Micro Focus Security ArcSight ESM CIP for GDPR

Software Version: 1.0

Solutions Guide

Document Release Date: November 2021
Software Release Date: January 2022

MICRO FOCUS®

Legal Notices

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/
ArcSight Product Documentation	https://community.softwaregrp.com/t5/ArcSight-Product-Documentation/ct-p/productdocs

About this PDF Version of Online Help

This document is a PDF version of the online help. This PDF file is provided so you can easily print multiple topics from the help information or read the online help in PDF format. Because this content was originally created to be viewed as online help in a web browser, some topics may not be formatted properly. Some interactive topics may not be present in this PDF version. Those topics can be successfully printed from within the online help.

Contents

Chapter 1: Compliance Insight Package for GDPR Overview and Architecture

The General Data Protection Regulation (GDPR) provides a single set of rules for protecting the personal data of all European Union (EU) residents and visitors.

GDPR consists of two components: the articles (99) and recitals (173). The articles constitute the legal requirements organizations must follow to demonstrate compliance. The recitals provide additional information and supporting context to supplement the articles.

CIP for GDPR

Compliance Insight Package for GDPR (CIP for GDPR) provides an essential foundation for your GDPR compliance program. CIP for GDPR uses ArcSight™ ESM features, such as event and asset categorization, threat prioritization, real time monitoring, to easily identify and address activities and anomalies involving systems that are subject to GDPR. compliance CIP for GDPR is made up of a comprehensive and easily customizable set of ArcSight ESM resources (rules, dashboards, data monitors, active channels, and so on), which enable you to measure and report on your compliance with GDPR by addressing the following objectives:

- **Compliance reporting:** Supports the presentation of requirements to internal and external audit teams, as well as upper management.
- **Real-time detection of compliance breaches:** Pro-actively addresses compliance violations.
- **Security best practices:** Due diligence in complying with GDPR standard, as well as security policies and best practices.
- **Automation of Monitoring-IT control:** CIP for GDPR follows and adapts to changes in the IT environment. More than 90 correlation rules can be used to monitor policy compliance violations in real-time.
- **Harmful User and Machine Monitoring:** Tracks potentially harmful users and machines.
- **Visualizing Security Events:** Displaying security events graphically which allows analysts to quickly analyze situations
- **Vulnerabilities and Configuration Changes Monitoring:** Tracking vulnerabilities and configuration changes

Solution Architecture

CIP for GDPR helps ensure compliance with GDPR requirements by providing a set of use cases that address and support the GDPR security controls as listed in Chapter 3, CIP for GDPR Use Cases,

Resources are organized into use cases by security purpose or area such as Audit Log Cleared or Personal identifiable information monitoring. These use cases are represented in ArcSight ESM as use case resources and provide a central location for managing content. The CIP for GDPR use cases are listed in the Use Case tab of the Navigator panel as shown in the following figure

```
Navigator
Resources | Packages | Use Cases
├─ Use Cases
│   ├─ admin's Use Cases
│   └─ Shared
│       └─ All Use Cases
│           ├─ ArcSight Administration
│           ├─ ArcSight Foundation
│           └─ ArcSight Solutions
│               └─ GDPR
│                   ├─ Account Lockouts
│                   ├─ Assets not Scanned for Longer than Policy Standard
│                   ├─ Attacks and Suspicious Activity
│                   ├─ Audit Log Cleared
│                   ├─ Audit Log Failures
│                   ├─ Botnet Activity
│                   ├─ Clear Text Password Transmission
│                   ├─ Covert Channel Activity
│                   ├─ Critical Configuration Changes
│                   ├─ CRM and ERP Flaws
│                   ├─ Data Flow between GDPR Systems and non EU Countries
│                   ├─ Database Flaws
│                   ├─ Directory Traversal Attacks
│                   ├─ DoS Activity
│                   ├─ Email Activity
│                   ├─ Encrypted Communication Information Leak
│                   ├─ Exploit Executed on Databases
│                   ├─ Exploit Executed on PII Assets
│                   ├─ Failed Anti-Virus Signature Updates
│                   ├─ Failed Login Overview
│                   ├─ Firewall Blocked Events
│                   ├─ Format String Vulnerabilities
│                   ├─ Frequent Unsuccessful Logins by User Name
│                   ├─ Frequent Unsuccessful Logins from Attacker Host
│                   ├─ Frequent Unsuccessful Logins from non EU Countries to PII Asset
│                   ├─ Frequent Unsuccessful Logins to Target Host
│                   ├─ High Risk Events
│                   ├─ High Risk Vulnerabilities
│                   ├─ Information Disclosure Vulnerabilities
│                   ├─ Information Interception
│                   ├─ Insecure Cryptographic Storages
│                   ├─ Invalid or Expired Certificate
│                   ├─ Malware Monitoring
│                   ├─ MITRE ATT&CK Activity on PII Assets
│                   ├─ MITRE ATT&CK Overview
│                   ├─ Non EU Login Activity
│                   ├─ Organizational Information monitoring
│                   ├─ Overflow Vulnerabilities
│                   ├─ Password and Authentication Weaknesses
│                   ├─ Password not Changed for Longer than Policy Standard
│                   ├─ Password Spray Attacks
│                   ├─ Personal identifiable information monitoring
│                   ├─ Policy Violations
│                   ├─ Privileged Account Changes
│                   ├─ Reconnaissance Activities
│                   ├─ Removal of Access Rights
│                   ├─ Security Application Stopped or Paused
│                   ├─ Security Patches
│                   ├─ Shell Code Attacks
```

For example, the following figure shows the resources that make up the Data Flow between GDPR Systems and non EU Countries use case resource.

For instructions on viewing the resources associated with a use case, see "View Use Case Resources" on chapter 2.

In addition to the resources supplied to help address specific GDPR Article there are a common set of filters and active lists that support the entire solution. These common resources are described in "Solution Installation and Configuration" , These resources require configuration to tailor the content for your environment, such as privileged account names or the DMZ Assets in your organization.

GDPR Rules Overview

GDPR Rules Overview dashboard summarize the compliance state determined by correlation rules for whole GDPR regulation. The GDPR Rules Overview dashboards are available from the GDPR/Overview group as shown in the following figure.
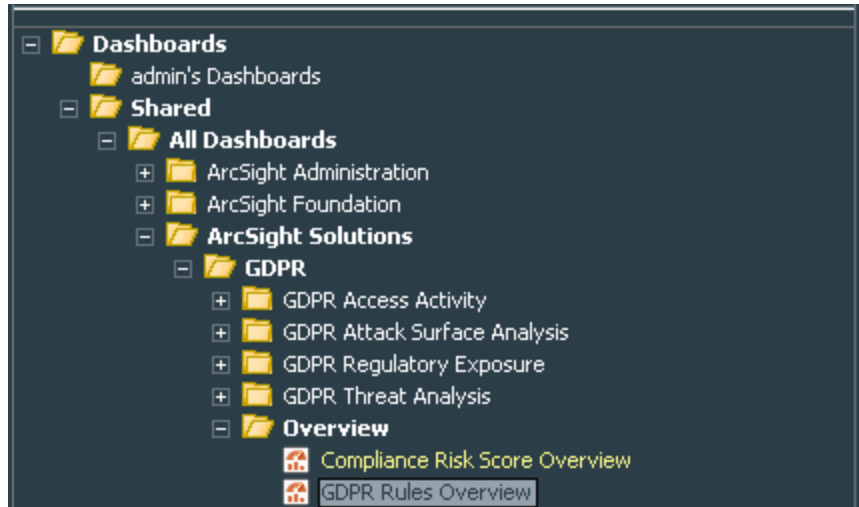
The dashboard presents:

- An event graph to show the relationships of the non-compliant systems with other systems on the network
- A bar chart that shows the top the 10 triggered rules.
- A bar chart that shows the top 10 targets of the triggered rules.
- A bar chart that shows the top 10 attackers of the triggered rules.

The following figure shows the GDPR Rules Overview dashboard

Risk Score Overview Dashboard

In addition to the GDPR Rules overview dashboard, GDPR for ESM provides Compliance Risk Score dashboard which provides high-level overview of the risk associated with each ARTICLE on the GDPR

regulation in your environment.

The Compliance Risk Score Overview dashboard summarizes your environment's overall state of compliance with the GDPR standard as determined by correlation rules triggered for each ARTICLE as shown in the following figure.

The following figure shows the compliance risk score overview dashboard:
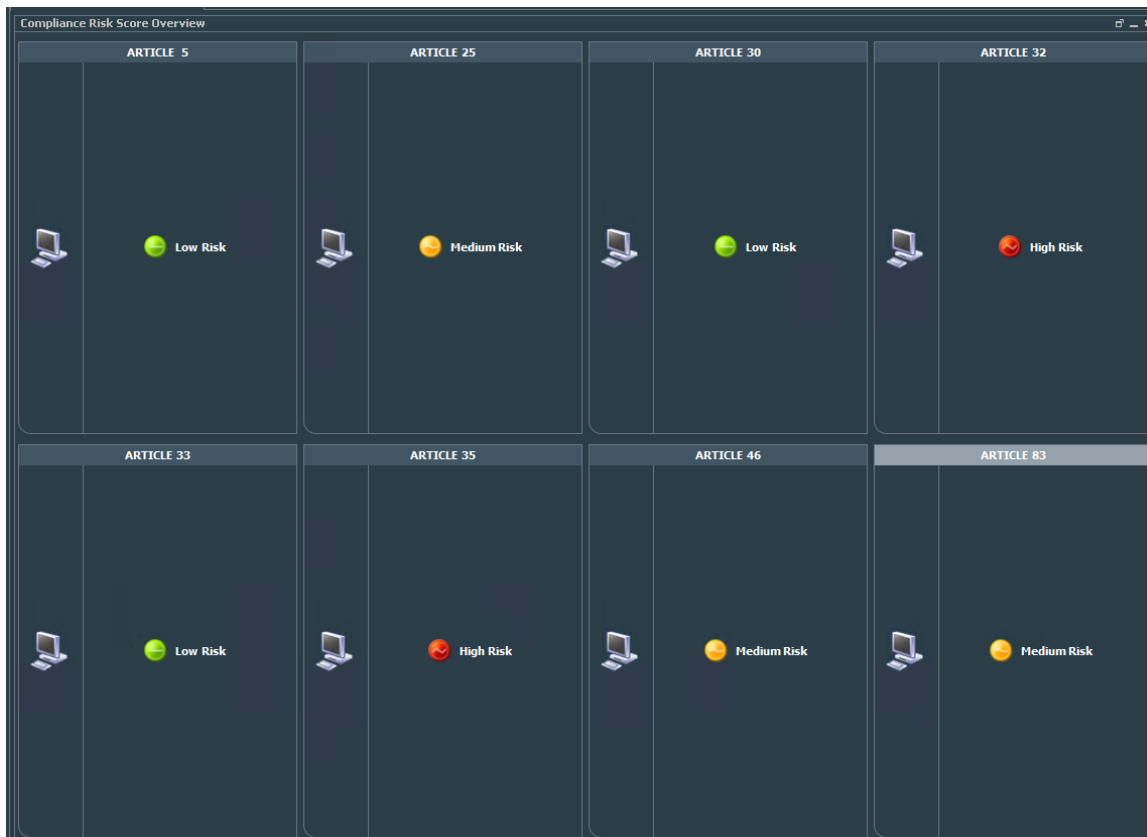
The dashboard is populated when a possible violation or an actual violation occurs. A yellow or red data monitor can be turned to green manually when the situation is remedied by right-clicking the data monitor and selecting Override Status

The colors of the traffic lights indicate the current state as described in the following table:

Color	State	Description
Red	Violation	This situation occurs when one or more rules are triggered by event activity that violates compliance for this GDPR ARTICLE section
Yellow	Possible Violation	This situation occurs when one or more marginal events occur that could indicate a policy problem, or is a borderline compliance violation
Green	Compliant	Systems are considered compliant when any events related to this GDPR Remain under the threshold of Yellow.

Before running the Compliance Risk Score Overview dashboard make sure of the following:

- Data monitor Compliance Risk Score Overview which available also from GDPR/Overview should be enabled refer to chapter 2 "Enabling data monitors".

- Rule Compliance Score Update which available also from GDPR/Overview should be enabled. Refer to chapter 2 "Enabling GPDR Rules."

- Rule Manual Status Change which available also from GDPR/Overview should be enabled. Refer to chapter 2 "Enabling GPDR Rules."

Solution for GDPR CIP Device Coverage

Solution for GDPR CIP leverages event feeds from multiple sources. For a list of devices that are capable of generating events to populate the Solution for GDPR resources, see "CIP for GDPR Use Cases" in Chapter 3.

To gather events from physical access devices, such as badge readers, you must build FlexConnectors tailored to the type of physical access devices you use. For instructions about how to build and configure a FlexConnector for a physical access device, see "Build FlexConnector(s) for Physical Access Devices" in chapter 2

Chapter 2: Solution Installation and Configuration

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

Prepare for Installation

Before installing CIP for GDPR, complete the following preparation tasks:

1. "Prepare Environment" below
2. "Verify Environment" below

Prepare Environment

Before installing, prepare your environment for the CIP for GDPR:

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 GDPR Requirements. Verify that zones and networks are defined for your environment and that networks are assigned to the connectors reporting GDPR-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 ArcSight ESM installation. Compliance Insight Package for GDPR is supported on ArcSight ESM. Refer to the ESM 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 GDPR is a self-contained solution that does not rely on any other ArcSight solution. You can install CIP for GDPR alongside other solutions on the same ArcSight Manager. Before installing new solutions, Micro Focus recommends that you back up any existing solutions installed on the Manager.

Install Solution for GDPR CIP

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

To install the CIP for GDPR package:

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

`ArcSight- ComplianceInsightPackage-GDPR.1.0.<nnnn>.arb`

Where `<nnnn>` is the 4 character build number. (The exact build number is specified in the *ESM CIP for GDPR Release Notes*.)

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

2. Log into the ArcSight 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 as shown in the following figure.
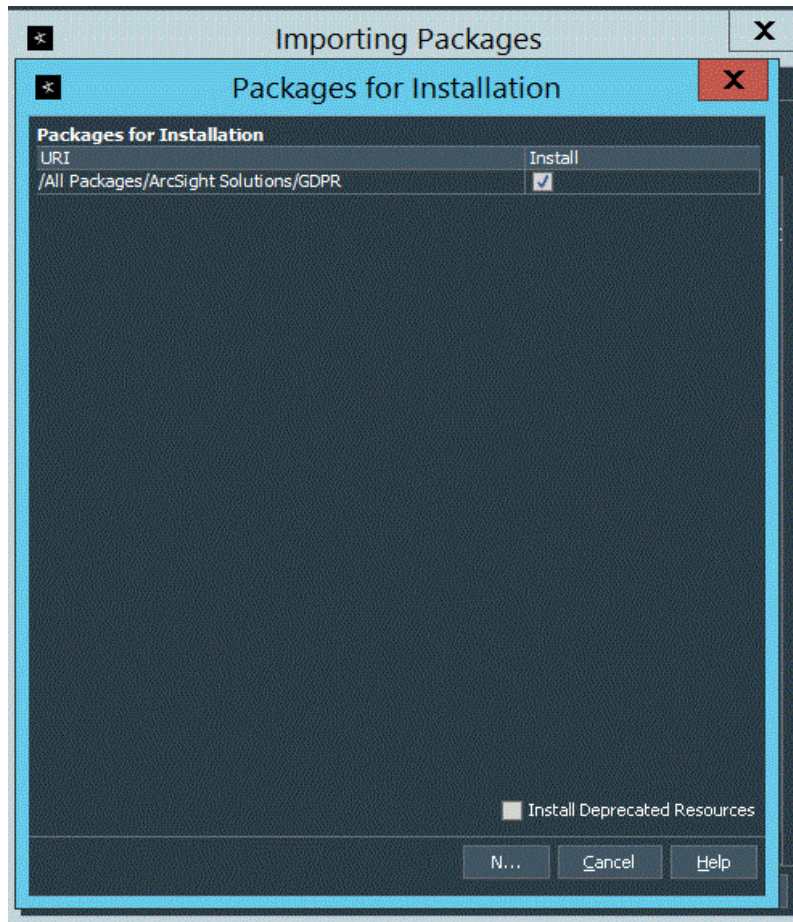
6. Leave the **GDPR** checkbox selected and in the Packages for Installation dialog, click **Next**.

   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/GDPR` group.
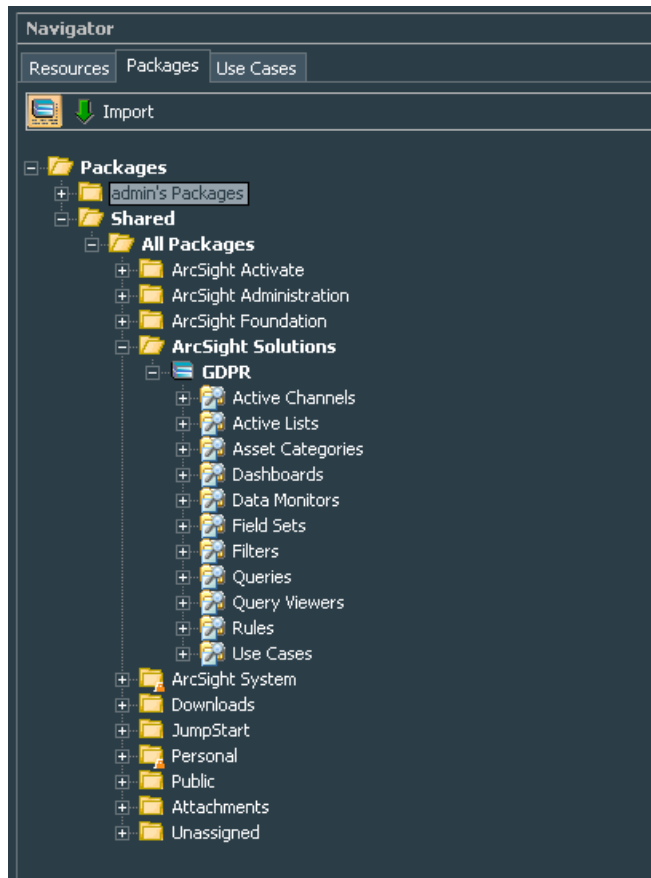
Assign User Permissions

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

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

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

- Active channels
- Active lists
- Dashboards
- Data monitors
- Field Sets
- Filters
- Queries
- 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/GDPR`.

   b. Right-click the **GDPR** 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 GDPR resources and click **OK**.

Configure CIP for GDPR Solution

Several of the CIP for GDPR 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 GDPR and where to find instructions for performing the configuration.

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

- "Model Assets (Assign Asset Categories)" below
- "Configure Active Lists" on page 17
- "Configure My Filters" on page 21
- "Deploy the CIP for GDPR Rules" on page 22

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

Model Assets (Assign Asset Categories)

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

- Some of the *CIP for GDPR* 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 GDPR*.

CIP for GDPR Categorization

CIP for GDPR uses the asset categories under the `/ArcSight Solutions/Compliance Insight Package/` group shown below.
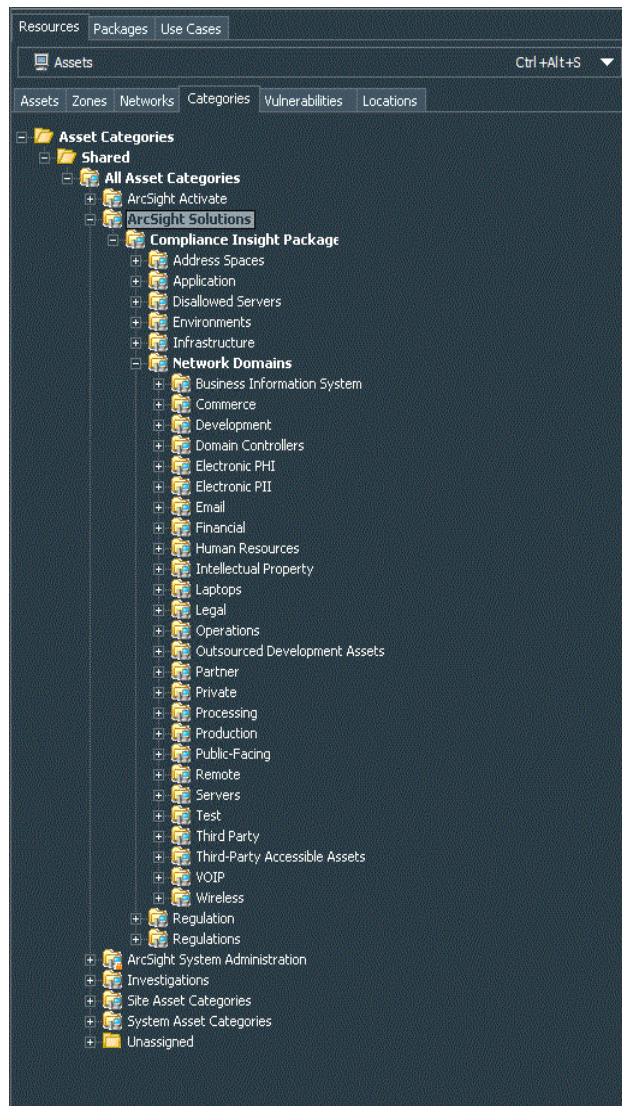
Categorizing Assets and Zones

CIP for GDPR 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 "Appendix A: CIP for GDPR Resource Reference" on page 103.

- For a list of all use cases and which assets and zones need to be categorized for each use case refer to "CIP for GDPR Use Cases" on page 46.

- For a list of all categorization used and the resources which use those categorizations, see "Appendix B: Asset and Zones Categories" on page 104.

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

One-by-one using the ArcSight Console

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

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

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

Using the ArcSight Asset Import File Connector

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

Configure Active Lists

CIP for GDPR 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 GDPR 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" on page 20. This method can be used to populate active lists with one, two, or more columns.
- Add entries in batch to active list from a comma separated value (CSV) file. For detailed instructions see

"Configure Active Lists by Importing a CSV File" on page 21. 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 GDPR. Some active lists are intended to be populated by rules. Also, there are Active Lists requiring manual Configuration for the CIP GDPR. For a complete listing (with descriptions) of all active lists provided with CIP for GDPR that require configuration, see the table below.

Active Lists that Require Configuration

Active List	Description	Expected Input Per Entry
Administrative Accounts	This active list should be populated with the usernames that have administrative privileges in your domain. Admins (those responsible for managing administrative users) populate this list manually whenever a new administrative user is added. Entries to this list are read by reports supplied in the content pack, but the list can also be added to or referenced in new content built around the provided infrastructure. This active list should be populated with the usernames that have administrative privileges in your domain. Entries in this list should be in all lower case. For example, the user Administrator should be added as "administrator".	User name, in lowercase.
Badges to Accounts	This list contains the computer account and employee type for every physical device badge. Populate this active list with the badge ID, primary computer account for the badgeholder (in case its a visitor use the vistor user name), and the employee type for users in your organization (in lowercase). Specifically, ensure that contractors and visitors are identified with the word "Contractor" (case insensitive) in the employee type field.	Badge ID, primary computer account for the badgeholder (in case its a visitor use the vistor user name), the employee type (in lowercase). Specifically, ensure that Contractors and vistors are identified with the word "Contractor" "Vistor" (case insensitive) in the employee type field.

Active List	Description	Expected Input Per Entry
DMZ Assets	This List should contains DMZ assets on the organization like DNS,WEB,SMTP servers. it contains 2 fields : IPAddres and AssetType where the IPAddress is the IP Address of the asset and the AssetType is the type of the asset on lower case (by default supported 3 types dns,web,smtp). for example if your web server ip is x.y.z.w you should add it as IPAddress=x.y.z.w ,AssetType=web	IP Address of authorized DNS,WEB, SMTP servers on your organization, Asset Type one of the following dns ,web smtp on lower case.
Important Emails	This list stores important emails of high-profile targets on the organization like C-lever executives which could be targeted by spear phishing attacks. entries in this list should be in all lower case.	Email and UserName , in lowercase
Insecure Ports	This active list includes ports related to unencrypted and thus insecure communication services.	Port Number
Insecure Processes	This active list includes the names of processes that provide unencrypted and thus insecure communications.	Process name, in lowercase

Configure Active Lists Using Console Active List Editor

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

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

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

Configure Active Lists by Importing a CSV File

Active lists can be populated in a single step, by importing entries from an existing CSV file. The number of columns in the active list must match the number of comma separated values in the CSV file. For example, if the active list has two columns of data, the imported CSV file must have two comma-separated fields.

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

   A file browser opens.

2. Browse to find the CSV file you want to import, select it, and click **Open**. The Import Preview dialog displays the data from the CSV file to be imported into the active list.

3. To add the entries from the selected file into the active list, in the Import Preview dialog, click **OK**. The new entries from the file are appended to the existing entries in the active list.

4. To verify that your entries were imported as expected, right-click the active list you just populated with the CSV file and select **Show Entries**.

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

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

Configure My Filters

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

- "After Hours Filter" below
- "Limit Regulation Filter" on the next page

After Hours Filter

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

The filter uses two variables:

- `DayOfWeek`
- `HourOfDay`

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

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

(DayOfWeek >= Monday AND DayOfWeek <= Friday).

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

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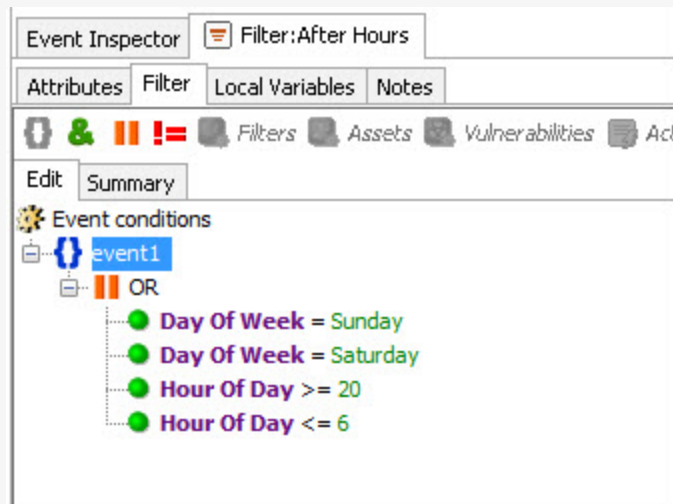
Limit Regulation Filter

The Limit Regulation filter limits event processing to only those events addressed by the GDPR regulation. Customize it to reflect your environment.

For example, you could configure it to specify the following conditions:

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

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

Deploy the CIP for GDPR Rules

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

To enable a rule:

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

Enable Data Monitors

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

To enable the data monitors:

1. In the Navigator panel, go to **Dashboards** and click the **Data Monitors** tab.

2. Navigate to the **/All Data Monitors/ArcSight Solutions/GDPR** group.

3. Right-click the CIP group and select **Enable Data Monitor** to enable all the data monitors in the group.

Configure Additional Resources

Additional configuration may be required or desired for the individual resources provided to address a specific GDPR Requirements. For more information, see "Appendix A: CIP for GDPR Resource Reference" on page 103.

Build FlexConnector(s) for Physical Access Devices

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

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

Field Mappings

ArcSight Field	Physical Access System Value
deviceEventClassId	Unique value for event type used for categorization
deviceReceiptTime	Access Time

Field Mappings, continued

ArcSight Field	Physical Access System Value
destinationUserId	Users badge Id
deviceCustomString1	Location Accessed / Building

Use the following event categories for the following event types:

Event Categories

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

Chapter 3: CIP for GDPR Use Cases

The Compliance Insight Package for GDPR contains different use case resources. A use case resource provides a way to group and view a set of resources that help you to measure and report on compliance with the GDPR regulation.

To view the resources associated with a use case resource:

1. In the Navigator panel select the Use Cases tab.
2. Browse for the use case resource (such as ArcSight Solutions/GDPR/Data Flow between GDPR Systems and non EU Countries).
3. Right click the use case resource and select the Open Use Case option.

The resources that make up a use case resource are displayed as shown in Figure 4-1. The use case resource tables listed below contain all the resources that have been explicitly assigned to the use case.
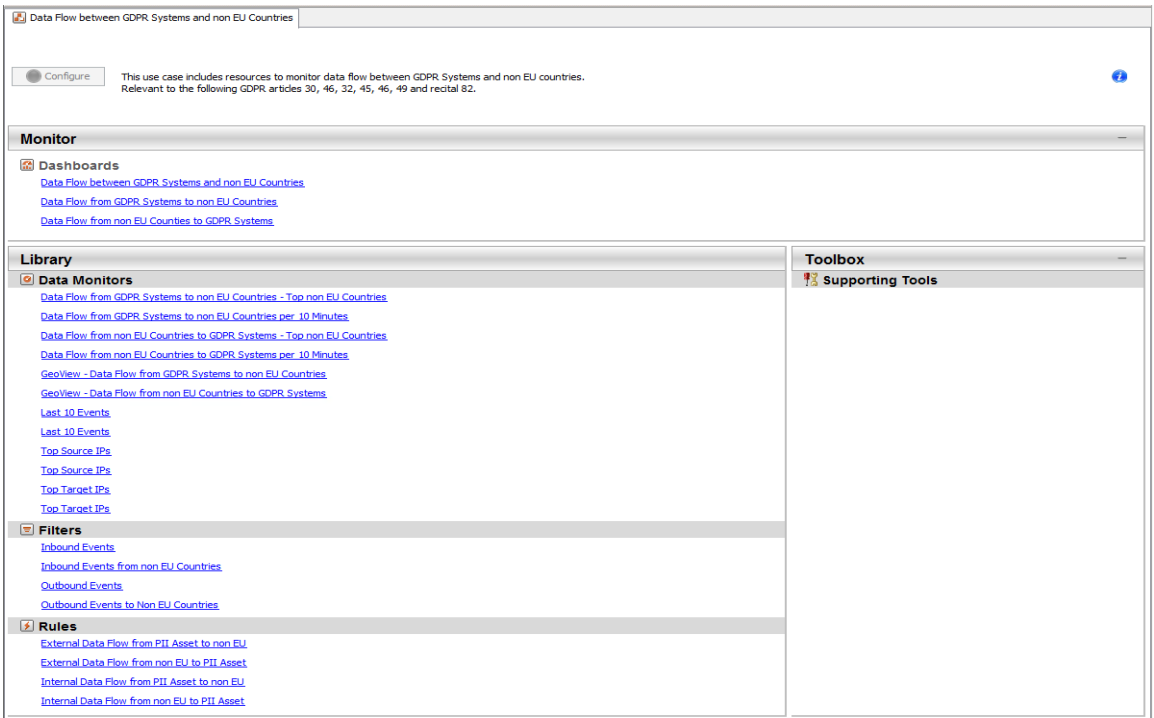
General Use Cases

Resource	Description	Supported Devices	Special Configuration
Account Lockouts	This use case monitor account lockout events. Relevant to the following GDPR Articles 24,25,28,32 and Recital 49.	Operating Systems	Edit the Account Lockouts filter to add conditions for lockout events from other devices in your environment. By default, the Account Lockouts filter identifies account lockouts on Microsoft Windows and UNIX systems. Verify that the Account Lockouts filter detects events in your environment that match the expected behaviour.
Assets not Scanned for Longer than Policy Standard	This use case provide resources to monitor assets not scanned for Longer than organization Policy Standard . organization policy standard time limit is defined by the TTL in the active list of this use case (default 60 days). Relevant to GDPR Articles 32, 35, 83 and Recitals 76, 77, 78, 83	Vulnerability Assessments	When a vulnerability scan event is detected on specific asset the scan are placed on the "Vulnerability Scanned Assets" active list. An entry expiring from this active list indicates that the there was no vulnerability scan for this asset for longer than allowed by policy (as indicated by the TTL of the active list). In that case, vulnerability scan not conducted for Longer than Policy Standard a rule will detect the event. If a vulnerability scan on specific asset conducted on time defined by the policy, a rule will detect this event and update the entry on the active list so it will not expire. This use case requires the following configuration for your environment: In the" Vulnerability Scanned Assets" active list, edit the TTL to reflect the maximum amount of time allowed to conduct vulnerability scan. Enable the following rules : 1. Vulnerability Scans 2. Asset not Scanned for Longer than Policy Standard for Longer than Policy Standard

Resource	Description	Supported Devices	Special Configuration
Attacks and Suspicious Activity	This use case provides information about events that are identified as attacks or suspicious activity based on Arcsight categorization. Relevant to GDPR Article 30, 32 and Recital 49.	Intrusion Detection Systems Intrusion Prevention Systems Network Based Anomaly Detection Firewalls Network Equipment Content Security Web Filtering Antivirus Wireless Applications	
Audit Log Cleared	This use case provides information about events that occur when an audit log is cleared or modified manually. Relevant to the following GDPR Articles 5, 25 and Recital 49.	Operating Systems	By default, the Audit Log Cleared filter returns events indicating that audit logs have been cleared on Microsoft Windows or detected by Symantec HostID systems. Edit this filter to add conditions for additional events known to indicate audit log clearing in your environment
Audit Log Failures	This use case provides resources to monitor audit log failure. Relevant to the following GDPR Articles 5, 25 and Recital 49.	Operating Systems	
Botnet Activity	This use case provides information about possible botnet activity on the organization. Relevant to GDPR Article 30, 32 and Recital 49.	Proxy	1. Make Sure the active list : "DMZ Assets" is configured 2. Make sure the following rule "Possible Botnet Activity" is enabled and deployed before using other resources for this use case.
CRM and ERP Flaws	This use case provides resources for monitoring flaws and vulnerabilities on customer relation management and enterprise resource planning products. Relevant to GDPR Articles 32, 35, 83 and Recitals 76, 77, 78, 83.	Vulnerability Assessments	
Clear Text Password Transmission	This use case provides resources to monitor password transmitted on clear text.		

Resource	Description	Supported Devices	Special Configuration
Covert Channel Activity	This use case provides information about covert channel activity. Relevant to GDPR Article 32,33,34 and Recital 49,85,86.	Intrusion Detection Systems Intrusion Prevention Systems	
Critical Configuration Changes	This use case includes resources to monitor critical configuration changes. Relevant to the following GDPR Articles 32.	Operating System Database	Database assets should be categorized with this category "/All Asset Categories/Site Asset Categories/Business Impact Analysis/Business Role/Service/Database". PII assets should be categorized with the /All Assets Categories/Compliance Insight Package/Network Domains/Electronic PII.
Data Flow between GDPR Systems and non EU Countries	This use case includes resources to monitor data flow between GDPR Systems and non EU countries. Relevant to the following GDPR articles 30, 46, 32, 45, 46, 49 and recital 82.	Proxy Firewall	
Database Flaws	This use case provides resources for monitoring different database flaws and vulnerabilities. Relevant to GDPR Articles 32, 35, 83 and Recitals 76, 77, 78, 83.	Vulnerability Assessments	
Directory Traversal Attacks	This use case identifies and reports on possible kinds of directory traversal attacks. Relevant to GDPR Article 32 and Recital 49.	Intrusion Detection Systems Intrusion Prevention Systems Web Servers	

Resource	Description	Supported Devices	Special Configuration
DoS Activity	This use case provides overview of Denial of Service activity on the organization. Relevant to GDPR Article 32 and Recital 49.	Network Equipment Intrusion Detection Systems Intrusion Prevention Systems Firewalls Network Based Anomaly Detection Content Security Web Filtering	
Email Activity	This use case provides resources for monitoring email attacks. Relevant to GDPR Article 32 Recital 49.	Email Servers (Microsoft Exchange) Intrusion Detection Systems Intrusion Prevention Systems	Before deploying "Potential Spear Phishing Attack" rule please make sure to add high profile email addresses to the "Important Emails" active list. This list stores important emails of high-profile targets on the organization like C- level executives which could be targeted by spear phishing attacks. Entries in this list should be in all lower case.
Encrypted Communication Information Leak	This use case provides resources for monitoring encrypted communication for information leakage on the organization. Relevant to GDPR Article 32,33,34 and Recital 49,85,86	Intrusion Detection Systems Intrusion Prevention Systems Network Based Anomaly Detection Firewalls Network Equipment Content Security Web Filtering Antivirus Wireless Applications	

Resource	Description	Supported Devices	Special Configuration
Exploit Executed on Databases	This use case contains resources for monitoring exploits executed against databases. Relevant to GDPR Article 32 and Recital 49.	Intrusion Detection Systems Intrusion Prevention Systems Anti-Virus Content Security	Database assets should be categorized with this category "/All Asset Categories/Site Asset Categories/Business Impact Analysis/Business Role/Service/Database".
Exploit Executed on PII Assets	This use case contains resources for monitoring exploits executed against PII Assets. Relevant to GDPR Article 32 and Recital 49.	Intrusion Detection Systems Intrusion Prevention Systems Anti-Virus Content Security	PII assets should be categorized with the /All Assets Categories/Compliance Insight Package/Network Domains/Electronic PII.
Failed Anti-Virus Signature Updates	This use case provides information about failed anti-virus signature updates on the organization. Relevant to GDPR Article 32 and Recital 49.	Anti-Virus	
Failed Login Overview	This use case contains resources to monitor failed login activity across the organization. Relevant to the following GDPR Articles 24,25,28,32 and Recital 49.	Operating Systems	
Firewall Blocked Events	This use case provides resources for monitoring firewall blocked events. Relevant to the following GDPR article 32 and recital 49.	Firewall	
Format String Vulnerabilities	This use case provides information about format string vulnerabilities on the organization. Relevant to GDPR Articles 32, 35, 83 and Recitals 76, 77, 78, 83.	Vulnerability Assessments	
Frequent Unsuccessful Logins by User Name	This use case contains resources for monitoring frequent unsuccessful ogins by user name. Relevant to the following GDPR Articles 24,25,28,32 and Recital 49.	Operating Systems	

Resource	Description	Supported Devices	Special Configuration
Frequent Unsuccessful Logins from Attacker Host	This use case contains resources for monitoring frequent unsuccessful logins from attacker host. Relevant to the following GDPR Articles 24,25,28,32 and Recital 49.	Operating Systems	
Frequent Unsuccessful Logins from non EU Countries to PII Asset	This use case contains resources for monitoring frequent unsuccessful user login from non EU countries to PII Asset. Relevant to the following GDPR Articles 24,25,28,32 and Recital 49.	Operating Systems	PII assets should be categorized with the /All Assets Categories/Compliance Insight Package/Network Domains/Electronic PII.
Frequent Unsuccessful Logins to Target Host	This use case contains resources for monitoring frequent unsuccessful logins to target host. Relevant to the following GDPR Articles 24,25,28,32 and Recital 49.	Operating Systems	
High Risk Events	This use case includes resources for monitoring high risk events. Relevant to GDPR Articles 32, 83 and Recital 49.	Intrusion Detection Systems Intrusion PreventionSystems Databases Operating Systems Firewalls Virtual Private Networks (VPN) Vulnerability Assessments Identity Management Policy Management Network Equipment Content Security Web Filtering Anti-Virus Physical Security Systems Wireless Applications Network Based Anomaly Detection	

Resource	Description	Supported Devices	Special Configuration
High Risk Vulnerabilities	This use case provides resources for monitoring high risk vulnerabilities on the organization. Relevant to GDPR Articles 32, 35, 83 and Recitals 76, 77, 78, 83.	Vulnerability Assessments	
Information Disclosure Vulnerabilities	This use case provides resources for monitoring information disclosure vulnerabilities on the organization. Relevant to GDPR Articles 32, 35, 83 and Recitals 76, 77, 78, 83.	Vulnerability Assessments	
Information Interception	This use case identifies and reports on possible kinds of information interception events incidents such as spoofing attempts, man-in-the-middle attacks or instant messaging. Relevant to GDPR Article 32,33,34 and Recital 49,85,86.	Intrusion Detection Systems Intrusion Prevention Systems Network Based Anomaly Detection	
Insecure Cryptographic Storages	This use case provides resources for monitoring flaws on cryptographic storage devices. Relevant to Article 35.	Vulnerability Assessments	
Internal Insecure Communications	This use case provides information about unencrypted and thus insecure communications inside the network. Relevant to the following GDPR Article 32 and Recital 49.	Firewall Proxy Intrusion Detection Systems Intrusion Prevention Systems	1. In the Insecure Processes active list, add any processes that your organization knows to be insecure. 2. In the Insecure Ports active lists, add the ports that your organization knows to be insecure. 3. Verify that the Inbound Events, Outbound Events, Insecure Services filters detects events in your environment that match the expected behavior. 4.Internal Assets should be categorized as with the /All Assets Categories/Compliance Insight Package/Address Spaces/Protected.

Resource	Description	Supported Devices	Special Configuration
Invalid or Expired Certificate	This use case contains resources for monitoring invalid or expired certificates. Relevant to GDPR Article 32 and Recital 49.	Intrusion Detection System Intrusion Prevention System Vulnerability Assessments	
MITRE ATT&CK Activity on PII Assets	This use case provides different resources for monitoring MITRE ATT&CK activity on PII assets. Relevant to GDPR Article 32 and Recital 49.	Security Information Managers Operating System Intrusion Detection System Intrusion Prevention Systems Vulnerability Assessments Network Equipments Anti-Virus EDR	PII assets should be categorized with the /All Assets Categories/Compliance Insight Package/Network Domains/Electronic PII.
MITRE ATT&CK Overview	This use case provides resources to monitor MITRE ATT&CK reported techniques on the organization.	Security Information Managers Operating System Intrusion Detection System Intrusion Prevention Systems Vulnerability Assessments Network Equipments Anti-Virus EDR	
Malware Monitoring	This use case provides resources for monitoring malware. Relevant to GDPR Articles 32, 33, 34 and Recitals 49, 83.	Anti-Virus Intrusion Detection Systems Intrusion Prevention Systems	

Resource	Description	Supported Devices	Special Configuration
Non EU Login Activity	This use case provides an overview of login activity from non EU countries. Relevant to the following GDPR articles 5,25,30, 46, 32, 45, 46, 49 and recital 49,82.	Operating Systems Intrusion Detection Systems Intrusion Prevention Systems	
Organizational Information monitoring	This use case provides different resources for monitoring organizational information. Relevant to GDPR Article 32,33,34 and Recital 49,85,86.	Intrusion Detection Systems Intrusion Prevention Systems Network Based Anomaly Detection Firewalls Network Equipment Content Security Web Filtering Antivirus Wireless Applications	
Overflow Vulnerabilities	This use case provides information about overflow vulnerabilities on the organization. Relevant to GDPR Articles 32, 35, 83 and Recitals 76, 77, 78, 83.	Vulnerability Assessments	
Password Spray Attacks	This use case provides resources to monitor password spray attacks. Relevant to the following GDPR Articles 24,25,28,32 and Recital 49.	OperatingSystems (Windows)	
Password and Authentication Weaknesses	This use case provides resources for monitoring password and authentication weaknesses on the organization. Relevant to GDPR Articles 32, 35, 83 and Recitals 76, 77, 78, 83.	Vulnerabilit Assessments	

Resource	Description	Supported Devices	Special Configuration
Password not Changed for Longer than Policy Standard	This use case provide resources to monitor password not changed for Longer than organization Policy Standard . organization policy standard time limit is defined by the TTL in the active list of this use case (default 90 days). Relevant to the following GDPR Articles 24,25,28,32 and Recital 49.	Operating Systems	1. When a successful password change event is detected, the user name for whom the password was changed and the device that reported the event are placed on the Password Changes active list. An entry expiring from this active list indicates that the user has not changed the password on that device for longer than allowed by policy (as indicated by the TTL of the active list). In that case, Password not Changed for Longer than Policy Standard rule will detect the event. If the user changes his/her password within the time defined by the policy, a rule will detect this event and update the entry on the active list so it will not expire. The Password Management use case requires the following configuration for your environment. a. In the Password Changes active, edit the TTL to reflect the maximum amount of time allowed between password changes according to your organization's policy. b· Edit the Password Change Attempts filter to identify all password change attempts from devices on your system. By default, the filter detects only password change attempts on Microsoft Windows. Verify that the Password Change Attempts filter detects events in your environment that match the expected behaviour. c. Enable the following rules : "Password not Changed for Longer than Policy Standard" and "Successful Password Change"

Resource	Description	Supported Devices	Special Configuration
Personal identifiable information monitoring	This use case provides different resources for monitoring personal identifiable information assets. Relevant to GDPR Article 32,33,34 and Recital 49,85,86.	Intrusion Detection Systems Intrusion Prevention Systems Network Based Anomaly Detection Firewalls Network Equipment Content Security Web Filtering Antivirus Wireless Applications	
Physical Access	This use case detects violations on events related to physical security devices such as badge readers. Specifically, it detects after hour building access by contractors. Relevant to the following Articles 24,32 and Recital 46.	Physical Security Systems	1.Before enabling and deploying this rule "After Hours Building Access by Contractors" Populate the Badges to Accounts active list with the badge ID, primary computer account for the badge holder, and the employee type for users in your organization (in lowercase). Specifically, ensure that contractors are identified with the words "Contractor" (case insensitive) in the employee type field. 2.Modify the After Hours filter to specify the appropriate after-business-hours window for your organization. 3,Before enabling and deploying this rule "Failed Access by the Same User to Multiple Buildings" please make sure the following rule: "Failed Building Access" is enabled and deployed

Resource	Description	Supported Devices	Special Configuration
Policy Violations	This use case provides information about policy violations. Relevant to GDPR Articles 32, 83 and Recital 49.	Intrusion Detection Systems Intrusion Prevention System Firewalls Operating Systems Assessment Tools Applications Security Information Managers Identity Management Virtual Private Networks (VPN) Policy Management Wireless Applications	
Privileged Account Changes	This use case monitors changes to privileged accounts.	Operating Systems	In the Administrative Accounts active list, define usernames that have administrative privileges in your environment.
Reconnaissance Activities	This use case provides overview of recon activity. Relevant to GDPR Article 30, 32 and Recital 49.	Intrusion Detection Systems Intrusion Prevention System Network Based Anomaly Detection Firewalls Network Equipment Content Security Web Filtering Antivirus Wireless Applications	
Removal of Access Rights	This use case provides resources to monitor when an access right of a user is removed. Relevant to GDPR Articles 5,18,24,29,32 and Recital 39.	Operating Systems	

Resource	Description	Supported Devices	Special Configuration
SQL Injection Vulnerabilities	This use case provides resources for monitoring SQL injection vulnerabilities. Relevant to GDPR Articles 32, 35, 83 and Recitals 76, 77, 78, 83.	Vulnerability Assessments	
SSL and TLS Vulnerabilities	This use case provides overview about SSL and TLS vulnerabilities. Relevant to GDPR Articles 32, 35, 83 and Recitals 76, 77, 78, 83.	Vulnerability Assessments	
Security Application Stopped or Paused	This use case provides overview of security application stopped or paused (it focuses on Anti-Virus products). Relevant to GDPR Article 32 and Recital 49.	Operating Systems	
Security Patches	This Use Case provides information about missing security patches. Relevant to GDPR Articles 32, 35, 83 and Recitals 76, 77, 78, 83.	Vulnerability Assessments	
Shell Code Attacks	This use case provides resources to detect shell code attacks. Relevant to GDPR Article 32 and Recital 49.	Intrusion Detection Systems Intrusion Prevention Systems	
Successful Login Overview	This use case contains resources to monitor successful login activity across the organization. Relevant to the following GDPR Articles 24,25,28,32 and Recital 49.	Operating Systems	

Resource	Description	Supported Devices	Special Configuration
Threats Geo Overview	This use case provides geographical view of events that identified as threats against the organization. Relevant to GDPR Article 30, 32 and Recital 49.	Intrusion Detection Systems Intrusion Prevention Systems Network Based Anomaly Detection Firewalls Network Equipment Content Security Web Filtering Antivirus Wireless Applications Security Information Managers	
Threats from non EU Countries	Thise use case contains resources for monitoring threats from non EU countries. Relevant to GDPR Articles 32, 35, 83 and Recitals 76, 77, 78, 83.	Intrusion Detection Systems Intrusion Prevention Systems Network Based Anomaly Detection Firewalls Network Equipment Content Security Web Filtering Antivirus Wireless Applications Security Information Managers	
User Logged In From Two Countries	This use case shows login attempts with the same user name from two different countries. Relevant to the following GDPR Articles 24,25,28,32 and Recital 49.	Operating Systems	

Resource	Description	Supported Devices	Special Configuration
User Logged in from different IP Addresses	This use case provides resources for monitoring single user names that have been used to login from different IP addresses on short period of time. Relevant to the following GDPR Articles 24,25,28,32 and Recital 49.	Operating Systems	
User Logged in from non EU Countries to PII Asset	This use case shows logins from non EU countries to PII assets. Relevant to the following GDPR Articles 24,25,28,32 and Recital 49.	Operating Systems	PII assets should be categorized with the /All Assets Categories/Compliance Insight Package/Network Domains/Electronic PII.
User Logged in to different Host Names	This use case provides resources for monitoring single user names that have been used to login to different host names on short period of time. Relevant to the following GDPR Articles 24,25,28,32 and Recital 49.	Operating Systems	
Wordpress GDPR Plugin Exploits and Vulnerabilities	This use case monitor both exploits and vulnerabilities targeting WordPress GDPR Plugin. Relevant to GDPR Articles 32, 35, 83 and Recitals 49, 76, 77, 78, 83.	Vulnerability Assessments Intrusion Detection Systems Intrusion PreventionSystems	

Resource	Description	Supported Devices	Special Configuration
Worm Activity	This use case provides overview of Worm activity on the organization. Relevant to GDPR Articles 32, 35, 83 and Recitals 76, 77, 78, 83.	Antivirus Intrusion Detection Systems Intrusion Prevention Systems Network Based Anomaly Detection Firewalls Content Security Web Filtering	
XSRF Vulnerabilities	This use case provides overview of XSRF vulnerabilities on the organization. Relevant to GDPR Articles 32, 35, 83 and Recitals 76, 77, 78, 83.	Vulnerability Assessments	
XSS Vulnerabilities	This use case provides overview of XSS vulnerabilities on the organization. Relevant to GDPR Articles 32, 35, 83 and Recitals 76, 77, 78, 83.	Vulnerability Assessments	

Appendix A: GDPR Resource Reference

Resource	Type	URI	Description
Removal of Access Rights	ActiveChannel	/All Active Channels/ArcSight Solutions/GDPR/GDPR Access Activity/Access Activity/	Shows a live feed of events reflecting the removal of a user's access privileges.
Data Flow from GDPR Systems to non EU Countries	ActiveChannel	/All Active Channels/ArcSight Solutions/GDPR/GDPR Regulatory Exposure/Composite Regulatory Exposure/	Shows a live feed of reported events reflecting data flow from GDPR Systems to non EU Countries.
Data Flow from non EU Countries to GDPR Systems	ActiveChannel	/All Active Channels/ArcSight Solutions/GDPR/GDPR Regulatory Exposure/Composite Regulatory Exposure/	Shows a live feed of reported events reflecting data flow fro non EU Countries to GDPR Systems.
Personal Information Leak	ActiveChannel	/All Active Channels/ArcSight Solutions/GDPR/GDPR Threat Analysis/Internet Threat Analysis/	Shows a live feed of events of personal information leaks.
Vulnerability Scanned Assets	ActiveList	/All Active Lists/ArcSight Solutions/GDPR/	This active list stores all the assets that scanned by vulnerability scanners on the last x days. The default is 60 days. Do not manually update this active list.
Password Changes	ActiveList	/All Active Lists/ArcSight Solutions/GDPR/	This active is updated with the user and product information when a successful password change occurs.
Missing Security Patches	ActiveList	/All Active Lists/ArcSight Solutions/GDPR/	This active list stores all the missing security patches reported on the environment. By default, the active list TTL is set to zero which means it will hold all of the unfixed security patches indefinitely. Note: User can manually remove the fixed issues or set a custom reasonable TTL so that the removal is done automated.

Resource	Type	URI	Description
Insecure Processes	ActiveList	/All Active Lists/ArcSight Solutions/GDPR/	This active list includes the names of processes that provide unencrypted and thus insecure communications.
Insecure Ports	ActiveList	/All Active Lists/ArcSight Solutions/GDPR/	This active list includes ports related to unencrypted and thus insecure communication services.
DMZ Assets	ActiveList	/All Active Lists/ArcSight Solutions/GDPR/	This List should contain DMZ assets of the organization like DNS, WEB, SMTP servers. It contains 2 fields: IPAddress and AssetType where the IPAddress is the IP Address of the asset and the AssetType is the type of the asset in lower case (by default supported 3 types dns, web, smtp). For example, if your web server IP is x.y.z.w you should add it as IPAddress=x.y.z.w, AssetType=web.
Compliance Risk Score	ActiveList	/All Active Lists/ArcSight Solutions/GDPR/	This active list maintains the compliance risk score for each regulation section. The compliance risk score is calculated based on the triggered rules in the solution package. You can manually change the score as required. This change will be reflected in the Compliance Risk Score dashboard.
Badges to Accounts	ActiveList	/All Active Lists/ArcSight Solutions/GDPR/	This list contains the computer account and employee type for every physical device badge. Populate this active list with the badge ID, primary computer account for the badgeholder (in case its a visitor use the vistor user name), and the employee type for users in your organization (in lowercase). Specifically, ensure that contractors and visitors are identified with the word â€œContractorâ€, "Visitor" (case insensitive) in the employee type field.

Resource	Type	URI	Description
Administrative Accounts	ActiveList	/All Active Lists/ArcSight Solutions/GDPR/	This active list should be populated with the usernames that have administrative privileges in your domain. Admins (those responsible for managing administrative users) populate this list manually whenever a new administrative user is added. Entries to this list are read by reports supplied in the content pack, but the list can also be added to or referenced in new content built around the provided infrastructure. This active list should be populated with the usernames that have administrative privileges in your domain. Entries in this list should be in all lower case. For example, the user Administrator should be added as "administrator".
Important Emails	ActiveList	/All Active Lists/ArcSight Solutions/GDPR/	This list stores important emails addresses of high-profile targets on the organization like C-level executives which could be targeted by spear phishing attacks. entries in this list should be in all lower case.
Physical Access Activity	Dashboard	/All Dashboards/ArcSight Solutions/GDPR/GDPR Access Activity/Access Activity/	Displays information around physical access. In order for this dashboard component to allow contractor access after hours to populate data, please make sure the following rule : "After Hours Building Access by Contractors" is enabled and deployed.
Coordinated Failed Logins	Dashboard	/All Dashboards/ArcSight Solutions/GDPR/GDPR Access Activity/Access Activity/	This Dashboard provides overview of possible coordinated failed login events reported on the organization.
Failed Login Activity	Dashboard	/All Dashboards/ArcSight Solutions/GDPR/GDPR Access Activity/Access Activity/	This dashboard provides overview of failed login activity.
Non EU Login Activity	Dashboard	/All Dashboards/ArcSight Solutions/GDPR/GDPR Access Activity/Access Activity/	This dashboard provides an overview of successful login activity from non EU countries.
Successful Login Activity	Dashboard	/All Dashboards/ArcSight Solutions/GDPR/GDPR Access Activity/Access Activity/	This dashboard provides an overview of successful login activity.

Resource	Type	URI	Description
DoS Activity	Dashboard	/All Dashboards/ArcSight Solutions/GDPR/GDPR Attack Surface Analysis/Security Controls Risk Identification/	This dashboard provides an overview of events associated with denial of service and availability attacks.
Data Flow between GDPR Systems and non EU Countries	Dashboard	/All Dashboards/ArcSight Solutions/GDPR/GDPR Regulatory Exposure/Composite Regulatory Exposure/	This dashboard displays data flow between GDPR systems and non EU countries.
Data Flow from GDPR Systems to non EU Countries	Dashboard	/All Dashboards/ArcSight Solutions/GDPR/GDPR Regulatory Exposure/Composite Regulatory Exposure/	This dashboard displays data flow from GDPR systems and non EU countries.
Data Flow from non EU Countries to GDPR Systems	Dashboard	/All Dashboards/ArcSight Solutions/GDPR/GDPR Regulatory Exposure/Composite Regulatory Exposure/	This dashboard displays data flow from non EU countries to GDPR Systems.
High Risk Events	Dashboard	/All Dashboards/ArcSight Solutions/GDPR/GDPR Regulatory Exposure/Composite Regulatory Exposure/	This dashboard provides real-time overview of high risk events reported on the organization.
Policy Violations	Dashboard	/All Dashboards/ArcSight Solutions/GDPR/GDPR Regulatory Exposure/Composite Regulatory Exposure/	Displays information about policy violations and violators.
Threats Overview	Dashboard	/All Dashboards/ArcSight Solutions/GDPR/GDPR Regulatory Exposure/Composite Regulatory Exposure/	This dashboard provides an overview of threats reported on the organization.
Worm Activity	Dashboard	/All Dashboards/ArcSight Solutions/GDPR/GDPR Threat Analysis/Internet Threat Analysis/	This dashboard provides overview of worm activity on the organization.
Personal Information Leakage	Dashboard	/All Dashboards/ArcSight Solutions/GDPR/GDPR Threat Analysis/Internet Threat Analysis/	This Dashboard provides overview of personal information leakage events.

Resource	Type	URI	Description
Recon Activity	Dashboard	/All Dashboards/ArcSight Solutions/GDPR/GDPR Threat Analysis/Internet Threat Analysis/	This dashboard provides an overview of reconnaissance activity reported on the organization.
MITRE ATT&CK Overview	Dashboard	/All Dashboards/ArcSight Solutions/GDPR/GDPR Threat Analysis/Internet Threat Analysis/	This dashboard provides overview of MITRE ATT&CK related events reported on the organization.
Attacks and Suspicious Activity	Dashboard	/All Dashboards/ArcSight Solutions/GDPR/GDPR Threat Analysis/Internet Threat Analysis/	This dashboard provides overview of attacks and suspicious related events reported on the organization based on ArcSight Categorization.
Compliance Risk Score Overview	Dashboard	/All Dashboards/ArcSight Solutions/GDPR/Overview/	This dashboard displays information about the compliance risk score for each GDPR article. Note: In case you need to override the risk score status of a specific article, just right click on the article and choose the Override Status option. Before using this dashboard make sure the following rules are enabled and deployed : All Rules/ArcSight Solutions/GDPR/Overview/Compliance Score Update All Rules/ArcSight Solutions/GDPR/Overview/Manual Status Change
GDPR Rules Overview	Dashboard	/All Dashboards/ArcSight Solutions/GDPR/Overview/	This dashboard shows high-level information about GDPR rule firings.
Coordinated Failed Logins Target IPs - Event Graph	DataMonitor	/All Data Monitors/ArcSight Solutions/GDPR/GDPR Access Activity/Access Activity/Coordinated Failed Logins/	This data monitor shows coordinated failed logins between attacker IP, attacker countries, target IPs as they appear in failed login events.
Coordinated Failed Logins Target Users - Event Graph	DataMonitor	/All Data Monitors/ArcSight Solutions/GDPR/GDPR Access Activity/Access Activity/Coordinated Failed Logins/	This data monitor shows coordinated failed logins between attacker IP, attacker countries, target user as they appear in failed login events.

Resource	Type	URI	Description
GeoView - Failed Logins	DataMonitor	/All Data Monitors/ArcSight Solutions/GDPR/GDPR Access Activity/Access Activity/Coordinated Failed Logins/	This data monitor shows failed login events on a map.
Last 10 Failed Logins	DataMonitor	/All Data Monitors/ArcSight Solutions/GDPR/GDPR Access Activity/Access Activity/Coordinated Failed Logins/	This data monitor displays the last 10 failed login events.
Frequent Failed Login per 10 Minutes	DataMonitor	/All Data Monitors/ArcSight Solutions/GDPR/GDPR Access Activity/Access Activity/Failed Login Activity/	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 300%.
Failed Login per 10 Minutes	DataMonitor	/All Data Monitors/ArcSight Solutions/GDPR/GDPR Access Activity/Access Activity/Failed Login Activity/	Shows a moving average of failed login events. It displays data for the last 10 minutes and will generate a correlation event if the moving average is increased by 300%.
Failed Login - Top Attacker IPs	DataMonitor	/All Data Monitors/ArcSight Solutions/GDPR/GDPR Access Activity/Access Activity/Failed Login Activity/	Shows the top 10 attacker addresses involved in failed login activity.
Failed Login - Top Target IPs	DataMonitor	/All Data Monitors/ArcSight Solutions/GDPR/GDPR Access Activity/Access Activity/Failed Login Activity/	Shows the top 10 target addresses involved in failed login activity.
Failed Login - Top Users	DataMonitor	/All Data Monitors/ArcSight Solutions/GDPR/GDPR Access Activity/Access Activity/Failed Login Activity/	Shows the top 10 users involved in failed login activity.

Resource	Type	URI	Description
GeoView - Non EU Login Activity	DataMonitor	/All Data Monitors/ArcSight Solutions/GDPR/GDPR Access Activity/Access Activity/Non EU Login Activity/	This data monitor shows login activity from non EU countries on a map.
Non EU Login Activity - Top Attacker IPs	DataMonitor	/All Data Monitors/ArcSight Solutions/GDPR/GDPR Access Activity/Access Activity/Non EU Login Activity/	Shows the top 10 attacker addresses involved in successful login activity from non EU countries.
Non EU Login Activity - Top Target IPs	DataMonitor	/All Data Monitors/ArcSight Solutions/GDPR/GDPR Access Activity/Access Activity/Non EU Login Activity/	Shows the top 10 target addresses involved in successful login activity from non EU countries.
Non EU Login Activity - Top Users	DataMonitor	/All Data Monitors/ArcSight Solutions/GDPR/GDPR Access Activity/Access Activity/Non EU Login Activity/	Shows the top 10 users involved in successful login activity from non EU countries.
Building Access - Event Graph	DataMonitor	/All Data Monitors/ArcSight Solutions/GDPR/GDPR Access Activity/Access Activity/Physical Access Activity/	Used to show the hour of day that users are accessing buildings.
Last 10 Building Access Events	DataMonitor	/All Data Monitors/ArcSight Solutions/GDPR/GDPR Access Activity/Access Activity/Physical Access Activity/	Shows the last 10 physical access events.
Top Users Accessing Buildings	DataMonitor	/All Data Monitors/ArcSight Solutions/GDPR/GDPR Access Activity/Access Activity/Physical Access Activity/	Shows the top 10 users accessing buildings.

Resource	Type	URI	Description
Contractor Access After Hours	DataMonitor	/All Data Monitors/ArcSight Solutions/GDPR/GDPR Access Activity/Access Activity/Physical Access Activity/	Shows the top contractors accesses after hours.
Successful Login Activity - Login per 10 Minutes	DataMonitor	/All Data Monitors/ArcSight Solutions/GDPR/GDPR Access Activity/Access Activity/Succesful Login Activity/	Shows a 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%.
Successful Login Activity - Top Attacker IPs	DataMonitor	/All Data Monitors/ArcSight Solutions/GDPR/GDPR Access Activity/Access Activity/Succesful Login Activity/	Shows the top 10 attacker addresses involved in successful login activity.
Successful Login Activity - Top Target IPs	DataMonitor	/All Data Monitors/ArcSight Solutions/GDPR/GDPR Access Activity/Access Activity/Succesful Login Activity/	Shows the top 10 target addresses involved in successful login activity.
Successful Login Activity - Top Users	DataMonitor	/All Data Monitors/ArcSight Solutions/GDPR/GDPR Access Activity/Access Activity/Succesful Login Activity/	Shows the top 10 users involved in successful login activity.
Suspicious Logins per 10 Minutes	DataMonitor	/All Data Monitors/ArcSight Solutions/GDPR/GDPR Access Activity/Access Activity/Succesful Login Activity/	Shows a moving average of suspicious login events. It displays data for the last 10 minutes and will generate a correlation event if the moving average is increased by 300%.
Top 10 DoS Targets	DataMonitor	/All Data Monitors/ArcSight Solutions/GDPR/GDPR Attack Surface Analysis/Security Controls Risk Identification/	This data monitor shows the top 10 DoS targets.

Resource	Type	URI	Description
Top 10 DoS Attackers	DataMonitor	/All Data Monitors/ArcSight Solutions/GDPR/GDPR Attack Surface Analysis/Security Controls Risk Identification/	This data monitor shows the top 10 DoS Attackers.
DoS Attacks Event Ports - Event Graph	DataMonitor	/All Data Monitors/ArcSight Solutions/GDPR/GDPR Attack Surface Analysis/Security Controls Risk Identification/	This data monitor shows connection between attacker and target machines and ports as they appear in denial of service attack events.
DoS Attacks Event Countries - Event Graph	DataMonitor	/All Data Monitors/ArcSight Solutions/GDPR/GDPR Attack Surface Analysis/Security Controls Risk Identification/	This data monitor shows connection between attacker, target countries, machines and ports as they appear in denial of service attack events.
GeoView - Data Flow from GDPR Systems to non EU Countries	DataMonitor	/All Data Monitors/ArcSight Solutions/GDPR/GDPR Regulatory Exposure/Composite Regulatory Exposure/Data Flow from and to GDPR Systems/	This data monitor shows Data Flow from GDPR Systems to non EU countries on a map.
Data Flow from non EU Countries to GDPR Systems - Top non EU Countries	DataMonitor	/All Data Monitors/ArcSight Solutions/GDPR/GDPR Regulatory Exposure/Composite Regulatory Exposure/Data Flow from and to GDPR Systems/	Shows the top 10 non EU source countries involved on data flow from to GDPR Systems.
Data Flow from GDPR Systems to non EU Countries - Top non EU Countries	DataMonitor	/All Data Monitors/ArcSight Solutions/GDPR/GDPR Regulatory Exposure/Composite Regulatory Exposure/Data Flow from and to GDPR Systems/	Shows the top 10 non EU target countries involved on data flow from GDPR systems.

Resource	Type	URI	Description
GeoView – Data Flow from non EU Countries to GDPR Systems	DataMonitor	/All Data Monitors/ArcSight Solutions/GDPR/GDPR Regulatory Exposure/Composite Regulatory Exposure/Data Flow from and to GDPR Systems/	This data monitor shows Data Flow from non EU countries to GDPR systems.
Last 10 Events	DataMonitor	/All Data Monitors/ArcSight Solutions/GDPR/GDPR Regulatory Exposure/Composite Regulatory Exposure/Data Flow from GDPR Systems to non EU Countries/	This data monitor displays the last 10 data flow events from GDPR systems to non EU Countries.
Data Flow from GDPR Systems to non EU Countries per 10 Minutes	DataMonitor	/All Data Monitors/ArcSight Solutions/GDPR/GDPR Regulatory Exposure/Composite Regulatory Exposure/Data Flow from GDPR Systems to non EU Countries/	Shows a moving average of data flow from GDPR systems events to non EU Countries. It displays data for the last hour and will generate a correlation event if the moving average is increased by 500%.
Top Target IPs	DataMonitor	/All Data Monitors/ArcSight Solutions/GDPR/GDPR Regulatory Exposure/Composite Regulatory Exposure/Data Flow from GDPR Systems to non EU Countries/	Shows the top 10 target addresses involved on data flow from GDPR systems to non EU countries.
Top Source IPs	DataMonitor	/All Data Monitors/ArcSight Solutions/GDPR/GDPR Regulatory Exposure/Composite Regulatory Exposure/Data Flow from GDPR Systems to non EU Countries/	Shows the top 10 source addresses involved on data flow from GDPR systems to non EU countries.

Resource	Type	URI	Description
Data Flow from non EU Countries to GDPR Systems per 10 Minutes	DataMonitor	/All Data Monitors/ArcSight Solutions/GDPR/GDPR Regulatory Exposure/Composite Regulatory Exposure/Data Flow from non EU Countries to GDPR Systems/	Shows a moving average of data flow from non EU countries to GDPR system events. It displays data for the last hour and will generate a correlation event if the moving average is increased by 500%.
Last 10 Events	DataMonitor	/All Data Monitors/ArcSight Solutions/GDPR/GDPR Regulatory Exposure/Composite Regulatory Exposure/Data Flow from non EU Countries to GDPR Systems/	This data monitor displays the last 10 data flow events from non EU Countries to GDPR Systems
Top Source IPs	DataMonitor	/All Data Monitors/ArcSight Solutions/GDPR/GDPR Regulatory Exposure/Composite Regulatory Exposure/Data Flow from non EU Countries to GDPR Systems/	Shows the top 10 source addresses involved on data flow from non EU countries to GDPR systems.
Top Target IPs	DataMonitor	/All Data Monitors/ArcSight Solutions/GDPR/GDPR Regulatory Exposure/Composite Regulatory Exposure/Data Flow from non EU Countries to GDPR Systems/	Shows the top 10 target addresses involved on data flow from non EU countries to GDPR systems.
Top 10 Attackers with High Risk Events	DataMonitor	/All Data Monitors/ArcSight Solutions/GDPR/GDPR Regulatory Exposure/Composite Regulatory Exposure/High Risk Events/	This data monitor shows the top 10 attackers involved on high risk events.

Resource	Type	URI	Description
GeoView - High Risk Events	DataMonitor	/All Data Monitors/ArcSight Solutions/GDPR/GDPR Regulatory Exposure/Composite Regulatory Exposure/High Risk Events/	This data monitor shows high risk reported events on a map.
High Risk Events per 10 Minutes	DataMonitor	/All Data Monitors/ArcSight Solutions/GDPR/GDPR Regulatory Exposure/Composite Regulatory Exposure/High Risk Events/	Shows a moving average of high risk event. It displays data for the last 10 minutes and will generate a correlation event if the moving average is increased by 300%.
Last 10 High Risk Events	DataMonitor	/All Data Monitors/ArcSight Solutions/GDPR/GDPR Regulatory Exposure/Composite Regulatory Exposure/High Risk Events/	This data monitor displays in real-time the last 10 high risk events.
Top 10 Targets with High Risk Events	DataMonitor	/All Data Monitors/ArcSight Solutions/GDPR/GDPR Regulatory Exposure/Composite Regulatory Exposure/High Risk Events/	Provides an ordered list of the top 10 hosts with high priority events.
Top 10 Policy Violators	DataMonitor	/All Data Monitors/ArcSight Solutions/GDPR/GDPR Regulatory Exposure/Composite Regulatory Exposure/Policy Violations/	Shows the top 10 policy violators.
Top 10 Policy Violations	DataMonitor	/All Data Monitors/ArcSight Solutions/GDPR/GDPR Regulatory Exposure/Composite Regulatory Exposure/Policy Violations/	Shows the top 10 policy violation events.

Resource	Type	URI	Description
GeoView - DoS Activity	DataMonitor	/All Data Monitors/ArcSight Solutions/GDPR/GDPR Regulatory Exposure/Composite Regulatory Exposure/Threats/	This data monitor shows geo view of DoS Activity.
GeoView - MITRE ATT&CK Activity	DataMonitor	/All Data Monitors/ArcSight Solutions/GDPR/GDPR Regulatory Exposure/Composite Regulatory Exposure/Threats/	This data monitor shows geo view of MITRE ATT&CK Activity.
GeoView - Reconnaissance Activity	DataMonitor	/All Data Monitors/ArcSight Solutions/GDPR/GDPR Regulatory Exposure/Composite Regulatory Exposure/Threats/	This data monitor shows geo view of Reconnaissance Activity.
Last 10 Threats	DataMonitor	/All Data Monitors/ArcSight Solutions/GDPR/GDPR Regulatory Exposure/Composite Regulatory Exposure/Threats/	This data monitor displays the last 10 events that indicate compromise, reconnaissance, hostile, or suspicious activity and MITRE Attacks.
Worm Propagation - Event Graph	DataMonitor	/All Data Monitors/ArcSight Solutions/GDPR/GDPR Threat Analysis/Internet Threat Analysis/	This data monitor shows connection between attacker and target machines as they appear in worm events.
Personal Information Leakage per 10 Minutes	DataMonitor	/All Data Monitors/ArcSight Solutions/GDPR/GDPR Threat Analysis/Internet Threat Analysis/	Shows a moving average of personal information leakage. It displays data for the last 10 minutes and will generate a correlation event if the moving average is increased by 300%.
Personal Information Leakage - Top Users by Agent Severity Distribution	DataMonitor	/All Data Monitors/ArcSight Solutions/GDPR/GDPR Threat Analysis/Internet Threat Analysis/	Shows the top 10 users involved on personal information leakage activity by Agent Severity Distribution.

Resource	Type	URI	Description
Personal Information Leakage - Top 10 Target IPs	DataMonitor	/All Data Monitors/ArcSight Solutions/GDPR/GDPR Threat Analysis/Internet Threat Analysis/	Shows the top 10 target addresses involved on personal information leakage activity.
Personal Information Leakage - Top 10 Attacker IPs	DataMonitor	/All Data Monitors/ArcSight Solutions/GDPR/GDPR Threat Analysis/Internet Threat Analysis/	Shows the top 10 attacker addresses involved on personal information leakage activity.
Last 10 Worm Events	DataMonitor	/All Data Monitors/ArcSight Solutions/GDPR/GDPR Threat Analysis/Internet Threat Analysis/	This data monitor displays the last 10 worm events.
Worm Activity per 10 Minutes	DataMonitor	/All Data Monitors/ArcSight Solutions/GDPR/GDPR Threat Analysis/Internet Threat Analysis/	Shows a moving average of worm event. It displays data for the last hour and will generate a correlation event if the moving average is increased by 500%.
Top 10 Target IPs	DataMonitor	/All Data Monitors/ArcSight Solutions/GDPR/GDPR Threat Analysis/Internet Threat Analysis/Attacks and Suspicious Activity/	Shows the top 10 target addresses involved on attack and suspicious activity.
Top 10 Attacker IPs	DataMonitor	/All Data Monitors/ArcSight Solutions/GDPR/GDPR Threat Analysis/Internet Threat Analysis/Attacks and Suspicious Activity/	Shows the top 10 attacker addresses involved on attack and suspicious activity.
Last 5 Attacks and Suspicious Activity Events	DataMonitor	/All Data Monitors/ArcSight Solutions/GDPR/GDPR Threat Analysis/Internet Threat Analysis/Attacks and Suspicious Activity/	This data monitor displays the last 5 attack and suspicious activity events.
Attacks and Suspicious Activity per 10 Minutes	DataMonitor	/All Data Monitors/ArcSight Solutions/GDPR/GDPR Threat Analysis/Internet Threat Analysis/Attacks and Suspicious Activity/	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%.

Resource	Type	URI	Description
Ports Used in Attacks and Suspicious Activity Events	DataMonitor	/All Data Monitors/ArcSight Solutions/GDPR/GDPR Threat Analysis/Internet Threat Analysis/Attacks and Suspicious Activity/	This data monitor shows the ports used in attack and suspicious activity events. By default the data monitor shows data from the last 2 hours.
Last 20 MITRE ATT&CK Attack Events	DataMonitor	/All Data Monitors/ArcSight Solutions/GDPR/GDPR Threat Analysis/Internet Threat Analysis/MITRE ATT&CK/	This data monitor displays the last 20 MITRE ATT&CK events.
Top 10 Attackers	DataMonitor	/All Data Monitors/ArcSight Solutions/GDPR/GDPR Threat Analysis/Internet Threat Analysis/MITRE ATT&CK/	This data monitor shows the top 10 MITRE ATT&CK Attackers.
Top 10 Targets	DataMonitor	/All Data Monitors/ArcSight Solutions/GDPR/GDPR Threat Analysis/Internet Threat Analysis/MITRE ATT&CK/	This data monitor shows the top 10 MITRE ATT&CK targets.
Last 20 MITRE ATT&CK Attack Events	DataMonitor	/All Data Monitors/ArcSight Solutions/GDPR/GDPR Threat Analysis/Internet Threat Analysis/MITRE ATT&CK/	This data monitor displays the last 20 MITRE ATT&CK events.
Top 10 Users	DataMonitor	/All Data Monitors/ArcSight Solutions/GDPR/GDPR Threat Analysis/Internet Threat Analysis/MITRE ATT&CK/	This data monitor shows the top 10 MITRE ATT&CK users.
Top 10 Attackers IPs	DataMonitor	/All Data Monitors/ArcSight Solutions/GDPR/GDPR Threat Analysis/Internet Threat Analysis/Recon Activity/	This data monitor shows the top 10 reconnaissance activity attackers.

Resource	Type	URI	Description
Top 10 Target IPs	DataMonitor	/All Data Monitors/ArcSight Solutions/GDPR/GDPR Threat Analysis/Internet Threat Analysis/Recon Activity/	This data monitor shows the top 10 reconnaissance activity targets.
Last 10 Recon Events	DataMonitor	/All Data Monitors/ArcSight Solutions/GDPR/GDPR Threat Analysis/Internet Threat Analysis/Recon Activity/	This data monitor displays the last 10 of reconnaissance events.
Recon Activity per 10 Minutes	DataMonitor	/All Data Monitors/ArcSight Solutions/GDPR/GDPR Threat Analysis/Internet Threat Analysis/Recon Activity/	Shows a moving average of reconnaissance activity. It displays data for the last 10 minutes and will generate a correlation event if the moving average is increased by 300%.
Compliance Risk Score Overview	DataMonitor	/All Data Monitors/ArcSight Solutions/GDPR/Overview/	This data monitor displays an icon indicating the compliance risk score for each regulation section. The compliance score is maintained in the Compliance Score active list, and is calculated based on the severity of the rules that were triggered in the solution package.
Rules Attackers and Targets	DataMonitor	/All Data Monitors/ArcSight Solutions/GDPR/Overview/	Event graph to show attacker-target pair relationship for the various rule firings from this regulation.
Top 10 Attackers in Rule Firings	DataMonitor	/All Data Monitors/ArcSight Solutions/GDPR/Overview/	This data monitor shows which attackers are most frequently involved in rule firings for this regulation. This may reveal a trend about certain attackers.
Top 10 Rules Fired	DataMonitor	/All Data Monitors/ArcSight Solutions/GDPR/Overview/	This data monitor shows which rules are most frequently fired for this regulation. This may reveal a trend about certain attacks.
Top 10 Targets in Rule Firings	DataMonitor	/All Data Monitors/ArcSight Solutions/GDPR/Overview/	This data monitor shows which targets are most frequently involved in rule firings for this regulation. This may reveal a trend about certain targets.
Attacks and Suspicious Activity	FieldSet	/All Field Sets/ArcSight Solutions/GDPR/	This field set contains essential fields required to investigate attacks and suspicious activity through active channels and data monitors.
Data Flow Events	FieldSet	/All Field Sets/ArcSight Solutions/GDPR/	This field set shows data flow event fields.
MITRE ATT&CK	FieldSet	/All Field Sets/ArcSight Solutions/GDPR/	This field sets selects fields related Mitre Att&ck.

Resource	Type	URI	Description
User Authentication	FieldSet	/All Field Sets/ArcSight Solutions/GDPR/	This field set selects fields related to authentication events.
Removal of Access Rights	Filter	/All Filters/ArcSight Solutions/GDPR/GDPR Access Activity/Access Activity/	Identifies events indicating user access right is removed.
Suspicious Logins	Filter	/All Filters/ArcSight Solutions/GDPR/GDPR Access Activity/Access Activity/	This filter identifies Frequent Unsuccessful logins by both administrative and non-administrative users.
Privileged Account Changes	Filter	/All Filters/ArcSight Solutions/GDPR/GDPR Access Activity/Access Activity/	Selects events where a change is attempted to a privileged account (as defined by the referenced active list).
Account Lockouts	Filter	/All Filters/ArcSight Solutions/GDPR/GDPR Access Activity/Access Activity/	This filter is used to identify account lockouts. By default it will recognize lockouts on Microsoft Windows and Unix systems.
Access Rights Changes	Filter	/All Filters/ArcSight Solutions/GDPR/GDPR Access Activity/Access Activity/	Selects events where a change was attempted for account access rights.
Frequent Unsuccessful Logins	Filter	/All Filters/ArcSight Solutions/GDPR/GDPR Access Activity/Access Activity/	This filter identifies Frequent Unsuccessful logins by both administrative and non-administrative users.
Building Access	Filter	/All Filters/ArcSight Solutions/GDPR/GDPR Access Activity/Physical Access Activity/	This filter selects all building access events.
Contractor Access After Hours	Filter	/All Filters/ArcSight Solutions/GDPR/GDPR Access Activity/Physical Access Activity/	Identifies contractors accessing buildings after hours.
Physical Access Events	Filter	/All Filters/ArcSight Solutions/GDPR/GDPR Access Activity/Physical Access Activity/	Selects all events sent to ArcSight ESM by physical security systems.
Successful After Hours Building Access	Filter	/All Filters/ArcSight Solutions/GDPR/GDPR Access Activity/Physical Access Activity/	Selects all events indicating successful occurrences of physical access after business hours. The actual time definition is defined in the After Hours filter.

Resource	Type	URI	Description
Successful Badge In	Filter	/All Filters/ArcSight Solutions/GDPR/GDPR Access Activity/Physical Access Activity/	Identifies a successful badge-in event.
Unsuccessful Badge In	Filter	/All Filters/ArcSight Solutions/GDPR/GDPR Access Activity/Physical Access Activity/	Identifies an unsuccessful badge-in event.
XSRF Vulnerability Detected	Filter	/All Filters/ArcSight Solutions/GDPR/GDPR Attack Surface Analysis/Attack Surface Identification/	Selects events indicating that an XSRF vulnerability was detected.
XSS Vulnerability Detected	Filter	/All Filters/ArcSight Solutions/GDPR/GDPR Attack Surface Analysis/Attack Surface Identification/	Selects events indicating that an XSS vulnerability was detected.
Security Patch Missing	Filter	/All Filters/ArcSight Solutions/GDPR/GDPR Attack Surface Analysis/Attack Surface Identification/	Selects events indicating that a security patch is missing.
SQL Injection Vulnerability Detected	Filter	/All Filters/ArcSight Solutions/GDPR/GDPR Attack Surface Analysis/Attack Surface Identification/	Selects events indicating that SQL injection vulnerability was detected.
SSL|TLS Vulnerability Detected	Filter	/All Filters/ArcSight Solutions/GDPR/GDPR Attack Surface Analysis/Attack Surface Identification/	Selects events indicating that an SSL/TLS vulnerability was detected.
Overflow Vulnerability Detected	Filter	/All Filters/ArcSight Solutions/GDPR/GDPR Attack Surface Analysis/Attack Surface Identification/	Selects events indicating that an overflow vulnerability was detected.
Information Disclosure Vulnerability Detected	Filter	/All Filters/ArcSight Solutions/GDPR/GDPR Attack Surface Analysis/Attack Surface Identification/	Selects events indicating that an information disclosure vulnerability was detected.

Resource	Type	URI	Description
Format String Vulnerability Detected	Filter	/All Filters/ArcSight Solutions/GDPR/GDPR Attack Surface Analysis/Attack Surface Identification/	Selects events indicating that a format string vulnerability was detected.
Password and Authentication Weaknesses Detected	Filter	/All Filters/ArcSight Solutions/GDPR/GDPR Attack Surface Analysis/Attack Surface Identification/	Selects events indicating that Password and Authentication Weaknesses was detected.
WordPress GDPR Plugins Vulnerabilities	Filter	/All Filters/ArcSight Solutions/GDPR/GDPR Attack Surface Analysis/Attack Surface Identification/	Selects events indicating that a WordPress GDPR Plugin vulnerability was detected.
Audit Log Cleared	Filter	/All Filters/ArcSight Solutions/GDPR/GDPR Attack Surface Analysis/Security Controls Risk Identification/	Selects all events where an audit log was cleared from a host. By default it will recognize events on Microsoft Windows and Symantec Host IDS systems, modify this filter to include events from other devices.
Failed Anti-Virus Updates	Filter	/All Filters/ArcSight Solutions/GDPR/GDPR Attack Surface Analysis/Security Controls Risk Identification/	Looks for events when an attempt to update a virus signature on a host failed.
Password Change Attempts	Filter	/All Filters/ArcSight Solutions/GDPR/GDPR Attack Surface Analysis/Security Controls Risk Identification/	Identifies password change attempts. By default, it only identifies these events on Microsoft Windows systems. Configure this filter to identify password change events from other systems as necessary.
Security Log is Full	Filter	/All Filters/ArcSight Solutions/GDPR/GDPR Attack Surface Analysis/Security Controls Risk Identification/	The security log is now full.
Successful Password Change	Filter	/All Filters/ArcSight Solutions/GDPR/GDPR Attack Surface Analysis/Security Controls Risk Identification/	Identifies successful password change events.

Resource	Type	URI	Description
Policy Violations	Filter	/All Filters/ArcSight Solutions/GDPR/GDPR Regulatory Exposure/Composite Regulatory Exposure/	Filter in events with violation of policy.
Microsoft SQL Server Vulnerability Detected	Filter	/All Filters/ArcSight Solutions/GDPR/GDPR Threat Analysis/Data Store Risk/	Selects events indicating that Microsoft SQL Server vulnerability was detected.
ORACLE Vulnerability Detected	Filter	/All Filters/ArcSight Solutions/GDPR/GDPR Threat Analysis/Data Store Risk/	Selects events indicating that ORACLE vulnerability was detected.
MySQL Vulnerability Detected	Filter	/All Filters/ArcSight Solutions/GDPR/GDPR Threat Analysis/Data Store Risk/	Selects events indicating that MySQL vulnerability was detected.
MongoDB Vulnerability Detected	Filter	/All Filters/ArcSight Solutions/GDPR/GDPR Threat Analysis/Data Store Risk/	Selects events indicating that MongoDB vulnerability was detected.
MariaDB Vulnerability Detected	Filter	/All Filters/ArcSight Solutions/GDPR/GDPR Threat Analysis/Data Store Risk/	Selects events indicating that MariaDB vulnerability was detected.
PostgreSQL Vulnerability Detected	Filter	/All Filters/ArcSight Solutions/GDPR/GDPR Threat Analysis/Data Store Risk/	Selects events indicating that PostgreSQL vulnerability was detected.
Elasticsearch Vulnerability Detected	Filter	/All Filters/ArcSight Solutions/GDPR/GDPR Threat Analysis/Data Store Risk/	Selects events indicating that Elasticsearch vulnerability was detected.
DB2 Vulnerability Detected	Filter	/All Filters/ArcSight Solutions/GDPR/GDPR Threat Analysis/Data Store Risk/	Selects events indicating that DB2 vulnerability was detected.
Cassandra Vulnerability Detected	Filter	/All Filters/ArcSight Solutions/GDPR/GDPR Threat Analysis/Data Store Risk/	Selects events indicating that Cassandra vulnerability was detected.

Resource	Type	URI	Description
Insecure Cryptographic Storage Detected	Filter	/All Filters/ArcSight Solutions/GDPR/GDPR Threat Analysis/Data Store Risk/	Selects events indicating that Insecure cryptographic storage has been detected.
Redis Vulnerability Detected	Filter	/All Filters/ArcSight Solutions/GDPR/GDPR Threat Analysis/Data Store Risk/	Selects events indicating that Redis vulnerability was detected.
Trojan Activity	Filter	/All Filters/ArcSight Solutions/GDPR/GDPR Threat Analysis/Internet Threat Analysis/	Selects events where trojan activity is detected.
Shell Code Execution Detected	Filter	/All Filters/ArcSight Solutions/GDPR/GDPR Threat Analysis/Internet Threat Analysis/	Selects events where shellCode execution is detected.
Worm Activity	Filter	/All Filters/ArcSight Solutions/GDPR/GDPR Threat Analysis/Internet Threat Analysis/	Selects events where worm activity is detected.
Virus Activity	Filter	/All Filters/ArcSight Solutions/GDPR/GDPR Threat Analysis/Internet Threat Analysis/	Identifies virus activities reported by either an Intrusion Detection System (IDS) or an anti-virus application.
Malware Activity	Filter	/All Filters/ArcSight Solutions/GDPR/GDPR Threat Analysis/Internet Threat Analysis/	Selects events where malicious code activity is detected.
Spyware Activity	Filter	/All Filters/ArcSight Solutions/GDPR/GDPR Threat Analysis/Internet Threat Analysis/	Identifies spyware activity reported by either an Intrusion Detection System (IDS) or an anti-virus application.
Email Attacks	Filter	/All Filters/ArcSight Solutions/GDPR/GDPR Threat Analysis/Internet Threat Analysis/	This filter detects events indicating an email attack (like phishing, spam) occurred.
Covert Channel	Filter	/All Filters/ArcSight Solutions/GDPR/GDPR Threat Analysis/Internet Threat Analysis/	This filter detects events indicating a covert channel is being used.

Resource	Type	URI	Description
Information Interception	Filter	/All Filters/ArcSight Solutions/GDPR/GDPR Threat Analysis/Internet Threat Analysis/	This filter detects events indicating an information interception is being used.
Clear Text Password Transmission	Filter	/All Filters/ArcSight Solutions/GDPR/GDPR Threat Analysis/Internet Threat Analysis/	This filter identifies a successful login or access to a login page through unencrypted ports, which indicates that a user password might be transferred in clear text over the network.
Anti-Virus Clean or Quarantine Attempt	Filter	/All Filters/ArcSight Solutions/GDPR/GDPR Threat Analysis/Internet Threat Analysis/	Looks for anti-virus events that indicate a quarantine or cleaning attempt of a detected malware instance.
Internal Recon Activity	Filter	/All Filters/ArcSight Solutions/GDPR/GDPR Threat Analysis/Intranet Threat Analysis/	This filter identifies events which indicate internal reconnaissance.
Windows Events with a Non-Machine User	Filter	/All Filters/ArcSight Solutions/GDPR/General Filters/	This filters identified Microsoft Windows events that have a non machine/system user either in the attacker or the target fields.
Target User Present	Filter	/All Filters/ArcSight Solutions/GDPR/General Filters/	This filter checks whether the Target User Name field is populated.
Target Host or Address Present	Filter	/All Filters/ArcSight Solutions/GDPR/General Filters/	This filter identifies events that have either the Target Host Name or Target Address event fields populated.
High Priority Events with Target Info	Filter	/All Filters/ArcSight Solutions/GDPR/General Filters/	This filter shows events in which the Priority field is 9 or 10 with target info.
High Priority Events with Attacker Info	Filter	/All Filters/ArcSight Solutions/GDPR/General Filters/	This filter shows events in which the Priority field is 9 or 10 with attacker info.
High Priority Events	Filter	/All Filters/ArcSight Solutions/GDPR/General Filters/	This filter shows events in which the Priority field is 9 or 10.
Attacker or Target User Present	Filter	/All Filters/ArcSight Solutions/GDPR/General Filters/	This filter identifies events that have either the Attacker User Name or Target User Name event fields populated.
Attacker User Present	Filter	/All Filters/ArcSight Solutions/GDPR/General Filters/	This filter identifies events that have the Attacker User Name event fields populated.

Resource	Type	URI	Description
Target Asset is EU	Filter	/All Filters/ArcSight Solutions/GDPR/General Filters/Assets/	This filter selects events targeting EU Countries.
Target Asset is Database	Filter	/All Filters/ArcSight Solutions/GDPR/General Filters/Assets/	This filter selects events targeting database hosts.
Internal Targets	Filter	/All Filters/ArcSight Solutions/GDPR/General Filters/Assets/	This filter looks for events targeting systems inside the organization network.
Internal Attackers	Filter	/All Filters/ArcSight Solutions/GDPR/General Filters/Assets/	This filter looks for events coming from systems inside the organization network.
Attacker Asset is PII	Filter	/All Filters/ArcSight Solutions/GDPR/General Filters/Assets/	This filter selects events originated from PII assets.
Attacker Asset is EU	Filter	/All Filters/ArcSight Solutions/GDPR/General Filters/Assets/	This filter selects events originated from EU Countries.
Target Asset is PII	Filter	/All Filters/ArcSight Solutions/GDPR/General Filters/Assets/	This filter selects events targeting PII hosts.
MITRE ATT&CK Activity with User Info	Filter	/All Filters/ArcSight Solutions/GDPR/General Filters/Attacks/	This filter identifies MITRE ATT&CK events with user info.
Threats	Filter	/All Filters/ArcSight Solutions/GDPR/General Filters/Attacks/	This filter identifies events that indicate compromise, reconnaissance, hostile, or suspicious activity and MITRE Attacks.
Recon Activity	Filter	/All Filters/ArcSight Solutions/GDPR/General Filters/Attacks/	This filter identifies events that indicate reconnaissance activity.
MITRE ATT&CK Activity with Target Info	Filter	/All Filters/ArcSight Solutions/GDPR/General Filters/Attacks/	This filter identifies MITRE ATT&CK events with target info.
Attacks with Port Info	Filter	/All Filters/ArcSight Solutions/GDPR/General Filters/Attacks/	This filter identifies events with port info which indicate compromise, reconnaissance, hostile, or suspicious activity.
MITRE ATT&CK Activity	Filter	/All Filters/ArcSight Solutions/GDPR/General Filters/Attacks/	This filter identifies MITRE ATT&CK events.

Resource	Type	URI	Description
Exploitation Activity	Filter	/All Filters/ArcSight Solutions/GDPR/General Filters/Attacks/	This filter identifies events which indicate exploitation activity.
DoS Attacks with Geo Information	Filter	/All Filters/ArcSight Solutions/GDPR/General Filters/Attacks/	This filter identifies denial of service attacks with geo information.
DoS Attacks	Filter	/All Filters/ArcSight Solutions/GDPR/General Filters/Attacks/	This filter identifies reported denial of service attacks.
Attacks with Target Info	Filter	/All Filters/ArcSight Solutions/GDPR/General Filters/Attacks/	This filter identifies events with target info which indicate compromise, reconnaissance, hostile, or suspicious activity.
Attacks with Geo Information	Filter	/All Filters/ArcSight Solutions/GDPR/General Filters/Attacks/	This filter selects attack events with populated Geo fields for both the attacker and target addresses.
Attacks with Attacker Info	Filter	/All Filters/ArcSight Solutions/GDPR/General Filters/Attacks/	This filter identifies events with attacker info which indicate compromise, reconnaissance, hostile, or suspicious activity.
Attacks and Suspicious Activity	Filter	/All Filters/ArcSight Solutions/GDPR/General Filters/Attacks/	This filter identifies events which indicate compromise, reconnaissance, hostile, or suspicious activity.
MITRE ATT&CK Activity with Attacker Info	Filter	/All Filters/ArcSight Solutions/GDPR/General Filters/Attacks/	This filter identifies MITRE ATT&CK events with attacker info.
Unsuccessful Logins with Attacker and Target Info	Filter	/All Filters/ArcSight Solutions/GDPR/General Filters/Authentication/	This filter identified failed logins by both administrative and non-administrative users with attacker and target info.
Unsuccessful Logins with Target Info	Filter	/All Filters/ArcSight Solutions/GDPR/General Filters/Authentication/	This filter identified failed logins by both administrative and non-administrative users with target info.
Unsuccessful Logins with Attacker and User Info	Filter	/All Filters/ArcSight Solutions/GDPR/General Filters/Authentication/	This filter identified failed logins by both administrative and non-administrative users with attacker and user info.
Unsuccessful Logins with Attacker Info	Filter	/All Filters/ArcSight Solutions/GDPR/General Filters/Authentication/	This filter identified failed logins by both administrative and non-administrative users with attacker info.

Resource	Type	URI	Description
Successful Logins with Target Info	Filter	/All Filters/ArcSight Solutions/GDPR/General Filters/Authentication/	This filter identifies successful logins by both administrative and non-administrative users with target info.
Successful Logins from non EU Countries with Target Info	Filter	/All Filters/ArcSight Solutions/GDPR/General Filters/Authentication/	This filter identifies successful logins by both administrative and non-administrative users from non EU countries with target info.
Successful Logins with Attacker Info	Filter	/All Filters/ArcSight Solutions/GDPR/General Filters/Authentication/	This filter identifies successful logins by both administrative and non-administrative users with attacker info.
Successful Logins from non EU Countries with User Info	Filter	/All Filters/ArcSight Solutions/GDPR/General Filters/Authentication/	This filter identifies successful logins by both administrative and non-administrative users from non EU countries with user info.
Successful Logins	Filter	/All Filters/ArcSight Solutions/GDPR/General Filters/Authentication/	This filter identifies successful logins by both administrative and non-administrative users.
Successful Logins from non EU Countries with Attacker Info	Filter	/All Filters/ArcSight Solutions/GDPR/General Filters/Authentication/	This filter identifies successful logins by both administrative and non-administrative users from non EU countries with attacker info.
Successful Logins from non EU Countries	Filter	/All Filters/ArcSight Solutions/GDPR/General Filters/Authentication/	This filter identifies successful logins by both administrative and non-administrative users from non EU countries.
Unsuccessful Logins	Filter	/All Filters/ArcSight Solutions/GDPR/General Filters/Authentication/	This filter identified failed logins by both administrative and non-administrative users.
Login Attempts	Filter	/All Filters/ArcSight Solutions/GDPR/General Filters/Authentication/	This filter selects any attempts at logging into systems. It excludes machine logins into Microsoft Windows systems.
Configuration Modifications	Filter	/All Filters/ArcSight Solutions/GDPR/General Filters/Configuration Changes/	Detects non-arcsight configuration modifications events.
Inbound Events	Filter	/All Filters/ArcSight Solutions/GDPR/General Filters/Data Flow/	This filter looks for events coming from outside the organization network targeting internal networks .
Inbound Events from non EU Countries	Filter	/All Filters/ArcSight Solutions/GDPR/General Filters/Data Flow/	This filter looks for events coming from non EU Countries targeting internal networks .

Resource	Type	URI	Description
Outbound Events	Filter	/All Filters/ArcSight Solutions/GDPR/General Filters/Data Flow/	This filter looks for events coming from inside the organization network targeting the public network.
Outbound Events to Non EU Countries	Filter	/All Filters/ArcSight Solutions/GDPR/General Filters/Data Flow/	This filter looks for events coming from inside the organization network targeting non EU countries.
Firewall Deny	Filter	/All Filters/ArcSight Solutions/GDPR/General Filters/Firewall/	This filter selects events where a firewall denied passage to traffic.
Personal Records Information Leak with User Info	Filter	/All Filters/ArcSight Solutions/GDPR/General Filters/Information Leakage/	This filter identifies information leaks with regard to personal information.
Organizational Records Information Leak	Filter	/All Filters/ArcSight Solutions/GDPR/General Filters/Information Leakage/	This filter identifies information leaks with regard to company information.
Encrypted Communication Information Leaks	Filter	/All Filters/ArcSight Solutions/GDPR/General Filters/Information Leakage/	This filter identifies information leaks with regard to encrypted communication on the network.
Personal Records Information Leak	Filter	/All Filters/ArcSight Solutions/GDPR/General Filters/Information Leakage/	This filter identifies information leaks with regard to personal information.
Insecure Services	Filter	/All Filters/ArcSight Solutions/GDPR/General Filters/Insecure Services/	Selects events based on inherently insecure services.
GDPR Rule Firing with Target Info	Filter	/All Filters/ArcSight Solutions/GDPR/General Filters/Overview/Risk Score Dashboard Overview/	This filter selects all rule firing events, where the rule is a part of the compliance content and has target info.
Compliance Score Updates	Filter	/All Filters/ArcSight Solutions/GDPR/General Filters/Overview/Risk Score Dashboard Overview/	This filter identifies events that are generated when values in the Compliance Score active list are changed.
GDPR Rule Firing with Attacker Info	Filter	/All Filters/ArcSight Solutions/GDPR/General Filters/Overview/Risk Score Dashboard Overview/	This filter selects all rule firing events, where the rule is a part of the compliance content and has attacker info.

Resource	Type	URI	Description
GDPR Rule Firing	Filter	/All Filters/ArcSight Solutions/GDPR/General Filters/Overview/Risk Score Dashboard Overview/	This filter selects all GDPR rules firing events.
GDPR Rule Firing with Attacker and Target Info	Filter	/All Filters/ArcSight Solutions/GDPR/General Filters/Overview/Risk Score Dashboard Overview/	This filter selects all rule firing events, where the rule is a part of the compliance content and has attacker and target info.
Vulnerability Scanner Events	Filter	/All Filters/ArcSight Solutions/GDPR/General Filters/Vulnerabilities/	This filter identifies scanner-generated events.
Limit Regulation	Filter	/All Filters/ArcSight Solutions/GDPR/My Filters/	The purpose of this filter is to ensure that the solution only processes events that are addressed by the regulation.
After Hours	Filter	/All Filters/ArcSight Solutions/GDPR/My Filters/	This filter defines the time period of 'after hours'. Change this filter to adjust the default settings.
	Query	/All Queries/ArcSight Solutions/GDPR/Overview/	Provides a listing of GDPR correlation events on the last 2 hours.
GDPR Rule Firing Events	QueryViewer	/All Query Viewers/ArcSight Solutions/GDPR/Overview/	Provides a listing of GDPR correlation events on the last hour.
Privileged Account Changes	Rule	/All Rules/ArcSight Solutions/GDPR/GDPR Access Activity/Access Activity/	Fires whenever an access/authorization change is attempted to be made to an administrative account.
User Logged in to different Targets on Short Period of Time	Rule	/All Rules/ArcSight Solutions/GDPR/GDPR Access Activity/Access Activity/	Fires when someone is using the same user name to login to different targets, This may indicate user name sharing.
Password Spray Attack	Rule	/All Rules/ArcSight Solutions/GDPR/GDPR Access Activity/Access Activity/	Detects password spray attack on windows systems.
User Logged in from Two Countries	Rule	/All Rules/ArcSight Solutions/GDPR/GDPR Access Activity/Access Activity/	This rule fires when someone is using the same user name to login from two different countries. This may indicate user name sharing.

Resource	Type	URI	Description
User Logged in from different IP Addresses	Rule	/All Rules/ArcSight Solutions/GDPR/GDPR Access Activity/Access Activity/	Fires when someone is using the same user name to login from different ip addresses. This may indicate user name sharing.
Suspicious Logins Activity Increased Exponentially in less than 10 Minutes	Rule	/All Rules/ArcSight Solutions/GDPR/GDPR Access Activity/Access Activity/	This rule looks for an exponential increase of suspicious login events. Before deploying this rule make sure the following data monitor Suspicious Logins per10 Minutes and the following rules : User Logged in from different IP Addresses User Logged in from Two Countries User Logged in to different Targets on Short Period of Time are enabled.
Frequent Unsuccessful Logins to Target Host	Rule	/All Rules/ArcSight Solutions/GDPR/GDPR Access Activity/Access Activity/	Fires when it notices a high frequency of unsuccessful logins on the same target host. Note : This rule works against every target application on GDPR environment, in case some applications produce false positive results you can exclude those targets on the conditions tab of the rule.
Removal of Access Rights	Rule	/All Rules/ArcSight Solutions/GDPR/GDPR Access Activity/Access Activity/	Triggers when events indicating removal of access rights happen.
Frequent Unsuccessful Logins from Attacker Host	Rule	/All Rules/ArcSight Solutions/GDPR/GDPR Access Activity/Access Activity/	Fires when it notices a continuous set of unsuccessful logins from the same attacker host.

Resource	Type	URI	Description
Frequent Unsuccessful Logins by User Name	Rule	/All Rules/ArcSight Solutions/GDPR/GDPR Access Activity/Access Activity/	Fires when it notices the same user is responsible for a continuous set of unsuccessful logins.
Frequent Unsuccessful Logins Activity Increased Exponentially in less than 10 Minutes	Rule	/All Rules/ArcSight Solutions/GDPR/GDPR Access Activity/Access Activity/	This rule looks for an exponential increase of frequent failed login events. Before deploying this rule make sure the following data monitor Frequent Failed Login per 10 Minutes and the following rules : Frequent Unsuccessful Logins by User Name Frequent Unsuccessful Logins from Attacker Host Frequent Unsuccessful Logins to Target Host are enabled.
Failed Building Access	Rule	/All Rules/ArcSight Solutions/GDPR/GDPR Access Activity/Access Activity/	Detects failed physical building access.
Failed Access by the Same User to Multiple Buildings	Rule	/All Rules/ArcSight Solutions/GDPR/GDPR Access Activity/Access Activity/	Detects failed physical access by the same user to multiple buildings on short period of time. Before enabling and deploying this rule, please make sure the following rule: "Failed Building Access" is enabled and deployed

Resource	Type	URI	Description
After Hours Building Access by Contractors	Rule	/All Rules/ArcSight Solutions/GDPR/GDPR Access Activity/Access Activity/	Detects building access events after business hours by contractors.
Account Lockout	Rule	/All Rules/ArcSight Solutions/GDPR/GDPR Access Activity/Access Activity/	This rule detects account lockouts.
Frequent Unsuccessful Logins from non EU Countries to PII Asset	Rule	/All Rules/ArcSight Solutions/GDPR/GDPR Access Activity/Access Activity/	This rule fires when it notices a continuous set of unsuccessful user logins from non EU countries to PII assets. Please use this rule when you didn't expect login from non EU countries to your PII Asset. Note : In order for this rule to be triggered the PII assets should be categorized with the "/All Assets Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/Electronic PII".
User Logged in from non EU Countries to PII Asset	Rule	/All Rules/ArcSight Solutions/GDPR/GDPR Access Activity/Access Activity/	This rule fires when there is a login from non EU countries to PII Assets. Please use this rule when you didn't expect login from non EU countries to your PII Asset. Note : In order for this rule to be triggered the PII assets should be categorized with the "/All Assets Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/Electronic PII".
XSS Vulnerabilities	Rule	/All Rules/ArcSight Solutions/GDPR/GDPR Attack Surface Analysis/Attack Surface Identification/	Triggers when XSS vulnerability is detected.
XSRF Vulnerabilities	Rule	/All Rules/ArcSight Solutions/GDPR/GDPR Attack Surface Analysis/Attack Surface Identification/	Triggers when XSRF vulnerability is detected.

Resource	Type	URI	Description
WordPress GDPR Plugins Vulnerabilities	Rule	/All Rules/ArcSight Solutions/GDPR/GDPR Attack Surface Analysis/Attack Surface Identification/	Triggers when a WorldPress GDPR Plugin vulnerability is detected.
Specific Vulnerability Detected - Template	Rule	/All Rules/ArcSight Solutions/GDPR/GDPR Attack Surface Analysis/Attack Surface Identification/	Triggers when a specific CVE Id vulnerability or vendor signature ID is detected. Before enabling and deploying this rule make sure that either : 1.CVE ID is defined using deviceCustomString2 = <CVE ID> on the Conditions tab. OR 2.Signature ID is defined using device Event Class Id =<Signature ID> on the conditions tab.
Security Patch Missing	Rule	/All Rules/ArcSight Solutions/GDPR/GDPR Attack Surface Analysis/Attack Surface Identification/	Triggers when a security patch missing vulnerability is detected.
SQL Injection Vulnerabilities	Rule	/All Rules/ArcSight Solutions/GDPR/GDPR Attack Surface Analysis/Attack Surface Identification/	Triggers when SQL Injection vulnerability is detected.
Password and Authentication Weaknesses	Rule	/All Rules/ArcSight Solutions/GDPR/GDPR Attack Surface Analysis/Attack Surface Identification/	Triggers when a password and authentication weaknesses are detected.
SSL|TLS Vulnerabilities	Rule	/All Rules/ArcSight Solutions/GDPR/GDPR Attack Surface Analysis/Attack Surface Identification/	Triggers when SSL|TLS vulnerability is detected.

Resource	Type	URI	Description
Non Fixed Security Patch Detected	Rule	/All Rules/ArcSight Solutions/GDPR/GDPR Attack Surface Analysis/Attack Surface Identification/	Triggers when a non fixed security patch detected. before enabling and deploying this rule please make sure the following rule: Security Patch Missing is enabled and deployed.
Invalid or Expired Certificate	Rule	/All Rules/ArcSight Solutions/GDPR/GDPR Attack Surface Analysis/Attack Surface Identification/	Detects invalid or expired Certificates.
Information Disclosure Vulnerability Detected on Multiple PII Assets	Rule	/All Rules/ArcSight Solutions/GDPR/GDPR Attack Surface Analysis/Attack Surface Identification/	This rule looks for information disclosure vulnerability detected on multiple PII Assets. Note : In order for this rule to be triggered the PII assets should be categorized with the "/All Assets Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/Electronic PII".
Information Disclosure Vulnerability Detected	Rule	/All Rules/ArcSight Solutions/GDPR/GDPR Attack Surface Analysis/Attack Surface Identification/	Triggers when information disclosure vulnerability is detected.
High Risk Vulnerability Detected	Rule	/All Rules/ArcSight Solutions/GDPR/GDPR Attack Surface Analysis/Attack Surface Identification/	Triggers when a high risk vulnerability is detected.
Format String Vulnerabilities	Rule	/All Rules/ArcSight Solutions/GDPR/GDPR Attack Surface Analysis/Attack Surface Identification/	Triggers when format string vulnerability is detected.
Overflow Vulnerabilities	Rule	/All Rules/ArcSight Solutions/GDPR/GDPR Attack Surface Analysis/Attack Surface Identification/	Triggers when overflow vulnerability is detected.

Resource	Type	URI	Description
Successful Password Change	Rule	/All Rules/ArcSight Solutions/GDPR/GDPR Attack Surface Analysis/Security Controls Risk Identification/	Detects when a user's password is changed.Will then take the user name off the list where it was kept to track whether or not the default password was changed.
Security Log is Full	Rule	/All Rules/ArcSight Solutions/GDPR/GDPR Attack Surface Analysis/Security Controls Risk Identification/	Triggers when security Log is full.
Potential Distributed DoS	Rule	/All Rules/ArcSight Solutions/GDPR/GDPR Attack Surface Analysis/Security Controls Risk Identification/	This rule looks for Potential Distributed DoS. Before deploying this rule make sure rule "DoS Detected" is enabled .
Password not Changed for Longer than Policy Standard	Rule	/All Rules/ArcSight Solutions/GDPR/GDPR Attack Surface Analysis/Security Controls Risk Identification/	Fires when an entry expires out of the referenced active list, signifying that the new (default) password was not changed within the prescribed time. Time limit is defined by the TTL in the active list.
Failed Anti-Virus Updates	Rule	/All Rules/ArcSight Solutions/GDPR/GDPR Attack Surface Analysis/Security Controls Risk Identification/	This rule detects failed anti-virus updates.
Critical Change on multiple PII Assets	Rule	/All Rules/ArcSight Solutions/GDPR/GDPR Attack Surface Analysis/Security Controls Risk Identification/	Triggers when there are PII environment configuration change detected and has Very-High agent severity. Note : In order for this rule to be triggered the PII assets should be categorized with the "/All Assets Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/Electronic PII".
Asset not Scanned for Longer than Policy Standard	Rule	/All Rules/ArcSight Solutions/GDPR/GDPR Attack Surface Analysis/Security Controls Risk Identification/	Fires when an entry expires out of the referenced active list, signifying that asset didnâ€™t scanned within the prescribed time. Time limit is defined by the TTL in the active list (default 60 days). Before deploying this rule make sure "Asset Scanned" rule is enabled and deployed.

Resource	Type	URI	Description
Asset Scanned	Rule	/All Rules/ArcSight Solutions/GDPR/GDPR Attack Surface Analysis/Security Controls Risk Identification/	This rule detects vulnerability scans against a specific asset and adds the asset to the active list.
DoS Detected	Rule	/All Rules/ArcSight Solutions/GDPR/GDPR Attack Surface Analysis/Security Controls Risk Identification/	This rule looks for DoS.
Audit Log Cleared	Rule	/All Rules/ArcSight Solutions/GDPR/GDPR Attack Surface Analysis/Security Controls Risk Identification/	Monitors for events on clearing of the audit log on Windows systems.
Security Software Stopped or Paused	Rule	/All Rules/ArcSight Solutions/GDPR/GDPR Attack Surface Analysis/Security Controls Risk Identification/	Triggers when a security software service has been disabled, refer to the condition tab of this rule for the list of such services.
Multiple Policy Violations Against PII Assets	Rule	/All Rules/ArcSight Solutions/GDPR/GDPR Regulatory Exposure/Composite Regulatory Exposure/	This rule looks for multiple policy violations against PII assets. Note : In order for this rule to be triggered : 1.the assets which match the condition should be categorized with the /All Assets Categories/Compliance Insight Package/Network Domains/Electronic PII/. 2.Before deploying this rule make sure rule "Policy Violations" is enabled .
Policy Violations	Rule	/All Rules/ArcSight Solutions/GDPR/GDPR Regulatory Exposure/Composite Regulatory Exposure/	This rule looks for policy violations.

Resource	Type	URI	Description
Internal Data Flow from non EU to PII Asset	Rule	/All Rules/ArcSight Solutions/GDPR/GDPR Regulatory Exposure/Composite Regulatory Exposure/	This rule looks for internal data flow non EU countries to PII asset. Note : In order for this rule to be triggered the PII assets should be categorized with the "/All Assets Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/Electronic PII" and your internal assets should be categorized with "/All Assets Categories/ArcSight Solutions/Compliance Insight Package/Address Spaces/Protected/".
Threats from non EU to PII Asset	Rule	/All Rules/ArcSight Solutions/GDPR/GDPR Regulatory Exposure/Composite Regulatory Exposure/	This rule looks for threats from non EU to PII asset. Note : In order for this rule to be triggered the PII assets should be categorized with the "/All Assets Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/Electronic PII".
High Risk Events Increased Exponentially in less than 10 Minutes	Rule	/All Rules/ArcSight Solutions/GDPR/GDPR Regulatory Exposure/Composite Regulatory Exposure/	This rule looks for an exponential increase of high risk events. Before deploying this rule make sure this data monitor "High Risk Events per 10 Minutes" is enabled.
External Data Flow from non EU to PII Asset	Rule	/All Rules/ArcSight Solutions/GDPR/GDPR Regulatory Exposure/Composite Regulatory Exposure/	This rule looks for external data flow non EU countries to PII asset. Note : In order for this rule to be triggered the PII assets should be categorized with the "/All Assets Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/Electronic PII" and your internal assets should be categorized with "/All Assets Categories/ArcSight Solutions/Compliance Insight Package/Address Spaces/Protected/".

Resource	Type	URI	Description
External Data Flow from PII Asset to non EU	Rule	/All Rules/ArcSight Solutions/GDPR/GDPR Regulatory Exposure/Composite Regulatory Exposure/	This rule looks for external data flow from PII asset to non EU countries. Note : In order for this rule to be triggered the PII assets should be categorized with the "/All Assets Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/Electronic PII" and your internal assets should be categorized with "/All Assets Categories/ArcSight Solutions/Compliance Insight Package/Address Spaces/Protected/".
Internal Data Flow from PII Asset to non EU	Rule	/All Rules/ArcSight Solutions/GDPR/GDPR Regulatory Exposure/Composite Regulatory Exposure/	This rule looks for internal data flow from PII asset to non EU countries. Note : In order for this rule to be triggered the PII assets should be categorized with the "/All Assets Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/Electronic PII" and your internal assets should be categorized with "/All Assets Categories/ArcSight Solutions/Compliance Insight Package/Address Spaces/Protected/".
Redis Vulnerabilities	Rule	/All Rules/ArcSight Solutions/GDPR/GDPR Threat Analysis/Data Store Risk/	Triggers when Redis vulnerability is detected.
PostgreSQL Vulnerabilities	Rule	/All Rules/ArcSight Solutions/GDPR/GDPR Threat Analysis/Data Store Risk/	Triggers when PostgreSQL vulnerability is detected.
ORACLE Vulnerabilities	Rule	/All Rules/ArcSight Solutions/GDPR/GDPR Threat Analysis/Data Store Risk/	Triggers when ORACLE vulnerability is detected.
MongoDB Vulnerabilities	Rule	/All Rules/ArcSight Solutions/GDPR/GDPR Threat Analysis/Data Store Risk/	Triggers when MongoDB vulnerability is detected.
Microsoft SQL Server Vulnerabilities	Rule	/All Rules/ArcSight Solutions/GDPR/GDPR Threat Analysis/Data Store Risk/	Triggers when Microsoft SQL Server vulnerability is detected.

Resource	Type	URI	Description
MariaDB Vulnerabilities	Rule	/All Rules/ArcSight Solutions/GDPR/GDPR Threat Analysis/Data Store Risk/	Triggers when MariaDB vulnerability is detected.
MySQL Vulnerabilities	Rule	/All Rules/ArcSight Solutions/GDPR/GDPR Threat Analysis/Data Store Risk/	Triggers when MySQL vulnerability is detected.
Exploit Executed on Database Asset	Rule	/All Rules/ArcSight Solutions/GDPR/GDPR Threat Analysis/Data Store Risk/	This rule detects exploit executed against database assets. Note: In order for this rule to be triggered the database assets should be categorized with this category "/All Asset Categories/Site Asset Categories/Business Impact Analysis/Business Role/Service/Database".
Elasticsearch Vulnerabilities	Rule	/All Rules/ArcSight Solutions/GDPR/GDPR Threat Analysis/Data Store Risk/	Triggers when Elasticsearch vulnerability is detected.
DB2 Vulnerabilities	Rule	/All Rules/ArcSight Solutions/GDPR/GDPR Threat Analysis/Data Store Risk/	Triggers when DB2 vulnerability is detected.
Critical Database Change Detected	Rule	/All Rules/ArcSight Solutions/GDPR/GDPR Threat Analysis/Data Store Risk/	Triggers when a configuration change is detected on a database asset and has Very-High agent severity. Note: In order for this rule to be triggered the database assets should be categorized with this category "/All Asset Categories/Site Asset Categories/Business Impact Analysis/Business Role/Service/Database".
Cassandra Vulnerabilities	Rule	/All Rules/ArcSight Solutions/GDPR/GDPR Threat Analysis/Data Store Risk/	Triggers when Cassandra vulnerability is detected.
CRM or ERP Vulnerabilities	Rule	/All Rules/ArcSight Solutions/GDPR/GDPR Threat Analysis/Data Store Risk/	Triggers when CRM or ERP vulnerability is detected.

Resource	Type	URI	Description
Insecure Cryptographic Storage Detected	Rule	/All Rules/ArcSight Solutions/GDPR/GDPR Threat Analysis/Data Store Risk/	Triggers when insecure cryptographic storage detected.
Possible DNS Based Zombie	Rule	/All Rules/ArcSight Solutions/GDPR/GDPR Threat Analysis/Internet Threat Analysis/	This rule looks for command and control DNS zombies in the organization. Before enabling and deploying this rule, please make sure the following rule: "Possible Botnet Activity" is enabled and deployed and the following active list: "DMZ Assets" include the DNS relevant assets.
Possible Directory Traversal	Rule	/All Rules/ArcSight Solutions/GDPR/GDPR Threat Analysis/Internet Threat Analysis/	This rule looks for events indicating a directory traversal attack is being used.
Possible Email Attack	Rule	/All Rules/ArcSight Solutions/GDPR/GDPR Threat Analysis/Internet Threat Analysis/	This rule looks for attacks where email activity involved.
Possible HTTP Based Zombie	Rule	/All Rules/ArcSight Solutions/GDPR/GDPR Threat Analysis/Internet Threat Analysis/	This rule looks for command and control HTTP based zombies on the organization. Before enabling and deploying this rule, please make sure the following rule: "Possible Botnet Activity" is enabled and deployed and the following active list: "DMZ Assets" include the web relevant assets.
Possible Information Interception	Rule	/All Rules/ArcSight Solutions/GDPR/GDPR Threat Analysis/Internet Threat Analysis/	This rule looks for attacks where information could be redirected and collected by an unintended party.
Possible Spear Phishing Attack	Rule	/All Rules/ArcSight Solutions/GDPR/GDPR Threat Analysis/Internet Threat Analysis/	This rule identifies potential spear phishing attack, before deploying this rule please make sure to add high profile email addresses to the â€œImportant Emailsâ€ active list.

Resource	Type	URI	Description
Possible SMTP Based Zombie	Rule	/All Rules/ArcSight Solutions/GDPR/GDPR Threat Analysis/Internet Threat Analysis/	This rule looks for command and control SMTP based zombies in the organization. Before enabling and deploying this rule, please make sure the following rule: "Possible Botnet Activity" is enabled and deployed and the following active list: "DMZ Assets" include the SMTP relevant assets.
Potential Worm Propagated Internally	Rule	/All Rules/ArcSight Solutions/GDPR/GDPR Threat Analysis/Internet Threat Analysis/	Triggers when a worm propagated internally. Before deploying this rule please make sure the following rule : Worm Detected is enabled and deployed
Shellcode Execution Detected	Rule	/All Rules/ArcSight Solutions/GDPR/GDPR Threat Analysis/Internet Threat Analysis/	This rule detects shellcode execution.
Possible Covert Channel	Rule	/All Rules/ArcSight Solutions/GDPR/GDPR Threat Analysis/Internet Threat Analysis/	This rule looks for events indicating a covert channel is being used.
Worm Detected	Rule	/All Rules/ArcSight Solutions/GDPR/GDPR Threat Analysis/Internet Threat Analysis/	Triggers when a worm is reported by either an Intrusion Detection System (IDS) or an anti-virus application.
Possible Botnet Activity	Rule	/All Rules/ArcSight Solutions/GDPR/GDPR Threat Analysis/Internet Threat Analysis/	This rule looks for command and control zombies in the organization. Before enabling and deploying this rule, please make sure the following active list: "DMZ Assets" includes the relevant assets.

Resource	Type	URI	Description
Exploit Executed Against PII Asset	Rule	/All Rules/ArcSight Solutions/GDPR/GDPR Threat Analysis/Internet Threat Analysis/	This rule detects exploit executed against PII assets. Note : In order for this rule to be triggered the PII assets should be categorized with the /All Assets Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/Electronic PII.
Personal Information Leak	Rule	/All Rules/ArcSight Solutions/GDPR/GDPR Threat Analysis/Internet Threat Analysis/	This rule looks for any personal information being sent out of the corporate network.
Organizational Data Information Leak	Rule	/All Rules/ArcSight Solutions/GDPR/GDPR Threat Analysis/Internet Threat Analysis/	This rule looks for any organizational information being sent out of the corporate network.
Malware Detected on PII Asset	Rule	/All Rules/ArcSight Solutions/GDPR/GDPR Threat Analysis/Internet Threat Analysis/	Triggers when malware detected on PII asset. Note : In order for this rule to be triggered the PII assets should be categorized with the /All Assets Categories/Compliance Insight Package/Network Domains/Electronic PII.
MITRE ATT&CK Techniques Detected on Multiple PII Asset	Rule	/All Rules/ArcSight Solutions/GDPR/GDPR Threat Analysis/Internet Threat Analysis/	This rule looks for mitre techniques detected on multiple PII Assets on short period of time. Note : In order for this rule to be triggered the PII assets should be categorized with the /All Assets Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/Electronic PII.
Exploit Executed Against WordPress GDPR Plugins	Rule	/All Rules/ArcSight Solutions/GDPR/GDPR Threat Analysis/Internet Threat Analysis/	This rule detects exploit executed against WordPress GDPR Plugins.
Excessive Blocked Firewall Traffic from the same Source	Rule	/All Rules/ArcSight Solutions/GDPR/GDPR Threat Analysis/Internet Threat Analysis/	This rule looks for possible excessive blocked firewall traffic from the same source.
Encrypted Communication Information Leaks	Rule	/All Rules/ArcSight Solutions/GDPR/GDPR Threat Analysis/Internet Threat Analysis/	This rule looks for any encrypted communication Information Leaks on the network.

Resource	Type	URI	Description
Clear Text Password Transmission	Rule	/All Rules/ArcSight Solutions/GDPR/GDPR Threat Analysis/Internet Threat Analysis/	This rule looks for events indicating a clear text password transmission.
Attacks Increased Exponentially in less than 10 Minutes	Rule	/All Rules/ArcSight Solutions/GDPR/GDPR Threat Analysis/Internet Threat Analysis/	This rule looks for an exponential increase of attack and suspicious activity events. Before deploying this rule make sure this data monitor "Attacks and Suspicious Activity per 10 Minutes" is enabled .
Personal Information Leak Increased Exponentially in less than 10 Minutes	Rule	/All Rules/ArcSight Solutions/GDPR/GDPR Threat Analysis/Internet Threat Analysis/	This rule looks for an exponential increase of personal information leaks events. Before deploying this rule make sure this data monitor "Personal Information Leakage per 10 Minutes" is enabled .
Multiple MITRE ATT&CK Techniques Detected on PII Asset	Rule	/All Rules/ArcSight Solutions/GDPR/GDPR Threat Analysis/Internet Threat Analysis/	This rule looks for multiple mitre techniques detected on PII Asset on short period of time. Note : In order for this rule to be triggered the PII assets should be categorized with the /All Assets Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/Electronic PII.
Internal Insecure Service Provider Detected	Rule	/All Rules/ArcSight Solutions/GDPR/GDPR Threat Analysis/Intranet Threat Analysis/	Detects when insecure protocols, such as Telnet or RSH, are used inside the network when triggered. Note : In order for this rule to be triggered the internal assets should be categorized with the "/All Assets Categories/ArcSight Solutions/Compliance Insight Package/Address Spaces/Protected/".

Resource	Type	URI	Description
Internal Recon Detected	Rule	/All Rules/ArcSight Solutions/GDPR/GDPR Threat Analysis/Intranet Threat Analysis/	This rule looks for internal reconnaissance activity. Note : In order for this rule to be triggered the internal assets should be categorized with the "/All Assets Categories/ArcSight Solutions/Compliance Insight Package/Address Spaces/Protected/".
Compliance Score Update	Rule	/All Rules/ArcSight Solutions/GDPR/Overview/	This rule is triggered by other GDPR rules and updates the Compliance Risk Score active list.
Manual Status Change	Rule	/All Rules/ArcSight Solutions/GDPR/Overview/	This rule is triggered when a section's status on the Compliance Risk Score dashboard is changed manually.

Appendix B: GDPR Categories

The following table shows all the categories used and the resources which use those categorizations.

Resource	Type	URI	Category URI
Frequent Unsuccessful Logins from non EU Countries to PII Asset	Rule	/All Rules/ArcSight Solutions/GDPR/GDPR Access Activity/Access Activity/	/All Assets Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/Electronic PII
User Logged in from non EU Countries to PII Asset	Rule	/All Rules/ArcSight Solutions/GDPR/GDPR Access Activity/Access Activity/	/All Assets Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/Electronic PII
Information Disclosure Vulnerability Detected on Multiple PII Assets	Rule	/All Rules/ArcSight Solutions/GDPR/GDPR Attack Surface Analysis/Attack Surface Identification	/All Assets Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/Electronic PII
Critical Change on multiple PII Assets	Rule	/All Rules/ArcSight Solutions/GDPR/GDPR Attack Surface Analysis/Security Controls Risk Identification	/All Assets Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/Electronic PII
External Data Flow from non EU to PII Asset	Rule	/All Rules/ArcSight Solutions/GDPR/GDPR Regulatory Exposure/Composite Regulatory Exposure	/All Assets Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/Electronic PII /All Assets Categories/AcSight Solutions/Compliance Insight Package/Address Spaces/Protected
External Data Flow from PII Asset to non EU	Rule	/All Rules/ArcSight Solutions/GDPR/GDPR Regulatory Exposure/Composite Regulatory Exposure	/All Assets Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/Electronic PII /All Assets Categories/AcSight Solutions/Compliance Insight Package/Address Spaces/Protected
Internal Data Flow from non EU to PII Asset	Rule	/All Rules/ArcSight Solutions/GDPR/GDPR Regulatory Exposure/Composite Regulatory Exposure	/All Assets Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/Electronic PII /All Assets Categories/AcSight Solutions/Compliance Insight Package/Address Spaces/Protected

Resource	Type	URI	Category URI
Internal Data Flow from PII Asset to non EU	Rule	/All Rules/ArcSight Solutions/GDPR/GDPR Regulatory Exposure/Composite Regulatory Exposure	/All Assets Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/Electronic PII /All Assets Categories/AcSight Solutions/Compliance Insight Package/Address Spaces/Protected
Multiple Policy Violations Against PII Assets	Rule	/All Rules/ArcSight Solutions/GDPR/GDPR Regulatory Exposure/Composite Regulatory Exposure	/All Assets Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/Electronic PII
Threats from non EU to PII Asset	Rule	/All Rules/ArcSight Solutions/GDPR/GDPR Regulatory Exposure/Composite Regulatory Exposure	/All Assets Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/Electronic PII
Critical Database Change Detected	Rule	/All Rules/ArcSight Solutions/GDPR/GDPR Threat Analysis/Data Store Risk	/All Asset Categories/Site Asset Categories/Business Impact Analysis/Business Role/Service/Database
Exploit Executed on Database Asset	Rule	/All Rules/ArcSight Solutions/GDPR/GDPR Threat Analysis/Data Store Risk	/All Asset Categories/Site Asset Categories/Business Impact Analysis/Business Role/Service/Database
MITRE ATT&CK Techniques Detected on Multiple PII Asset	Rule	/All Rules/ArcSight Solutions/GDPR/GDPR Threat Analysis/Internet Threat Analysis	/All Assets Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/Electronic PII
Multiple MITRE ATT&CK Techniques Detected on PII Asset	Rule	/All Rules/ArcSight Solutions/GDPR/GDPR Threat Analysis/Internet Threat Analysis	/All Assets Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/Electronic PII
Exploit Executed Against PII Asset	Rule	/All Rules/ArcSight Solutions/GDPR/GDPR Threat Analysis/Internet Threat Analysis	/All Assets Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/Electronic PII
Malware Detected on PII Asset	Rule	/All Rules/ArcSight Solutions/GDPR/GDPR Threat Analysis/Internet Threat Analysis	/All Assets Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/Electronic PII
Internal Insecure Service Provider Detected	Rule	/All Rules/ArcSight Solutions/GDPR/GDPR Threat Analysis/Intranet Threat Analysis	/All Assets Categories/ArcSight Solutions/Compliance Insight Package/Address Spaces/Protected
Internal Recon Detected	Rule	/All Rules/ArcSight Solutions/GDPR/GDPR Threat Analysis/Intranet Threat Analysis	/All Assets Categories/ArcSight Solutions/Compliance Insight Package/Address Spaces/Protected

Send Documentation Feedback

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

Feedback on Solutions Guide (ESM CIP for GDPR 1.0)

Just add your feedback to the email and click send.

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

We appreciate your feedback!