opentext™

OpenText
SIEM CIP for PCI DSS

Compliance Insight Package for Payment Card Industry Data Security Standard Solutions Guide

Document Release Date: July 2025
Software Release Date: July 2025

Legal Notices

Open Text Corporation

275 Frank Tompa Drive, Waterloo, Ontario, Canada, N2L 0A1

Copyright Notice

Trademark Notices

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/
OpenText™ SIEM Product Documentation	https://www.microfocus.com/documentation/arcsight/

Contents

Chapter 1: Overview

This section contains the following topics:

The PCI DSS

The Payment Card Industry (PCI) Data Security Standard (DSS) PCI 4.0 is a comprehensive standard defined by the Payment Card Industry Security Standards Council to help organizations protect cardholder data and to advance the broad adoption of consistent data security measures across the globe. The standard includes twelve requirements, each with many sub-requirements, for security management, policies, procedures, network architecture, software design, and other key protective measures.

Compliance Insight Package for Payment Card Industry (CIP for PCI) coupled with OpenText SIEM ESM can assist you in complying with the requirements specified in the (DSS) PCI DSS 4.0, and includes support for logs, like those generated by Supported Devices.

The following table lists the PCI DSS requirements.

Note: Excerpts from the PCI DSS and related control statements are provided courtesy of PCI Security Standards Council, LLC and/or its licensors. © 2023 PCI Security Standards Council, LLC. All Rights Reserved.

Objectives	PCI DSS Requirements
Build and Maintain a Secure Network and Systems	**1.** Install and maintain network security controls. **2.** Apply secure configurations to all system components.
Protect Account Data	**3.** Protect stored account data. **4.** Protect cardholder data with strong cryptography during transmission over open, public networks.
Maintain a Vulnerability Management Program	**5.** Protect all systems and networks from malicious software. **6.** Develop and maintain secure systems and software.

Objectives	PCI DSS Requirements
Implement Strong Access Control Measures	**7.** Restrict access to system components and cardholder data by business need to know. **8.** Identify users and authenticate access to system components. **9.** Restrict physical access to cardholder data.
Regularly Monitor and Test Networks	**10.** Log and monitor all access to system components and cardholder data. **11.** Test security of systems and networks regularly.
Maintain an Information Security Policy	**12.** Support information security with organizational policies and programs.

CIP for PCI Resources

contains the following OpenText SIEM ESM resources:

- **Active Lists**— capture static and dynamic data about compliance-related assets and events to aid in compiling and correlating data for the various PCI requirements.
- **Dashboards** and **Data Monitors**— help you demonstrate appropriate risk management and monitoring practices.
- **Filters**— focus package content on activity that involves compliance-relevant categorized assets.
- **Queries**— gather the compliance-related event data displayed by reports.
- **Query Viewers**— allow you to drill down and investigate anomalies or other interesting events without having to create low-level active channels. Query viewers use events and other resources, such as trends, active lists, session lists, assets, cases, and notifications, as data sources.
- **Reports**— focus on several aspects of regulation compliance.
- **Rules**— immediately identify activity that presents a high risk to the integrity of your systems that store and process compliance-relevant data.

All resources are listed and described in "Compliance Insight Package for the Payment Card Industry Resources by Type" on page 18.

Supported Devices

OpenText's PCI package acts on events from systems that store and process credit card data, and the systems that interact with and protect those systems, including the following:

- Applications that process cardholder data
- Databases that store cardholder data
- Operating systems
- Host and network-based IDS
- Firewalls
- Anti-virus solutions
- Vulnerability scanners that monitor system state
- Web servers
- Authentication systems
- Network devices
- Cloud Services

Chapter 1: Solution Installation and Configuration

This chapter contains information on installing and configuring the Compliance Insight Package for PCI DSS (CIP for PCI DSS).

Prepare for Installation

Before installing CIP for PCI DSS, complete the following preparation tasks:

1. "Prepare Environment" below
2. "Verify Environment" on the next page

Prepare Environment

Before installing, prepare your environment for the CIP for PCI DSS:

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

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

   Note: RFC 1918 addresses (10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16) are automatically categorized as protected because their zones already are categorized as protected.

Verify Environment

Before installing, verify your OpenText Enterprise Security Manager installation. Compliance Insight Package for PCI DSS is supported on OpenText Enterprise Security Manager. Refer to the OpenText Enterprise Security Manager technical requirements for operating system requirements. Refer also to the applicable release notes for the version in question.

Verify that your system has the supported ArcSight Console connected to the Manager.

Note: CIP for PCI DSS is a self-contained solution that does not rely on any other ArcSight solution. You can install CIP for PCI DSS alongside other solutions on the same ArcSight Manager. Before installing new solutions, OpenText recommends that you back up any existing solutions installed on the Manager.

Install Solution for PCI DSS CIP

The solution is supplied in a single ArcSight package bundle file called `ArcSight-ComplianceInsightPackage-PCI DSS.1.0.<nnnn>.arb`, where <nnnn> is the 4 character build number.

To install the CIP for PCI DSS package:

1. Using the login credentials supplied to you, download the CIP for PCI DSS bundle from the software download site to the machine where you plan to launch the ArcSight Console:

`ArcSight_ESM_Compliance_Pack_PCI DSS.v1.0.0.0.arb`

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 Console as an ArcSight Administrator.
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 `PCI DSS` 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/PCI DSS` group.

Assign User Permissions

By default, users in the `Default` user group can view CIP for PCI DSS 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 lists
- Dashboards
- Data monitors
- Field Sets
- Filters
- Queries
- Query Viewers

- Reports
- Rules

To assign user permissions:

1. Log into the Console as ArcSight Administrator.
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/PCI DSS`.
   b. Right-click the **PCI DSS** 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 CIP for PCI DSS resources and click **OK**.

Configure CIP for PCI DSS Solution

Several of the CIP for PCI DSS resources should be configured with values specific to your environment. Some features also require some additional SmartConnector configuration. This section describes these configuration processes.

Depending on the features you want to implement and how your network is set up, some configuration is required and some are optional. The list below shows all the configuration tasks involved with the CIP for PCI DSS and where to find instructions for performing the configuration.

This section contains the instructions required to enable content for the CIP for PCI DSS and contains the following topics:

The configuration processes outlined in this section apply to resources that feed the CIP for PCI DSS.

Model Assets (Assign Asset Categories)

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

- Some of the *CIP for PCI DSS* 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 *CIP for PCI DSS*.

CIP for PCI DSS Categorization

CIP for PCI DSS uses the asset categories under the `/ArcSight Solutions/Compliance Insight Package/`.

Categorizing Assets and Zones

CIP for PCI DSS solution relies on ArcSight asset and zone categorization to define your environment. Certain content does not display unless assets or zones are categorized. For detailed information about which assets and zones need to be categorized for each resource, refer to CIP for the Payment Card Industry Resources by Type.

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

Categorizing assets using the Console

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

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 CIP 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 Console (menu option **Tools > Network Model**). The Network Model wizard enables you to quickly populate the OpenText Enterprise Security Manager 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 on how to use this connector to configure your assets for CIP PCI DSS, see the *ArcSight Asset Import File SmartConnector Configuration Guide*.

Using the Limit Regulation Filter

To separate and monitor only the PCI assets and events in your environment, add the resources you want to be monitored in the form of network zones, categories, or individual assets to `/All Filters/ArcSight Solutions/PCI DSS/My Filters/Limit Regulation`. This filter ensures the solution processes only events relevant to PCI DSS regulations. By default, this filter is empty and will catch all events.

Customize it to your environment by specifying conditions such as:

- The source machine is a PCI-scoped asset.
- The source machine's zone is categorized as PCI.
- The destination machine is a PCI-scoped asset.
- The destination machine belongs to a PCI asset group.
- The destination machine's zone is categorized as PCI.
- The device machine is a PCI-scoped asset.
- The device machine belongs to a PCI asset group.
- The device machine's zone is categorized as PCI.

Configure Active Lists

CIP for PCI DSS contains numerous active lists that retain specific data that is cross-referenced dynamically during run-time by ArcSight resources that use conditions, such as filters, rules, and query viewers..

You can populate the PCI DSS active lists using any of the following processes:

- Add entries to active lists, one-by-one, using the Active List editor in the ArcSight Console. For detailed instructions, see "Configure Active Lists Using Console Active List Editor". 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". This method can be used to populate active lists with one, two, or more columns.

Active Lists Requiring Configuration defines the active lists that require configuration for the CIP for PCI DSS. Some active lists are intended to be populated by rules. Also, there are Active Lists requiring manual Configuration for the CIP PCI DSS.

Deploy the CIP for PCI DSS Rules

In order for the CIP for PCI DSS to process PCI DSS-related events, the solution rules have to be enabled By default, CIP for PCI DSS rules are disabled.

To enable a rule:

1. In the **Navigator** panel, go to **Rules** and navigate to the **Real-time Rules/PCI DSS** 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.

For more information about working with rules, see the *Rules Authoring* topic in the *ArcSight Console User's Guide*.

Appendix A: Backing Up and Uninstalling a Package

This chapter provides instructions on how back up a solution package, and uninstall the package.

Caution: There is no migration path from CIP for PCI 3.x or earlier. If you are running CIP for PCI DSS 3.x or earlier and you need to keep your current data, do not **uninstall** your earlier version; instead install 4.0 on a different system.

Generating a List of Resource Changes

Before backing up a solution package, you can generate a list of the 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.

Note: Every time a package is exported, the change history resets.

To generate a list of resource changes:

1. Log into the ArcSight Console with an account that has administrative privileges.
2. In the **Packages** tab of the Navigator panel, navigate to the solution group.

   For the CIP for PCI DSS, navigate to `ArcSight Solutions`.
3. Right-click the package for which you want to generate resource changes 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`.
4. Optional—For future reference, you can copy and paste the cells from this table into a spreadsheet.

Backing Up the Solution Package

Keep a backup of the current state before making content changes or installing and uninstalling solution packages. Before backing up a solution, you can obtain a list of changed resources. You can then back up only those resources that have been modified or added. For detailed instructions, see "Generating 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 with an account that has administrative privileges.
2. In the **Packages** tab of the Navigator panel, navigate to the solution group.

   For CIP for PCI DSS, navigate to `ArcSight Solutions/PCI DSS`.
3. Right-click the 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 complete, 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.

Uninstalling the Package

Before uninstalling the package, back up all the packages ( ) for all the solutions currently installed on the ArcSight Manager. For example, if the CIP for PCI and the CIP for SOX solutions are both installed on the same ArcSight Manager, export the package for each solution before uninstalling either solution. Back up the CIP for SOX package into a package bundle (ARB) file and then back up the CIP for PCI DSS into a different package bundle (ARB) file before uninstalling either solution. For detailed instructions, see "Backing Up the Solution Package" on the previous page. To generate a list of resource changes before the uninstall, see "Generating a List of Resource Changes" on page 15.

To uninstall the :

1. Log into the ArcSight Console with an account that has administrative privileges.

   Note: Uninstall packages using an `admin` account.

2. Click the **Packages** tab in the Navigator panel.
3. Navigate to `ArcSight Solutions`, right-click the package, and select **Uninstall Package**.
4. In the Uninstall Packages dialog, click **OK**. The progress of the uninstall displays in the Progress tab of the Uninstalling Packages dialog.
5. Choose the **Uninstall this and remaining packages without saving changes** option and will completely erase the selected package (but no others).
   If a message indicates that resources are locked, select the **Skip** option in the **Resolution Options** area and click **OK**.

   If a message indicates a conflict about changed package content, select the **Continue without saving changes** option and click **OK**.
6. When the uninstall is complete, review the summary and click **OK**.
7. Right-click the package and select **Delete Package.**

Appendix B: Compliance Insight Package for the Payment Card Industry Resources by Type

This appendix lists all the Compliance Insight Package for the Payment Card Industry resources by type.

Active Lists

The following table lists all the active lists in .

Active Lists Resources

Resource	Description	URI
Administrative Accounts	Contains the usernames that have administrative privileges in your domain. The administrator in charge of managing users with administrative privileges must populate this list manually when a new administrator is added to your environment. PCI Reports utilize this active list to track administrators and administrator activity. **Note:** Entries in this list should be in all lower case. For example, user "Administrator" should be added as "administrator."	/All Dashboards/ArcSight Solutions/PCI DSS/Requirement 1-Install and Maintain Network Security Controls
Allowed Ports	Contains all permissible destination ports (all permissible services). This active list should be populated according to your site policy.	/All Active Lists/ArcSight Solutions/PCI DSS
Anonymous Accounts	Contains the account names of anonymous users that are not unique and do not belong to a single individual user. All the entries in this list must be in lowercase.	/All Active Lists/ArcSight Solutions/PCI DSS
Badges to Accounts	Contains the computer account and employee type for every physical device badge. Populate this active list with badge IDs, primary computer account for badge holders (in case of visitors, use the visitor user name), and employee types for users in your organization (in lowercase). **Note:** Specifically, ensure that contractors and visitors are identified with the word “Contractor”or "Visitor" (case insensitive) in the employee type field.	/All Active List/ArcSight Solutions/PCI DSS/
Compliance Risk Score	Contains 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/PCI DSS

Active Lists Resources, continued

Resource	Description	URI
Default Vendor Accounts	Contains 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.	/All Active Lists/ArcSight Solutions/PCI DSS
Disallowed Ports	Contains all disallowed destination ports. This active list should be populated according to your site policy.	/All Active Lists/ArcSight Solutions/PCI DSS
File Integrity Monitoring	Contains the list of events from a particular vendor, product and hostname to track file integrity monitoring events. **Note:** To populate this active list, enable the following rule: File Integrity Monitoring.	/All Rules/ArcSight Solutions/PCI DSS/Requirement 11-Test Security of Systems and Networks Regularly
Insecure Ports	Contains ports that are used for insecure communication.	/All Active Lists/ArcSight Solutions/PCI DSS
Insecure Processes	Contains the names of processes that provide unencrypted and thus insecure communications.	/All Active Lists/ArcSight Solutions/PCI DSS
Password Changes	Contains the user and product information when a successful password change occurs.	/All Active Lists/ArcSight Solutions/PCI DSS
PCI Violations	Contains PCI violations.	/All Active Lists/ArcSight Solutions/PCI DSS

Dashboards

The following table lists all the dashboards in . You can find each resource under: `/All Dashboards/ArcSight Solutions/PCI DSS/(Requirement)/(Resource Name)`.

Dashboards Resources

Requirement	Resource	Description
N/A	Compliance Risk Score Overview	Displays information about the compliance risk score for each PCI Requirement. If you need to override the risk score status of a specific article, just right click on the article and choose the Override Status option. **Note:** To populate this dashboard, enable the rules in the following folder: `/All Rules/ArcSight Solutions/PCI DSS/Overview`
N/A	PCI Rules Overview	Displays a centralized view of security events and alerts related to the Payment Card Industry Data Security Standard.
PCI 1	Data Flow from CDE to non-CDE	Displays an overview of data flow from cardholder data environments to non cardholder data environments.
PCI 1	Data Flow from non-CDE to CDE	Displays an overview of data flow from non cardholder data environments to cardholder data environments.
PCI 1	Inbound Data Flow to Cardholder Data Environment	Displays an overview of data flow from non cardholder data environments to cardholder data environments.
PCI 1	Outbound Data Flow from Cardholder Data Environment	Displays an overview of data flow from cardholder data environments to non cardholder data environments.
PCI 5	Malware Overview	Displays an overview of malware activity in the organization.
PCI 5	Worm Activity	Displays a real-time overview of worm activity in your environment.
PCI 6	Vulnerability Overview	Displays a centralized view of vulnerabilities detected across the organization's PCI environment.
PCI 9	Physical Access Activity	Displays information around physical access. **Note:** For the Contractor Access After Hours" widget to populate, enable: `/All Rules/ArcSight Solutions/PCI DSS/Requirement 9-Restrict Physical Access to Cardholder Data/After Hours Building Access by Contractors`
PCI 10	Account Creation Deletion Modification Overview	Displays account creation, deletion, and modification activity which is a crucial tool for monitoring user activity and detecting potential security threats.

Dashboards Resources, continued

Requirement	Resource	Description
PCI 10	Administrative Actions Overview	Displays a comprehensive overview of administrative actions and privileged activities occurring within the organization's IT environment.
PCI 10	Failed Login Activity	Displays an overview of failed login activity.
PCI 10	Geo Threats Overview	Displays a geography-based threats reported on the organization.
PCI 10	Successful Login Activity	Displays provides an overview of successful login activity.
PCI 11	Attacks Overview	Displays an overview of attacks and suspicious related events reported on the organization based on ArcSight Categorization.
PCI 11	Traffic Anomaly	Displays an overview of traffic anomaly related events reported on the organization based on ArcSight Categorization.
PCI 12	Policy Violations Overview	Displays a centralized view of policy violations detected across the organization's IT environment.

Data Monitors

The following table lists all the data monitors in .

Data Monitors Resources

Resource	Description	URI
Account - Addition or Removal from Security Groups - Graph	Shows if an account is added or removed from a security group in the form of an event graph.	/All Data Monitors/ArcSight Solutions/PCI DSS/Requirement 10-Log and Monitor All Access to System Components and Cardholder Data/Account Activity Overview
Activity per 10 Minutes	Shows a moving average of outbound traffic from CDE, It displays data for the last hour and will generate a correlation event if the moving average is increased by 500%.	/All Data Monitors/ArcSight Solutions/PCI DSS/Requirement 1-Install and Maintain Network Security Controls/Data Flow from CDE to non-CDE
Activity per 10 Minutes	Shows a moving average of inbound traffic to CDE, It displays data for the last hour and will generate a correlation event if the moving average is increased by 500%.	/All Data Monitors/ArcSight Solutions/PCI DSS/Requirement 1-Install and Maintain Network Security Controls/Data Flow from non-CDE to CDE

Data Monitors Resources, continued

Resource	Description	URI
Attacks - Event Grpah	Shows attacker and target relationships.	/All Data Monitors/ArcSight Solutions/PCI DSS/Requirement 11-Test Security of Systems and Networks Regularly/Attacks and Suspicious Activity
Attacks and Suspicious Activity per 10 Minutes	Shows a moving average of attacks. It displays data for the last 10 minutes and will generate a correlation event if the moving average is increased by 300%.	/All Data Monitors/ArcSight Solutions/PCI DSS/Requirement 11-Test Security of Systems and Networks Regularly/Attacks and Suspicious Activity
Building Access - Event Graph	Shows the hour of day that users are accessing buildings.	/All Data Monitors /ArcSight Solutions/PCI DSS/Requirement 9-Restrict Physical Access to Cardholder Data/Physical Access Activity
Compliance Risk Score Overview	Shows 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/PCI DSS/Overview
Contractor Access After Hours	Shows the top contractors accesses after hours.	/All Data Monitors /ArcSight Solutions/PCI DSS/Requirement 9-Restrict Physical Access to Cardholder Data/Physical Access Activity
Failed Logins - Activity Graph	Shows failed login attacker and target relationships.	/All Data Monitors/ArcSight Solutions/PCI DSS/Requirement 10-Log and Monitor All Access to System Components and Cardholder Data/Failed Login Activitiy/
Failed Login - Top 10 Source IPs	Shows the top 10 attacker addresses involved in failed login activity.	/All Data Monitors/ArcSight Solutions/PCI DSS/Requirement 10-Log and Monitor All Access to System Components and Cardholder Data/Failed Login Activitiy/
Failed Login - Top 10 Target IPs	Shows the top 10 target addresses involved in failed login activity.	/All Data Monitors/ArcSight Solutions/PCI DSS/Requirement 10-Log and Monitor All Access to System Components and Cardholder Data/Failed Login Activitiy/

Data Monitors Resources, continued

Resource	Description	URI
Failed Login - Top 10 Users	Shows the top 10 users with failed login activity.	/All Data Monitors/ArcSight Solutions/PCI DSS/Requirement 10-Log and Monitor All Access to System Components and Cardholder Data/Failed Login Activitiy/
Frequent Failed Login per 10 Minutes	Shows a moving average of frequent failed login events. It displays data for the last 10 minutes and will generate a correlation event if the moving average is increased by 100%.	/All Data Monitors/ArcSight Solutions/PCI DSS/Requirement 10-Log and Monitor All Access to System Components and Cardholder Data/Failed Login Activitiy/
GeoView - DoS Activity	Shows a geographic view of DoS activity.	/All Data Monitors/ArcSight Solutions/PCI DSS/Requirement 10-Log and Monitor All Access to System Components and Cardholder Data/Geo Threats Overview
GeoView - MITRE ATT&CK Activity	Shows a geographic view of MITRE ATT&CK activity.	/All Data Monitors/ArcSight Solutions/PCI DSS/Requirement 10-Log and Monitor All Access to System Components and Cardholder Data/Geo Threats Overview
GeoView - Reconnaissance Activity	Shows a geographic view of reconnaissance activity.	/All Data Monitors/ArcSight Solutions/PCI DSS/Requirement 10-Log and Monitor All Access to System Components and Cardholder Data/Geo Threats Overview
Last Reported Events	Shows the last five data flow events from cardholder data environment to non-cardholder data environment.	/All Data Monitors/ArcSight Solutions/PCI DSS/Requirement 1-Install and Maintain Network Security Controls/Data Flow from CDE to non-CDE
Last Reported Events	Shows the last five data flow events from non-cardholder data environment to cardholder data environment.	/All Data Monitors/ArcSight Solutions/PCI DSS/Requirement 1-Install and Maintain Network Security Controls/Data Flow from non-CDE to CDE
Last 5 Attacks and Suspicious Activity Events	Shows the last five attack and suspicious activity events.	/All Data Monitors/ArcSight Solutions/PCI DSS/Requirement 11-Test Security of Systems and Networks Regularly/Attacks and Suspicious Activity

Data Monitors Resources, continued

Resource	Description	URI
Last 5 Traffic Anomaly Events	Shows the last five traffic anomaly activity events.	/All Data Monitors/ArcSight Solutions/PCI DSS/Requirement 11-Test Security of Systems and Networks Regularly/Attacks and Suspicious Activity
Last 10 Accounts Created	Shows the last 10 created accounts.	/All Data Monitors/ArcSight Solutions/PCI DSS/Requirement 10-Log and Monitor All Access to System Components and Cardholder Data/Account Activity Overview
Last 10 Accounts Deleted	Shows the last 10 deleted accounts.	/All Data Monitors/ArcSight Solutions/PCI DSS/Requirement 10-Log and Monitor All Access to System Components and Cardholder Data/Account Activity Overview
Last 10 Building Access Events	Shows the last 10 physical access events.	/All Data Monitors /ArcSight Solutions/PCI DSS/Requirement 9-Restrict Physical Access to Cardholder Data/Physical Access Activity
Last 10 Failed Administrative Action Events	Shows the last 10 failed administrative actions.	/All Data Monitors/ArcSight Solutions/PCI DSS/Requirement 10-Log and Monitor All Access to System Components and Cardholder Data/Administrative Actions
Last 10 Threats	Shows the last 10 events that indicate compromise, reconnaissance, hostile, or suspicious activity and MITRE Attacks.	/All Data Monitors/ArcSight Solutions/PCI DSS/Requirement 10-Log and Monitor All Access to System Components and Cardholder Data/Geo Threats Overview
Last 10 Worm Events	Shows the last ten worm events.	/All Data Monitors/Real-time Rules/PCI DSS/Requirement 5-Protect All Systems and Networks from Malicious Software
Malware Activity per 10 Minutes	Shows a moving average of malware event. It displays data for the last hour and will generate a correlation event if the moving average is increased by 500%.	/All Data Monitors/Requirement 5-Protect All Systems and Networks from Malicious Software/Malware Activity

Data Monitors Resources, continued

Resource	Description	URI
Outcome of Administrative Actions	Shows a moving average of the outcome of administrative actions.	/All Data Monitors/ArcSight Solutions/PCI DSS/Requirement 10-Log and Monitor All Access to System Components and Cardholder Data/Administrative Actions
PCI Requirements Distribution	Shows the 12 PCI requirements distribution from which the rules have triggered and needs more attention.	/All Data Monitors/ArcSight Solutions/PCI DSS/Overview
Rules Fired by Attacker and Target	Shows an event graph with attacker-target pair relationships for the various rule firings in your PCI environment.	/All Data Monitors/ArcSight Solutions/PCI DSS/Overview
Successful Login Activity - Top Attacker IPs	Shows the top 10 attacker addresses involved in successful login activity.	/All Data Monitors/ArcSight Solutions/PCI DSS/Requirement 10-Log and Monitor All Access to System Components and Cardholder Data/Succesful Login Activity/
Successful Login Activity - Top Users	Shows the top 10 users involved in successful login activity.	/All Data Monitors/ArcSight Solutions/PCI DSS/Requirement 10-Log and Monitor All Access to System Components and Cardholder Data/Succesful Login Activity/
Successful Login Activity - Top Source IPs	Shows the top 10 sources involved in successful login activity.	/All Data Monitors/ArcSight Solutions/PCI DSS/Requirement 10-Log and Monitor All Access to System Components and Cardholder Data/Succesful Login Activity/
Successful Login Activity - Login per 10 Minutes	Shows the moving average of successful login events. It displays data for the last 10 minutes and will generate a correlation event if the moving average is increased by 300%.	/All Data Monitors/ArcSight Solutions/PCI DSS/Requirement 10-Log and Monitor All Access to System Components and Cardholder Data/Succesful Login Activity/
Successful Login Activity - Top Target IPs	Shows the top 10 target addresses involved in successful login activity.	/All Data Monitors/ArcSight Solutions/PCI DSS/Requirement 10-Log and Monitor All Access to System Components and Cardholder Data/Succesful Login Activity/
Top Source IPs	Shows the top five source IPs involved on data flow from cardholder data environment to non cardholder data environment.	/All Data Monitors/ArcSight Solutions/PCI DSS/Requirement 1-Install and Maintain Network Security Controls/Data Flow from CDE to non-CDE

Data Monitors Resources, continued

Resource	Description	URI
Top Source IPs	Shows the top five source IPs involved on data flow from non-cardholder data environment to cardholder data environment.	/All Data Monitors/ArcSight Solutions/PCI DSS/Requirement 1-Install and Maintain Network Security Controls/Data Flow from non-CDE to CDE
Top Target IPs	Shows the top five target IPs involved on data flow from cardholder data environment to non cardholder data environment.	/All Data Monitors/ArcSight Solutions/PCI DSS/Requirement 1-Install and Maintain Network Security Controls/Data Flow from CDE to non-CDE
Top Target IPs	Shows the top five target IPs involved on data flow from non-cardholder data environment to cardholder data environment.	/All Data Monitors/ArcSight Solutions/PCI DSS/Requirement 1-Install and Maintain Network Security Controls/Data Flow from non-CDE to CDE
Top Target Ports	Shows the top five target ports involved on data flow from cardholder data environment to non cardholder data environment.	/All Data Monitors/ArcSight Solutions/PCI DSS/Requirement 1-Install and Maintain Network Security Controls/Data Flow from CDE to non-CDE
Top Target Ports	Shows the top five target ports involved on data flow from non-cardholder data environment to cardholder data environment.	/All Data Monitors/ArcSight Solutions/PCI DSS/Requirement 1-Install and Maintain Network Security Controls/Data Flow from non-CDE to CDE
Top 5 Administrative Users - Failed Actions	Shows the top five administrative users with failed actions in the last hour.	/All Data Monitors/ArcSight Solutions/PCI DSS/Requirement 10-Log and Monitor All Access to System Components and Cardholder Data/Administrative Actions
Top 5 Administrative Users - Successful Actions	Shows the top five administrative users with successful actions in the last hour.	/All Data Monitors/ArcSight Solutions/PCI DSS/Requirement 10-Log and Monitor All Access to System Components and Cardholder Data/Administrative Actions
Top 5 Target IPs	Shows the top five target IPs affected by malware.	/All Data Monitors/Real-time Rules/PCI DSS/Requirement 5-Protect All Systems and Networks from Malicious Software

Data Monitors Resources, continued

Resource	Description	URI
Top 5 Target IPs	Shows the top five target IPs for the Worm Activity dashboard.	/All Data Monitors/Real-time Rules/PCI DSS/Requirement 5-Protect All Systems and Networks from Malicious Software
Top 10 Attacker IPs	Shows the top 10 attacker IPs.	/All Data Monitors/ArcSight Solutions/PCI DSS/Requirement 11-Test Security of Systems and Networks Regularly/Attacks and Suspicious Activity
Top 10 Devices - Failed Administrative Actions	Shows the top 10 device products with failed actions by administrative users in the last hour.	/All Data Monitors/ArcSight Solutions/PCI DSS/Requirement 10-Log and Monitor All Access to System Components and Cardholder Data/Administrative Actions
Top 10 Devices - Successful Administrative Actions	Shows the top 10 device products with successful actions by administrative users in the last hour.	/All Data Monitors/ArcSight Solutions/PCI DSS/Requirement 10-Log and Monitor All Access to System Components and Cardholder Data/Administrative Actions
Top 10 Policy Violations	Shows the top 10 policy breach events.	/All Data Monitors/ArcSight Solutions/PCI DSS/Requirement 12-Support Information Security with Organizational Policies and Programs
Top 10 Policy Violated Users	Shows the top 10 policy violated target users.	/All Data Monitors/ArcSight Solutions/PCI DSS/Requirement 12-Support Information Security with Organizational Policies and Programs
Top 10 Policy Violators	Shows the top 10 policy violator source users.	/All Data Monitors/ArcSight Solutions/PCI DSS/Requirement 12-Support Information Security with Organizational Policies and Programs
Top 10 Rules Fired	Shows the top 10 rules fired in your PCI environment.	/All Data Monitors/ArcSight Solutions/PCI DSS/Overview
Top 10 Target Hosts Affected	Shows the top 10 targer hosts involved in rule firings in your PCI environment.	/All Data Monitors/ArcSight Solutions/PCI DSS/Overview
Top 10 Target IPs	Shows the top 10 target IPs.	/All Data Monitors/ArcSight Solutions/PCI DSS/Requirement 11-Test Security of Systems and Networks Regularly/Attacks and Suspicious Activit

Data Monitors Resources, continued

Resource	Description	URI
Top 10 Vulnerable Assets	Shows the top 10 vulnerable assets in your PCI environment.	/All Data Monitors/ArcSight Solutions/PCI DSS/Requirement 6-Develop and Maintain Secure Systems and Software
Top 10 Vulnerabilities Reported	Shows the top 10 vulnerabilities in your PCI environment.	/All Data Monitors/ArcSight Solutions/PCI DSS/Requirement 6-Develop and Maintain Secure Systems and Software
Top Users Accessing Buildings	Shows the top 10 users accessing buildings.	/All Data Monitors /ArcSight Solutions/PCI DSS/Requirement 9-Restrict Physical Access to Cardholder Data/Physical Access Activity
Traffic Anomaly - Event Graph	Shows traffic anomaly attacker and target relationships.	/All Data Monitors/ArcSight Solutions/PCI DSS/Requirement 11-Test Security of Systems and Networks Regularly/Traffic Anomaly
Traffic Anomaly per 10 Minutes	Shows a moving average of traffic anomaly. It displays data for the last 10 minutes and will generate a correlation event if the moving average is increased by 300%.	/All Data Monitors/ArcSight Solutions/PCI DSS/Requirement 11-Test Security of Systems and Networks Regularly/Traffic Anomaly
Very-High and High Severity Vulnerabilities	Shows very high and high severity vulnerabilities.	/All Data Monitors/ArcSight Solutions/PCI DSS/Requirement 6-Develop and Maintain Secure Systems and Software
Vulnerability Asset Graph	Shows recent vulnerability activity in the form of an event graph.	/All Data Monitors/ArcSight Solutions/PCI DSS/Requirement 6-Develop and Maintain Secure Systems and Software
Worm Activity per 10 Minutes	Shows real-time worm activity over the last ten minutes.	/All Data Monitors/Real-time Rules/PCI DSS/Requirement 5-Protect All Systems and Networks from Malicious Software
Worm Propagation	Shows worm propagation in your environment.	/All Data Monitors/Real-time Rules/PCI DSS/Requirement 5-Protect All Systems and Networks from Malicious Software

Field Sets

The following table lists all the field sets in .

Field Set Resources

Resource	Description	URI
Attacks and Suspicious Activity	Contains essential fields required to investigate attacks and suspicious activity.	/All Field Sets/ArcSight Solutions/PCI DSS/
Attacks and Suspicious Activity	Contains essential fields required to investigate attacks and suspicious activity.	/All Dashboards/ArcSight Solutions/PCI DSS/Requirement 11-Test Security of Systems and Networks Regularly/
Data Flow Events	Contains data flow event fields.	/All Field Sets/ArcSight Solutions/PCI DSS
User Authentication	Contains fields related to authentication events.	/All Field Sets/ArcSight Solutions/PCI DSS/

Filters

The following table lists all the filters in .

Filters Resources

Resource	Description	URI
Account Creation	Identifies account creation events.	/All Filters/ArcSight Solutions/PCI DSS/Requirement 10-Log and Monitor All Access to System Components and Cardholder Data/Accounts
Account Deletion	Identifies account deletion events.	/All Filters/ArcSight Solutions/PCI DSS/Requirement 10-Log and Monitor All Access to System Components and Cardholder Data/Accounts
Account Numbers Transmitted in Cleartext	Identifies events where primary account numbers are transmitted in cleartext.	/All Filters/ArcSight Solutions/PCI DSS/Requirement 4-Protect Cardholder Data with Strong Cryptography During Transmission Over Open, Public Networks
Administrative User	Identifies events with administrative users. These events include occurrences when the source or destination users are administrative users. **Note:** Administrative accounts have to be defined *in all lower case* in the active list Administrative Accounts.	/All Filters/ArcSight Solutions/PCI DSS/Requirement 10-Log and Monitor All Access to System Components and Cardholder Data
After Hours	Defines the time period of 'after hours'. Change this filter to adjust the default settings.	/All Filters/ArcSight Solutions/PCI DSS/My Filters

Filters Resources, continued

Resource	Description	URI
A Member was Added or Removed from a Group	Identifies when a user is added or removed from a group using windows events.	/All Filters/ArcSight Solutions/PCI DSS/Requirement 10-Log and Monitor All Access to System Components and Cardholder Data/Accounts
Anti-Malware Failed Update	Identifies failed anti-virus software update events.	/All Filters/Real-time Rules/PCI DSS/Requirement 5-Protect All Systems and Networks from Malicious Software
Anti-Virus Clean or Quarantine Attempt	Identifies anti-virus events that indicate a quarantine or cleaning attempt of a detected malware instance.	/All Filters/ArcSight Solutions/PCI DSS/Requirement 5-Protect All Systems and Networks from Malicious Software
Attacker Host or Address Present	Identifies events that have either the Attacker Host Name or Attacker Address event fields populated.	/All Filters/ArcSight Solutions/PCI DSS/General Filters
Attacks and Suspicious Activity	Identifies events which indicate compromise, reconnaissance, hostile, or suspicious activity.	/All Filters/ArcSight Solutions/PCI DSS/General Filters
Attacks and Suspicious Activity	Identifies events which indicate compromise, reconnaissance, hostile, or suspicious activity.	/All Filters/ArcSight Solutions/PCI DSS/Requirement 11-Test Security of Systems and Networks Regularly/Attacks and Suspicious Activity/
Attacks with Attacker Info	Identifies events with attacker info which indicate compromise, reconnaissance, hostile, or suspicious activity.	/All Filters/ArcSight Solutions/PCI DSS/Requirement 11-Test Security of Systems and Networks Regularly/Attacks and Suspicious Activity/
Attacks with Target Info	Identifies events with target info which indicate compromise, reconnaissance, hostile, or suspicious activity.	/All Filters/ArcSight Solutions/PCI DSS/Requirement 11-Test Security of Systems and Networks Regularly/Attacks and Suspicious Activity/
Audit Log Tool Access Events - ESM	Identifies user logins to OpenText Enterprise Security Manager, from where audit logs can be monitored.	/All Filters/ArcSight Solutions/PCI DSS/Requirement 10-Log and Monitor All Access to System Components and Cardholder Data
Building Access	Identifies building access events.	/All Filters/ArcSight Solutions/PCI DSS/Requirement 9-Restrict Physical Access to Cardholder Data

Filters Resources, continued

Resource	Description	URI
Cardholder Data Environment Inbound Events	Identifies all the cardholder data environment inbound traffic.	/All Filters/ArcSight Solutions/PCI DSS/General Filters/Data Flow
Cardholder Data Environment Outbound Events	Identifies all the cardholder data environment outbound traffic.	/All Filters/ArcSight Solutions/PCI DSS/General Filters/Data Flow
Compliance Score Updates	Identifies events that are generated when values in the Compliance Score active list are changed.	/All Filters/ArcSight Solutions/PCI DSS/General Filters/Overview/Risk Score Dashboard Overview
Cryptographic Protocols Flaws Events	Identifies cryptographic protocols flaw events.	/All Filters/ArcSight Solutions/PCI DSS/Requirement 6-Develop and Maintain Secure Systems and Software
Default Vendor Account Credential Observed	Identifies events where system access with vendor-supplied accounts is observed.	/All Filters/ArcSight Solutions/PCI DSS/Requirement 2-Apply Secure Configurations to All System Components
Default Vendor Account Detected	Identifies default accounts reported by vulnerability scans.	/All Filters/ArcSight Solutions/PCI DSS/Requirement 2-Apply Secure Configurations to All System Components
Destination Asset is CDE	Identifies events with destination in the cardholder data environment.	/All Filters/ArcSight Solutions/PCI DSS/General Filters/Assets
Destination Asset is Production	Identifies destination assets that belong to the production environment.	/All Filters/ArcSight Solutions/PCI DSS/General Filters/Assets
Destination Asset is Test	Identifies test environment assets in destination.	
DoS Attacks	Identifies reported denial of service attacks.	/All Filters/ArcSight Solutions/PCI DSS/Requirement 10-Log and Monitor All Access to System Components and Cardholder Data/Geo Threats Overview/
Failed Administrative Actions	Identifies failed administrative actions.	/All Filters/ArcSight Solutions/PCI DSS/Requirement 10-Log and Monitor All Access to System Components and Cardholder Data
Firewall Configuration Modifications	Identifies events when the configuration of a firewall is changed.	/All Filters/ArcSight Solutions/PCI DSS/General Filters/Configuration Changes

Filters Resources, continued

Resource	Description	URI
Vulnerabilities/High Risk Vulnerability Events	Identifies events related to very high and high risk vulnerabilities.	/All Filters/ArcSight Solutions/PCI DSS/General Filters
Limit Regulation	Ensures that the solution only processes events that are addressed by the regulation.	/All Filters/ArcSight Solutions/PCI DSS/My Filters
Login Attempts	Identifies any attempts at logging into systems. It excludes machine logins into Microsoft Windows systems.	/All Filters/ArcSight Solutions/PCI DSS/General Filters/Authentication/
Malicious Traffic to Cardholder Data Environment	Identifies malicious inbound traffic to the cardholder data environment.	/All Filters/ArcSight Solutions/PCI DSS/Requirement 1-Install and Maintain Network Security ControlsRequirement 1-Install and Maintain Network Security Controls
Malware Activity	Identifies events where malware activity is detected.	/All Filters/ArcSight Solutions/PCI DSS/Requirement 5-Protect All Systems and Networks from Malicious Software
Modifications to Log Files	Identifies modifications to log files.	/All Filters/ArcSight Solutions/PCI DSS/Requirement 10-Log and Monitor All Access to System Components and Cardholder Data
Multi-Factor Authentication Factor Deleted	Identifies events where a registered multi-factor authentication (MFA) factor has been removed or deleted from a user's account or system.	/All Filters/ArcSight Solutions/PCI DSS/Requirement 8-Identify Users and Authenticate Access to System Components
Network Device Configuration Modifications	Identifies events when the configuration of an infrastructural equipment (router, switch) is changed.	/All Filters/ArcSight Solutions/PCI DSS/General Filters/Configuration Changes
Network IDS Configuration Modifications	Identifies events when the configuration of NIDS equipment is changed.	/All Filters/ArcSight Solutions/PCI DSS/General Filters/Configuration Changes
Network Routing Configuration Modifications	Identifies events when a modification to the routing table of infrastructure equipment (router, switch) is made.	/All Filters/ArcSight Solutions/PCI DSS/General Filters/Configuration Changes
PCI Rule Alert with Attacker IP and Target IP Info	Identifies all PCI-DSS rules firing events with attacker and target IPs populated.	/All Filters/ArcSight Solutions/PCI DSS/General Filters/Overview
PCI Rule Alert with Target Host Info	Identifies all PCI-DSS rules firing events with target host information populated.	/All Filters/ArcSight Solutions/PCI DSS/General Filters/Overview

Filters Resources, continued

Resource	Description	URI
PCI Rule Firing	Identifies all PCI-DSS rules firing events.	/All Filters/ArcSight Solutions/PCI DSS/General Filters/Overview/Risk Score Dashboard Overview
Personal Records Information Leak	Identifies information leaks with regard to personal information.	/All Filters/ArcSight Solutions/PCI DSS/General Filters/Information Leakage
Physical Access Events	Identifies events sent to OpenText Enterprise Security Manager by physical security systems.	/All Filters/ArcSight Solutions/PCI DSS/Requirement 9-Restrict Physical Access to Cardholder Data
Policy Violations	Identifies policy violation events.	/All Filters/ArcSight Solutions/PCI DSS/Requirement 12-Support Information Security with Organizational Policies and Programs
Recon Activity	Identifies events that indicate reconnaissance activity.	/All Filters/ArcSight Solutions/PCI DSS/Requirement 10-Log and Monitor All Access to System Components and Cardholder Data/Geo Threats Overview/
Security Software Stopped or Paused	Identifies indicating security software stopped or paused.	/All Filters/ArcSight Solutions/PCI DSS/General Filters
Source Asset is CDE	Identifies events with source in the cardholder data environment.	/All Filters/ArcSight Solutions/PCI DSS/General Filters/Assets
Source Asset is Production	Identifies source assets that belong to the production environment.	/All Filters/ArcSight Solutions/PCI DSS/General Filters/Assets
Source Asset is Test	Identifies test environment assets in source.	/All Filters/ArcSight Solutions/PCI DSS/General Filters/Assets
Successful Administrative Actions	Identifies successful administrative actions.	/All Filters/ArcSight Solutions/PCI DSS/Requirement 10-Log and Monitor All Access to System Components and Cardholder Data
Successful After Hours Building Access	Identifies successful building access attempts after hours. The actual time definition is defined in the After Hours filter.	/All Filters/ArcSight Solutions/PCI DSS/Requirement 9-Restrict Physical Access to Cardholder Dat
Successful Badge In	Identifies successful badge-in events.	/All Filters/ArcSight Solutions/PCI DSS/Requirement 9-Restrict Physical Access to Cardholder Dat
Successful Logins	Identifies successful login events.	/All Filters/ArcSight Solutions/PCI DSS/General Filters/Authentication/

Filters Resources, continued

Resource	Description	URI
Successful Logins with Attacker Info	Identifies successful logins by both administrative and non-administrative users with attacker info.	/All Filters/ArcSight Solutions/PCI DSS/General Filters/Authentication/
Successful Logins with Target Info	Identifies successful logins by both administrative and non-administrative users with target info.	/All Filters/ArcSight Solutions/PCI DSS/General Filters/Authentication/
Suspicious and Anomalous Activity	Identifies unusual and anomalous events with exhibit suspicious characteristics.	/All Filters/ArcSight Solutions/PCI DSS/Requirement 10-Log and Monitor All Access to System Components and Cardholder Data
Spyware Activity	Identifies spyware activity events reported by either an Intrusion Detection System (IDS) or an anti-virus application.	/All Filters/ArcSight Solutions/PCI DSS/Requirement 5-Protect All Systems and Networks from Malicious Software
System Failure Events	Identifies system failure events.	/All Filters/ArcSight Solutions/PCI DSS/Requirement 10-Log and Monitor All Access to System Components and Cardholder Data
Target Host or Address Present	Identifies events that have either the Target Host Name or Target Address event fields populated.	/All Filters/ArcSight Solutions/PCI DSS/General Filters
Target User is Admin	Identifies events with administrative users where the target user is an admin.	/All Filters/ArcSight Solutions/PCI DSS/Requirement 10-Log and Monitor All Access to System Components and Cardholder Data
Target User Present	Identifies if the Target User Name field is populated.	/All Filters/ArcSight Solutions/PCI DSS/General Filters
Traffic Anomaly	Identifies traffic anomaly attacks.	/All Filters/ArcSight Solutions/PCI DSS/Requirement 11-Test Security of Systems and Networks Regularly/Traffic Anomaly/
Traffic Anomaly with Attacker Info	Identifies traffic anomalies with attacker info.	/All Filters/ArcSight Solutions/PCI DSS/Requirement 11-Test Security of Systems and Networks Regularly/Traffic Anomaly/
Traffic Anomaly with Target Info	Identifies traffic anomalies with target info.	/All Filters/ArcSight Solutions/PCI DSS/Requirement 11-Test Security of Systems and Networks Regularly/Traffic Anomaly/

Filters Resources, continued

Resource	Description	URI
Threats	Identifies events that indicate compromise, reconnaissance, hostile, or suspicious activity and MITRE Attacks.	/All Filters/ArcSight Solutions/PCI DSS/Requirement 10-Log and Monitor All Access to System Components and Cardholder Data/Geo Threats Overview/
Trojan Activity	Identifies trojan activity.	/All Filters/ArcSight Solutions/PCI DSS/Requirement 5-Protect All Systems and Networks from Malicious Software
Unsuccessful Badge In	Identifies unsuccessful badge in events.	/All Filters/ArcSight Solutions/PCI DSS/Requirement 9-Restrict Physical Access to Cardholder Data
Unsuccessful Logins	Identifies unsuccessful logins.	/All Filters/ArcSight Solutions/PCI DSS/Requirement 10-Log and Monitor All Access to System Components and Cardholder Data/Authentication/Unsuccessful Logins
Unsuccessful Logins with Attacker Info	Identifies failed logins by both administrative and non-administrative users with attacker information.	/All Filters/ArcSight Solutions/PCI DSS/General Filters
Unsuccessful Logins with Attacker and User Info	Identifies failed logins by both administrative and non-administrative users with attacker and user info.	/All Filters/ArcSight Solutions/PCI DSS/General Filters
Unsuccessful Logins with Target Info	Identifies failed logins by both administrative and non-administrative users with target information.	/All Filters/ArcSight Solutions/PCI DSS/General Filters
Virus Activity	Identifies virus activity events reported by either an Intrusion Detection System (IDS) or an anti-virus application.	/All Filters/ArcSight Solutions/PCI DSS/Requirement 5-Protect All Systems and Networks from Malicious Software
VPN Configuration Modifications	Identifies events indicating that a VPN configuration change has occurred.	/All Filters/ArcSight Solutions/PCI DSS/General Filters/Configuration Changes
Vulnerability Events	Identifies vulnerability related events.	/All Filters/ArcSight Solutions/PCI DSS/General Filters/Vulnerabilities
Vulnerability Events by Non-Scanners	Identifies vulnerability events reported by non-scanner devices.	/All Filters/ArcSight Solutions/PCI DSS/Requirement 6-Develop and Maintain Secure Systems and Software

Filters Resources, continued

Resource	Description	URI
Vulnerability Scanner Events	Identifies scanner-generated events.	/All Filters/ArcSight Solutions/PCI DSS/Requirement 6-Develop and Maintain Secure Systems and Software
Weak Password	Identifies Identifies events with user accounts that have weak or easily guessable passwords.	/All Filters/ArcSight Solutions/PCI DSS/Requirement 8-Identify Users and Authenticate Access to System Components
Windows Events with a Non-Machine User	Identifies Microsoft Windows events that have a non machine/system user either in the attacker or the target fields.	/All Filters/ArcSight Solutions/PCI DSS/General Filters/Authentication/
Wireless Related Events	Identifies wireless events reported from those products AirDefense, AirPatrolCorp, AirMagnet or events related to assets which categorized as/All Asset Categories/Industrial Control Systems/Wireless Network.	/All Filters/ArcSight Solutions/PCI DSS/General Filters/Wireless
Wireless Vulnerability or Misconfiguration Detected	Identifies wireless-related vulnerabilities and misconfigurations reported by vulnerability scans.	/All Filters/ArcSight Solutions/PCI DSS/Requirement 2-Apply Secure Configurations to All System Components
Worm Activity	Identifies events where worm activity is detected based on both correlation and base events reported by ArcSight Connectors.	/All Filters/ArcSight Solutions/PCI DSS/Requirement 5-Protect All Systems and Networks from Malicious Software
Worm Reported Events	Identifies events where worm activity is reported by ArcSight Connectors.	/All Filters/ArcSight Solutions/PCI DSS/Requirement 5-Protect All Systems and Networks from Malicious Software

Queries

The following table lists all the queries in .

Queries Resources

Resources	Description	URI
Accesses from Third Party Entities	Identifies all access attempts to third party assets.	/All Queries/ArcSight Solutions/PCI DSS/Requirement 8-Identify Users and Authenticate Access to System Components
Audit Log Tool Access Events	Identifies all access events related to the audit log tool itself.	/All Queries/ArcSight Solutions/PCI DSS/Requirement 10-Log and Monitor All Access to System Components and Cardholder Data
Cardholder Data Environment Inbound Traffic	Identifies cardholder data environment inbound traffic.	/All Queries/ArcSight Solutions/PCI DSS/Requirement 1-Install and Maintain Network Security Controls
Cardholder Data Environment Outbound Traffic	Identifies cardholder data environment outbound traffic.	/All Queries/ArcSight Solutions/PCI DSS/Requirement 1-Install and Maintain Network Security Controls
Cryptographic Protocols Flaws Summary	Identifies an overview of the cryptographic protocols flaws summary on PCI assets.	/All Queries/ArcSight Solutions/PCI DSS/Requirement 6-Develop and Maintain Secure Systems and Software
DoS Summary	Identifies DoS events.	/All Queries/ArcSight Solutions/PCI DSS/ Requirement 11-Test Security of Systems and Networks Regularly
Firewall Configuration Modifications	Identifies any configuration modifications of any firewall. Default time window: Last 24 hours.	/All Queries/ArcSight Solutions/PCI DSS/Requirement 1-Install and Maintain Network Security Controls
Firewall Configuration Modifications by Name	Identifies the top configuration modifications of any firewall.	/All Queries/ArcSight Solutions/PCI DSS/Requirement 1-Install and Maintain Network Security Controls
IDS Configuration Modifications	Identifies any configuration modifications of any network IDS. Default time window: Last 24 hours.	/All Queries/ArcSight Solutions/PCI DSS/Requirement 1-Install and Maintain Network Security Controls
IDS Configuration Modifications by Name	Identifies the top configuration modifications of any network IDS.	/All Queries/ArcSight Solutions/PCI DSS/Requirement 1-Install and Maintain Network Security Controls

Queries Resources, continued

Resources	Description	URI
List of Default Vendor Account Used	Identifies a list of default vendor account used. The default time is 24 hours.	/All Queries/ArcSight Solutions/PCI DSS/Requirement 2-Apply Secure Configurations to All System Components
List of Failed Logins	Identifies failed login events.	/All Queries/ArcSight Solutions/PCI DSS/Requirement 10-Log and Monitor All Access to System Components and Cardholder Data
List of Failed Physical Access Attempts	Identifies failed physical access attempts. The default time is 24 hours.	/All Queries/ArcSight Solutions/PCI DSS/Requirement 9-Restrict Physical Access to Cardholder Data
List of Malware	Identifies malware activity across your environment.	/All Queries/ArcSight Solutions/PCI DSS/Requirement 5-Protect All Systems and Networks from Malicious Software/List of Malware
List of Non Unique Accounts	Identifies non unique accounts. The default time is 24 hours.	/All Queries/ArcSight Solutions/PCI DSS/Requirement 8-Identify Users and Authenticate Access to System Components
List of Operating System Configuration Changes	Identifies a list of operating system configuration changes. The default time is 24 hours.	/All Queries/ArcSight Solutions/PCI DSS/Requirement 10-Log and Monitor All Access to System Components and Cardholder Data
List of Physical Reporting Devices	Identifies a list of physical reporting devices. The default time is 24 hours.	/All Queries/ArcSight Solutions/PCI DSS/Requirement 9-Restrict Physical Access to Cardholder Data
List of Successful Physical Access Attempts	Identifies successful physical access attempts. The default time is 24 hours.	/All Queries/ArcSight Solutions/PCI DSS/Requirement 9-Restrict Physical Access to Cardholder Data
List of Wireless Vulnerabilities and Misconfigurations	Identifies a list of wireless vulnerabilities and misconfigurations reported by vulnerability scanner devices. The default time is 24 hours.	/All Queries/ArcSight Solutions/PCI DSS/Requirement 2-Apply Secure Configurations to All System Components
Log Files Modification Summary	Identifies log file modifications.	/All Queries/ArcSight Solutions/PCI DSS/Requirement 10-Log and Monitor All Access to System Components and Cardholder Data
Network Routing Configuration Modifications	Identifies any configuration modifications of any network routing. The default time is 24 hours.	/All Queries/ArcSight Solutions/PCI DSS/Requirement 1-Install and Maintain Network Security Controls

Queries Resources, continued

Resources	Description	URI
Network Routing Configuration Modifications by Name	Identifies the top configuration modifications of any network routing.	/All Queries/ArcSight Solutions/PCI DSS/Requirement 1-Install and Maintain Network Security Controls
PAN in Cleartext Transmission Events	Identifies the data of clear text credit card and bank account numbers transmitted in the network.	/All Queries/ArcSight Solutions/PCI DSS/Requirement 4-Protect Cardholder Data with Strong Cryptography During Transmission Over Open, Public Networks
Password Weakness Summary	Identifies events with user accounts that have weak or easily guessable passwords.	/All Queries/ArcSight Solutions/PCI DSS/Requirement 8-Identify Users and Authenticate Access to System Components
PCI Rule Firing Events	Identifies triggered PCI rules.	/All Queries/ArcSight Solutions/PCI DSS/Overview
Policy Violations from Third-Party Assets	Identifies events categorized by ArcSight as policy violations coming from assets categorized as Third-Party.	/All Queries/ArcSight Solutions/PCI DSS/Requirement 12-Support Information Security with Organizational Policies and Programs
Security Software Stopped or Paused	Identifies security software stopped or paused.	/All Queries/ArcSight Solutions/PCI DSS/Requirement 1-Install and Maintain Network Security Controls
Summary of Failed Physical Access Attempts	a list of failed physical access attempts	/All Reports/ArcSight Solutions/PCI DSS/Requirement 9-Restrict Physical Access to Cardholder Data
Summary of System Failures	Identifies system failure events.	/All Queries/ArcSight Solutions/PCI DSS/Requirement 10-Log and Monitor All Access to System Components and Cardholder Data
Suspicious and Anomalous Activity	Identifies potentially harmful activities within an organization's IT environment that deviate from established baselines or normal behavior patterns.	/All Queries/ArcSight Solutions/PCI DSS/Requirement 10-Log and Monitor All Access to System Components and Cardholder Data
Top Default Vendor Accounts	Identifies the top default vendor accounts.	/All Queries/ArcSight Solutions/PCI DSS/Requirement 2-Apply Secure Configurations to All System Components
Top DoS Attackers	Identifies top DoS attackers. The default time is 24 hours.	/All Queries/ArcSight Solutions/PCI DSS/ Requirement 11-Test Security of Systems and Networks Regularly
Top DoS Targets	Identifies top DoS targets. The default time is 24 hours.	/All Queries/ArcSight Solutions/PCI DSS/ Requirement 11-Test Security of Systems and Networks Regularly

Queries Resources, continued

Resources	Description	URI
Top Failed Physical Access Buildings	Identifies the top failed physical access buildings. The default time is 24 hours.	/All Queries/ArcSight Solutions/PCI DSS/Requirement 9-Restrict Physical Access to Cardholder Data
Top Failed Physical Access Users	Identifies the top failed physical access users. The default time is 24 hours.	/All Queries/ArcSight Solutions/PCI DSS/Requirement 9-Restrict Physical Access to Cardholder Data
Top Non Unique Accounts	Identifies the top non unique accounts. Default time window: Last 24 hours.	/All Queries/ArcSight Solutions/PCI DSS/Requirement 8-Identify Users and Authenticate Access to System Components
Top Operating System Configuration Changes	Identifies the top operating system configuration changes.	/All Queries/ArcSight Solutions/PCI DSS/Requirement 10-Log and Monitor All Access to System Components and Cardholder Data
Top Physical Reporting Devices	Identifies the top physical reporting devices. The default time is 24 hours.	/All Queries/ArcSight Solutions/PCI DSS/Requirement 9-Restrict Physical Access to Cardholder Data
Top Successful Physical Access Users	Identifies the top successful physical access users. The default time is 24 hours.	/All Queries/ArcSight Solutions/PCI DSS/Requirement 9-Restrict Physical Access to Cardholder Data
Top Successful Physical Access Buildings	Identifies the top successful physical access buildings. The default time is 24 hours.	/All Queries/ArcSight Solutions/PCI DSS/Requirement 9-Restrict Physical Access to Cardholder Data
Unmasked Primary Account Numbers	Identifies data of stored or transmitted unmasked PAN.	/All Queries/ArcSight Solutions/PCI DSS/Requirement 3-Protect Stored Account Data/
VPN Configuration Modifications	Identifies any configuration modifications of any vpn device. Default time window: Last 24 hours.	/All Queries/ArcSight Solutions/PCI DSS/Requirement 1-Install and Maintain Network Security Controls
VPN Configuration Modifications by Name	Identifies the top configuration modifications of any vpn device.	/All Queries/ArcSight Solutions/PCI DSS/Requirement 1-Install and Maintain Network Security Controls
Vulnerabilities Summary	Identifies a vulnerability summary of PCI assets.	/All Queries/ArcSight Solutions/PCI DSS/Requirement 6-Develop and Maintain Secure Systems and Software

Query Viewers

The following table lists all the query viewers in .

Query Viewers Resources

Resource	Description	URI
PCI Rule Firing Events	Provides a listing of PCI correlation events on the last hour.	/All Query Viewers/ArcSight Solutions/PCI DSS/Overview

Reports

The following table lists all the reports in . You can find each resource under: `/All Reports/ArcSight Solutions/PCI DSS/(Requirement)/(Resource Name)`.

Requirement	Resource	Description
PCI 1	Cardholder Data Environment Inbound Traffic	Summarizes cardholder data environment inbound traffic.
PCI 1	Cardholder Data Environment Outbound Traffic	Summarizes cardholder data environment outbound traffic.
PCI 1	Firewall Configuration Modifications	Summarizes any configuration modifications of any firewall.
PCI 1	IDS Configuration Modifications	Summarizes any configuration modifications of any network IDS.
PCI 1	Network Routing Configuration Modifications	Summarizes any configuration modifications of any network routing.
PCI 1	Security Software Stopped or Paused	Summarizes security software stopped or paused events.
PCI 1	VPN Configuration Modifications	Summarizes any configuration modifications of any vpn device.
PCI 2	Summary of Default Vendor Accounts	Summarizes default vendor accounts used.
PCI 2	Summary of Wireless Vulnerabilities and Misconfigurations	Summarizes wireless vulnerabilities and misconfigurations.

, continued

Requirement	Resource	Description
PCI 3	Unmasked PAN Summary	Summarizes the data of unmasked plain text Primary Account Numbers like bank, credit cards, and others stored or transmitted in the network on an hourly basis.
PCI 4	Summary of Cleartext Account Numbers Transmission Events	Summarizes the data of clear text credit card and bank account numbers transmitted in the network.
PCI 5	Malware Summary	Summarizes malware activity. This report features prominent malware types, threats, and malware event information.
PCI 6	Summary of Cryptographic Protocols Flaws	Summarizes of the cryptographic protocols flaws in the last 24 hours.
PCI 6	Summary of Configuration Changes	Summarizes configuration changes within the PCI environment.
PCI 6	Summary of Outbound Communication between Production and Pre-Production Environment	Summarizes outbound communications between production and pre-production within the PCI environment.
PCI 6	Summary of Vulnerabilities	Summarizes the vulnerabilities in the last 24 hours.
PCI 7	Summary of Account Changes	Summarizes the account changes within the PCI environment.
PCI 7	Summary of Unauthorized Accesses to Cardholder Data	Summarizes unauthorized access attempts to your cardholder data. **Note:** The cardholder cata assets should be categorized under: `All Assets Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/Cardholder Data`
PCI 8	Access from Third Party Entities	Summarizes all access attempts to third party assets.
PCI 8	Account Lockout Activity	Summarizes account lockout activity in your PCI environment.
PCI 8	Password Weakness Summary	Summarizes events with user accounts that have weak or easily guessable passwords.
PCI 8	Summary of Non Unique Accounts	Summarizes non unique accounts.
PCI 9	Summary of Successful Physical Access Events	Summarizes successful physical access events.
PCI 9	Summary of Failed Physical Access Attempts	Summarizes failed physical access attempts.

, continued

Requirement	Resource	Description
PCI 9	Summary of Physical Reporting Devices	Summarizes physical reporting devices.
PCI 10	Audit Log Tool Access Summary	Summarizes all access and activity related to the organization's audit log tool.
PCI 10	Summary of System Failures	Summarizes system failures detected within the specified reporting period.
PCI 10	Log Files Modification Summary	Summarizes modifications made to log files within the organization's IT infrastructure.
PCI 10	Summary of Failed Logins	Summarizes failed login attempts.
PCI 10	Summary of Insecure Ports	Summarizes insecure ports.
PCI 10	Summary of Operating System Configuration Changes	Summarizes operating system configuration changes.
PCI 10	Suspicious and Anomalous Activity Summary	Summarizes suspicious and anomalous activities detected within the organization's IT environment over a specific period.
PCI 11	Attempted File Changes in Cardholder Data Originated from Third Party	Summarizes attempted file changes originating from third parties.
PCI 11	Attempted File Changes in Cardholder Data Originated from Non-Production	Summarizes attempted file changes originating from non-production.
PCI 11	Attempted File Changes in Cardholder Data Originated from Production	Summarizes attempted file changes originating from production.
PCI 11	DoS Summary	Summarizes DoS events.
PCI 12	Policy Violations from Third-Party Assets	Summarizes events categorized by ArcSight as policy violations coming from assets categorized as Third-Party.
PCI 12	Summary of Reporting Devices	Summarizes reporting devices.
PCI 12	Summary of Third-Party Access	Summarizes attempts to access third-parties.

Rules

The following table lists all the rules in . You can find each resource under: `/All Rules/ArcSight Solutions/PCI DSS/(Requirement)/(Resource Name)`.

Requirement 1: Install and Maintain Network Security Controls

Requirement	Resource	Description
PCI 1.2, 1.2.1, 1.2.2	Critical Configuration Change to NSC device	Detects changes in the configuration of NSC Devices that are classified with a “very-high” agent severity. Devices include Firewalls, VPNs, Network Equipment, Network Routings, and Network Intrusion Detection Systems.
PCI 1.3.1, 1.4.1, 1.4.2	Unauthorized Traffic to Cardholder Data Environment	Detects unauthorized inbound traffic to the cardholder data environment. **Note:** To trigger this rule, categorize the cardholder data environment assets under: `All Asset Categories/ArcSight Solutions/Compliance Insight Package/Regulations/PCI/Cardholder Data`

PCI 1.3.1,
1.4.1,
1.4.2
	Unauthorized Traffic to Cardholder Data Environment from DMZ	Detects unauthorized outbound traffic to the cardholder data environment from DMZ.
		Note: To trigger this rule, ensure:
		1. The DMZ assets are categorized under:
		`/All Assets Categories/ArcSight Solutions/Compliance Insight Package/Address Spaces/DMZ`
		2. Enable:
		`/All Rules/ArcSight Solutions/PCI DSS/Requirement 1-Install and Maintain Network Security ControlsRequirement 1-Install and Maintain Network Security Controls/Unauthorized Traffic from Cardholder Data Environment`

Requirement 1: Install and Maintain Network Security Controls, continued

Requirement	Resource	Description

PCI 1.3.1,
1.4.1,
1.4.2
	Unauthorized Traffic to Cardholder Data Environment from Third Party Asset	Detects unauthorized outbound traffic to the cardholder data environment from third-party assets.
		Note: To trigger this rule, ensure:
		1. The third-party Assets are categorized under:
		`/All Assets Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/Third Party`
		2. Enable:
		`/All Rules/ArcSight Solutions/PCI DSS/Requirement 1-Install and Maintain Network Security ControlsRequirement 1-Install and Maintain Network Security Controls/Unauthorized Traffic from Cardholder Data Environment`

PCI 1.3.1,
1.4.1,
1.4.2
	Unauthorized Traffic to Cardholder Data Environment from Wireless Environment	Detects unauthorized outbound traffic to the cardholder data environment from the wireless environment.
		Note: To trigger this rule, ensure:
		1. The wireless assets are categorized under:
		`/All Assets Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/Wireless`
		2. Enable:
		`/All Rules/ArcSight Solutions/PCI DSS/Requirement 1-Install and Maintain Network Security ControlsRequirement 1-Install and Maintain Network Security Controls/Unauthorized Traffic from Cardholder Data Environment`

PCI 1.3.2, 1.4.1	Unauthorized Traffic from Cardholder Data Environment	Detects unauthorized outbound traffic from the cardholder data environment. **Note:** To trigger this rule, categorize the cardholder data environment assets under: `Asset Categories/ArcSight Solutions/Compliance Insight Package/Regulations/PCI/Cardholder Data`

Requirement 1: Install and Maintain Network Security Controls, continued

Requirement	Resource	Description

PCI 1.3.2,
1.4.1
	Unauthorized Traffic from Cardholder Data Environment to DMZ	Detects unauthorized outbound traffic from the cardholder data environment to DMZ.
		Note: To trigger this rule, ensure:
		1. The DMZ assets are categorized under:
		`/All Assets Categories/ArcSight Solutions/Compliance Insight Package/Address Spaces/DMZ`
		2. Enable:
		`/All Rules/ArcSight Solutions/PCI DSS/Requirement 1-Install and Maintain Network Security ControlsRequirement 1-Install and Maintain Network Security Controls/Unauthorized Traffic from Cardholder Data Environment`

PCI 1.3.2,
1.4.1
	Unauthorized Traffic from Cardholder Data Environment to Third Party Asset	Detects unauthorized outbound traffic from the cardholder data environment to third-party assets.
		Note: To trigger this rule, ensure:
		1. Categorize third-party assets under:
		`/All Assets Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/Third Party`
		2. Enable:
		`/All Rules/ArcSight Solutions/PCI DSS/Requirement 1-Install and Maintain Network Security ControlsRequirement 1-Install and Maintain Network Security Controls/Unauthorized Traffic from Cardholder Data Environment`

Requirement 1: Install and Maintain Network Security Controls, continued

Requirement	Resource	Description

PCI 1.3.2,
1.4.1
	Unauthorized Traffic from Cardholder Data Environment to Wireless Environment	Detects unauthorized outbound traffic from the cardholder data environment to the wireless environment.
		Note: To trigger this rule, ensure:
		1. Categorize wireless assets under:
		`/All Assets Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/Wireless`
		2. Enable:
		`/All Rules/ArcSight Solutions/PCI DSS/Requirement 1-Install and Maintain Network Security ControlsRequirement 1-Install and Maintain Network Security Controls/Unauthorized Traffic from Cardholder Data Environment`

PCI 1.4.4	Personal Information Leakage	Detects personal information leakage.
PCI 1.4.4	Personal Information Leakage from Database	Detects personal Information Leakage from Database on Cardholder Data Environment. **Note:** To trigger this rule, categorize the database assets under: `/All Assets Categories/ArcSight Solutions/Compliance Insight Package/Application/Type/Database`
PCI 1.4.5	Database Reachable from Internet	Detects events coming from outside the organization network targeting database assets. **Note:** To trigger this rule, categorize the database assets under: `/All Assets Categories/ArcSight Solutions/Compliance Insight Package/Application/Type/Database`
PCI 1.5.1	Malicious Traffic to Cardholder Data Environment	Detects malicious inbound traffic to the cardholder data environment.
PCI 1.5.1, 5.3.1, 5.3.5, 10.7.1	Security Software Stopped or Paused	Detects that a security software service has been disabled. Refer to the condition tab of this rule for the list of services.
PCI 1.5.1	Wireless Malicious Traffic Detected	Detects wireless malicious traffic based on events reported from AirDefense, AirPatrolCorp, AirMagnet or events related to assets categorized under: `/All Asset Categories/Industrial Control Systems/Wireless Network`.

Requirement 2: Apply Secure Configurations to All System Components

Requirement	Resource	Description
PCI 2.2.2	Default Password Detected	Detects default passwords via vulnerability scanners.
PCI 2.2.2	Default Vendor Account Activity Detected	Detects authentication attempts made to accounts designated as default vendor accounts. Default vendor accounts are those listed in the active list: `/All Active Lists/ArcSight Solutions/PCI DSS/Default Vendor Accounts`. These accounts are typically associated with third-party vendors and may have elevated privileges or access levels. Detecting authentication attempts to these accounts is crucial for ensuring compliance with PCI DSS requirements and mitigating potential security risks associated with privileged access.
PCI 2.2.2	Default Vendor Account Detected	Detects default accounts via vulnerability scanners.

PCI 2.2.2	Default Wireless Password Detected	Detects default passwords on a Wireless asset.
		Note: To trigger this rule, ensure:
		1. That wireless assets are added to the following Asset Category:
		`/All Assets Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/Wireless`
		2. Enable:
		`/All Rules/ArcSight Solutions/PCI DSS/Requirement 2-Apply Secure Configurations to All System Components/Default Password Detected`

PCI 2.2.3	Multiple Functions Implemented on a Server	Detects both a web server and a database are installed on the same machine, indicating multiple functionalities on a single asset. **Note:** To trigger this rule, categorize the database assets should are categorized under: `/All Assets Categories/ArcSight Solutions/Compliance Insight Package/Application/Type/Database`

Requirement 2: Apply Secure Configurations to All System Components, continued

Requirement	Resource	Description
PCI 2.2.4	Insecure Processes Detected	Detects insecure services or processes.
PCI 2.2.7	Cleartext Non-Console Admin Access Detected	Detects cleartext non-console admin access attempts.
PCI 2.3.1	Wireless Vulnerability or Misconfiguration Detected	Detects wireless vulnerabilities or misconfigurations.

Requirement 3: Protect Stored Account Data

Requirement	Resource	Description
PCI 3.4.1, 3.4.2	Unmasked Primary Account Numbers Detected	Detects sensitive information such as credit card account numbers is stored or transmitted as plain text.
PCI 3.6.1	Vendor Default Password Detected	Detects default passwords via vulnerability scanners.
PCI 3.6.1	Violation Detected related to Cryptographic Key	Detects violations related to cryptographic keys.
PCI 3.7.5	Weak Key Exchange Detected	Detects weak key algorithms in the environment.

Requirement 4: Protect Cardholder Data with Strong Cryptography During Transmission Over Open, Public Networks

Requirement	Resource	Description
PCI 4.2.1	Account Numbers Transmitted in Cleartext	Detects transmissions of account numbers in cleartext.
PCI 4.2.1	Anonymous Key Exchange Detected	Detects anonymous key exchanges that happens in the network.
PCI 4.2.1, 12.3.3	Deprecated TLS Protocol Version Detected	Detects the usage of deprecated version of TLS protocols.
PCI 4.2.1	Exploit against Cryptographic Protocol	Detects exploited vulnerabilities in a cryptographic algorithm that is being used in the network.
PCI 4.2.1	Insecure Communication Detected	Detects when there is an insecure communication in the network.
PCI 4.2.1	Invalid or Expired Certificate Detected	Detects expired or invalid certificates.
PCI 4.2.1	SSH Weak Algorithm Detected	Detects weak SSH algorithms in the network.

Requirement 4: Protect Cardholder Data with Strong Cryptography During Transmission Over Open, Public Networks, continued

Requirement	Resource	Description
PCI 4.2.1, 12.3.3	SSL Protocol Detected	Detects SSL protocol usage in network communications.
PCI 4.2.1	Violations Detected on Wireless Network	Detects a violation on a wireless network that is being used.
PCI 4.2.1	Vulnerability Detected on Cryptographic Protocol	Detects a vulnerability in a cryptographic algorithm that is being used.

Requirement 5: Protect All Systems and Networks from Malicious Software

Requirement	Resource	Description
PCI 5.2.2	Malware Detected	Detects potential malware activity in the environment.
PCI 5.2.2	Ransomware Detected	Detects ransomware within the monitored environment. This rule monitors various indicators and behaviors associated with ransomware software based on ArcSight categorization.
PCI 5.2.2	Spyware Detected	Detects spyware reported by an Intrusion Detection System (IDS) or an anti-virus application. **Note:** To trigger this rule, enable: `/All Rules/ArcSight Solutions/PCI DSS/Requirement 5-Protect All Systems and Networks from Malicious Software/Malware Detected`
PCI 5.2.2	Worm Detected	Detects a worm via an Intrusion Detection System (IDS) or an anti-virus application. **Note:** To trigger this rule, enable: `/All Rules/ArcSight Solutions/PCI DSS/Requirement 5-Protect All Systems and Networks from Malicious Software/Malware Detected`
PCI 5.3.1, 10.7.1	Anti-Malware Failed Update	Detects failed anti-virus software updates.
PCI 5.3.1, 5.3.5, 1.5.1, 10.7.1	Security Software Stopped or Paused	Detects that a security software service has been disabled. Refer to the condition tab of this rule for the list of services.

Requirement 5: Protect All Systems and Networks from Malicious Software, continued

Requirement	Resource	Description
PCI 5.4	DMARC Weakness Detected	Detects DMARC protocol related vulnerabilities.
PCI 5.4	DKIM Based Attack Detected	Detects DomainKeys Identified Mail (DKIM) attacks.
PCI 5.4	Okta FastPass Phishing Detection	Detects when Okta FastPass prevents a user from authenticating to a phishing website.
PCI 5.4	SPF Based Attack Detected	Detects Sender Policy Framework (SPF) protocol attacks.
PCI 5.4.1	Phishing Detected	Detects phishing activity in your environment.

Requirement 6: Develop and Maintain Secure Systems and Software

Requirement	Resource	Description
PCI 6.2.4	Authentication and Authorization Weakness Detected	Detects authentication and authorization weaknesses via vulnerability scanners.
PCI 6.2.4	CSRF Vulnerability Detected	Detects cross-site request forgery attacks that trick the user into performing unwanted actions on a web application.
PCI 6.2.4	Memory Based Vulnerability Detected	Detects memory based vulnerabilities that could lead to memory corruption, buffer overflows, or other security issues.
PCI 6.2.4	LDAP Vulnerability Detected	Detects application failures to sanitize user input for LDAP queries, leading to potential LDAP injection vulnerabilities.
PCI 6.2.4	SQL Vulnerability Detected	Detects SQL vulnerabilities or injection attacks.
PCI 6.2.4	XPATH Vulnerability Detected	Detects XPATH vulnerabilities or injection attacks.
PCI 6.2.4	XSS Vulnerability Detected	Detects XSS vulnerabilities.
PCI 6.3.1	High Risk Vulnerability Detected	Detects high risk or critical vulnerabilities that could lead to a data breach or system compromise.
PCI 6.3.2	Database Vulnerability Detected	Detects database vulnerabilities via vulnerability scanners.

Requirement 6: Develop and Maintain Secure Systems and Software, continued

Requirement	Resource	Description
PCI 6.3.2	Exploit on Third Party Asset	Detects exploits performed on third party assets. **Note:** To trigger this rule, categorize third party assets under: `/All Assets Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/Third Party`
PCI 6.3.3	Security Patch Missing	Detects security patch installation or update failures and then found missing.
PCI 6.4.1	Exploit on a Public Facing Asset	Detects exploits performed on public-facing web applications. **Note:** Categorize public facing assets under: `/All Assets Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/Public-Facing`

PCI 6.4.1	High Risk Vulnerability on Public-Facing Asset	Detects high risk vulnerabilities on public-facing web applications.
		Note: To trigger this rule, ensure:
		1. Categorize public facing assets under:
		`/All Assets Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/Public-Facing`
		2. Enable:
		`/All Rules/ArcSight Solutions/PCI DSS/Requirement 6-Develop and Maintain Secure Systems and Software/High Risk Vulnerability Detected`

PCI 6.4.1	High Risk Vulnerability on Third-Party Asset	Detects high risk vulnerabilities on third-party applications.
		Note: To trigger this rule, ensure:
		1. Categorize the third-party assets under:
		`/All Assets Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/Third-Party`
		2. Enable:
		`/All Rules/ArcSight Solutions/PCI DSS/Requirement 6-Develop and Maintain Secure Systems and Software/High Risk Vulnerability Detected`

Requirement 6: Develop and Maintain Secure Systems and Software, continued

Requirement	Resource	Description
PCI 6.4.2	Insecure Cryptographic Implementation Detected	Detects when there is a weak cryptographic implementation.
PCI 6.5.1	Database Configuration Change Detected	Detects database change configurations.
PCI 6.5.1	Misconfiguration Detected	Detects misconfigurations in any application.
PCI 6.5.3	Communication between Test and Production Environments	Detects communications between test and production environments.
PCI 6.5.3	Communication between Development and Production Environments	Detects communications between development and production environments.
PCI 6.5.5	Cleartext PAN Detected in Pre-Production Environment	Detects when Primary Account Numbers (PANs), such as credit card numbers, bank account numbers, are transmitted or stored in plaintext within the pre-production environment.
PCI 6.5.6	Developer or Test Accounts Found on Production Environment	Detects developer or test accounts found on production environment.

Requirement 7: Restrict Access to System Components and Cardholder Data by Business Need to Know

Requirement	Resource	Description
PCI 7.2.2, 7.3.1, 7.2.5	Unauthorized Access to Cardholder Data	Detects any unauthorized access of cardholder data. **Note:**To trigger this rule, categorize the cardholder data assets under: `/All Assets Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/Cardholder Data`
PCI 7.2.4	Privileged Account Changes Detected	Detects attempts to access or change authorizations to an administrative account.
PCI 7.2.4, 7.2.5.	Removal of Access Rights	Detects revoked or restricted access to certain resources or systems.
PCI 7.2.4, 7.2.5.	User Removed from Privileged Group	Detects a user addition to a privileged group.
PCI 7.2.4, 7.2.5.	User Added to Privileged Group	Detects user removal from a privileged group.

Requirement 8: Identify Users and Authenticate Access to System Components

Requirement	Resource	Description
PCI 8.2.1	Non Unique Account Detected	Detects non-unique accounts in your PCI environment.
PCI 8.2.8	System Idle Time-out Value Modified	Detects changes to system idle time-out settings, which control how long a user's session remains active before being automatically logged off due to inactivity.
PCI 8.3.1	Authentication Bypass Detected	Detects attempts to bypass or circumvent normal authentication mechanisms.
PCI 8.3.1	Authentication Factor Implementation Missing in Applications	Detects applications or systems that lack an adequate level of multi-factor authentication (MFA) implementation, increasing the risk of unauthorized access and data breaches.
PCI 8.3.2	Clear-text Authentication Detected	Detects sensitive authentication information such as usernames, passwords, or API keys are transmitted or stored in clear-text.
PCI 8.3.2	Cleartext Password Detected	Detects potential security breaches by identifying user accounts with passwords that are considered weak or easily guessable.
PCI 8.3.6	Maximum Password Age Changed to more than Policy Specified	Detects the maximum password age setting on a system is configured to exceed the organization's established security policy.
PCI 8.3.6	Minimum Password History Set Less than Policy Standard	Detects the minimum password history setting on a system is configured below the organization's established security policy.
PCI 8.3.6	Minimum Password Length Set Less than Policy Standard	Detects the minimum password length setting on a system is configured below the organization's established security policy.

Requirement 8: Identify Users and Authenticate Access to System Components, continued

Requirement	Resource	Description
PCI 8.3.6	Password not Changed for Longer than Policy Standard	Detects user accounts that have not changed their passwords within the time frame specified by the organization's security policy. **Note:** In addition to the usual conditions, this rules also tracks when an entry expires from the Password Changes active list. When an entry expires out of this active list, it means the user never reset the password within the prescribed time and OpenText Enterprise Security Manager is alerted. Time limit is defined by the TTL in the active list. The default time is set to 90 days. For the above condition to alert, enable: `/All Rules/ArcSight Solutions/PCI DSS/Requirement 6-Develop and Maintain Secure Systems and Software/Password Changed Successfully`
PCI 8.3.6	Password Changed Successfully	Lightweight rule that populates the Password Changes active list whenever the password change conditions are met.
PCI 8.4.2	Multi-Factor Authentication Disabled	Detects multi-factor authentication (MFA) has been disabled or deactivated on systems or accounts where it is required.
PCI 8.5.1	Multi-Factor Authentication Flaw Detected	Detects potential vulnerabilities or misconfigurations related to the implementation of multi-factor authentication.
PCI 8.6.2	Weak Password Detected	Detects potential security breaches by identifying user accounts with weak or easily guessable passwords.
PCI 8.6.2	Inactive User Account Detected	Detects inactive user accounts based on a specified number of days a user has not logged on to the account.

Requirement 9: Restrict Physical Access to Cardholder Data

Requirement	Resource	Description
PCI 9.2.1.1	Failed Building Access	Detects failed physical building access attempts.
PCI 9.2.1.1	Potential Piggybacking Attack	Detects when an employee badge used more than one time on short period of time to access specific building.

Requirement 9: Restrict Physical Access to Cardholder Data, continued

Requirement	Resource	Description
PCI 9.2.1.1	Failed Access by the Same User to Multiple Buildings	Detects failed physical access attempts by the same user to multiple buildings in a short period of time. **Note:** To trigger this rule, enable: `/All Rules/ArcSight Solutions/PCI DSS/Requirement 9-Restrict Physical Access to Cardholder Data/Failed Building Access`
PCI 9.2, 9.3, 9.4	After Hours Building Access by Contractors	Detects building access events by contractors after business hours. **Note:** To trigger this rule, enable: `/All Active List/ArcSight Solutions/PCI DSS/Badges to Account`

Requirement 10: Log and Monitor All Access to System Components and Cardholder Data

Requirement	Resource	Description
PCI 10.2.1.2	Administrative Authorization Changes Detected	Detects any modifications made to administrative user privileges or authorizations within your organization's IT infrastructure.
PCI 10.2.1.4	Possible Password Spraying Attack	Detects potential password spraying attacks, where attackers attempt to use a small set of common or easily guessable passwords against a large number of user accounts.
PCI 10.2.1.4	Multiple Unsuccessful Admin Logins Detected	Detects multiple unsuccessful login attempts targeting administrative accounts. These attempts can indicate potential brute-force attacks, credential stuffing, or other malicious activity.
PCI 10.2.1.4	Frequent Unsuccessful Logins Activity Increased Exponentially in less than 10 Minutes	Detects exponential increases of frequent failed login events. **Note:** To trigger this rule, enable: `/All Data Monitors/ArcSight Solutions/PCI DSS/Requirement 10-Log and Monitor All Access to System Components and Cardholder Data/Failed Login Activitiy/Frequent Failed Login per 10 Minutes`
PCI 10.2.1.5	Privilege Escalation Attempt Detected	Detects attempts to gain elevated privileges on systems or within the network.
PCI 10.2.1.6	Audit Log Modification Detected	Detects any modifications made to audit logs.

Requirement 10: Log and Monitor All Access to System Components and Cardholder Data, continued

Requirement	Resource	Description
PCI 10.2.1.6	System Audit Policy Modified	Detects changes to system audit policies.
PCI 10.3.2	Security Logs Reached its Maximum Capacity	Detects when security logs have reached their maximum storage capacity.
PCI 10.3.2	Audit Log Cleared	Detects when audit logs are cleared or deleted.
PCI 10.3.2	Log File Related Traffic Anomaly Detected	Detects unusual or suspicious network traffic related to log files.
PCI 10.3.2	Unauthorized Access to Log Files	Detects user or system attempts to access log files without proper authorization.
PCI 10.3.4	File Integrity Compromised	Detects when system file integrity has been compromised. This includes unauthorized modifications, deletions, or other changes that could indicate malicious activity.
PCI 10.4	User Logged in to different Targets on Short Period of Time	Detects sets of four consecutive successful logins for the same account to different targets within one minute.
PCI 10.4.1	Multiple High Risk Events in Short Period of Time	Detects when 20 or more high risk events are received in 2 or less minutes.
PCI 10.6.1	Clock Synchronization Issue Detected	Detects system clocks that are not synchronized correctly.

PCI 10.6.2	Critical System Misconfiguration Detected	Detects critical system misconfigurations that can significantly increase the risk of security breaches.
		Note: To trigger this rule, classify assets under either of the following:
		`/Asset Categories/All Asset Categories/System Asset Categories/Criticality/Very High`
		`/Asset Categories/All Asset Categories/System Asset Categories/Criticality/High`

PCI 10.7.1	Information System Failure	Detects failures within information systems, encompassing a broad range of events that disrupt normal operations or compromise system integrity.

Requirement 10: Log and Monitor All Access to System Components and Cardholder Data, continued

Requirement	Resource	Description

PCI 10.7.1	System Failures of Highly Critical Machine	Detects critical system failures of designated "highly critical machines" within the organization's infrastructure.
		Note: To trigger this rule, classify assets under either of the following:
		`/Asset Categories/All Asset Categories/System Asset Categories/Criticality/Very High`
		`/Asset Categories/All Asset Categories/System Asset Categories/Criticality/High`

PCI 10.7.1, 5.3.1	Anti-Malware Failed Update	Detects failed anti-virus software updates.
PCI 10.7.1, 5.3.1, 5.3.5, 1.5.1	Security Software Stopped or Paused	Detects that a security software service has been disabled. Refer to the condition tab of this rule for the list of services.

Requirement 11: Test Security of Systems and Networks Regularly

Requirement	Resource	Description
PCI 11.2.1	Rogue Wireless Device Detected	Detects rogue devices based on events reported from AirDefense, AirPatrolCorp, AirMagnet or events related to assets categorized under: `/All Asset Categories/Industrial Control Systems/Wireless Network`.
PCI 11.4.4	Exploitable Vulnerabilities Detected	Detects the presence of known exploitable vulnerabilities within the organization's IT infrastructure.
PCI 11.5.1	Covert Channel Malware Activity	Detects potential covert channel activity, where malware may be communicating with a command and control server or exfiltrating data using hidden or unusual methods.
PCI 11.5.1	Network Intrusion Attack Detected	Detects network intrusion attacks, such as exploitation of vulnerabilities, unauthorized access attempts, and malicious activity originating from or targeting the network.
PCI 11.5.1	DoS Attack Detected	Detects potential Denial-of-Service (DoS) attacks targeting network resources or services.

Requirement 11: Test Security of Systems and Networks Regularly, continued

Requirement	Resource	Description
PCI 11.5.1	Distributed DoS Attack Detected	Detects Distributed Denial-of-Service (DDoS) attacks, which involve multiple compromised systems (often forming a botnet) flooding a target with traffic, rendering it unavailable to legitimate users.
PCI 11.5.1	Traffic Anomaly Detected	Detects unusual or suspicious network traffic patterns that deviate significantly from established baselines or normal network behavior.
PCI 11.5.1	Unauthorized Access Due to Network Intrusion	Detects unauthorized access to systems or data as a result of a successful network intrusion.
PCI 11.5.2	File Integrity Monitoring	Populates the File Monitoring List active list with file integrity monitoring events.
PCI 11.5.2	File Integrity Monitoring not Reported beyond Policy Standard	Detects systems where File Integrity Monitoring (FIM) agents are failing to report changes or are reporting changes outside of the expected frequency defined by the organization's policy. **Note:** As per PCI requirments, the TTL for the Active List is set to 7 days. If the file integrity monitoring device does not report beyond 7 days, then this rule is triggered.
PCI 11.5.2	Unauthorized Access to Payment Page	Detects attempts to access payment pages or related resources by unauthorized users or systems.
PCI 11.5.2	Unauthorized Modification of Critical Files	Detects any unauthorized modifications to critical files within the organization's IT environment.
PCI 11.6.1	Content Security Policy Bypass Attempt	Detects potential bypasses of the Content Security Policy implemented within web applications.
PCI 11.6.1	Skimming Attack Detected	Detects potential card skimming attacks, where attackers attempt to steal cardholder data.

Requirement 12: Support Information Security with Organizational Policies and Programs

Requirement	Resource	Description
PCI 12.1.1	Policy Violation Detected	Detects when a user or system activity violates established security policies, operational procedures, or regulatory requirements.
PCI 12.1.2	Domain Policy Modified	Detects any modification done to the domain policy.

Requirement 12: Support Information Security with Organizational Policies and Programs, continued

Requirement	Resource	Description
PCI 12.3.3	Weak Hash Algorithm Detected	Detects the usage of weak or outdated hash algorithms within the organization's systems or applications.
PCI 12.3.3, 4.2.1	Deprecated TLS Protocol Version Detected	Detects the usage of deprecated version of TLS protocols.
PCI 12.3.3, 4.2.1	SSL Protocol Detected	Detects SSL protocol usage in network communications.
PCI 12.10.7	Cleartext PAN Detected	Detects Primary Account Numbers (PANs), such as credit card numbers, bank account numbers, that are transmitted or stored in plaintext.
PCI 12.10.5	Suspicious Activity in Payment Page	Detects suspicious activity occurring within payment pages.
PCI 12.10.7	Data Leak Detected	Detects potential data leaks, where sensitive information is unintentionally or maliciously exposed to unauthorized individuals or systems.

Use Cases

The following table lists all the use cases in .

Use Cases Resources

Resource	Description	URI
Access Control	Provides a high-level overview of resources that belong to the Access Control domain.	All Use Cases/ArcSight Solutions/PCI DSS
Critical Configuration Change to NSC device PCI 1.2, 1.2.1, 1.2.2	Provides resources that monitor critical configuration changes to NSC devices.	All Use Cases/ArcSight Solutions/PCI DSS
Cryptography	Provides a high-level overview of resources that belong to the Cryptography domain.	All Use Cases/ArcSight Solutions/PCI DSS

Use Cases Resources, continued

Resource	Description	URI
Database Reachable from Internet	Provides resources that monitor if the database can be reached by the internet.	All Use Cases/ArcSight Solutions/PCI DSS
Default Accounts	Provides resources to monitor default accounts.	All Use Cases/ArcSight Solutions/PCI DSS
Firewall Configuration Modifications PCI 1.2.1, 1.2.2, 1.2.7, 1.2.8	Provides resources that monitor firewall configuration changes.	All Use Cases/ArcSight Solutions/PCI DSS
General	Provides a high-level overview of cross-domain resources. These resources do not belong to a specific domain and may be used by various compliance scenarios.	All Use Cases/ArcSight Solutions/PCI DSS
IDS Configuration Modifications	Provides resources that monitor IDS configuration changes.	All Use Cases/ArcSight Solutions/PCI DSS
Inbound Traffic to CDE PCI 1.3.1, 1.4.1, 1.4.2	Providess resources that monitor inbound traffic to CDE.	/All Use Cases/ArcSight Solutions/PCI DSS/
Insecure Communication Detected	Provides resources that monitor insecure communications.	/All Use Cases/ArcSight Solutions/PCI DSS/
Invalid or Expired Certificate Detected PCI 4.2.1	Provides resources that monitor invalid or expired certificates.	/All Use Cases/ArcSight Solutions/PCI DSS/
Malware Monitoring PCI 5.2	Provides a high-level overview of resources that monitor and analyze malware events and devices in real-time.	All Use Cases/ArcSight Solutions/PCI DSS

Use Cases Resources, continued

Resource	Description	URI
Malicious Traffic to Cardholder Data Environment PCI 1.5.1	Provides Resources that monitor malicious traffic to cardholder data environments.	All Use Cases/ArcSight Solutions/PCI DSS
Monitoring	Provides a high-level overview of resources that belong to the Monitoring domain.	All Use Cases/ArcSight Solutions/PCI DSS
Network Routing Configuration Changes PCI 1.21, 1.2.2, 1.2.7, 1.2.8	Provides resources that monitor network routing configuration changes.	All Use Cases/ArcSight Solutions/PCI DSS
Network Security	Provides a high-level overview of resources that belong to the Network Security domain.	All Use Cases/ArcSight Solutions/PCI DSS
Outbound Traffic from CDE	Provides resources to monitor outbound traffic from CDE.	All Use Cases/ArcSight Solutions/PCI DSS
PCI DSS Compliance Status	Provides a high-level overview of PCI DSS compliance.	All Use Cases/ArcSight Solutions/PCI DSS
Personal Information Leakage from Database 1.4.4	Provides resources that monitor personal information leakages from your databases.	All Use Cases/ArcSight Solutions/PCI DSS
Physical Security	Provides a high-level overview of resources that belong to the Physical Security domain.	All Use Cases/ArcSight Solutions/PCI DSS
Privacy Protection	Provides a high-level overview of resources that belong to the Privacy Protection domain.	All Use Cases/ArcSight Solutions/PCI DSS
Ransomware Monitoring	Provides resources that monitor for ransomware activity in your environment.	

Use Cases Resources, continued

Resource	Description	URI
Security Software Stopped or Paused PCI 5.3.1, 5.3.5, 1.5.1, 10.7.1	Provides resources that monitor security software stoppages or pauses.	All Use Cases/ArcSight Solutions/PCI DSS
System Hardening	Provides a high-level overview of resources that belong to the System Hardening domain.	All Use Cases/ArcSight Solutions/PCI DSS
Unauthorized Traffic from Cardholder Data Environment PCI 1.3.1, 1.4.1, 1.4.2	Provides resources that monitor unauthorized traffic from cardholder data environments with a specific focus on port-connection monitoring. By default, all connection types and ports are allowed. Disallowed ports are either ports entered into the Disallowed Ports active list or any port that is not entered into the Allowed Ports Active list. Explicit port entries on the Disallowed Ports active list always take precedence over entries on the Allowed Ports active list. Conditions are located in the Disallowed Ports Access filter.	All Use Cases/ArcSight Solutions/PCI DSS
Unauthorized Traffic to Cardholder Data Environment PCI 1.3.1, 1.4.1, 1.4.2	Provides resources that monitor unauthorized traffic to cardholder data environments with a specific focus on port-connection monitoring. By default, all connection types and ports are allowed. Disallowed ports are either ports entered into the Disallowed Ports active list or any port that is not entered into the Allowed Ports Active list. Explicit port entries on the Disallowed Ports active list always take precedence over entries on the Allowed Ports active list. Conditions are located in the Disallowed Ports Access filter.	All Use Cases/ArcSight Solutions/PCI DSS
Unmasked Primary Account Numbers PCI 3.4.1 and 3.4.2	Provides resources to monitor the usage of unmasked primary account numbers.	All Use Cases/ArcSight Solutions/PCI DSS
VPN Configuration Modifications PCI 1.2.1, 1.2.2, 1.2.7, 1.2.8	Provides resources that monitor VPN configuration modifications.	All Use Cases/ArcSight Solutions/PCI DSS
Wireless Malicious Traffic Detected PCI 1.5.1	Provides resources to monitor malicious wireless traffic.	All Use Cases/ArcSight Solutions/PCI DSS
Worm Activity Monitoring	Provides a high-level overview of resources that monitor and analyze worm activity in real-time.	All Use Cases/ArcSight Solutions/PCI DSS