/CIP-007 System Security Management/
Unsuccessful Administrative Logins to Medium Impact BES Cyber Systems	This report displays all failed logins with an administrative account to assets categorized as Medium Impact BES Cyber Systems.	/All Reports/ArcSight Solutions/NERC/CIP-007 System Security Management/
Unsuccessful Administrative Logins to Third Party Systems	This report displays all failed logins with an administrative account to assets categorized as Third Party.	/All Reports/ArcSight Solutions/NERC/CIP-007 System Security Management/
Unsuccessful Changes to Operating Systems	This report lists a count of unsuccessful changes attempted on operating systems.	/All Reports/ArcSight Solutions/NERC/CIP-010 Configuration Change Management and Vulnerability/
Unsuccessful High or Critical Configuration Changes	This report shows all unsuccessful non ArcSight internal high or critical configuration modifications.	/All Reports/ArcSight Solutions/NERC/CIP-010 Configuration Change Management and Vulnerability/
Unsuccessful User Logins	This report provides a listing of unsuccessful user login attempts.	/All Reports/ArcSight Solutions/NERC/CIP-007 System Security Management/

Reports Resources, continued

Resource	Description	URI
Unsuccessful User Logins from Third Party Systems	This report displays all failed logins with a non-administrative account from assets categorized as Third Party.	/A11 Reports/ArcSight Solutions/NERC/CIP-007 System Security Management/
Unsuccessful User Logins to High Impact BES Cyber Systems	This report displays all failed logins with a non-administrative account to assets categorized as High Impact BES Cyber Systems.	/A11 Reports/ArcSight Solutions/NERC/CIP-007 System Security Management/
Unsuccessful User Logins to Low Impact BES Cyber Systems	This report displays all failed logins with a non-administrative account to assets categorized as Low Impact BES Cyber Systems.	/A11 Reports/ArcSight Solutions/NERC/CIP-007 System Security Management/
Unsuccessful User Logins to Medium Impact BES Cyber Systems	This report displays all failed logins with a non-administrative account to assets categorized as Medium Impact BES Cyber Systems.	/A11 Reports/ArcSight Solutions/NERC/CIP-007 System Security Management/
Unsuccessful User Logins to Third Party Systems	This report displays all failed logins with a non-administrative account to assets categorized as Third Party.	/A11 Reports/ArcSight Solutions/NERC/CIP-007 System Security Management/
Unsuccessful VPN Access	This report provides a listing of failed VPN access, the number of such failed events and the last failure time.	/A11 Reports/ArcSight Solutions/NERC/CIP-005 Electronic Security Perimeter (s)/
User Group Account Creations	This reports shows all user group creations.	/A11 Reports/ArcSight Solutions/NERC/CIP-004 Personnel and Training/
User Group Account Deletions	This reports shows all user group deletions.	/A11 Reports/ArcSight Solutions/NERC/CIP-004 Personnel and Training/

Reports Resources, continued

Resource	Description	URI
User Group Account Modifications	This reports shows all user group modifications.	/All Reports/ArcSight Solutions/NERC/CIP-004 Personnel and Training/
Users Added to Groups	This reports shows all user accounts added to groups.	/All Reports/ArcSight Solutions/NERC/CIP-004 Personnel and Training/
Users Removed from Groups	This reports shows all users accounts removed from groups.	/All Reports/ArcSight Solutions/NERC/CIP-004 Personnel and Training/
Virus Activities	This report shows a summary of virus activities detected on systems sorted by virus.	/All Reports/ArcSight Solutions/NERC/CIP-007 System Security Management/
Vulnerabilities by IP Address	Displays vulnerability overview by IP Address for the last 14 days.	/All Reports/ArcSight Solutions/NERC/CIP-010 Configuration Change Management and Vulnerability/
Vulnerability Summary	This report provides overview of the vulnerability summary in the last 24 hours.	/All Reports/ArcSight Solutions/NERC/CIP-010 Configuration Change Management and Vulnerability/
Weekly Trend - Configuration Modification Summary	This report shows several top-level views related to firewall configuration modifications.	/All Reports/ArcSight Solutions/NERC/CIP-010 Configuration Change Management and Vulnerability/

Reports Resources, continued

Resource	Description	URI
Windows Domain Policy Changes	This report displays changes to Microsoft Domain Policy for the last 24 hours.	/All Reports/ArcSight Solutions/NERC/CIP-010 Configuration Change Management and Vulnerability/
Windows Group Policy Changes	This report displays changes to Microsoft Active Directory for the last 24 hours.	/All Reports/ArcSight Solutions/NERC/CIP-010 Configuration Change Management and Vulnerability/
Worm Activity Summary	This report shows a summary of worm activities detected on systems, sorted by host.	/All Reports/ArcSight Solutions/NERC/CIP-007 System Security Management/

Rules

The following table lists all the rules.

Rules Resources

Resource	Description	URI
Account Lockout	This rule detects account lockouts. This activity is suspicious.	/All Rules/ArcSight Solutions/NERC/CIP-007 System Security Management/
After Hours Building Access by Contractors	This rule detects building access events after business hours by contractors.	/All Rules/ArcSight Solutions/NERC/CIP-006 Physical Security of BES Cyber Systems/
Audit Log Cleared	This rule monitors for events on clearing of the audit log on Windows systems.	/All Rules/ArcSight Solutions/NERC/CIP-010 Configuration Change Management and Vulnerability/
Badged Out Employee	This rule detects when someone leaves a building and adds the user to the Badged Out active list.	/All Rules/ArcSight Solutions/NERC/CIP-006 Physical Security of BES Cyber Systems/

Rules Resources, continued

Resource	Description	URI
Brute Force Login Attempts	This rule identifies brute force login attempts.	/All Rules/ArcSight Solutions/NERC/CIP-007 System Security Management/
Compliance Score Update	This rule is triggered by other CIP rules and updates the Compliance Score active list.	/All Rules/ArcSight Solutions/NERC/Overview/
Consecutive Unsuccessful Logins to Administrative Account	This rule fires when it notices a set of 10 consecutive unsuccessful logins by an attacker and target user name pair within 5 minutes .	/All Rules/ArcSight Solutions/NERC/CIP-007 System Security Management/
Critical Network Device Configuration Change Detected	This rule triggers when a network device configuration change is detected and has Very-High agent severity. devices includes : Firewalls VPNs Network Equipments Network Routings Network Intrusion Detection Systems	/All Rules/ArcSight Solutions/NERC/CIP-010 Configuration Change Management and Vulnerability/
Critical Operating System Change Detected	Triggers when operating system change is detected on critical asset and has Very-High agent severity.	/All Rules/ArcSight Solutions/NERC/CIP-010 Configuration Change Management and Vulnerability/
Critical Vulnerability Detected	This rule triggers when a critical vulnerability is detected.	/All Rules/ArcSight Solutions/NERC/CIP-010 Configuration Change Management and Vulnerability/
Disallowed Ports Access	This rule triggers when traffic to a forbidden target port occurs.	/All Rules/ArcSight Solutions/NERC/CIP-005 Electronic Security Perimeter(s)/
DoS Detected	This rule looks for DoS .	/All Rules/ArcSight Solutions/NERC/CIP-007 System Security Management/

Rules Resources, continued

Resource	Description	URI
Failed Building Access	This rule detects failed physical building access.	/All Rules/ArcSight Solutions/NERC/CIP-006 Physical Security of BES Cyber Systems/
Former Employee Account Activity	This rule looks for any activity of users that have been placed on the Former Employees active list. This rule creates a case for each unique user name that is attempted in the ArcSight Solutions/Compliance Insight Package folder in the case tree.	/All Rules/ArcSight Solutions/NERC/CIP-004 Personnel and Training/
Former Employee Account Detected	This rule detects events that list former employee accounts. When triggered, the rule adds as well as deletes users from the appropriate active lists.	/All Rules/ArcSight Solutions/NERC/CIP-004 Personnel and Training/
Former Employee User Account Access Attempt	This rule detects any authentication event, whether failed or successful, where the username has been placed on the Former Employees active list. This rule creates a case in the ArcSight Solutions folder in the case tree for each unique user name that is attempted.	/All Rules/ArcSight Solutions/NERC/CIP-004 Personnel and Training/
Frequent Unsuccessful Logins by User Name	This rule fires when it notices the same user is responsible for a continuous set of unsuccessful logins.	/All Rules/ArcSight Solutions/NERC/CIP-007 System Security Management/
Frequent Unsuccessful Logins from Attacker Host	This rule fires when it notices a continuous set of unsuccessful logins from the same attacker host.	/All Rules/ArcSight Solutions/NERC/CIP-007 System Security Management/
Frequent Unsuccessful Logins to Target Host	This rule fires when it notices a high frequency of unsuccessful logins on the same target host.	/All Rules/ArcSight Solutions/NERC/CIP-007 System Security Management/
High to Low Classified Traffic Information Leak	This rule looks for information leak events which originated from a high-security classified system.	/All Rules/ArcSight Solutions/NERC/CIP-011 Information Protection/
Inactive User Account Detected	This rule fires every time an entry ages out of the Stale Accounts active list.	/All Rules/ArcSight Solutions/NERC/CIP-004 Personnel and Training/
Information Security Incident	This rule fires for various kinds of information security incidents such as malicious code activities, denial of service attacks and policy violations.	/All Rules/ArcSight Solutions/NERC/CIP-008 Incident Reporting and Response Planning/

Rules Resources, continued

Resource	Description	URI
Information System Failures of Highly Critical Machine	This rule looks for information system failure events from highly critical machines.	/All Rules/ArcSight Solutions/NERC/CIP-009 Recovery Plans for BES Cyber Systems/
Intellectual Property Rights Violation	This rule looks for intellectual property rights violations. The filter references should be configured to contain all the events pertaining to this use-case. The filter is located in the My Filters group.	/All Rules/ArcSight Solutions/NERC/CIP-003 Security Management Controls/
Internal Insecure Service Provider Detected	This rule detects when insecure protocols, such as Telnet or RSH, are used inside the network. When triggered, it adds an entry to the Internal Systems with Insecure Services active list.	/All Rules/ArcSight Solutions/NERC/CIP-005 Electronic Security Perimeter(s)/
Internal Recon Detected	This rule looks for internal reconnaissance activity.	/All Rules/ArcSight Solutions/NERC/CIP-008 Incident Reporting and Response Planning/
Local Logon from Badged Out Employee	This rule detects a local logon event though the employee is badged out.	/All Rules/ArcSight Solutions/NERC/CIP-006 Physical Security of BES Cyber Systems/
Login Activity by a Stale Account	This rule identifies login activities by accounts that are on the Stale Accounts active list.	/All Rules/ArcSight Solutions/NERC/CIP-004 Personnel and Training/
Malware or Spyware Detected	This rule triggers when a spyware or malware activity is reported by either an Intrusion Detection System (IDS) or an anti-virus application.	/All Rules/ArcSight Solutions/NERC/CIP-007 System Security Management/
Manual Status Change	This rule is triggered when a section's status on the Compliance Risk Score dashboard is changed manually.	/All Rules/ArcSight Solutions/NERC/Overview/
Multiple Cases Created on Short Period	This rule triggers when multiple cases created on short period of time.	/All Rules/ArcSight Solutions/NERC/CIP-008 Incident Reporting and Response Planning/
New Hire Identification	This rule looks for newly created or renamed user accounts. It writes the new user names to the New Hire Accounts active list.	/All Rules/ArcSight Solutions/NERC/CIP-004 Personnel and Training/
New Host Detected	This rule triggers when new hosts are found on the network.	/All Rules/ArcSight Solutions/NERC/CIP-002 BES Cyber System Categorization/

Rules Resources, continued

Resource	Description	URI
New Service Detected	This rule fires when new services are found on machines.	/All Rules/ArcSight Solutions/NERC/CIP-002 BES Cyber System Categorization/
Organizational Data Information Leak	This rule looks for any organizational information being sent out of the corporate network.	/All Rules/ArcSight Solutions/NERC/CIP-011 Information Protection/
Overflow Vulnerabilities	This rule triggers when an overflow vulnerability is detected.	/All Rules/ArcSight Solutions/NERC/CIP-010 Configuration Change Management and Vulnerability/
Password not Changed for Longer than Policy Standard	This rule fires when an entry expires out of the referenced active list, signifying that the new (default) password was not changed within the prescribed time. Time limit is defined by the TTL in the active list.	/All Rules/ArcSight Solutions/NERC/CIP-007 System Security Management/
Personal Information Leak	This rule looks for any personal information being sent out of the corporate network.	/All Rules/ArcSight Solutions/NERC/CIP-011 Information Protection/
Policy Violations	This rule looks for policy violations.	/All Rules/ArcSight Solutions/NERC/CIP-003 Security Management Controls/
Possible Covert Channel	This rule looks for events indicating a covert channel is being used.	/All Rules/ArcSight Solutions/NERC/CIP-005 Electronic Security Perimeter(s)/
Possible Email Attack	This rule looks for attacks where email activity involved .	/All Rules/ArcSight Solutions/NERC/CIP-005 Electronic Security Perimeter(s)/
Possible Information Interception	This rule looks for attacks where information could be redirected and collected by an unintended party.	/All Rules/ArcSight Solutions/NERC/CIP-005 Electronic Security Perimeter(s)/
Possible Redirection Attack	This rule looks for attacks where information could be redirected .	/All Rules/ArcSight Solutions/NERC/CIP-005 Electronic Security Perimeter(s)/

Rules Resources, continued

Resource	Description	URI
Possible Traffic Anomaly	This rule looks for attacks where information could be redirected and collected by an unintended party.	/All Rules/ArcSight Solutions/NERC/CIP-005 Electronic Security Perimeter(s)/
Potential Distributed DoS	This rule looks for Potential Distributed DoS .	/All Rules/ArcSight Solutions/NERC/CIP-007 System Security Management/
Privileged Account Change	This rule fires whenever an access/authorization change is attempted to be made to an administrative account. A case is created for each such incident.	/All Rules/ArcSight Solutions/NERC/CIP-004 Personnel and Training/
Removal of Access Rights	This rule triggers when events indicating the following are detected: 1). Either a user is removed from a host, or 2). User's authentication privileges are modified.	/All Rules/ArcSight Solutions/NERC/CIP-004 Personnel and Training/
Resource Exhaustion of Highly Critical Machine	This rule looks for Resource Exhaustion events from highly critical machines.	/All Rules/ArcSight Solutions/NERC/CIP-009 Recovery Plans for BES Cyber Systems/
SSL Vulnerabilities	This rule triggers when SSL vulnerability is detected.	/All Rules/ArcSight Solutions/NERC/CIP-010 Configuration Change Management and Vulnerability/
Security Patch Missing	This rule triggers when a security patch missing vulnerability is detected.	/All Rules/ArcSight Solutions/NERC/CIP-010 Configuration Change Management and Vulnerability/
Security Software Stopped or Paused	This rule triggers when a security software service has been disabled.	/All Rules/ArcSight Solutions/NERC/CIP-007 System Security Management/
Severely Attacked System	This rule looks for an accumulation in attacks targeting a single machine.	/All Rules/ArcSight Solutions/NERC/CIP-008 Incident Reporting and Response Planning/
Shutdown of Highly Critical Machine	This rule looks for shutdown events from highly critical machines.	/All Rules/ArcSight Solutions/NERC/CIP-009 Recovery Plans for BES Cyber Systems/

Rules Resources, continued

Resource	Description	URI
Successful Attack - Brute Force Login	This rule detects successful brute force login attacks.	/All Rules/ArcSight Solutions/NERC/CIP-007 System Security Management/
Successful Badge In	This rule identifies when an employee badges in and puts the badge id and other information on the Badged In active list.	/All Rules/ArcSight Solutions/NERC/CIP-006 Physical Security of BES Cyber Systems/
Successful Badge Out	This rule detects when someone leaves a building and removes the user from the badged in active list.	/All Rules/ArcSight Solutions/NERC/CIP-006 Physical Security of BES Cyber Systems/
Successful Default Vendor Account Used	This rule looks for successful access to system using default user accounts.	/All Rules/ArcSight Solutions/NERC/CIP-004 Personnel and Training/
Successful Password Change	This rule detects when a user's password is changed. This rule will then take the user name off the list where it was kept to track whether or not the default password was changed.	/All Rules/ArcSight Solutions/NERC/CIP-007 System Security Management/
Suspicious Activities by New Hires	This rule identifies suspicious activity by new hires.	/All Rules/ArcSight Solutions/NERC/CIP-004 Personnel and Training/
Suspicious Internal Trojan Detected	This rule triggers when there are trojan events coming from inside the network or successful trojan events from outside the network.	/All Rules/ArcSight Solutions/NERC/CIP-007 System Security Management/
Unsuccessful Logins to Multiple Administrative Accounts	This rule fires when it notices a set of 20 continuous unsuccessful logins by different administrative attacker and target user pairs within 5 minutes .	/All Rules/ArcSight Solutions/NERC/CIP-007 System Security Management/
User Logged in - Added to Active Accounts List	This rule adds a user account to the Active Users session list upon a successful login.	/All Rules/ArcSight Solutions/NERC/CIP-004 Personnel and Training/
Vulnerabilities on Critical Machine	This rule triggers when a vulnerability is detected on critical machine.	/All Rules/ArcSight Solutions/NERC/CIP-010 Configuration Change Management and Vulnerability/

Rules Resources, continued

Resource	Description	URI
Wireless Malicious Traffic Detected	This rule detects when wireless malicious traffic is detected.	/All Rules/ArcSight Solutions/NERC/CIP-005 Electronic Security Perimeter(s)/
Worm Detected	This rule triggers when a worm is reported by either an Intrusion Detection System (IDS) or an anti-virus application.	/All Rules/ArcSight Solutions/NERC/CIP-007 System Security Management/
XSRF Vulnerabilities	This rule triggers when XSRF vulnerability is detected.	/All Rules/ArcSight Solutions/NERC/CIP-010 Configuration Change Management and Vulnerability/
XSS Vulnerabilities	This rule triggers when XSS vulnerability is detected.	/All Rules/ArcSight Solutions/NERC/CIP-010 Configuration Change Management and Vulnerability/

Trends

The following table lists all the trends.

Trends Resources

Resource	Description	URI
Attacks and Suspicious Activities Trend	This trend stores long term aggregated information about attacks and suspicious activity events.	/All Trends/ArcSight Solutions/NERC/CIP-008 Incident Reporting and Response Planning/
Case History	This trend stores all case audit events.	/All Trends/ArcSight Solutions/NERC/CIP-008 Incident Reporting and Response Planning/
Configuration Changes	This Trend collects hourly data using the "Configuration Changes - Trend Base" query. Used by other queries to show configuration changes.	/All Trends/ArcSight Solutions/NERC/CIP-010 Configuration Change Management and Vulnerability/
Count of Administrative Logins	This trend stores a count of successful and unsuccessful administrative logins.	/All Trends/ArcSight Solutions/NERC/CIP-007 System Security Management/

Trends Resources, continued

Resource	Description	URI
Daily Trend of Anti-Virus Stopped or Paused Events	This daily trend stores all events when a Anti-Virus service is stopped or paused.	/All Trends/ArcSight Solutions/NERC/CIP-007 System Security Management/
DoS Attacks Trend	This trend stores long term aggregated information about DoS attack events.	/All Trends/ArcSight Solutions/NERC/CIP-008 Incident Reporting and Response Planning/
Failed Administrative Logins - Long Term Trend	This trend stores long term information about failed administrative logins.	/All Trends/ArcSight Solutions/NERC/CIP-007 System Security Management/
User Login Count	This trend stores a daily count of user login attempts.	/All Trends/ArcSight Solutions/NERC/CIP-007 System Security Management/
Vulnerabilities	This Trend collects hourly data using the "Vulnerabilities - Trend Base" query. Feeds query viewers related to vulnerabilities shown under CIP-010.	/All Trends/ArcSight Solutions/NERC/CIP-010 Configuration Change Management and Vulnerability/

Use Cases

The following table lists all the use cases.

Use Cases Resources

Resource	Description	URI
Account Creations, Deletions, and Modifications	This use case provides information about account management activities.	/All Use Cases/ArcSight Solutions/NERC/
Account Lockouts	This use case displays account lockout events. By default, the use case is configured to display only Microsoft Windows and ArcSight ESM lockout events. Additional configuration is required.	/All Use Cases/ArcSight Solutions/NERC/
Administrator Logins and Logouts	This use case provides information about the administrative logins and logouts.	/All Use Cases/ArcSight Solutions/NERC/
Anti-Virus Activity	This use case provides insight into Anti-Virus activity on the organization.	/All Use Cases/ArcSight Solutions/NERC/

Use Cases Resources, continued

Resource	Description	URI
Asset Activity	This use case provides information about the kinds of activities in which assets are engaging (like creations ,deletions ,modifications of assets) .	/All Use Cases/ArcSight Solutions/NERC/
Attacks and Suspicious Activity	This use case provides information about events that are identified as attacks or suspicious activity.	/All Use Cases/ArcSight Solutions/NERC/
Audit Log Cleared	This use case provides information about events that occur when an audit log is cleared or modified manually.	/All Use Cases/ArcSight Solutions/NERC/
BES Cyber Systems Login Activity	This use case identifies and reports logins to BES Cyber systems .	/All Use Cases/ArcSight Solutions/NERC/
Brute Force Logins	This use case identifies and provides information about brute force login attempts. The brute force login attempts can either be identified by rules in this use case or by Intrusion Detection Systems.	/All Use Cases/ArcSight Solutions/NERC/
Changes to Privileges Accounts	This use case provides information about changes made to privilege accounts.	/All Use Cases/ArcSight Solutions/NERC/
Covert Channel Activity	This use case report on covert channel activity, such sending TCP traffic over an ICMP channel.	/All Use Cases/ArcSight Solutions/NERC/
Default Vendor Accounts	This use case provides information about logins using default vendor accounts.	/All Use Cases/ArcSight Solutions/NERC/
Disallowed Ports	This use case provides information about connections to non-allowed ports.	/All Use Cases/ArcSight Solutions/NERC/
DoS Attacks	This use case provides an insight into denial of service attacks.	/All Use Cases/ArcSight Solutions/NERC/
Email Attacks	This use case provides information about email attacks.	/All Use Cases/ArcSight Solutions/NERC/
Firewall Traffic Overview	This use case reports on various firewall traffic controls namely blocked inbound and outbound traffic and open ports in the enterprise.	/All Use Cases/ArcSight Solutions/NERC/
Former Employee Account Activity	This user case provides information about any activity performed by users who are known to be terminated.	/All Use Cases/ArcSight Solutions/NERC/

Use Cases Resources, continued

Resource	Description	URI
High Risk Events	This use case displays an overview of the events that require most attention.	/All Use Cases/ArcSight Solutions/NERC/
IM Traffic	The purpose of this use case is to provide information about IM messaging usage inside the network.	/All Use Cases/ArcSight Solutions/NERC/
Inactive User Account Detected	The purpose of this use case is to identify user accounts that have not been active for a certain period of time, and to then identify activity from such stale accounts.	/All Use Cases/ArcSight Solutions/NERC/
Incident Management	The Incident Management use case provides information and metrics about cases opened and closed in this Compliance Insight Package including stage, severity, time to resolution .	/All Use Cases/ArcSight Solutions/NERC/
Information Interception	This use case identifies and reports on possible kinds of information interception events incidents such as spoofing attempts, man-in-the-middle attacks or instant messaging.	/All Use Cases/ArcSight Solutions/NERC/
Information Leakage	This use case identifies and reports on all kinds of information leaks that may have occurred.	/All Use Cases/ArcSight Solutions/NERC/
Information System Failures	This use case identifies information system errors and resource exhaustions.	/All Use Cases/ArcSight Solutions/NERC/
Insecure Communications	This use case provides information about unencrypted and thus insecure communications inside the network.	/All Use Cases/ArcSight Solutions/NERC/
Intellectual Property Rights Violations	This use case provides information about Intellectual Property Rights Violations.	/All Use Cases/ArcSight Solutions/NERC/
Internal Reconnaissance Activity	This use case identifies and reports all reconnaissance activities conducted by internal hosts.	/All Use Cases/ArcSight Solutions/NERC/
Invalid Certificates	This use case provides insight into incidents where an invalid or expired Public Key Infrastructure (PKI) certificate was detected.	/All Use Cases/ArcSight Solutions/NERC/
Malicious Code Activity	The Malicious Code Activity use case monitors for malicious code (such as DoS activities, viruses, worms, trojans, or backdoor activities) on the network, allowing administrators to quickly remediate infected machines.	/All Use Cases/ArcSight Solutions/NERC/
Monitoring File Changes	This use case provides information about file activity .	/All Use Cases/ArcSight Solutions/NERC/

Use Cases Resources, continued

Resource	Description	URI
Network Equipments Changes	This use case provides information about changes to firewalls and network equipments.	/All Use Cases/ArcSight Solutions/NERC/
Operating System Configuration Changes	se case provides information about changes related to operating systems like domain changes and group policy changes .	/All Use Cases/ArcSight Solutions/NERC/
Password Management	The purpose of this use case is to monitor password change events as well as to alert if a password has not been changed for a longer time than allowed by policy.	/All Use Cases/ArcSight Solutions/NERC/
Physical Access	This use case detects violations and reports on events related to physical security devices such as badge readers. Specifically, it detects after hour building access by contractors and local Logon from badged out employees.	/All Use Cases/ArcSight Solutions/NERC/
Policy Violations	This use case provides information about policy violations.	/All Use Cases/ArcSight Solutions/NERC/
Port Activity	This use case provides information about port activity on the organization .	/All Use Cases/ArcSight Solutions/NERC/
Redirection Attacks	This use case provides information about redirection attacks.	/All Use Cases/ArcSight Solutions/NERC/
Removable Media Activity	This use case provides information about removable media activity.	/All Use Cases/ArcSight Solutions/NERC/
Removal of Access Rights	This use case provides information about all activities when an access right of a user is removed.	/All Use Cases/ArcSight Solutions/NERC/
Startup and Shutdown of Machines	The Startup and Shutdown of Machines use case identifies when machines are shut down in your environment.	/All Use Cases/ArcSight Solutions/NERC/
Suspicious Activity by New Hires	The purpose of this use case is to identify suspicious activities by recently hired employees.	/All Use Cases/ArcSight Solutions/NERC/
Third Party Access	This use case identifies and reports logins to and from third-party systems.	/All Use Cases/ArcSight Solutions/NERC/
Traffic Anomaly	This use case provides information about the traffic anomaly.	/All Use Cases/ArcSight Solutions/NERC/

Use Cases Resources, continued

Resource	Description	URI
Traffic Between Entities	This use case provides information about the traffic flowing between various network entities (like zones, external, internal ,operation ,development ,High/Medium/Low Impact BES cyber systems)	/All Use Cases/ArcSight Solutions/NERC/
User Group Activity	This use case provides information about user groups activities.	/All Use Cases/ArcSight Solutions/NERC/
User Logins and Logouts	This use case provides insight into login and logout activity for non-administrative users.	/All Use Cases/ArcSight Solutions/NERC/
VPN Access Reporting	This use case provides insight into VPN access events.	/All Use Cases/ArcSight Solutions/NERC/
Vulnerability Overview	This use case provides information about vulnerabilities.	/All Use Cases/ArcSight Solutions/NERC/

Appendix A: Supported Devices for Solution for NERC CIP v6.0 Reports

This appendix provides a list of devices that are capable of generating events to populate the Solution for NERC CIP reports and other resources. The device categories listed in the columns of the table below are capable of generating events to populate the listed reports. However, it is possible that not all products in the device category generate the required events. For example, CheckPoint NG firewalls may generate events that populate certain reports, but the Cisco Pix firewalls do not, even though they are both listed under the firewall category. It is possible that even though a device is capable of generating certain event types, it will not do so frequently and therefore it may take a long time for the event to appear. Some Solution for NERC CIP reports do not rely on the event data generated by devices to populate the report. Instead these reports use other types of data such as zones, user names, asset categorization, cases, and IP addresses to populate the reports. Some reports use a combination of event data and this additional data. For each Solution for NERC CIP report, the device categories indicated in the table are not the only devices that are capable of generating events that will populate it, but are the major and most likely sources for such events.

The following table lists the supported devices that may generate events used by Solution for NERC CIP reports and other resources.

Report Name	IDS/IP S	NBA D	D B	O S	F W	VP N	V A	ID M	P M	N E	CS/W F	A V	W	AP P	PS S	Comment
Asset Creation by Location							x									
Asset Deletion by Location							x									

Report Name	IDS/IPS	NBA	DB	OS	FW	VPN	VA	IDM	PM	NE	CS/WF	AV	W	AP	PS	Comment
Asset Identification Report																There is no specific input device required to populate this report. This report relies on how assets are defined and/or categorized.
Asset Modification by Location							x							x		
Assets Available to Third Parties by Domain																There is no specific input device required to populate this report. This report relies on how assets are defined and/or categorized.

Report Name	IDS/IP S	NBA D	D B	O S	F W	VP N	V A	ID M	P M	N E	CS/W F	A V	W	AP P	PS S	Comment
Assets Available to Third-Parties by Criticality																There is no specific input device required to populate this report. This report relies on how assets are defined and/or categorized.
Assets by Network Domain (Creation Time) - Template																There is no specific input device required to populate this report. This report relies on how assets are defined and/or categorized.
Assets by Network Domain - Template																There is no specific input device required to populate this report. This report relies on how assets are defined and/or categorized.

Report Name	IDS/IP S	NBA D	D B	O S	F W	VP N	V A	ID M	P M	N E	CS/W F	A V	W	AP P	PS S	Comment
Assets that Failed Technical Compliance Check							x									
Classification of Assets																There is no specific input device required to populate this report. This report relies on how assets are defined and/or categorized.
Critical Assets																There is no specific input device required to populate this report. This report relies on how assets are defined and/or categorized.

Report Name	IDS/IP S	NBA D	D B	O S	F W	VP N	V A	ID M	P M	N E	CS/W F	A V	W	AP P	PS S	Comment
Criticality of Assets																There is no specific input device required to populate this report. This report relies on how assets are defined and/or categorized.
Services by Asset - Template	x			x	x	x			x	x	x	x				
Intellectual Property Rights Violations	x	x									x					
Intellectual Property Rights Violators	x	x									x					
Machines Conducting Policy Breaches	x	x			x		x		x	x	x	x	x	x		
Policy Violations - Template	x	x		x	x	x		x	x	x	x	x	x			
Policy Violations from Third-Party Assets	x	x		x	x	x		x	x	x	x	x	x			
Top 20 Policy Breach Events	x	x		x	x	x		x	x	x	x	x	x			
Account Creations	x	x	x	x	x	x	x	x	x	x	x	x	x	x		

Report Name	IDS/IP S	NBA D	D B	O S	F W	VP N	V A	ID M	P M	N E	CS/W F	A V	W	AP P	PS S	Comment
Account Creations in Network Domain - Template	x	x	x	x	x	x	x	x	x	x	x	x	x	x		
Account Deletions	x	x	x	x	x	x	x	x	x	x	x	x	x	x		
Account Deletions in Network Domain - Template	x	x	x	x	x	x	x	x	x	x	x	x	x	x		
Account Modifications	x	x	x	x	x	x	x	x	x	x	x	x	x	x		
Account Modifications in Network Domain - Template	x	x	x	x	x	x	x	x	x	x	x	x	x	x		
Activity by Former Employees	x	x	x	x	x	x	x	x	x	x	x	x	x	x		
Attempted Default Vendor Accounts - Summary	x		x	x	x				x							
Attempted Direct Root or Administrator	x		x	x	x				x							
Detail Specific Default Vendor Account Uses	x		x	x	x				x							
Failed or Attempted Removal of Access Rights	x		x	x	x	x		x	x		x	x		x		

Report Name	IDS/IP S	NBA D	D B	O S	F W	VP N	V A	ID M	P M	N E	CS/W F	A V	W	AP P	PS S	Comment
Former Employee Account Access Attempt	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	
Inactive User Account Detected	x		x	x	x	x		x	x	x				x	x	
Login Activity by Inactive Users	x		x	x	x	x		x	x	x				x	x	
Privileged Account Change Details	x		x	x	x	x		x	x		x	x		x		
Successful Default Vendor Account Used - Summary	x		x	x	x					x						
Successful Removal of Access Rights	x		x	x	x	x		x	x		x	x		x		
Summary of Suspicious Activity by New Hires	x				x				x		x	x		x		
Suspicious Activity by New Hires	x				x				x		x	x		x		
Systems Accessed by Default Vendor Accounts	x		x	x	x					x						
User Group Account Creations				x										x		
User Group Account Deletions				x										x		

Report Name	IDS/IPS	NBA D	D B	O S	F W	VP N	V A	ID M	P M	N E	CS/W F	A V	W	AP P	PS S	Comment
User Group Account Modifications				x										x		
Users Added to Groups				x										x		
Users Removed from Groups				x										x		
All VPN Access Attempts					x	x										
Blocked Firewall Traffic from Assets in Network Domain - Template					x											
Blocked Firewall Traffic to Assets in Network Domain - Template					x											
Covert Channel Activity	x	x							x		x					
Detail Disallowed Port Access					x					x						
Development and Test Cross-Talk	x	x		x	x					x						
Disallowed Port Access Summary					x					x						
Email Attacks	x	x		x	x						x		x	x		
IM Traffic Summary	x	x			x					x	x					

Report Name	IDS/IPS	NBA D	D B	O S	F W	VP N	V A	ID M	P M	N E	CS/W F	A V	W	AP P	PS S	Comment
Inbound Insecure Transmissions	x		x	x					x							
Information Interception Activity	x	x			x	x					x		x			
Insecure Transmissions	x			x	x					x						
Internal IM Senders	x	x			x					x	x					
Internal Insecure Service Providers	x			x	x	x	x		x	x	x	x				
Low and High Impact BES Cyber Systems Cross-Talk																There is no specific input device required to populate this report. This report relies on how assets are defined and/or categorized.
Low and Medium Impact BES Cyber Systems Cross-Talk																There is no specific input device required to populate this report. This report relies on how assets are defined and/or categorized.

Report Name	IDS/IP S	NBA D	D B	O S	F W	VP N	V A	ID M	P M	N E	CS/W F	A V	W	AP P	PS S	Comment
Medium and High Impact BES Cyber Systems Cross-Talk																There is no specific input device required to populate this report. This report relies on how assets are defined and/or categorized.
Open Firewall Port Details					x											
Operations and Development Cross-Talk																There is no specific input device required to populate this report. This report relies on how assets are defined and/or categorized.
Privileged VPN Remote Access Attempts					x	x										
Redirection Attacks	x	x			x						x	x				

Report Name	IDS/IP S	NBA D	D B	O S	F W	VP N	V A	ID M	P M	N E	CS/W F	A V	W	AP P	PS S	Comment
Test and Operations Cross-Talk																There is no specific input device required to populate this report. This report relies on how assets are defined and/or categorized.
Third-Party Access	x		x	x	x	x		x		x				x		
Traffic Anomaly on Application Layer	x	x			x						x			x		
Traffic Anomaly on Network Layer	x	x			x					x						
Traffic Anomaly on Transport Layer	x	x			x					x						
Traffic Between High Impact BES Systems and External	x				x	x				x						
Traffic Between Internal and External Sources - All	x				x	x				x						
Traffic Between Low Impact BES Systems and External	x				x	x				x						

Report Name	IDS/IP S	NBA D	D B	O S	F W	VP N	V A	ID M	P M	N E	CS/W F	A V	W	AP P	PS S	Comment
Traffic Between Medium Impact BES Systems and External	x				x	x				x						
Traffic Between Zones	x				x	x				x						
Traffic Coming from Dark Address Space	x				x	x				x						
Traffic to Dark Address Space	x				x	x				x						
Unsuccessful VPN Access					x	x										
Failed After Hours Building Accesses															x	
Failed Building Access Events															x	
Successful After Hours Building Accesses															x	
Successful Building Access Events															x	
Account Lockouts per System				x												
Account Lockouts per User and System				x												

Report Name	IDS/IP S	NBA D	D B	O S	F W	VP N	V A	ID M	P M	N E	CS/W F	A V	W	AP P	PS S	Comment
Administrative Logins and Logouts per User			x	x	x	x		x	x	x	x		x	x	x	
All Password Change Events	x		x	x	x	x								x		
All User Logins per User			x	x	x	x		x	x	x	x		x	x	x	
Anti-Virus Stopped or Paused in the Last Month												x				
Application Brute Force Login Attempts	x			x												
Detail Daily Unsuccessful Administrative Logins			x	x	x	x		x	x	x	x		x	x	x	
Dynamic Open Ports							x									
Failed Anti-Virus Update												x				
Failed Password Changes	x		x	x	x	x								x		
Frequent Unsuccessful Logins by User Name			x	x	x	x		x	x	x	x		x	x	x	
Frequent Unsuccessful Logins from Attacker Host			x	x	x	x		x	x	x	x		x	x	x	
Frequent Unsuccessful Logins to Target Host			x	x	x	x		x	x	x	x		x	x	x	

Report Name	IDS/IP S	NBA D	D B	O S	F W	VP N	V A	ID M	P M	N E	CS/W F	A V	W	AP P	PS S	Comment
Malicious Code Sources	x	x			x				x		x	x				
Malware Activities	x	x			x				x		x	x				
Malware Activity Summary	x	x			x				x		x	x				
Monthly Trend of Unsuccessful Administrative Logins			x	x	x	x		x	x	x	x		x	x	x	
Number of Successful Administrative Logins by User and Host			x	x	x	x		x	x	x	x		x	x	x	
Number of Successful User Logins over the Past Week			x	x	x	x		x	x	x	x		x	x	x	
Number of Successful User Logins per Hour over the Past Day			x	x	x	x		x	x	x	x		x	x	x	
Number of Unsuccessful Administrative Logins by User and Host			x	x	x	x		x	x	x	x		x	x	x	
Number of Unsuccessful User Logins over the Past Month			x	x	x	x		x	x	x	x		x	x	x	
Number of Unsuccessful User Logins over the Past Week			x	x	x	x		x	x	x	x		x	x	x	

Report Name	IDS/IP S	NBA D	D B	O S	F W	VP N	V A	ID M	P M	N E	CS/W F	A V	W	AP P	PS S	Comment
Number of Unsuccessful User Logins per Hour over the Past Day			x	x	x	x		x	x	x	x		x	x	x	
Open Ports							x									
Passwords not Changed for Longer than Policy Standard				x												
Spyware Activities	x	x			x				x		x	x				
Successful Administrative Logins			x	x	x	x		x	x	x	x		x	x	x	
Successful Administrative Logins from Third Party Systems			x	x	x	x		x	x	x	x		x	x	x	
Successful Administrative Logins to High Impact BES Cyber Systems			x	x	x	x		x	x	x	x		x	x	x	
Successful Administrative Logins to Low Impact BES Cyber Systems			x	x	x	x		x	x	x	x		x	x	x	
Successful Administrative Logins to Medium Impact BES Cyber Systems			x	x	x	x		x	x	x	x		x	x	x	

Report Name	IDS/IPS	NBA D	D B	O S	F W	VP N	V A	ID M	P M	N E	CS/W F	A V	W	AP P	PS S	Comment
Successful Administrative Logins to Third Party Systems			x	x	x	x		x	x	x	x		x	x	x	
Successful Brute Force Logins	x															
Successful Password Changes	x		x	x	x	x								x		
Successful User Logins			x	x	x	x		x	x	x	x		x	x	x	
Successful User Logins from Third Party Systems			x	x	x	x		x	x	x	x		x	x	x	
Successful User Logins to High Impact BES Cyber Systems			x	x	x	x		x	x	x	x		x	x	x	
Successful User Logins to Low Impact BES Cyber Systems			x	x	x	x		x	x	x	x		x	x	x	
Successful User Logins to Medium Impact BES Cyber Systems			x	x	x	x		x	x	x	x		x	x	x	
Successful User Logins to Third Party Systems			x	x	x	x		x	x	x	x		x	x	x	
Unsecured Open Ports							x									
Unsuccessful Administrative Logins			x	x	x	x		x	x	x	x		x	x	x	

Report Name	IDS/IP S	NBA D	D B	O S	F W	VP N	V A	ID M	P M	N E	CS/W F	A V	W	AP P	PS S	Comment
Unsuccessful Administrative Logins from Third Party Systems			x	x	x	x		x	x	x	x		x	x	x	
Unsuccessful Administrative Logins to High Impact BES Cyber Systems			x	x	x	x		x	x	x	x		x	x	x	
Unsuccessful Administrative Logins to Low Impact BES Cyber Systems			x	x	x	x		x	x	x	x		x	x	x	
Unsuccessful Administrative Logins to Medium Impact BES Cyber Systems			x	x	x	x		x	x	x	x		x	x	x	
Unsuccessful Administrative Logins to Third Party Systems			x	x	x	x		x	x	x	x		x	x	x	
Unsuccessful User Logins			x	x	x	x		x	x	x	x		x	x	x	
Unsuccessful User Logins from Third Party Systems			x	x	x	x		x	x	x	x		x	x	x	
Unsuccessful User Logins to High Impact BES Cyber Systems			x	x	x	x		x	x	x	x		x	x	x	

Report Name	IDS/IPS	NBA D	D B	O S	F W	VP N	V A	ID M	P M	N E	CS/W F	A V	W	AP P	PS S	Comment
Unsuccessful User Logins to Low Impact BES Cyber Systems			x	x	x	x		x	x	x	x		x	x	x	
Unsuccessful User Logins to Medium Impact BES Cyber Systems			x	x	x	x		x	x	x	x		x	x	x	
Unsuccessful User Logins to Third Party Systems			x	x	x	x		x	x	x	x		x	x	x	
Virus Activities												x				
Worm Activity Summary											x	x				
Attacks and Suspicious Activities	x	x			x				x	x	x	x	x	x		
Attacks and Suspicious Activities on High Impact BES Cyber Systems	x	x			x				x	x	x	x	x	x		
Attacks and Suspicious Activities on Low Impact BES Cyber Systems	x	x			x				x	x	x	x	x	x		
Attacks and Suspicious Activities on Medium Impact BES Cyber Systems	x	x			x				x	x	x	x	x	x		

Report Name	IDS/IP S	NBA D	D B	O S	F W	VP N	V A	ID M	P M	N E	CS/W F	A V	W	AP P	PS S	Comment
Attacks and Suspicious Activity Monthly Trend	x	x			x				x	x	x	x	x	x		
Attacks and Suspicious Activity Weekly Trend	x	x			x				x	x	x	x	x	x		
Average Time to Resolution - By Case Severity																There is no specific input device required to populate this report. This report relies on data from the case groups
Average Time to Resolution - By Day																There is no specific input device required to populate this report. This report relies on data from the case groups
Average Time to Resolution - By User																There is no specific input device required to populate this report. This report relies on data from the case groups

Report Name	IDS/IPS	NBA D	D B	O S	F W	VP N	V A	ID M	P M	N E	CS/W F	A V	W	AP P	PS S	Comment
Cases by Stage																There is no specific input device required to populate this report. This report relies on data from the case groups
Count of Attacks and Suspicious Activities per Attacker Machine	x	x			x				x	x	x	x	x	x		
Count of Attacks and Suspicious Activities per Target Machine	x	x			x				x	x	x	x	x	x		
Count of Attacks and Suspicious Activity Event Names	x	x			x				x	x	x	x	x	x		
DoS Attacks Weekly Trend	x	x	x		x					x			x			
High Priority Events	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	
High Priority Events on High Impact BES Cyber Systems	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	
High Priority Events on Low Impact BES Cyber Systems	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	

Report Name	IDS/IPS	NBA D	D B	O S	F W	VP N	V A	ID M	P M	N E	CS/W F	A V	W	AP P	PS S	Comment
High Priority Events on Medium Impact BES Cyber Systems	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	
Internal Reconnaissance Sources	x	x			x						x					
Internal Reconnaissance Top Events	x	x			x						x					
Internal Reconnaissance Top Targets	x	x			x						x					
Open Cases by CIP																There is no specific input device required to populate this report. This report relies on data from the case groups
Open Cases by CIP and Severity																There is no specific input device required to populate this report. This report relies on data from the case groups

Report Name	IDS/IP S	NBA D	D B	O S	F W	VP N	V A	ID M	P M	N E	CS/W F	A V	W	AP P	PS S	Comment
Open Cases by Owner																There is no specific input device required to populate this report. This report relies on data from the case groups
Open Cases by Severity																There is no specific input device required to populate this report. This report relies on data from the case groups
Top DoS Attackers	x	x	x		x					x			x			
Top DoS Targets	x	x	x		x					x			x			
Critical Assets																There is no specific input device required to populate this report. This report relies on how assets are defined and/or categorized.
Fault Logs	x	x	x	x	x	x	x	x	x	x	x	x	x	x		

Report Name	IDS/IP S	NBA D	D B	O S	F W	VP N	V A	ID M	P M	N E	CS/W F	A V	W	AP P	PS S	Comment
Information System Failures by Hosts	x	x	x	x	x	x	x	x	x	x	x	x	x	x		
Resource Exhaustion Detected	x	x	x	x	x	x			x	x	x	x	x	x		
Shutdown of Critical Machines				x												
Shutdown of Machines				x												
Application Configuration Modifications	x		x	x	x	x		x	x		x	x	x	x		
Audit Log Cleared	x	x		x	x											
Audit Log Cleared per Attacker User Name	x	x		x	x											
Audit Log Cleared per Attacker and Target	x	x		x	x											
Audit Log Cleared per Target User Name	x	x		x	x											
CVSS Score Greater than or Equal to 8 Overview							x									
Configuration Changes to High Impact BES Cyber Systems	x	x	x	x	x	x	x	x	x	x	x	x	x	x		

Report Name	IDS/IPS	NBA D	D B	O S	F W	VP N	V A	ID M	P M	N E	CS/W F	A V	W	AP P	PS S	Comment
Configuration Changes to Low Impact BES Cyber Systems	x	x	x	x	x	x	x	x	x	x	x	x	x	x		
Configuration Changes to Medium Impact BES Cyber Systems	x	x	x	x	x	x	x	x	x	x	x	x	x	x		
Configuration Changes to Third Party Machines	x	x	x	x	x	x	x	x	x	x	x	x	x	x		
File Creations on Third Party Accessible Systems	x		x	x	x			x	x			x		x		
File Deletions on Third Party Accessible Systems	x		x	x	x			x	x			x		x		
File Modifications on Third Party Accessible Systems	x		x	x	x			x	x			x		x		
File Related Activity on High Impact BES Cyber Systems			x	x												
File Related Activity on Low Impact BES Cyber Systems			x	x												
File Related Activity on Medium Impact BES Cyber Systems			x	x												

Report Name	IDS/IP S	NBA D	D B	O S	F W	VP N	V A	ID M	P M	N E	CS/W F	A V	W	AP P	PS S	Comment
File Related Activity on Third Party Accessible Systems			x	x												
Firewall Configuration Modification Summary					x											
List of Firewall Configuration Modifications					x											
List of Network Device Configuration Modifications										x						
List of Network Routing Modifications										x						
Network Device Configuration Modification Summary										x						
Network Routing Modification Summary										x						
Operation System Modification Summary				x												
Potential Vulnerabilities on New Assets							x									
Removable Media Activity				x												

Report Name	IDS/IP S	NBA D	D B	O S	F W	VP N	V A	ID M	P M	N E	CS/W F	A V	W	AP P	PS S	Comment
Software Changes in High Impact BES Cyber Systems			x	x												
Software Changes in Low Impact BES Cyber Systems			x	x							x	x				
Software Changes in Medium Impact BES Cyber Systems			x	x							x	x				
Software Changes in Operations			x	x							x	x				
Successful Database Configuration Modification			x	x							x	x				
Successful Changes to Operating Systems			x	x							x	x				
Successful High or Critical Configuration Changes	x	x	x	x	x	x	x	x	x	x	x	x	x	x		
Top 10 Vulnerabilities							x									
Top 10 Vulnerabilities - High Impact BES Cyber Systems							x									

Report Name	IDS/IP S	NBA D	D B	O S	F W	VP N	V A	ID M	P M	N E	CS/W F	A V	W	AP P	PS S	Comment
Top 10 Vulnerabilities - Low Impact BES Cyber Systems							x									
Top 10 Vulnerabilities - Medium Impact BES Cyber Systems							x									
Top 10 Vulnerable Assets							x									
Top 10 Vulnerable Assets - High Impact BES Cyber Systems							x									
Top 10 Vulnerable Assets - Low Impact BES Cyber Systems							x									
Top 10 Vulnerable Assets - Medium Impact BES Cyber Systems							x									
Top 10 Vulnerable Assets - Public Facing							x									
Top 10 Vulnerable Assets - Third Party							x									
Unsuccessful Changes to Operating Systems				x												

Report Name	IDS/IP S	NBA D	D B	O S	F W	VP N	V A	ID M	P M	N E	CS/W F	A V	W	AP P	PS S	Comment
Unsuccessful High or Critical Configuration Changes	x	x	x	x	x	x	x	x	x	x	x	x	x	x		
Vulnerabilities by IP Address							x									
Vulnerability Summary							x									
Weekly Trend - Configuration Modification Summary	x	x	x	x	x	x	x	x	x	x	x	x	x	x		
Windows Domain Policy Changes			x													
Windows Group Policy Changes			x													
All Information Leaks	x	x			x						x					
All Information Leaks from High Impact BES Cyber Systems	x	x			x						x					
All Information Leaks from Low Impact BES Cyber Systems	x	x			x						x					
All Information Leaks from Medium Impact BES Cyber Systems	x	x			x						x					

Report Name	IDS/IP S	NBA D	D B	O S	F W	VP N	V A	ID M	P M	N E	CS/W F	A V	W	AP P	PS S	Comment
High to Low Classified Asset Communicatio n																There is no specific input device required to populate this report. This report relies on how assets are defined and/or categorize d.
Insecure Cryptographic Storage							x									
Invalid or Expired Certificate	x			x	x	x	x	x			x	x				
Low to High Classified Asset Communicatio n																There is no specific input device required to populate this report. This report relies on how assets are defined and/or categorize d.

Report Name	IDS/IPS	NBAD	DB	OS	FW	VPN	VA	IDM	PM	NE	CS/WF	AV	W	APP	PSS	Comment
Organizational Records Information Leaks	x	x			x						x					
Personal Information Leaks	x	x			x						x					
Unencrypted Services by Host Name							x									

Key

IDS = Intrusion Detection System

IPS = Intrusion Prevention System

DB = Database

NBAD = Network Behavior Anomaly Detection

OS = Operating System

FW = Firewall

VPN = Virtual Private Network

VA = Vulnerability Assessment

IDM = Identity Management

PM = Policy Management

NE = Network Equipment

CS, WF = Content Security, Web Filtering

AV = Antivirus

W = Wireless

PSS = Physical Security Systems

APP = Applications

Appendix B: Mapping End User Resources to NERC CIPS

End User Resource	Type	CIP	CIP Requirement ID
Asset Creation Deletion and Modifications	ActiveChannel	CIP-002	R2 2.1
New Hosts and Services	ActiveChannel	CIP-002	R2 2.1
Technical Compliance Check Failures	ActiveChannel	CIP-002	R2 2.2 CIP-003 R1
Asset Activity	Dashboard	CIP-002	R2 2.1
Technical Compliance Checking	Dashboard	CIP-002	R2 2.2 CIP-003 R1
Assets in High Impact BES Cyber Systems	FocusedReport	CIP-002	R2 2.1
Assets in Low Impact BES Cyber Systems	FocusedReport	CIP-002	R2 2.1
Assets in Medium Impact BES Cyber Systems	FocusedReport	CIP-002	R2 2.1
Assets in the Development Network Domain	FocusedReport	CIP-002	R2 2.1
Assets in the Development Network Domain (Creation-Time Sorted)	FocusedReport	CIP-002	R2 2.1
Assets in the Public-Facing Network Domain	FocusedReport	CIP-002	R2 2.1
Assets in the Public-Facing Network Domain (Creation-Time Sorted)	FocusedReport	CIP-002	R2 2.1
Asset Creation by Location	Report	CIP-002	R2 2.1
Asset Deletion by Location	Report	CIP-002	R2 2.1
Asset Identification Report	Report	CIP-002	R2 2.1
Asset Modification by Location	Report	CIP-002	R2 2.1
Assets Available to Third Parties by Domain	Report	CIP-002	R2 2.1
Assets Available to Third-Parties by Criticality	Report	CIP-002	R2 2.1

End User Resource	Type	CIP	CIP Requirement ID
Assets by Network Domain (Creation Time) - Template	Report	CIP-002	R2 2.1
Assets by Network Domain - Template	Report	CIP-002	R2 2.1
Assets that Failed Technical Compliance Check	Report	CIP-002	R2 2.1
Classification of Assets	Report	CIP-002	R2 2.1
Critical Assets	Report	CIP-002	R2 2.1
Criticality of Assets	Report	CIP-002	R2 2.1
Services by Asset - Template	Report	CIP-002	R2 2.1
New Host Detected	Rule	CIP-002	R2 2.1
New Service Detected	Rule	CIP-002	R2 2.1
Intellectual Property Rights Violations	ActiveChannel	CIP-003	R1
Policy Breaches	ActiveChannel	CIP-003	R1
Intellectual Property Rights Violations	Dashboard	CIP-003	R1
Policy Breaches	Dashboard	CIP-003	R1
Policy Violations In High Impact BES Cyber Assets	FocusedReport	CIP-003	R1
Policy Violations In Low Impact BES Cyber Assets	FocusedReport	CIP-003	R1
Policy Violations In Medium Impact BES Cyber Assets	FocusedReport	CIP-003	R1
Intellectual Property Rights Violations	Report	CIP-003	R1
Intellectual Property Rights Violators	Report	CIP-003	R1
Machines Conducting Policy Breaches	Report	CIP-003	R1
Policy Violations - Template	Report	CIP-003	R1
Policy Violations from Third-Party Assets	Report	CIP-003	R1
Top 20 Policy Breach Events	Report	CIP-003	R1
Intellectual Property Rights Violation	Rule	CIP-003	R1
Policy Violations	Rule	CIP-003	R1
Default Vendor Account Used	ActiveChannel	CIP-004	R3.1
Privileged Account Changed	ActiveChannel	CIP-004	R4.1 R4.3
Removal of Access Rights	ActiveChannel	CIP-004	R4.1 R4.3

End User Resource	Type	CIP	CIP Requirement ID
Account Activity	Dashboard	CIP-004	R4.1 R4.3
Default Vendor Account Activity	Dashboard	CIP-004	R3.1
Former Employee Activity	Dashboard	CIP-004	R5
New Hires Activity	Dashboard	CIP-004	R3.4 R3.5
User Group Activity	Dashboard	CIP-004	R4.1 R4.3
All Events by New Hires	QueryViewer	CIP-004	R3.4 R3.5
Former Employee Accounts in Use	QueryViewer	CIP-004	R5
Suspicious Activities by New Hires	QueryViewer	CIP-004	R3.4 R3.5
Account Creations	Report	CIP-004	R4.1 R4.3
Account Creations in Network Domain - Template	Report	CIP-004	R4.1 R4.3
Account Deletions	Report	CIP-004	R4.1 R4.3
Account Deletions in Network Domain - Template	Report	CIP-004	R4.1 R4.3
Account Modifications	Report	CIP-004	R4.1 R4.3
Account Modifications in Network Domain - Template	Report	CIP-004	R4.1 R4.3
Activity by Former Employees	Report	CIP-004	R5
Attempted Default Vendor Accounts - Summary	Report	CIP-004	R3.1
Attempted Direct Root or Administrator	Report	CIP-004	R3.1
Detail Specific Default Vendor Account Uses	Report	CIP-004	R3.1
Failed or Attempted Removal of Access Rights	Report	CIP-004	R4.1 R4.3
Former Employee Account Access Attempt	Report	CIP-004	R5
Inactive User Account Detected	Report	CIP-004	R5
Login Activity by Inactive Users	Report	CIP-004	R5
Privileged Account Change Details	Report	CIP-004	R4.1 R4.3
Successful Default Vendor Account Used - Summary	Report	CIP-004	R3.1
Successful Removal of Access Rights	Report	CIP-004	R4.1 R4.3

End User Resource	Type	CIP	CIP Requirement ID
Summary of Suspicious Activity by New Hires	Report	CIP-004	R3.4 R3.5
Suspicious Activity by New Hires	Report	CIP-004	R3.4 R3.5
Systems Accessed by Default Vendor Accounts	Report	CIP-004	R3.1
User Group Account Creations	Report	CIP-004	R4.1 R4.3
User Group Account Deletions	Report	CIP-004	R4.1 R4.3
User Group Account Modifications	Report	CIP-004	R4.1 R4.3
Users Added to Groups	Report	CIP-004	R4.1 R4.3
Users Removed from Groups	Report	CIP-004	R4.1 R4.3
Former Employee Account Activity	Rule	CIP-004	R5
Former Employee Account Detected	Rule	CIP-004	R5
Former Employee User Account Access Attempt	Rule	CIP-004	R5
Inactive User Account Detected	Rule	CIP-004	R5
Login Activity by a Stale Account	Rule	CIP-004	R5
New Hire Identification	Rule	CIP-004	R3.4 R3.5
Privileged Account Change	Rule	CIP-004	R4.1 R4.3
Removal of Access Rights	Rule	CIP-004	R4.1 R4.3
Successful Default Vendor Account Used	Rule	CIP-004	R3.1
Suspicious Activities by New Hires	Rule	CIP-004	R3.4 R3.5
User Logged in - Added to Active Accounts List	Rule	CIP-004	R5 CIP-007 4.1
Blocked Traffic Activity	Dashboard	CIP-005	R1.3
Disallowed Ports Communications	Dashboard	CIP-005	R1.5
High Impact BES Systems Blocked Traffic	Dashboard	CIP-005	R1.3
Information Interception	Dashboard	CIP-005	R1.5
Internal External Communications	Dashboard	CIP-005	R1.1
Low Impact BES Systems Blocked Traffic	Dashboard	CIP-005	R1.3
Medium Impact BES Systems Blocked Traffic	Dashboard	CIP-005	R1.3
Network Controls	Dashboard	CIP-005	R1.1 R1.3

End User Resource	Type	CIP	CIP Requirement ID
Traffic Anomaly	Dashboard	CIP-005	R1.5
Traffic Between Network Domains	Dashboard	CIP-005	R1.5
Open Firewall Port Summary	QueryViewer	CIP-005	R1.3
All VPN Access Attempts	Report	CIP-005	R2.2
Blocked Firewall Traffic from Assets in Network Domain - Template	Report	CIP-005	R1.3
Blocked Firewall Traffic to Assets in Network Domain - Template	Report	CIP-005	R1.3
Covert Channel Activity	Report	CIP-005	R1.5
Detail Disallowed Port Access	Report	CIP-005	R1.5
Development and Test Cross-Talk	Report	CIP-005	R1.1
Disallowed Port Access Summary	Report	CIP-005	R1.1
Email Attacks	Report	CIP-005	R1.5
IM Traffic Summary	Report	CIP-005	R1.5
Inbound Insecure Transmissions	Report	CIP-005	R1.5
Information Interception Activity	Report	CIP-005	R1.5
Insecure Transmissions	Report	CIP-005	R1.5 CIP-007-6 R1.1
Internal IM Senders	Report	CIP-005	R1.5 1.3 CIP-007-6 R1.1
Internal Insecure Service Providers	Report	CIP-005	R1.5 CIP-007-6 R1.1
Low and High Impact BES Cyber Systems Cross-Talk	Report	CIP-005	R1.1
Low and Medium Impact BES Cyber Systems Cross-Talk	Report	CIP-005	R1.1
Medium and High Impact BES Cyber Systems Cross-Talk	Report	CIP-005	R1.1
Open Firewall Port Details	Report	CIP-005	R1.3
Operations and Development Cross-Talk	Report	CIP-005	R1.1
Privileged VPN Remote Access Attempts	Report	CIP-005	R2.2
Redirection Attacks	Report	CIP-005	R1.5
Test and Operations Cross-Talk	Report	CIP-005	R1.1
Third-Party Access	Report	CIP-005	R1.1 R1.3
Traffic Anomaly on Application Layer	Report	CIP-005	R1.5

End User Resource	Type	CIP	CIP Requirement ID
Traffic Anomaly on Network Layer	Report	CIP-005	R1.5
Traffic Anomaly on Transport Layer	Report	CIP-005	R1.5
Traffic Between High Impact BES Systems and External	Report	CIP-005	R1.1
Traffic Between Internal and External Sources - All	Report	CIP-005	R1.1
Traffic Between Low Impact BES Systems and External	Report	CIP-005	R1.1
Traffic Between Medium Impact BES Systems and External	Report	CIP-005	R1.1
Traffic Between Zones	Report	CIP-005	R1.1
Traffic Coming from Dark Address Space	Report	CIP-005	R1.1 R1.5
Traffic to Dark Address Space	Report	CIP-005	R1.1 R1.5
Unsuccessful VPN Access	Report	CIP-005	R2.2
Disallowed Ports Access	Rule	CIP-005	R1.5 CIP-007-6 R1.1
Internal Insecure Service Provider Detected	Rule	CIP-005	R1.5 CIP-007-6 R1.1
Possible Covert Channel	Rule	CIP-005	R1.5
Possible Email Attack	Rule	CIP-005	R1.5
Possible Information Interception	Rule	CIP-005	R1.5
Possible Redirection Attack	Rule	CIP-005	R1.5
Possible Traffic Anomaly	Rule	CIP-005	R1.5
Wireless Malicious Traffic Detected	Rule	CIP-005	R1.5
Physical Security	ActiveChannel	CIP-006	R1.1 R1.4 R1.6 R1.8
Physical Security Overview	Dashboard	CIP-006	R1.1 R1.4 R1.6 R1.8
Failed After Hours Building Accesses	Report	CIP-006	R1.1 R1.4 R1.6 R1.8
Failed Building Access Events	Report	CIP-006	R1.1 R1.4 R1.6 R1.8
Successful After Hours Building Accesses	Report	CIP-006	R1.1 R1.4 R1.6 R1.8
Successful Building Access Events	Report	CIP-006	R1.1 R1.4 R1.6 R1.8
After Hours Building Access by Contractors	Rule	CIP-006	R1.5 R1.6 R1.7
Badged Out Employee	Rule	CIP-006	R1.5 R1.6 R1.7

End User Resource	Type	CIP	CIP Requirement ID
Failed Building Access	Rule	CIP-006	R1.5 R1.6 R1.7
Local Logon from Badged Out Employee	Rule	CIP-006	R1.5 R1.6 R1.7
Successful Badge In	Rule	CIP-006	R1.5 R1.6 R1.7
Successful Badge Out	Rule	CIP-006	R1.5 R1.6 R1.7
Account Lockouts	ActiveChannel	CIP-007	R5.7
Login Attempts	ActiveChannel	CIP-007	R4.1.1 R4.1.2 R4.2.2
Logouts	ActiveChannel	CIP-007	R4.1.1 R4.1.2 R4.2.2
Open Ports	ActiveChannel	CIP-007	R1.1 CIP-005 R1.5
Account Lockouts	Dashboard	CIP-007	R5.7
Administrative Logins and Logouts	Dashboard	CIP-007	R4.1.1 R4.1.2 R4.2.2
Anti-Virus Activity	Dashboard	CIP-007	R4.2.1 R3.1 CIP-005 R1.5
General User Login Attempts	Dashboard	CIP-007	R4.1.1 R4.1.2 R4.2.2
Malicious Code Activity	Dashboard	CIP-007	R4.2.1 R3.1 CIP-005 R1.5
Port Activity	Dashboard	CIP-007	R1.1 CIP-005 R1.5
Unsuccessful Administrative Logins	Dashboard	CIP-007	R4.1.2 R4.2.2
Unsuccessful User Logins	Dashboard	CIP-007	R4.1.2 R4.2.2
User Logins and Logouts	Dashboard	CIP-007	R4.1.1 R4.1.2 R4.2.2
Account Lockouts	QueryViewer	CIP-007	R5.7
Count of Successful Administrative Logins in the Last 30 Days	QueryViewer	CIP-007	R4.1.1 4.3
Count of Unsuccessful Administrative Logins in the Last 30 Days	QueryViewer	CIP-007	R4.1.2 4.3
Dynamic Open Ports	QueryViewer	CIP-007	R1.1 CIP-005 R1.5
Open Ports	QueryViewer	CIP-007	R1.1 CIP-005 R1.5
Password Changes	QueryViewer	CIP-007	R5.4 R5.6
Top 10 Hosts with Most Unsuccessful Administrative Logins in the Last 2 Hours	QueryViewer	CIP-007	R4.1.2
Unsecured Open Ports	QueryViewer	CIP-007	R1.1 CIP-005 R1.5
Unsuccessful Administrative Logins in the Last 2 Hours	QueryViewer	CIP-007	R4.1.2
Account Lockouts per System	Report	CIP-007	R5.7

End User Resource	Type	CIP	CIP Requirement ID
Account Lockouts per User and System	Report	CIP-007	R5.7
Administrative Logins and Logouts per User	Report	CIP-007	R4.1.1 R4.1.2
All Password Change Events	Report	CIP-007	R5.4 R5.6
All User Logins per User	Report	CIP-007	R4.1.1 R4.1.2
Anti-Virus Stopped or Paused in the Last Month	Report	CIP-007	R3.3
Application Brute Force Login Attempts	Report	CIP-007	R5.7
Detail Daily Unsuccessful Administrative Logins	Report	CIP-007	R4.1.2
Dynamic Open Ports	Report	CIP-007	R1.1 CIP-005 R1.5
Failed Anti-Virus Updates	Report	CIP-007	R3.3
Failed Password Changes	Report	CIP-007	R5.4 R5.6
Frequent Unsuccessful Logins by User Name	Report	CIP-007	R4.1.2
Frequent Unsuccessful Logins from Attacker Host	Report	CIP-007	R4.1.2
Frequent Unsuccessful Logins to Target Host	Report	CIP-007	R4.1.2
Malicious Code Sources	Report	CIP-007	R4.2.1 R3.1 CIP-005 R1.5
Malware Activities	Report	CIP-007	R4.2.1 R3.1 CIP-005 R1.5
Malware Activity Summary	Report	CIP-007	R4.2.1 R3.1 CIP-005 R1.5
Monthly Trend of Unsuccessful Administrative Logins	Report	CIP-007	R4.1.1 R4.3
Number of Successful Administrative Logins by User and Host	Report	CIP-007	R4.1.1
Number of Successful User Logins over the Past Week	Report	CIP-007	R4.1.1
Number of Successful User Logins per Hour over the Past Day	Report	CIP-007	R4.1.1
Number of Unsuccessful Administrative Logins by User and Host	Report	CIP-007	R4.1.1
Number of Unsuccessful User Logins over the Past Month	Report	CIP-007	R4.1.2 R4.3

End User Resource	Type	CIP	CIP Requirement ID
Number of Unsuccessful User Logins over the Past Week	Report	CIP-007	R4.1.2
Number of Unsuccessful User Logins per Hour over the Past Day	Report	CIP-007	R4.1.2
Open Ports	Report	CIP-007	R1.1 CIP-005 R1.5
Passwords not Changed for Longer than Policy Standard	Report	CIP-007	R5.6
Spyware Activities	Report	CIP-007	R4.2.1 R3.1 CIP-005 R1.5
Successful Administrative Logins	Report	CIP-007	R4.1.1
Successful Administrative Logins from Third Party Systems	Report	CIP-007	R4.1.1
Successful Administrative Logins to High Impact BES Cyber Systems	Report	CIP-007	R4.1.1
Successful Administrative Logins to Low Impact BES Cyber Systems	Report	CIP-007	R4.1.1
Successful Administrative Logins to Medium Impact BES Cyber Systems	Report	CIP-007	R4.1.1
Successful Administrative Logins to Third Party Systems	Report	CIP-007	R4.1.1
Successful Brute Force Logins	Report	CIP-007	R5.7
Successful Password Changes	Report	CIP-007	R5.4 R5.6
Successful User Logins	Report	CIP-007	R4.1.1
Successful User Logins from Third Party Systems	Report	CIP-007	R4.1.1
Successful User Logins to High Impact BES Cyber Systems	Report	CIP-007	R4.1.1
Successful User Logins to Low Impact BES Cyber Systems	Report	CIP-007	R4.1.1
Successful User Logins to Medium Impact BES Cyber Systems	Report	CIP-007	R4.1.1
Successful User Logins to Third Party Systems	Report	CIP-007	R4.1.1
Unsecured Open Ports	Report	CIP-007	R1.1 CIP-005 R1.5
Unsuccessful Administrative Logins	Report	CIP-007	R4.1.2
Unsuccessful Administrative Logins from Third Party Systems	Report	CIP-007	R4.1.2

End User Resource	Type	CIP	CIP Requirement ID
Unsuccessful Administrative Logins to High Impact BES Cyber Systems	Report	CIP-007	R4.12
Unsuccessful Administrative Logins to Low Impact BES Cyber Systems	Report	CIP-007	R4.12
Unsuccessful Administrative Logins to Medium Impact BES Cyber Systems	Report	CIP-007	R4.12
Unsuccessful Administrative Logins to Third Party Systems	Report	CIP-007	R4.12
Unsuccessful User Logins	Report	CIP-007	R4.12
Unsuccessful User Logins from Third Party Systems	Report	CIP-007	R4.12
Unsuccessful User Logins to High Impact BES Cyber Systems	Report	CIP-007	R4.12
Unsuccessful User Logins to Low Impact BES Cyber Systems	Report	CIP-007	R4.12
Unsuccessful User Logins to Medium Impact BES Cyber Systems	Report	CIP-007	R4.12
Unsuccessful User Logins to Third Party Systems	Report	CIP-007	R4.12
Virus Activities	Report	CIP-007	R4.2.1 R3.1 CIP-005 R1.5
Worm Activity Summary	Report	CIP-007	R4.2.1 R3.1 CIP-005 R1.5
Account Lockout	Rule	CIP-007	R5.7
Brute Force Login Attempts	Rule	CIP-007	R5.7 R4.12 R4.2.2
Consecutive Unsuccessful Logins to Administrative Account	Rule	CIP-007	R5.7 R4.12 R4.2.2
DoS Detected	Rule	CIP-007	R4.2.1 R3.1 CIP-005 R1.5
Frequent Unsuccessful Logins by User Name	Rule	CIP-007	R5.7 R4.12 R4.2.2
Frequent Unsuccessful Logins from Attacker Host	Rule	CIP-007	R5.7 R4.12 R4.2.2
Frequent Unsuccessful Logins to Target Host	Rule	CIP-007	R4.12 R4.2.2 R3.1
Malware or Spyware Detected	Rule	CIP-007	R4.2.1
Password not Changed for Longer than Policy Standard	Rule	CIP-007	R5.4 R5.6
Potential Distributed DoS	Rule	CIP-007	R4.2.1 R3.1

End User Resource	Type	CIP	CIP Requirement ID
Security Software Stopped or Paused	Rule	CIP-007	R3.3
Successful Attack - Brute Force Login	Rule	CIP-007	R5.7 R3.1 R4.1.2 R4.2.2
Successful Password Change	Rule	CIP-007	R5.4 R5.6
Suspicious Internal Trojan Detected	Rule	CIP-007	R4.2.1 R3.1 CIP-005 R1.5
Unsuccessful Logins to Multiple Administrative Accounts	Rule	CIP-007	R4.1.2 R4.2.2
Worm Detected	Rule	CIP-007	R4.2.1 R3.1 CIP-005 R1.5
All Attacks and Suspicious Activity Events	ActiveChannel	CIP-008	R1.1 CIP-007 R3.1
Attacks and Suspicious Activity Targeting High Impact BES Cyber Systems	ActiveChannel	CIP-008	R1.1 CIP-007 R3.1
Attacks and Suspicious Activity Targeting Low Impact BES Cyber Systems	ActiveChannel	CIP-008	R1.1 CIP-007 R3.1
Attacks and Suspicious Activity Targeting Medium Impact BES Cyber Systems	ActiveChannel	CIP-008	R1.1 CIP-007 R3.1
Attacks and Suspicious Activity Targeting Public Facing Resources	ActiveChannel	CIP-008	R1.1 CIP-007 R3.1
Attacks and Suspicious Activity Targeting Third Party Resources	ActiveChannel	CIP-008	R1.1 CIP-007 R3.1
Attacks and Suspicious Activity from High Impact BES Cyber Systems	ActiveChannel	CIP-008	R1.1 CIP-007 R3.1
Attacks and Suspicious Activity from Low Impact BES Cyber Systems	ActiveChannel	CIP-008	R1.1 CIP-007 R3.1
Attacks and Suspicious Activity from Medium Impact BES Cyber Systems	ActiveChannel	CIP-008	R1.1 CIP-007 R3.1
Attacks and Suspicious Activity from Public Facing Resources	ActiveChannel	CIP-008	R1.1 CIP-007 R3.1
Attacks and Suspicious Activity from Third Party Resources	ActiveChannel	CIP-008	R1.1 CIP-007 R3.1
DoS Attacks	ActiveChannel	CIP-008	R1.1 R1.4 CIP-007 R3.1
High Priority Events	ActiveChannel	CIP-008	R1.1 R1.4
Internal Reconnaissance	ActiveChannel	CIP-008	R1.1 CIP-007 R3.1
Attacks and Suspicious Activity	Dashboard	CIP-008	R1.1 CIP-007 R3.1

End User Resource	Type	CIP	CIP Requirement ID
Attacks and Suspicious Activity to and from High Impact BES Cyber Systems	Dashboard	CIP-008	R1.1 CIP-007 R3.1
Attacks and Suspicious Activity to and from Low Impact BES Cyber Systems	Dashboard	CIP-008	R1.1 CIP-007 R3.1
Attacks and Suspicious Activity to and from Medium Impact BES Cyber Systems	Dashboard	CIP-008	R1.1 CIP-007 R3.1
Attacks and Suspicious Activity to and from Third Party Resources	Dashboard	CIP-008	R1.1 CIP-007 R3.1
DoS Activity	Dashboard	CIP-008	R1.1 CIP-007 R3.1
Internal Reconnaissance	Dashboard	CIP-008	R1.1 CIP-007 R3.1
CIP-002 Case Overview	QueryViewer	CIP-008	R1.1
CIP-003 Case Overview	QueryViewer	CIP-008	R1.1
CIP-004 Case Overview	QueryViewer	CIP-008	R1.1
CIP-005 Case Overview	QueryViewer	CIP-008	R1.1
CIP-006 Case Overview	QueryViewer	CIP-008	R1.1
CIP-007 Case Overview	QueryViewer	CIP-008	R1.1
CIP-008 Case Overview	QueryViewer	CIP-008	R1.1
CIP-009 Case Overview	QueryViewer	CIP-008	R1.1
CIP-010 Case Overview	QueryViewer	CIP-008	R1.1
CIP-011 Case Overview	QueryViewer	CIP-008	R1.1
Attacks and Suspicious Activities	Report	CIP-008	R1.1 CIP-007 R3.1
Attacks and Suspicious Activities on High Impact BES Cyber Systems	Report	CIP-008	R1.1 CIP-007 R3.1
Attacks and Suspicious Activities on Low Impact BES Cyber Systems	Report	CIP-008	R1.1 CIP-007 R3.1
Attacks and Suspicious Activities on Medium Impact BES Cyber Systems	Report	CIP-008	R1.1 CIP-007 R3.1
Attacks and Suspicious Activity Monthly Trend	Report	CIP-008	R1.1 CIP-007 R3.1
Attacks and Suspicious Activity Weekly Trend	Report	CIP-008	R1.1 CIP-007 R3.1
Average Time to Resolution - By Case Severity	Report	CIP-008	R1.1
Average Time to Resolution - By Day	Report	CIP-008	R1.1
Average Time to Resolution - By User	Report	CIP-008	R1.1

End User Resource	Type	CIP	CIP Requirement ID
Cases by Stage	Report	CIP-008	R1.1
Count of Attacks and Suspicious Activities per Attacker Machine	Report	CIP-008	R1.1 CIP-007 R3.1
Count of Attacks and Suspicious Activities per Target Machine	Report	CIP-008	R1.1 CIP-007 R3.1
Count of Attacks and Suspicious Activity Event Names	Report	CIP-008	R1.1 CIP-007 R3.1
DoS Attacks Weekly Trend	Report	CIP-008	R1.1 CIP-007 R3.1
High Priority Events	Report	CIP-008	R1.1 R1.2
High Priority Events on High Impact BES Cyber Systems	Report	CIP-008	R1.1 R1.2
High Priority Events on Low Impact BES Cyber Systems	Report	CIP-008	R1.1 R1.2
High Priority Events on Medium Impact BES Cyber Systems	Report	CIP-008	R1.1 R1.2
Internal Reconnaissance Sources	Report	CIP-008	R1.1 CIP-007 R3.1
Internal Reconnaissance Top Events	Report	CIP-008	R1.1 CIP-007 R3.1
Internal Reconnaissance Top Targets	Report	CIP-008	R1.1 CIP-007 R3.1
Open Cases by CIP	Report	CIP-008	R1.1
Open Cases by CIP and Severity	Report	CIP-008	R1.1
Open Cases by Owner	Report	CIP-008	R1.1
Open Cases by Severity	Report	CIP-008	R1.1
Top DoS Attackers	Report	CIP-008	R1.1 CIP-007 R3.1
Top DoS Targets	Report	CIP-008	R1.1 CIP-007 R3.1
Information Security Incident	Rule	CIP-008	R1.1 R1.2 1.4
Internal Recon Detected	Rule	CIP-008	R1.1 CIP-007 R3.1
Multiple Cases Created on Short Period	Rule	CIP-008	R1.1 R1.2 1.4
Severely Attacked System	Rule	CIP-008	R1.1 R1.2
Information System Failures	ActiveChannel	CIP-009	R1.1 R1.5
Possible Availability Impacts	ActiveChannel	CIP-009	R1.1 R1.5
System Startup and Shutdown	ActiveChannel	CIP-009	R1.1 R1.5
Up Down Status of Highly Critical Assets	Dashboard	CIP-009	R1.1 R1.5
Critical Assets	Report	CIP-009	R1.1 R1.5

End User Resource	Type	CIP	CIP Requirement ID
Fault Logs	Report	CIP-009	R1.1 R1.5
Information System Failures by Hosts	Report	CIP-009	R1.1 R1.5
Resource Exhaustion Detected	Report	CIP-009	R1.1 R1.5
Shutdown of Critical Machines	Report	CIP-009	R1.1 R1.5
Shutdown of Machines	Report	CIP-009	R1.1 R1.5
Information System Failures of Highly Critical Machine	Rule	CIP-009	R1.1 R1.5
Resource Exhaustion of Highly Critical Machine	Rule	CIP-009	R1.1 R1.5
Shutdown of Highly Critical Machine	Rule	CIP-009	R1.1 R1.5
Audit Log Cleared	ActiveChannel	CIP-010	R2.1
Configuration Changes	ActiveChannel	CIP-010	R1 R.2
Database Configuration Changes	ActiveChannel	CIP-010	R1 R.2
Firewall Configuration Changes	ActiveChannel	CIP-010	R1 R.2
Network IDS Configuration Changes	ActiveChannel	CIP-010	R1 R.2
Network Routing Configuration Changes	ActiveChannel	CIP-010	R1 R.2
Operating System Configuration Changes	ActiveChannel	CIP-010	R1 R.2
Software Changes	ActiveChannel	CIP-010	R1 R.2
VPN Configuration Changes	ActiveChannel	CIP-010	R1 R.2
Vulnerability Events	ActiveChannel	CIP-010	R3
Audit Log Cleared	Dashboard	CIP-010	R2.1
Configuration Modifications Overview	Dashboard	CIP-010	R1 R.2
Firewall Configuration Modifications Overview	Dashboard	CIP-010	R1 R.2
Last 20 Vulnerabilities - by Type	Dashboard	CIP-010	R3
Last State External Devices Overview	Dashboard	CIP-010	R4 CIP-007 R1.2
Last State Vulnerability Overview	Dashboard	CIP-010	R3
Latest Vulnerabilities	Dashboard	CIP-010	R3
Network Devices Configuration Changes Overview	Dashboard	CIP-010	R1 R.2
Operating Systems Configuration Modifications Overview	Dashboard	CIP-010	R1 R.2

End User Resource	Type	CIP	CIP Requirement ID
Top 10 Vulnerable Assets	Dashboard	CIP-010	R3
Vulnerability Overview	Dashboard	CIP-010	R3
Top Critical Vulnerabilities	QueryViewer	CIP-010	R3
Top Vulnerable IP Addresses	QueryViewer	CIP-010	R3
Vulnerabilities	QueryViewer	CIP-010	R3
Vulnerability Events By Scanner	QueryViewer	CIP-010	R3
Vulnerability Scans	QueryViewer	CIP-010	R3
Application Configuration Modifications	Report	CIP-010	R1 R.2
Audit Log Cleared	Report	CIP-010	R2.1
Audit Log Cleared per Attacker User Name	Report	CIP-010	R2.1
Audit Log Cleared per Attacker and Target	Report	CIP-010	R2.1
Audit Log Cleared per Target User Name	Report	CIP-010	R2.1
CVSS Score Greater than or Equal to 8 Overview	Report	CIP-010	R3
Configuration Changes to High Impact BES Cyber Systems	Report	CIP-010	R1 R.2
Configuration Changes to Low Impact BES Cyber Systems	Report	CIP-010	R1 R.2
Configuration Changes to Medium Impact BES Cyber Systems	Report	CIP-010	R1 R.2
Configuration Changes to Third Party Machines	Report	CIP-010	R1 R.2
File Creations on Third Party Accessible Systems	Report	CIP-010	R1 R.2
File Deletions on Third Party Accessible Systems	Report	CIP-010	R1 R.2
File Modifications on Third Party Accessible Systems	Report	CIP-010	R1 R.2
File Related Activity on High Impact BES Cyber Systems	Report	CIP-010	R1 R.2
File Related Activity on Low Impact BES Cyber Systems	Report	CIP-010	R1 R.2

End User Resource	Type	CIP	CIP Requirement ID
File Related Activity on Medium Impact BES Cyber Systems	Report	CIP-010	R1 R.2
File Related Activity on Third Party Accessible Systems	Report	CIP-010	R1 R.2
Firewall Configuration Modification Summary	Report	CIP-010	R1 R.2
List of Firewall Configuration Modifications	Report	CIP-010	R1 R.2
List of Network Device Configuration Modifications	Report	CIP-010	R1 R.2
List of Network Routing Modifications	Report	CIP-010	R1 R.2
Network Device Configuration Modification Summary	Report	CIP-010	R1 R.2
Network Routing Modification Summary	Report	CIP-010	R1 R.2
Operation System Modification Summary	Report	CIP-010	R1 R.2
Potential Vulnerabilities on New Assets	Report	CIP-010	R3
Removable Media Activity	Report	CIP-010	R4 CIP-007 R1.2
Software Changes in High Impact BES Cyber Systems	Report	CIP-010	R1 R.2
Software Changes in Low Impact BES Cyber Systems	Report	CIP-010	R1 R.2
Software Changes in Medium Impact BES Cyber Systems	Report	CIP-010	R1 R.2
Software Changes in Operations	Report	CIP-010	R1 R.2
Successful Database Configuration Modification	Report	CIP-010	R1 R.2
Successful Changes to Operating Systems	Report	CIP-010	R1 R.2
Successful High or Critical Configuration Changes	Report	CIP-010	R1 R.2
Top 10 Vulnerabilities	Report	CIP-010	R3
Top 10 Vulnerabilities - High Impact BES Cyber Systems	Report	CIP-010	R3
Top 10 Vulnerabilities - Low Impact BES Cyber Systems	Report	CIP-010	R3

End User Resource	Type	CIP	CIP Requirement ID
Top 10 Vulnerabilities - Medium Impact BES Cyber Systems	Report	CIP-010	R3
Top 10 Vulnerable Assets	Report	CIP-010	R3
Top 10 Vulnerable Assets - High Impact BES Cyber Systems	Report	CIP-010	R3
Top 10 Vulnerable Assets - Low Impact BES Cyber Systems	Report	CIP-010	R3
Top 10 Vulnerable Assets - Medium Impact BES Cyber Systems	Report	CIP-010	R3
Top 10 Vulnerable Assets - Public Facing	Report	CIP-010	R3
Top 10 Vulnerable Assets - Third Party	Report	CIP-010	R3
Unsuccessful Changes to Operating Systems	Report	CIP-010	R1 R.2
Unsuccessful High or Critical Configuration Changes	Report	CIP-010	R1 R.2
Vulnerabilities by IP Address	Report	CIP-010	R3
Vulnerability Summary	Report	CIP-010	R3
Weekly Trend - Configuration Modification Summary	Report	CIP-010	R1
Windows Domain Policy Changes	Report	CIP-010	R2.1
Windows Group Policy Changes	Report	CIP-010	R2.1 CIP-007 5.5
Audit Log Cleared	Rule	CIP-010	R2.1
Critical Network Device Configuration Change Detected	Rule	CIP-010	R1 R.2
Critical Operating System Change Detected	Rule	CIP-010	R1 R.2
Critical Vulnerability Detected	Rule	CIP-010	R3
Overflow Vulnerabilities	Rule	CIP-010	R3
SSL Vulnerabilities	Rule	CIP-010	R3
Security Patch Missing	Rule	CIP-010	R3
Vulnerabilities on Critical Machine	Rule	CIP-010	R3
XSRF Vulnerabilities	Rule	CIP-010	R3
XSS Vulnerabilities	Rule	CIP-010	R3
All Information Leak Events	ActiveChannel	CIP-011	R1.2

End User Resource	Type	CIP	CIP Requirement ID
Invalid or Expired Certificate Events	ActiveChannel	CIP-011	R1.2
Personal and Organizational Records Information Leak	ActiveChannel	CIP-011	R1.2
Information Leaks	Dashboard	CIP-011	R1.2
All Information Leaks	Report	CIP-011	R1.2
All Information Leaks from High Impact BES Cyber Systems	Report	CIP-011	R1.2
All Information Leaks from Low Impact BES Cyber Systems	Report	CIP-011	R1.2
All Information Leaks from Medium Impact BES Cyber Systems	Report	CIP-011	R1.2
High to Low Classified Asset Communication	Report	CIP-011	R1.2
Insecure Cryptographic Storage	Report	CIP-011	R1.2
Invalid or Expired Certificate	Report	CIP-011	R1.2
Low to High Classified Asset Communication	Report	CIP-011	R1.2
Organizational Records Information Leaks	Report	CIP-011	R1.2
Personal Information Leaks	Report	CIP-011	R1.2
Unencrypted Services by Host Name	Report	CIP-011	R1.2
High to Low Classified Traffic Information Leak	Rule	CIP-011	R1.2
Organizational Data Information Leak	Rule	CIP-011	R1.2
Personal Information Leak	Rule	CIP-011	R1.2

Appendix C: Compare, Backup, and Uninstall Packages

This chapter provides instructions to allow you to generate a list of resource changes, back up the solution package or uninstall the Solution for NERC CIP at a later date.

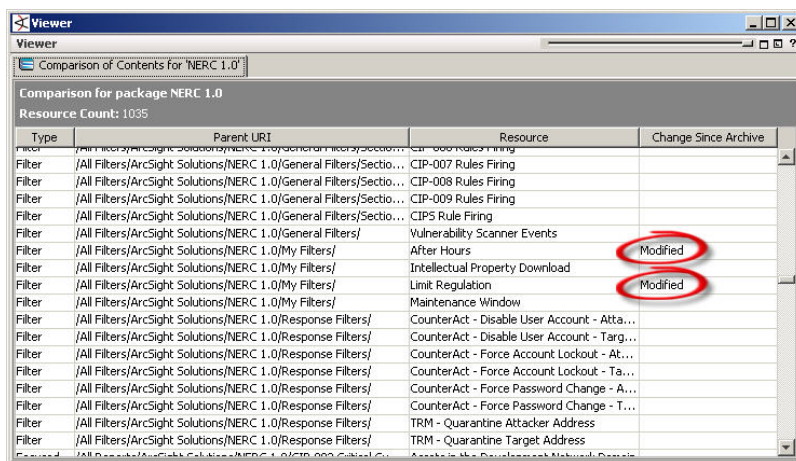
Generate a List of Resource Changes

Before backing up a solution package, you may want to generate a list of resource changes since the last time the package was exported to a package bundle. The current resources associated with the selected package are compared against the resources saved in the package bundle and any new, modified or deleted resources are reported.

To generate a list of resource changes:

1. Log into the ArcSight Console as ArcSight Administrator.
2. In the Packages tab of the Navigator panel, navigate to the solution group.
For Solution for NERC CIP, navigate to ArcSight Solutions/NERC 6.0.
3. Right-click the solution package (📁) and select **Compare Archive with Current Package Contents**.

In the Viewer panel, a list of resources associated with the package are displayed. In the right column called **Change Since Archive**, any changes with the resource since the last export are displayed, either **Added**, **Modified**, or **Removed**.



Type	Parent URI	Resource	Change Since Archive
Filter	/All Filters/ArcSight Solutions/NERC 1.0/General Filters/Section...	CIP-007 Rules Firing	
Filter	/All Filters/ArcSight Solutions/NERC 1.0/General Filters/Section...	CIP-008 Rules Firing	
Filter	/All Filters/ArcSight Solutions/NERC 1.0/General Filters/Section...	CIP-009 Rules Firing	
Filter	/All Filters/ArcSight Solutions/NERC 1.0/General Filters/Section...	CIPS Rule Firing	
Filter	/All Filters/ArcSight Solutions/NERC 1.0/General Filters/	Vulnerability Scanner Events	Modified
Filter	/All Filters/ArcSight Solutions/NERC 1.0/My Filters/	After Hours	
Filter	/All Filters/ArcSight Solutions/NERC 1.0/My Filters/	Intellectual Property Download	Modified
Filter	/All Filters/ArcSight Solutions/NERC 1.0/My Filters/	Limit Regulation	
Filter	/All Filters/ArcSight Solutions/NERC 1.0/My Filters/	Maintenance Window	
Filter	/All Filters/ArcSight Solutions/NERC 1.0/Response Filters/	CounterAct - Disable User Account - Atta...	
Filter	/All Filters/ArcSight Solutions/NERC 1.0/Response Filters/	CounterAct - Disable User Account - Targ...	
Filter	/All Filters/ArcSight Solutions/NERC 1.0/Response Filters/	CounterAct - Force Account Lockout - At...	
Filter	/All Filters/ArcSight Solutions/NERC 1.0/Response Filters/	CounterAct - Force Account Lockout - Ta...	
Filter	/All Filters/ArcSight Solutions/NERC 1.0/Response Filters/	CounterAct - Force Password Change - A...	
Filter	/All Filters/ArcSight Solutions/NERC 1.0/Response Filters/	CounterAct - Force Password Change - T...	
Filter	/All Filters/ArcSight Solutions/NERC 1.0/Response Filters/	TRM - Quarantine Attacker Address	
Filter	/All Filters/ArcSight Solutions/NERC 1.0/Response Filters/	TRM - Quarantine Target Address	
Endpoint	/All Endpoints/ArcSight Solutions/NERC 1.0/CDP-000 Critical Co...	Associate the Douchesack Network Device	


4. Optional—For future reference, you can copy and paste the cells from this table into a spreadsheet.

Back Up the Solution Package


ArcSight recommends that you have a backup of the current state before making content changes or installing/uninstalling solution packages. Before backing up a solution, you may want to get a list of changed resources. You may want to back up only those resources that have been modified or added. For detailed instructions, see ["Generate a List of Resource Changes" on the previous page](#).

You can back up the solution content to a package bundle file that ends in the `.arb` extension as described in the process below.

To back up a solution package:


1. Log into the ArcSight Console as ArcSight Administrator.
2. In the Packages tab of the Navigator panel, navigate to the solution group.
For Solution for NERC CIP, navigate to ArcSight Solutions/NERC 6.0.
3. Right-click the solution package () and select **Export Package(s) to Bundle**.
The Package Bundle Export dialog displays.
4. In the Package Bundle Export dialog, browse for a directory location, specify a file name and click **Next**.
The Progress tab of the Export Packages dialog displays the progress of the export.
5. When the export is finished, click **OK**.
The resources are saved into the package bundle file that ends with the `.arb` extension. You can restore the contents of this package at a later time by importing this package bundle file.

Uninstall the Solution for Solution for NERC CIP

Before uninstalling the Solution for NERC CIP, backup all the packages () for all the solutions currently installed on the ESM Manager.

For example, if the Solution for NERC CIP and the PCI solution are both installed on the same ArcSight ESM Manager, export the package(s) for each solution before uninstalling either solution. Back up the PCI package into a package bundle (ARB) file and then back up the Solution for NERC CIP into a different package bundle (ARB) file before uninstall either solution. For detailed instructions, see ["Back Up the Solution Package" above](#). You may also want to generate a list of changes before the uninstall. For detailed instructions, see ["Generate a List of Resource Changes" on the previous page](#).

To uninstall the Solution for NERC CIP:

1. Log into the ESM Console as a user with administrative privileges.
2. Click the Packages tab in the Navigator panel.
3. In the Packages tab of the Navigator panel, navigate to ArcSightSolutions/NERC 6.0.
4. Right-click the NERC 6.0 package () and select **Uninstall Package**.
5. In the Uninstall Packages dialog, click **OK**.
The progress of the uninstall displays in the Progress tab of the Uninstalling Packages dialog.
6. When the uninstall is finished, click **OK**.

Send Documentation Feedback

If you have comments about this document, you can [contact the documentation team](#) by email. If an email client is configured on this computer, click the link above and an email window opens with the following information in the subject line:

Feedback on Solutions Guide (ESM CIP for NERC 6.00)

Just add your feedback to the email and click send.

If no email client is available, copy the information above to a new message in a web mail client, and send your feedback to arc-doc@hpe.com.

We appreciate your feedback!