Micro Focus ArcSight Recon

User's Guide to ArcSight Recon 1.4.1

April 2022

Chapter 2: **Welcome to ArcSight Recon**

Recon provides a modern log search and hunt solution powered by a high-performance column-oriented, clustered database. The **Search** feature helps you investigate security issues by viewing search results and identifying outlier events. The **Reports Portal**, which includes OWASP content, enables you to hunt for undetected threats as well as create charts and dashboard to visualize filtered data with tables, charts, and gauges. With the **Outlier Analytics** feature you can identify anomalous behavior by comparing incoming event values to typical values for your environment.

Recon deploys within the **ArcSight Platform**, which provides common services such as the Dashboard, the Reports Portal, and user management.

- Search for alerts and events
- Analyze anomalous data with outlier analytics
- Check the integrity of your data
- Evaluate and manage the quality of your data
- Organize data into storage groups
- Comply with legal and governmental regulations
- Manage your user preferences

About This Book

Friday, May 13, 2022

This *User's Guide* provides concepts, use cases, and contextual help for ArcSight Recon.

- Search for alerts and events
- Analyze anomalous data with outlier analytics
- Check the integrity of your data
- Evaluate and manage the quality of your data
- Organize data into storage groups
- Comply with legal and governmental regulations
- Manage your user preferences

Intended Audience

This book provides information for individuals who investigate events and hunt for undetected threats. These individuals have experience in security operation centers or performing duties of a security analyst or operator.

Additional Documentation

The ArcSight Recon 1.4.1 documentation library includes the following resources:

- *Release Notes for ArcSight Platform*, which provides an overview of the products deployed in the containerized environment and their latest features or updates
- *Release Notes for ArcSight Recon*, which provides information about updates or new features available in the current release
- *Administrator's Guide to ArcSight Platform*, which provides information about deploying, configuring, and maintaining the products that you deploy in the containerized environment
- *Technical Requirements for ArcSight Platform*, which provides information about the hardware and software requirements for installing Recon as well as the other containerized capabilities

For the most recent version of this guide and other ArcSight documentation resources, visit the documentation for ArcSight Recon and for the ArcSight Platform.

Contact Information

We want to hear your comments and suggestions about this book and the other documentation included with this product. You can use the comment on this topic link at the bottom of each page of the online documentation, or send an email to Documentation-Feedback@microfocus.com.

For specific product issues, contact Micro Focus Customer Care at https://www.microfocus.com/support-and-services/.

Legal Notice

The only warranties for Micro Focus products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Micro Focus shall not be liable for technical or editorial errors or omissions contained herein.

No portion of this product's documentation may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying, recording, or information storage and retrieval systems, for any purpose other than the purchaser's internal use, without the express written permission of Micro Focus.

Notwithstanding anything to the contrary in your license agreement for Micro Focus ArcSight software, you may reverse engineer and modify certain open source components of the software in accordance with the license terms for those particular components. See below for the applicable terms.

U.S. Governmental Rights. For purposes of your license to Micro Focus ArcSight software, "commercial computer software" is defined at FAR 2.101. If acquired by or on behalf of a civilian agency, the U.S. Government acquires this commercial computer software and/or commercial computer software documentation and other technical data subject to the terms of the Agreement as specified in 48 C.F.R. 12.212 (Computer Software) and 12.211 (Technical Data) of the Federal Acquisition Regulation ("FAR") and its successors. If acquired by or on behalf of any agency within the Department of Defense ("DOD"), the U.S. Government acquires this commercial computer software and/or commercial computer software documentation subject to the terms of the Agreement as specified in 48 C.F.R. 227.7202-3 of the DOD FAR Supplement ("DFARS") and its successors. This U.S. Government Rights Section 18.11 is in lieu of, and supersedes, any other FAR, DFARS, or other clause or provision that addresses government rights in computer software or technical data.

For additional information, such as certification-related notices and trademarks, see https://www.microfocus.com/en-us/about/legal.

I Investigating Events

The Search feature enables you to look for and investigate events that meet specified criteria so you can detect anomalies that point to security threats. You can view the results in tabular and timeline formats. Each search consists of specifying query input, search result fields, and the time period for which you want to search events.

Queries are case sensitive. The query input determines the search type (full text, natural language, or contextual). As you specify the criteria for a search query, Search suggests items

and operators based on a schema data dictionary. You can also choose from predefined search queries.

Searching for Events

Search is contextual and has an auto-suggest capability to help you specify search criteria and improve productivity. You can retrieve events from an index; search for specific conditions within a rolling time window; create aggregate charts; and identify patterns in your data.

Understand the Search Feature

Recon ingests log data from ArcSight Logger and SmartConnectors routed through Transformation Hub and events from ArcSight Enterprise Security Manager. Each entry in a log is referred to as an **event**. Recon accepts events from Transformation Hub and organizes them to maximize search and storage efficiency.

The **Search** feature enables you to search events by entering a search command, a time window over which to search, and the fields from the Unified Event Schema. Search displays results in an Events Timeline chart, which a histogram shows the number of events returned over event occurrence time. The Events table below the Timeline shows events returned by search. When you select an event, Search displays the Event Details panel.

Search uses a database that serves as the main data store, as well as a cache. The search engine is a scalable server-side application that executes and caches large search queries in the database. In the backend, Recon saves your searches, user preferences, and proxy search requests to the search engine using a REST API. The database stores three timestamps for each event to provide more clarity in your search results. When creating a search, you specify the timestamp to use for retrieving events.

For the query's time range, you can choose a fixed start and end date, where you cannot refresh data, or a predefined date range. For example, for the last 30 minutes predefined search, you receive updates upon re-executing the search based on the most recent 30 minutes. Alternatively, you could specify dynamic dates, such as Midnight on the first day of the current month.

After initiating a search, you can pause, restart, and cancel the process as needed. A progress bar shows you the percent of retrieved data.

Initiate a Search from Enterprise Security Manager

From Enterprise Security Manager (ESM), you can initiate a search in the ArcSight Platform for a maximum of five fields, based on the available columns on the active channel. Within ArcSight Platform, you can filter ESM data for more specific results. ESM generates a URL, opens a browser, and creates the new search in Recon.

To perform this action, you must enable Recon in ESM. For more information, see the *ESM Installation Guide*.

Search Event Data from Logger

Logger data (including live and archive data) can be viewed and consumed using the same parameters as in regular searches. From the Search page, hunt for ArcSight Logger events by selecting the Logger drop down.

Before searching Logger events, the data must be imported to the ArcSight Database. The import process might require several imports from several Loggers. Otherwise, the dropdown will not be displayed in the Search page.

If Recon and Logger are set to the same timezone, there should be no discrepancy when searching the Logger data.

1. Select Search.
2. From the drop-down list next to the Search button, select Logger.
3. Add the required query details.
   You must use the search operators supported in ArcSight Platform.
4. Click Search.

Understand the Search Progress Indicators

As the **Search** feature retrieves data, it displays a **progress bar** to show its status, including the percent of data received. Rather than attempting to read all data at once, Search gathers data in chunks of time. The progress bar shows the time range from which the results are currently being retrieved.

You can **pause the search** and restart as needed.

NOTE: When performing a search with two or more identical queries the number of events returned for the second search will correspond to the next chunk of data. If you pause then resume the search, the first search will be moved to the next chunk as well, maintaining the same number of events retrieved. The identical queries can contain either one of the built-in queries or a custom query.

Configure Preferred Settings for Searches

Select [your_ID] > My Profile > Preferences.

You can specify the default settings that you want to apply for new searches. For example, you might want all of your searches to return results from the last 24 hours. Or, if you regularly use the same fieldset for a Search, you can specify that fieldset as your preferred default. You can always override your preferences as needed when you create a search. When you modify your Search preferences, the changes apply to new searches. Existing searches are not affected unless you re-run the search.

If you change your search preferences and you also have Scheduled Searches open in a separate browser tab, you must refresh the Scheduled Searches tab to ensure that the content in the tab reflects your changes.

Default Fieldset

Specifies the fieldset you regularly use for a search. The default value is *Base Event Fields*.

Default View

Specifies if the Events Table displays results in the Grid View or Raw View. The default value is *Grid View*.

Time Zone

Instructs Search to adjust the timestamp for events to the chosen time zone.

Date/Time Format

Specifies the format of dates and times you want Search to use. The default is MM/DD/YY.

Default Time Setting

Specifies the time range you want Search to find events. The default is *Last 30 minutes*.

Base Searches On

Specifies the timestamp Search associates with the event you want to find. The default value is Normalized Event Time.

Search Expires In

Specifies how often you want searches to expire, and thus for the sysem to remove them. Alternatively, you can choose to never remove a search.

Also, the expiration date resets whenever you access the search. Resetting the date includes resuming or re-running the search, as well as saving the search. The default value is 7 days.

Maximum Search Results

Specifies the maximum number of events Search returns. Search considers a search complete when the results reach the maximum limit. The default value is 10,000,000.

Highlight Query Syntax

Specifies whether Search uses color to differentiate the syntax terms from the operators and functions within the query. The default value is set as Yes.

Understanding the Search Parameters

To search for events or alerts, you specify the query input, the search result fields, and the time period. The query input determines the search type (full text, natural language, or contextual). As you specify the criteria for a search query, Search suggests search items and operators based on a schema data dictionary. You can also choose from predefined queries and specify default settings.

In the search query, you can enter the alias, or abbreviated term, for a field name rather than entering the full name. You can also use the **presentable field names**, such as Agent Address. Search suggests presentable names.

Understand the Types of Search Queries

Search supports the following types of search queries:

- "FULL TEXT SEARCH" on the next page
- "FIELD-BASED SEARCH" on the next page

- "HASHTAG (predefined searches)" below

FULL TEXT SEARCH

Searches across all columns using a 'contains' operation to determine if the value is found.

Syntax	Example
<value>	ssh

FIELD-BASED SEARCH

Searches based on the field and operator designation to determine if the value is found in the specified field.

Your search can reference fields with the Unified Schema to either retrieve the field in results, apply a filter criteria or create a user defined expression. The **Unified Schema** defines a consistent event model that can be used across all of ArcSight family of products.

Syntax	Example
<key> <operator> <value>	`sourceAddress = 10.0.111.5`

HASHTAG (predefined searches)

The Search feature includes several predefined queries out-of-the-box. In the query field, enter a hashtag, and then select the criteria to use. In addition to these predefined searches, you can use the session searches and save searches in the input field using a hashtag prefix.

This predefined query...	Uses this search criteria..
#Configuration Changes	categoryBehavior = /Modify/Configuration AND categoryOutcome = /Success
#DGA Events	deviceCustomNumber1 >= 1 AND deviceCustomNumber1Label contains DNS
#DNS Events	deviceEventCategory = PACKET
#DoS Events	#Category Technique =/DoS
#ESM Correlation Events	Type=Correlation
#Failed Logins	Category Behavior = /Authentication/Verify AND categoryOutcome != /Success
#Failed Logins For User $Username	Category Behavior = /Authentication/Verify AND categoryOutcome != /Success for user <username>
#Firewall Events	categoryDeviceGroup = /Firewall
#Firewall Drop	categoryDeviceGroup = /Firewall AND categoryObject starts with /Host/Application/Service AND (categoryBehavior starts with /Access OR categoryBehavior = /Communicate/Query) AND categoryOutcome = /Failure

#Firewall Drop For $Ip	categoryDeviceGroup = /Firewall AND categoryObject starts with /Host/Application/Service AND (categoryBehavior starts with /Access OR categoryBehavior = /Communicate/Query) AND categoryOutcome = /Failure for <IP_address>
#Malicious Code Activity	categoryObject STARTS WITH /Vector, /Host/Infection, /Host/Application/Malware OR categoryObject = /Host/Application/DoS Client, /Host/Application/Backdoor OR categoryTechnique STARTS WITH /Code
#MITRE ATT&CK Events	Device Custom String1 Label ='MITRE ID'
#Proxy Events	Category Technique=/Proxy
#SSH Authentication	categoryBehavior = /Authentication/Verify AND destinationUserName != Null and contains ssh
#VPN Connections	categoryDeviceGroup = /VPN AND Category Behavior = /Authentication/Verify AND categoryOutcome = /Success AND destinationUserName != Null
#Vulnerabilities Events	Category Technique= /scanner/device/vulnerability
#Windows Account Creation	deviceVendor = Microsoft AND deviceEventClassId = Microsoft-Windows-Security-Auditing:4720, Security:624
#Windows New Service Created	(deviceEventClassId='Microsoft-Windows-Security-Auditing:4697' or deviceEventClassId=' Service Control Manager:7045') and deviceProduct='Microsoft Windows'

Use GlobalEventID in a Query

To help you identify an event that might be seen by multiple ArcSight components, the connectors assign the event a unique 64-bit ID. To include a GEID in your search query, enter globalEventID. You can view the GEID of the event in the Event Details.

Syntax	Example
<geid> <value>	`global event id= 2864991913017849867`

For events to have a GEID, use ArcSight Management Center to configure connectors to include the ID. For more information, see the *Administrator's Guide to ArcSight Platform* or the guide for the connector.

Specify a Group of Fields

Search enables you to quickly select fields that have common groupings. In the query, you can specify a **group alias** that displays all fields or columns associated with the group. The following table provides some common group aliases.

Group Alias	Includes a list of these fields or columns...
category	All category fields
custom float	All custom float fields
domain	All domain fields
hostname	All hostname columns
id	All ID columns
ip	All IP address columns
ip6	All IPv6 address columns
label	All label columns
mac	All MAC address columns
path	All path columns
port	All port columns
timestamp or time	All time columns (device receipt time, agent receipt time)
uri	All URI columns
url	All URL columns
username or user	All user columns

Specify an Alias for a Field

In the search query, you can enter the alias, or abbreviated term, for a field name rather than entering the full name. For the fields shown in the following table, you can also use the **presentable field names**, such as Agent Address. Search suggests presentable names.

Field	Aliases
agentAddress	agt agent ip
agentHostName	ahost
agentId	aid
agentMacAddress	amac agent mac
agentReceiptTime	art
agentTimeZone	atz
agentTranslatedAddress	agent translated ip
agentType	at

Field	Aliases
agentVersion	av
applicatonProtocol	app protocol
baseEventCount	cnt
bytesIn	in
bytesOut	out
categoryBehavior	behavior
categoryDeviceGroup	device group
categoryObject	object
categorySignificance	significance
categoryTechnique	technique
destinationAddress	dst destination ip destinationip dst ip dest ip target ip targetip target
destinationHostName	dhost destination name
destinationMacAddress	dmac destination mac
destinationNtDomain	dntdom
destinationPort	dpt destination port dstport dest port targetport target port
destinationProcessId	dpid
destinationProcessName	dproc

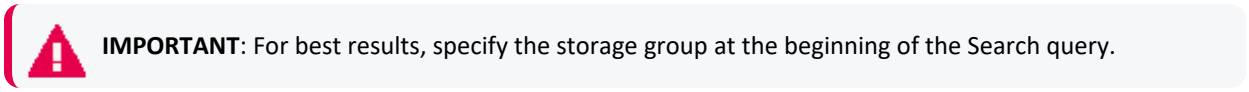
Field	Aliases
destinationTranslatedAddress	destination translated ip
destinationuserId	duid
destinationUserName	duser dst user dest user destination user dst usr
destinationUserPrivileges	dpriv
deviceAction	act
deviceAddress	dvc deviceaddr deviceip device ip
deviceCustomFloatingPoint*n* Valid values for *n* are integers between 1 and 4 For example: deviceCustomFloatingPoint1	cfp*n* For example: cfp1
deviceCustomFloatingPoint*n*Label Valid values for *n* are integers between 1 and 4 For example: deviceCustomFloatingPoint1Label	cfp*n*Label For example: cfp1Label
deviceCustomIPv6Address*n* Valid values for *n* are integers between 1 and 4 For example: deviceCustomIPv6Address2	c6a*n* device custom ipv6 *n* For example: c6a2
deviceCustomIPv6Address*n*Label Valid values for *n* are integers between 1 and 4 For example: deviceCustomIPv6Address2Label	c6a*n*Label For example: c6a2Label
deviceCustomNumber*n* Valid values for *n* are integers between 1 and 3 For example, deviceCustomNumber3	cn*n* For example: cn3
deviceCustomNumber*n*Label Valid values for *n* are integers between 1 and 6 For example: deviceCustomNumber6Label	cn*n*Label For example: cn6Label

Field	Aliases
deviceCustomString*n* Valid values for *n* are integers between 1 and 6 For example: deviceCustomString5	Cs*n* For example: Cs5
deviceEventCategory	cat
deviceHostName	dvchost
deviceMacAddress	dvcmac device mac
deviceProcessId	dvcpid
deviceReceiptTime	rt
deviceTimeZone	dtz
deviceTranslatedAddress	device translated ip
endTime	end
eventOutcome	outcome
fileNme	fname
fileSize	fsize
message	msg
requestUrl	request URL
sourceAddress	src source ip sourceip src ip
sourceHostName	shost
sourceMacAddress	smac source mac
sourceNtDomain	sntdomain
sourcePort	spt srcport src port
sourceProcessId	spid
sourceProcessName	sproc

Field	Aliases
sourceTranslatedAddress	source translated ip
sourceUserId	suid
sourceuserName	suser src user source user src usr
sourceUserPrivileges	spriv
startTime	start
transportProtocol	proto

Include a Storage Group's Filter in the Search Query

Search allows you to include a storage group in a query. For example, you have a storage group called *Firewall Events* that has the following query: `categoryDeviceGroup='/Firewall' or categoryDeviceGroup='/IDS'`. Rather than entering that query again in Search, specify the following for your Search query: `storageGroup=Firewall Events`.



IMPORTANT: For best results, specify the storage group at the beginning of the Search query.

Specify IP Addresses and Subnets

Your query can include IPv4, IPv6, and MAC addresses.

Enter an IP or MAC Address

You can enter IP addreses in the following formats:

- aa:aa:aa:aa:aa:aa
- aa-aa-aa-aa-aa-aa

The following table lists the query format and examples for the type of IP address.

Type of address	Format in a query...	Examples
IPv4	a.b.c.d	a.* a.b.* a.b.c.* a.b.c.d/8
IPv6	Full form	2001:0db8:0000:0000:0000:ff00:0042:8329
	Canonical form without leading zeroes in each group	2001:db8:0:0:0:ff00:42:8329
	Canonical form without consecutive sections of zeroes	2001:db8::ff00:42:8329
IPv6 in a subnet	Include CIDR notation	2001:0db8:0000:0000:0000:ff00:0042:8329 2001:0db8:0000:0000:0000:ff00:0042:8329/24 2001:db8::/32 **NOTE**: For the 2001:db8::/32 format, you can omit part of the IPv6 address, depending on the subnet that you are querying.
MAC	a:b:c:d:e:f a-b-c-d-e-f	94:18:82:6D:63:74 94-18-82-6D-63-74

Understand How Search Stores IP and MAC Addresses

Search stores IPv4, IPv6, and MAC addresses in a format that provides search flexibility and enables you to perform the following actions:

Compare IP addresses for optimum performance

For example, `Agent Address > 192.10.11.12`.

Specify a range of IP addresses

For example, you can enter the following types of queries:

- `Agent Address in between 192.2.13.1 and 192.2.13.11`
- `Source Address greater equal than 192.10.11.12`
- `Destination Address less than 192.112.98.33`

Use abbreviated input search notation

You can enter the following types of queries:

- To specify IP addresses in the subnet starting with a particular value:
  `Agent Address in subnet 192.*`
- To specify an IPv4 address in a subnet that uses CIDR notation. The first eight bits are the network part of the address, leaving the last 24 bits for specific host addresses.
  `Agent Address in subnet 192.0.0.0/8`
- To specify an agent address in a subnet that uses CIDR notation. The first 24 bits are the network part of the address, leaving the last 40 bits for specific host addresses.
  `Agent Address in subnet 2001:0db8:0000:0000:0000:ff00:0042:8329/24`

Search stores MAC addresses in their original format.

Understand the Query Syntax, Operators, and Functions

Search supports a variety of search operators and functions. The search query bar automatically displays related fields and operators as you enter your query.

For example, type the word "domain" to see all available fields that might contain that string or name.

Type an integer like "22", and Search displays a list of fields to choose from, such as Destination Port, Source Port or "any port."

You can also specify a storage group in the query.

Understand the Query Syntax Requirements

Depending on the type of search you create, the query must meet the requirements listed in the following table. Also, Search treats a comma (,) between search items and values as an OR operator.

By default, Search is case-sensitive to support faster performance. However, you can instruct the database to support case-insensitive searches. For more information, see the *Administrator's Guide to ArcSight Platform*.

Type	Full-text	Field-based	Hashtag (predefined)
Case sensitivity	Case-sensitive	Case-sensitive	Case-insensitive
Exact Match	Keyword treated as keyword*. Example: /Execute matches: /Execute, /Execute/Start, /Execute/Response,/Execute/Query	Enclose value in double quotes. Example: `Category Behavior ="/Execute"`	n/a

Nesting, including parenthetical clauses, such as (a OR b) AND c	Allowed Use Boolean operators to connect and nest keywords.	Allowed Use Boolean operators to connect and nest keywords.	Allowed Use Boolean operators to connect and nest keywords.
Implicit Operators	When you enter two values separated by a space, this is treated as an implicit AND condition. Example: `ssh fail`	The AND/OR treatment depends on the operator used in the search. For example, destinationAddress = 1.1.1.1, 2.2.2.2 is equivalent to destinationAddress = 1.1.1.1 or destinationAddress = 2.2.2.2 , while the query destinationAddress != 1.1.1.1, 2.2.2.2 is equivalent to destinationAddress != 1.1.1.1 and destinationAddress != 2.2.2.2	n/a
List Operations	n/a	Performs an inner join or a left join against a custom list. *Syntax for an Inner Join:* `source address in list CustomListName_CustomColumn Name` *Syntax for a Left Join:* `source address not in list CustomListName_CustomColumnName`	n/a
Time Format (when searching for events that occurred at a particular time)	No specific format The query needs to contain the exact timestamp string. Example: `"10:34:35"`	YYYY-MM-DD YYYY-MM-DD HH:mm YYYY-MM-DD HH:mm:ss.fff To narrow the time range, use the following operators: • in between (><) • greater than (>) • less than (<)	n/a

Special Characters: \ * ' "	Use the backslash (\) as an escape character.	Use the backslash (\) as an escape character.	n/a
Wildcard	Can appear anywhere in the value. Examples: *log log* lo*g* Searches for ablog, blog, long, etc.	Can appear anywhere in the field. Examples: name=*log Searches for ablog, blog, etc. in name field name="*log" name=*log Both search for *log	n/a
Escape a Wildcard Character	Can search for * by escaping the character. Example: log*	Can search for * by escaping the character. Example: log*	n/a

Understand the Search Query Functions and Operators

You can specify the following search operators in the query:

Operator	Alternative Operator	Examples
AND		#Firewall drop and sourceAddress equals 10.0.112.9 sourceAddress equals 10.0.112.9 and destinationAddress = 10.0.116.148
OR		fail OR ssh destinationAddress = 10.0.111.5 OR destinationAddress=10.0.116.148 destinationAddress =10.0.111.5, 10.0.116.48
not equal	<> !=	destinationPort not equal 21
equals	= == is equal to equal	name equals INVALID password device vendor equals CISCO
greater than	> is greater	bytes In greater than 100

less than	< is less is lower less	bytes out less than 1000
greater equal than	>= gte greater equal	End Time greater equal than 2017-07-25 End Time greater equal than 2017-07-25 09:07 End Time greater equal than 2017-07-25 09:07:43 End Time greater equal than 2017-07-25 09:31:22.685
less equal than	<= lte less equal	Base Event Count less equal than or equal 50
starts with	startwith	message starts with FIN
does not start with		name does not start with FIN
ends with	endswith	message ends with out
does not end with		message does not end with out
contains	contain like has substring	name contains TCP
does not contain	does not have	name does not contain TCP
in list	match in list of	device vendor equals CISCO and source address in list customListName_ customColumnName device vendor equals CISCO and source address in list badGuyIpList_badGuyIp
not in list	not match not in list of	source address not in list customListName_ customColumnName source address not in list badGuyIpList_ badGuyIp
in subnet	n/a	source address in subnet 10.0.0.0/8
not in subnet	n/a	source address not in subnet 10.0.0.0/8
| (Pipeline operator)	n/a	Combine various search functions separated by the | operator: ssh | eval test1 = abs (40) ssh | eval test1 = sin (Bytes In)

eval <expression> name	n/a	| eval URL_Length = length (Request URL)
rename	n/a	| rename source address as NewSourceAddress
where	n/a	| where Bytes In >= 3000| where Category Outcome = /Success

Understand the Functions for Building Eval Expressions

The Eval function allows you to define and name an expression that is returned in the search. To build an eval expression, you can use the following functions:

- "Comparison and Conditional Functions" below
- "Cryptographic Function" on the next page
- "Informational Function" on the next page
- "Mathematical Functions" on the next page
- "Statistical Functions" on page 25
- "Text Functions " on page 26
- "Trigonometry Functions" on page 27

Comparison and Conditional Functions

Function	Description	Example
coalesce(*X* [, *Y*, *Z*,*N*, ...])	Returns the value of the first non-null expression in the list. If all expressions evaluate to null, then COALESCE returns null. The list is up to 20 elements long. In the list of expressions, all elements must be of same type. The only supported types are numeric and string. *X* can be a number, field or expression.	... | eval username = coalesce (Source Username, Destination Username) *Returns*: 2
nullif(*X*,Y)	Compares two expressions. If the expressions are not equal, the function returns the first expression (expression1). If the expressions are equal, the function returns null. *X* and *Y* can be a number, field or expression. *Y* must have same data type that *X*.	... | eval newField = nullif(2, 3) *Returns*: 2 ... | eval newField = nullif(2, 2) *Returns*: null

Cryptographic Function

Function	Description	Example
md5(*X*)	Calculates the MD5 hash of string, returning the result as a string in hexadecimal. *X* must be a string.	... | eval usermd5 = md5 (Destination Username) *Returns*: 202cb962ac59075b964b07152d234b70

Informational Function

Function	Description	Example
isnull(*X*)	Returns true if the *X* is null otherwise returns false.	... | eval newField = isnull(2) *Returns*: false

Mathematical Functions

Function	Description	Example
abs(*X*)	Takes a number, *X*, and returns its absolute value. *X* can be a number, field or expression.	The function assigns the evaluated value to the new field. If the value of X is 3 or -3, the function assigns the evaluated value of 3 to the field absnum: ...| eval absnum=abs(number) ...| eval absnum = abs(bytesIn) ...| eval absnum = abs(1 - bytesIn)
cbrt(*X*)	Takes one numeric argument, *X*, and returns its cube root.	... | eval n=cbrt(2) *Returns*: 8
ceiling(*X*)	Rounds a number, *X*, up to the next highest integer. *X* can be a number, field or expression.	... | eval n=ceil(1.9) ... | eval n=ceiling(1.9) *Returns*: n=2
exp(*X*)	Takes a number, *X*, and returns e*X*. *X* can be a number, field or expression.	... | eval y=exp(3) *Returns*: y=20.0855369231877
floor(*X*)	Rounds a number, *X*, down to the nearest whole integer. *X* can be a number, field or expression.	... | eval n=floor(1.9) *Returns*: 1
mod(*X*, *Y*)	Returns the modulo of *X* and *Y*. (*X*%*Y*; the remainder of *X* divided by *Y*.)	... | eval newField = mod(25,10) *Returns*: 5

Function	Description	Example
ln(*X*)	Takes a number, *X*, and returns its natural log. *X* can be a number, field or expression.	... | eval lnBytes=ln(bytesIn) *Returns*: the natural log of the value of " bytesIn". If "bytesIn" contains 100, returns 4.605170186.
log(*X*, *Y*)	Returns the logarithm to the specified base of the argument. *X* is the base and *Y* can be a number, field or expression. *X* is optional. If not specified, it will take 10 as the default value.	... | eval test1= log (10,2) *Returns*: 0.301 ... | eval test1 = log (2) *Returns*: 0.301 as it takes the default base as 10
log10(*X*)	(Evaluates the log of number *X* with base 10. *X* can be a number, field or expression.	... | eval num=log10(10000) *Returns*: 4
power (*X*,*Y*)	Returns a value representing one number raised to the power of another number. *X* is the base and Y the exponent. *X* and *Y* can be a number, field or expression.	... | eval newField = power(2, 3) *Returns*: 8
round(*X*, *Y*)	Rounds *X* to the nearest integer. *Y* is the precision to use, if omitted the default precision is zero. *X* can be a number, field or expression. *Y* is a numeric value to indicate the precision.	... | eval n=round(1.4) *Returns*: 1 ... | eval n=round(1.5) *Returns*: 2
sign(*X*)	Returns a value of -1, 0, or 1 representing the arithmetic sign of the argument.	... | eval newField = sign(-8.4) *Returns*: -1 ... | eval newField = sign(4) *Returns*: 1 ... | eval newField = sign(0) *Returns*: 0
sqrt(*X*)	Takes one numeric argument, *X*, and returns its square root. *X* can be a number, field or expression.	... | eval n=sqrt(9) *Returns*: 3
trunc(*X*,*Y*)	Returns the expression value truncated (toward zero). *X* can be a number, field or expression. *Y* is a numeric value to indicate the precision.	... | eval newField = trunc(1.9) *Returns*: 1 ... | eval newField = trunc(2.89999, 2) *Returns*: 2.89

Statistical Functions

Function	Description	Example
greatest(*X*,*Y* [,*Z*,*N*, ...])	Returns the largest value in a list of expressions. The list is up to 20 elements long. In the list of expressions all elements must be of same type. The only supported types are numeric and string. *X* can be a number, field or expression.	... | eval newField = greatest(7, 5, 9) *Returns*: 9 ... | eval newField = greatest('sit', 'site', 'sight') *Returns*: site ... | eval newField = greatest (bytesIn, 100) *Returns*: 100, when bytesIn is less than 100
least(*X*,*Y*[,*Z*,*N*, ...])	Returns the smallest value in a list of expressions. The list is up to 20 elements long. In the list of expressions all elements must be of same type. The only supported types are numeric and string. *X* can be a number, field or expression.	... | eval newField = least (bytesIn, bytesOut) *Returns*: 5 ... | eval newField = least('sit', 'site', 'sight') *Returns*: sight ... | eval newField = least (bytesIn, 100) *Returns*: 100, when bytesIn is greater than 100
randomint(*X*)	Returns a random number between 0 and *X*-1. *X* can be any positive integer between the values 1 and 9,223,372,036,854,775,807.	... | eval newField = randomint (10) *Returns*: a random number between 0 and 9

Text Functions

Function	Description	Example
length(*X*)	Returns the character length of a string, *X*.	... | eval n=length(field) *Returns*: the length of (field). If the field is 256 characters long, it returns n=256. ... | eval n=length("abc") *Returns*: n=3 (abc is a literal string, surrounded by double quotes)
lower(*X*)	Takes a string argument, *X*, and returns the lowercase version.	... | eval name=lower("USERNAME") ... | eval name=tolower("USERNAME") *Returns*: the value of the field username in lowercase. If the username field contains FRED BROWN, it returns name=fredbrown.
substr (*X*,*Y*,*Z*)	This function returns a new string that is a substring of string *X*. The substring begins with the character at index *Y* and extends up to the character at index *Z*-1. The index is a number that indicates the location of the characters in string *X*, from left to right, starting with zero. *Y* can be negative. *Z* cannot be negative.	...| eval n=substr("ArcSight", 5, 6) *Returns*: "g" ...| eval n=substr("ArcSight", 2, 6) *Returns*: "cSig" ...| eval n=substr("ArcSight", 0, 3) *Returns*: "Arc"
trim(*X*) ltrim(*X*) rtrim(*X*)	trim(*X*) removes all spaces from both sides of the string *X*. ltrim(*X*) removes all spaces from the left side of the string *X*. rtrim(*X*) removes all spaces from the right side of the string *X*.	For the sake of these examples, assume that *X* is a literal string and _ represents any number of space characters. ... | eval trimmed=ltrim("_string_") *Returns*: trimmed="string_" ... | eval trimmed=rtrim("_string_") *Returns*: trimmed="_string" ... | eval trimmed=trim("_string_") *Returns*: "string"
upper(*X*)	Takes one string argument and returns the uppercase version.	... | eval name=upper("username") ... | eval name=toupper("username") *Returns*: the value of the field username in uppercase. If username contains fred brown, it returns name=FRED BROWN.

Trigonometry Functions

Function	Description	Example
acos(*X*)	Takes one numeric argument, *X*, and returns its trigonometric inverse cosine.	...| eval newField = acos(0.3) *Returns*: 1.2661036727795
asin(*X*)	Takes one numeric argument, *X*, and returns its trigonometric inverse sine.	...| eval newField = asin(3) *Returns*: 0.304692654015398
atan(*X*)	Takes one numeric argument, *X*, and returns its trigonometric inverse tangent.	...| eval newField = atan(3) *Returns*: 0.291456794477867
atan2(*X*,*Y*)	Returns a value representing the trigonometric inverse tangent of the arithmetic dividend of the arguments.	...| eval newField = atan2(2,1) *Returns*: 1.10714871
cos(*X*)	Takes one numeric argument, *X*, and returns its trigonometric cosine.	...| eval newField = cos(3) *Returns*: 2435538
cosh(*X*)	Takes one numeric argument, *X*, and returns its hyperbolic cosine.	...| eval newField = cosh(3) *Returns*: 10.0676619957778
cot(*X*)	Takes one numeric argument, *X*, and returns its trigonometric cotangent.	...| eval newField = cot(3) *Returns*: -7.01525255143453
sin(*X*)	Takes one numeric argument, *X*, and returns its trigonometric sine.	...| eval newField = sin (3) *Returns*: 0.141120008059867

Function	Description	Example
sinh(*X*)	Takes one numeric argument, *X*, and returns its hyperbolic sine.	...| eval newField = sinh(3) *Returns*: 10.0178749274099
tan(*X*)	Takes one numeric argument, *X*, and returns its trigonometric tangent.	...| eval newField = tan(3) *Returns*: -0.142546543074278
tanh(*X*)	Takes one numeric argument, *X*, and returns its hyperbolic tangent.	...| eval newField = tanh(3) *Returns*: 0.99505475368673

Extend the Search with a Lookup List

Select **Configuration** > **Lookup Lists**.

You can create CSV files, or **lookup lists**, that enables the **Search feature** to create additional tables with different fields and store them in the database. You can add lookup list fields to fieldsets and use them in search queries.

Understand Considerations for the Lookup List File

The CSV file for your lookup list must meet the following requirements:

- The first row must be a comma-separated list of field names.
- The field names cannot exceed 40 characters. The names can only contain alphanumeric characters and underscores. They must start with an alpha character.
- The remaining rows must be comma-separated values for the fields in the first row.
- All rows must contain the same number of values.
- You must select one of the columns as the key field, and the values of the key field must be unique.
- The **key field** is the field that you can use with the `in list` operator in queries.
- The file cannot exceed 25 fields and 2 million rows.
- The file cannot exceed 150 MB.

Create a Lookup List

1. Select Configuration > Lookup Lists.
2. Click Add.
3. Drag-and-drop your CSV file to the Lookup Lists page or select Browse to navigate to the file.
4. Specify a name for the lookup list.

   Once created, you cannot change the name of the lookup list. The name must meet the following requirements:

   - Does not exceed 20 characters
   - Contains only alphanumeric characters and underscores
   - Starts with an alpha character
5. Specify the key field, then either accept the recommended value type or specify a different one.

   The following are possible values:

Value type	Specifies
domain	The name of the lookup list.
float	A number whose radix point can be placed anywhere relative to the significant digits of the number
hostname	Fully qualified domain name
int	Integer value
ipv4	IPv4 address
ipv6	Ipv6 address
mac	MAC address
short text	Text that cannot exceed 1K of space
long text	Text that cannot exceed 4K of space
time	Time stamp
url	A URL address that cannot exceed 4K
username	A string type

6. To upload the file as a table in the database, click Upload.

Append a Lookup List

Use the **Append** feature to add more rows to a current lookup list.

- The file you need to append needs to have the same structure as the one you uploaded. For example, the same amount of columns.
- The file you need to append should not have an empty value in any of its rows.

1. Select Configuration > Lookup Lists.
2. Click the eye icon on the left side of the selected lookup list.
3. Click Append.
4. Select the list you want to append.
5. Click Upload. The original lookup list will be updated with the new rows added.

Replace a Lookup List

Replacing the contents of a lookup list does not affect queries that use the original lookup list. You cannot change the name of a lookup list. The field names in the replacement file must match the field names in the original file.

1. Select Configuration > Lookup Lists.
2. Select the list you want to replace.
3. Click the eye icon on the left side of the selected lookup list.
4. Click Replace.
5. Select the CSV file you want to use to replace the contents of the existing lookup list.

Delete a Lookup List

1. Select Configuration > Lookup Lists.
2. Select the list you want to delete.
3. Select the trash can icon.

Specify the Set of Fields for Search Results

You must have the **Create Fieldset***s permission.*

You can specify a **fieldset** that determines a group of search result fields the system displays in the Events table. In the table, each field can provide the ten most and less common values. Multiple searches can share a fieldset, and new searches display a default fieldset that contains the most common event fields. Use the fieldsets window to view and add the customize and system fieldsets, including lookup lists.

- **System**: Predefined fieldsets provided by the system.
- **Custom**: Customize the default fieldsets and lookup list fields for individual purposes.

New searches display the user´s default fieldset. These will remain selected in the fieldsets drop-down even when moving to other search tabs. If you select another fieldset, the popup window closes to display the new option. You can revert the change to the previously selected fieldset.

NOTE: Whenever you replace or update the fieldset, your search becomes out of sync, since the fields shown might differ from the new selection. Rerun the search with the new selection to correct this.

View and Create Fieldsets

To access the fieldsets window, from the **Search** page, click the fieldset located at the left of the time range selector. By default, the system displays the name of the last used fieldset. You can also perform the following actions:

- Filter fieldsets by lists
- Search fieldsets by name or specific field

You can designate a fieldset as your preferred default. The fieldset will only be used for your search results and will not affect other users connecting to the same system.

1. From the Search page, click the fieldset shown to the left of the time range selector.
2. Click Manage Fieldsets.

   The Manage Fieldsets window displays.
3. Click +.

   The Create Fieldset window displays.
4. To view the complete list of available fieldsets, click the filter icon.
   - Recently Created Fieldsets
   - My Fieldsets
   - Recently Updated Fieldsets
   - All Fieldsets

Create a Fieldset

1. From the Search page, click the fieldset name (at the left of the time range selector).
2. From the fieldsets window, click Create Fieldsets.
3. Click + to add a new fieldset.
4. Select or deselect the options, including lookup fields.

- Drag and drop any field to the Selected Fields column. Otherwise, select Text Editor to enter the fields that you need.
- To locate a specific field, use the search field.

> **NOTE**: The fieldset editor displays the coding-style name for search fields. For more information about which fields to choose or type, see "A1 Mapping Database Names to their Appropriate Search Fields" on page 194.

5. Specify a name for the new fieldset.
   - Each fieldset should have a unique name.
   - Fieldset names are not case sensitive.
6. To save the fieldset as default, select the checkbox at the bottom left corner.

   The fieldset is used only for your search results and does not affect other users connecting to the same system.
7. Click Save.
8. (Optional) Select Apply to this search to customize the original fieldset without overwriting or saving it.

   This new option displays in the custom category as Custom. The temporary fieldset will not be visible to other users, and it will only remain available on that session. After you log out, the system removes the temporary fieldset. You can have one temporal custom fieldset at a time.
9. To execute the query again, click Search.

Edit a Fieldset

You can edit custom fieldsets only. You cannot modify system fieldsets, and you can only edit one fieldset at the time.

- "Editing the Selected Fieldset" below
- "Editing a Different Fieldset" on the next page

Editing the Selected Fieldset

1. From the Search page, click the fieldset shown to the left of the time range selector.
2. From the fieldsets window, select Edit Fieldset.

   The Edit Fieldset window displays.
3. Drag and drop any field to the Selected Fields column OR select Text Editor to write the fields you need.
4. To locate a specific field, use the Search field.

5. In the Fieldset Name field, update the fieldset name as needed.
6. To save the fieldset as default, select the box at the bottom left corner.

   The fieldset is used only for your search results and does not affect other users connecting to the same system.
7. Click Save.
8. (Optional) Select Apply To This Search to customize the existing fieldset without overwriting or saving it.

   This option displays in the custom category as Custom. The temporary fieldset will not be visible to other users, and it will only remain available on that session. After you log out, the system removes the temporary fieldset. You can have one temporal custom fieldset at a time.

Editing a Different Fieldset

1. From the Search page, click the fieldset shown to the left of the time range selector.
2. Click Manage Fieldsets.
3. Select the fieldset checkbox.
4. Click the edit icon.

   The Edit Fieldset window displays.
5. Drag and drop any field to the Selected Fields column OR select Text Editor to write the fields you need.
6. To locate a specific field, use the Search field.
7. In the Fieldset Name field, update the fieldset name as needed.
8. To save the fieldset as default, select the box at the bottom left corner.

   The fieldset is used only for your search results and does not affect other users connecting to the same system.
9. Click Save.
10. (Optional) Select Apply To This Search to customize the existing fieldset without overwriting or saving it.

    This option displays in the custom category as Custom. The temporary fieldset will not be visible to other users, and it will only remain available on that session. After you log out, the system removes the temporary fieldset. You can have one temporal custom fieldset at a time.

Delete a Fieldset

You can delete a fieldset that you have created. If you delete a fieldset that's used in an active search, Search changes the fieldset name to **Custom** for that search. If you delete a fieldset

used in a saved search query or saved search criteria, Search will use the default fieldset saved in your user preferences.You cannot delete a system fieldset.

1. From the Search page, click the fieldset shown to the left of the time range selector.
2. Click Manage Fieldsets.
3. Select the fieldset checkbox.
4. Click the delete icon.
5. Click Yes to proceed.

Clone a Fieldset

When you clone a fieldset, Search creates a copy of the existing fieldset under the shared fieldsets category. You can update the cloned fieldset and give it a different name.

1. From the Search page, click the fieldset shown to the left of the time range selector.
2. Click Manage Fieldsets.
3. Select the fieldset check box.
4. Click the clone icon.
   The system adds the fieldset to the list.
5. To edit the fieldset, see "Edit a Fieldset " on page 32.

Managing Your Searches

You can save, refresh, and edit your searches. To help you investigate events, Search displays the results as a timeline, in a table, and in a detailed view. You can export the search results in the table to a CSV file. You can also schedule a search to run at specific intervals, then analyze the completed runs of that search over time.

Create and Modify a Search

For every search, you must enter the query input, search result fields, and the time period for which you want to search events. Queries are case sensitive. The query input determines the search type (full text, natural language, or contextual). As you specify the search query, Search suggests search items and operators based on a schema data dictionary. You can also choose from predefined queries.

If you tend to use the same settings for some search parameters, you might want to specify a preferred default setting. For example, you can configure a default time range.

NOTE: Recon treats a comma (,) between search items and values as an OR operator.

NOTE: Recon supports up to 10 active searches and 40 saved searches per user.

Create a Search

For every search, you must enter the query input, search result fields, and the time period for which you want to search events. Queries are case sensitive. The query input determines the search type (full text, natural language, or contextual). As you specify the criteria for a search query, Search suggests search items and operators based on a schema data dictionary. You can also choose from predefined queries.

If you tend to use the same settings for some search parameters, you might want to specify a preferred default setting. For example, you can configure a default time range.

NOTE: Recon treats a comma (,) between search items and values as an OR operator.

To create a search:

1. Select Search > + New Search. You can choose search data migrated from ArcSight Logger.
2. Specify the query parameters.

   For example:

   ```
   Source Address = 192.10.11.12 and Destination Address less than
   192.10.11.12
   ```

   To use a predefined search query or criteria, type #.
3. To search for a field without data, enter [field_name] = Null.
4. Specify the fieldset you want for the search results.

   By default, Search displays the your preferred default fieldset. If you have not specified one, Search display the Base Event Fields fieldset.
5. For the time range, perform **one** of the following actions:
   - Accept the default time (Last 30 minutes)
   - From the drop-down menu, select a pre-defined value under Quick Ranges
   - From the drop-down menu, use the Custom Range fields to specify a time range
   - From the drop-down menu, select Dynamic, and then enter a dynamic date value

You can also specify the timestamp you want to use for the retrieved events. Search uses Normalized Event Time (NET) by default.

6. Click Search.

   Search begins populating the Events Timeline and Events table. Depending on the number of events retrieved, the search might pause to indicate that the amount of data could impact the search performance. You might want to select a smaller time range. To resume a search, click the play button in the progress bar.
7. (Optional) To more easily find the search later, give the search a name.
8. To save the search for future use, select Save.

Modify the Search Settings

When viewing a search, you can change the query, a fieldset, and the range selector.

1. In the saved search, change the query, fieldset, or time range.
2. To return to your original settings, select Revert Changes.
3. To update the search results with the modified settings, select Search Now or Search.

Name a Search

By default, Recon gives each search the title *Search <N>*. You can apply a custom name to the search at any time.

1. In the top-left corner of your screen, hover over the search name and then click the pencil icon .
2. Enter the custom name.
3. To save your changes, select the Check icon.
4. (Optional) To save the search, click Save.

Save a Search

Select Search.

Search temporarily stores your query, criteria, and results as you use the ArcSight Platform features. However, you will lose the content if you log out or close the browser tab. To keep any searches you have created, you must **save** your changes.

- Save the full search results
- Save the search query
- Save the search query and criteria

View Search Results

Search displays results in an **Events Timeline**, **Events** table, and **Event Details panel**. If connectors are configured to send raw events, the table and details panel can include **raw event data**. Also, the maximum number of events that a search can return is 10 million. If your searches regularly stop at the maximum limit, consider splitting the query into separate searches.

View the Events Timeline

The **Events Timeline** displays data points in a segmented timeline across the specified time range. The time range in the Timeline corresponds with the data listed in the Events table.

If you have a large number of data points or a wide time range, you can see the big, overall picture, but you might not be able to clearly identify specific data points. To **narrow the scope** of the displayed data, select Enable Range Selector then adjust the boundaries of the selector.

To view the **details of a data point** or moment in time, select Disable Range Selector, and then hover over the data point.

View the Events Table

The **Events** table contains all the fields specified in the fieldset. You can choose to display the table in Grid View or Raw View. To view details of a specific event, select the event.

While viewing the table, you can perform the following actions:

View all details for an event

When you select an event in the table, Search opens the Event Details panel. Within the panel, you can further expand the fields for more information.

View raw event data

When you click the Raw View icon, the Events table replaces the fieldset columns with a Raw Data column, which displays the whole raw syslog event.

Although the Raw Event field is most applicable for syslog events, you can also display the raw event associated with CEF events.

To do so, make sure the connector that is sending events to the database populates the *rawEvent* field with the raw event.

View all event data for a field value

Right-click a value in a table row, then select Search For.

Search displays all of the event data based on the selected field value.

View the most and least common values for an event record field

Right-click a column heading, then select Preview Top/Bottom.

To help filter data for security threats, you can quickly display the most and least common values for a field. Search displays the count and percentage of hits for the value.

For example, the *Device Vendor* field might have a top value of "bluecoat" with a count of 3,000 hits, accounting for 30 percent of 10,000 results.

View authenticated users

Applies only when the fieldset for the original search includes the Device Receipt Time field.

Right-click an IP address or host name, then select Get Authenticated Users.

Search displays users who have successfully authenticated to the IP address or host name in the last 24 hours.

Copy a value from an event

To use a value from an event elsewhere, simply right-click and copy the value.

Search for an event value

To add a value from an event to your query, right-click the value.

Compare data in columns

Right-click a column heading, then select Pin Column or Unpin Column.

By pinning a column, you can compare the column's values against those of other columns. Search moves the pinned column to the extreme left location in the table. You can pin multiple columns.

Remove or hide columns

If you do not want to view a column, right-click the column heading, then select Hide Column.

Alternatively, you can click the Wrench icon, and then select the column.

Reorder columns

To rearrange the order of the columns, drag each column to new position.

Sort the data in columns

Select the up or down arrow in the column heading to change the sort order.

Refresh Search Results

If the time range for your search is based on a predefined range, such as Last 30 minutes, you can refresh the search results as desired. However, refreshing the browser as you update a search does not save your changes. You must save the refreshed results.

Identify Fields without Data

If an event does not have data for a schema field, Search represents the absence of data (*null*) in the results in the following ways:

Affected Field	Displayed Result
Search field	Null, NULL and null query formats
Events table	Empty cell
Empty field from ESM (for example, name='')	name = '', NULL
Event Details panel	--- in the cell

Use Search Results to Build a Report

Search assigns a unique **Search Results ID**, which is a link to the temporary table containing the search results that you see in the Events table.

- You can copy the ID to build a report around those events.
- You can also build a report based on the Search Results ID for a completed run of a scheduled search.

For more information about building a report, see the *User's Guide for Fusion in the ArcSight Platform*.

View and Use the Details of an Event

When you select an event in the Events table, Search opens the **Event Details** panel. In this panel, you can scroll through the specific details of the event. Search groups the details by categories such as Agent and Source.

You can view the raw data details for the event, as well as instruct the panel to include fields with *null* data. For example, you could view details about the agent, category, device, source, or severity. Details displayed in blue text are part of the query filter.

- "Export All or Some Event Details" below
- "Apply Event Details to Other Searches or Share with Colleagues" below

Export All or Some Event Details

You might want to share the selected event's details with a colleague or use the details in a report or other media. You can export all content in the Event Details panel with or without empty values.

Apply Event Details to Other Searches or Share with Colleagues Search allows you to copy the URL of a detail to share with colleagues or open in a separate browser tab. You can also choose to use the detail in a new search query and in an nslookup or WhoIs search.

For example, you might select a domain name and use a nslookup to check whether the domain is valid.

Apply Event Details to Other Searches or Share with Colleagues

Search allows you to copy the URL of a detail to share with colleagues or open in a separate browser tab. You can also choose to use the detail in a new search query and in an nslookup or WhoIs search.

For example, you might select a domain name and use a nslookup to check whether the domain is valid.

Save the Search Results

After you execute the search query, Search automatically preserves the search results including its query and criteria, in case you must navigate away from the search page to another feature in the ArcSight Platform. However, your search is not automatically saved if you close the browser or tab, or when you log out. To permanently save your search, you can add it to the Search Results list.

You can delete the search results from the saved list at any time. You can also configure Search to automatically delete searches after a specific time.

1. When viewing the results of a search, select Save.
2. Click Search Results.

   Note that you can also save just the search query or the query and the criteria.
3. Specify a name for the search results.

- Each search result must have a unique name.
- We do not recommend using the same names for saved search queries, criteria, and results.

4. Select Save.
5. To view your saved search results, select Search > Search Results.

Export the Search Results

You can export the Events table to a CSV file. Search exports data based on the specified fieldset for the search. The export process limits the file to one million event records.

1. In the table's header, select the CSV icon.
2. Choose to save the file or open in a desired application.

Manage Saved Search Results

Select Search > Search Results.

If you have saved the results of a search, you can regularly review those results, export the data to a CSV file, or delete the saved results. You can sort the table of saved search results by the search name, query, number of results, or date it was saved.

When you view saved search results, you can update the query and criteria as needed, then save those changes to the current search results. Alternatively, you save your changes as a new search query, criteria, or results.

Manage Saved Search Queries

You must have the **Manage Search Queries** *permission.*

A **query expressio**n is a set of conditions used to select events when a search is performed. An expression can specify a very simple term to match such as "login" or an IP address; or it can be more complex to match events that include multiple IP addresses and reference a lookup list. Search provides default queries, labeled as *system*. However, you can also set your own queries. Once a custom query is saved, you have the option to load, clone, modify, or remove the query at any time.

Create and Save a Search Query

You must have the **Manage Search Queries** *permission.*

You can easily save a query to display only the events that you are interested in. Once you save a query, you can load the query as many times as needed.

- Use the Search Query Tab to Create and Save Queries
- Use the Search Page to Create and Save Queries

Use the Search Query Tab to Create and Save Queries

1. Select Search > Search Query.
2. Click **+** .
3. For Search query and metadata, specify the query or type # to choose a saved query or criteria.
4. Specify a name for the new query.
   - Each search query must have a unique name.
   - We do not recommend using the same names for saved search queries, criteria, and results.
5. Click Save.

Use the Search Page to Create and Save Queries

1. Select Search.
2. Enter the search query.
3. Click Save.
4. Select Search Query.
5. Specify a name for the search query.
6. Click Save.

Modify a Search Query

You must have the **Manage Search Queries** *permission.*

Once the query has been saved, you have the option to modify the query expression at any time.

IMPORTANT: The modifying option will be disabled (gray out) for system searches as these cannot be edited. Micro Focus recommends to clone the search query and update it instead.

1. Select the query that you want to edit.
2. Click (edit icon).

3. Edit the query as needed.
4. Save the changes.

Clone a Search Query

You must have the **Manage Search Queries** *permission.*

You can create a copy of an existent system query and later update the query expression as needed.

1. Select Search> Search Query.
2. Select the query that you want to clone.
3. Click  .

   Search adds the clone, using the original name plus a consecutive number. For example: `entityName > entityName (1)`.

   By default, the sharing type of the duplicate will be Private.

Delete a Search Query

You must have the **Manage Search Queries** *permission.*

You can delete a private search query. However, system search queries cannot be deleted.

1. Select Search > Search Query.
2. Select the query that you want to delete.
3. Click the delete icon.
4. To acknowledge the deletion, click Yes.

View and Load Search Queries

You must have the **Manage Search Queries** *permission.*

- "View a Search Query " below
- "Load a Search Query" on the next page

View a Search Query

By default, search queries are sorted alphabetically by name, followed by sharing type. To resort alphabetically mixing together all categories, simply click the name column. You can sort the table by only one column at a time. Date columns are displayed according to your user preferences.

Load a Search Query

Search will load the search query and its correspondent details.

If a search query and search criteria are saved under the same name, only one will be displayed in the search box.

TIP: Any query updates after loading will be discarded unless you click **Save**, and then select **Overwrite**.

From the Search Query main table

1. Select Search > Search Query.
2. For the search query you want to view, click the load icon.

   The query will load in the main search page.

   CAUTION: Search displays an error message if there are already 10 active searches in the search navigation bar.

From the Main Search Page

1. Select Search.
2. Click Load.
3. Select the search query that you want to load.
4. Click Load.

TIP: The maximum search result is based on the hit limit configured in the User Preferences.

Understand the Sharing Status of Saved Queries and Criteria

Search allows you to share your saved search queries and criteria. When viewing the list of saved queries or criteria, the Sharing column includes the following categories:

System
Indicates that the search query or criteria is provided by the system

Private
Indicates that only you can view, edit, and delete the saved query or criteria

Manage Saved Search Criteria

You must have the **Manage Search Criteria** *permission.*

A **search criteria** combines a query expression and other Search elements such as fieldsets and the time range. A fieldset determines the fields that are displayed in the search results for each event that matched a search query. Search provides several default criteria that you can view and load, such as DoS Events, MITRE ATT&CK Events, and Failed Login Event. However, you can also save custom search criteria. If a search includes a query with default parameters, you have the option to load the search, modify, or remove any parameter at any time.

Understand the System Search Criteria

The following system out of the box search criteria are available for view and load. All queries are set in Normalized Event Time.

Out of the box	Query	Time Range	Fields
DoS Events	categoryTechnique=/DoS	$Now , $Now -2h	Normalized Event Time, Name ,Source IP , Source Port, Source Geo Country Code, Destination IP, Destination Hostname ,Destination Zone URI, Destination Port , Transport Protocol , Device Vendor, Device Product, Device Event class ID.
MITRE ATT&CK Events	deviceCustomString6Label=MITRE ID	$Now ,$Now -1d	Normalized Event Time, Name, Agent Severity, Source MAC Address, Source IP Address, Source Host Name, Source Zone URI, Destination MAC Address, Destination IP Address, Destination Host Name, Destination Zone URI, Destination Port, Destination Process Name, Destination Service Name, Destination User Name, Category Technique, Category Object, Category Outcome, Category Behavior, Category Device Group, Category Significance, Category Device Type, Message, DeviceCustomString6, Device Custom String6Label, Device Custom string1Label, Device Custom string1, Device Custom string2Label, Device Custom string2, Device Custom string3Label , Device Custom String3, Device Custom String4Label, Device Custom String 4, Device Custom String5Label, Device Custom String5, Originator, File Path.

Out of the box	Query	Time Range	Fields
Failed Login Events	category behaviour=/Authentication/Verify and category outcome!=Success	$Now ,$Now -2h	Normalized Event Time, Source IP Address, Source Geo Country Code, Source User Name, Destination IP Address, Destination Host Name, Destination NT Domain, Destination Zone URI, Destination User Name, Destination User ID, Device Event Class ID, Device Product, Device Vendor, Category Object, Category Outcome.
Vulnerabilities	categoryTechnique=/scanner/device/vulnerability	$Now ,$Now -2w	Normalized Event Time, Destination Host Name, Destination IP Address, Destination Mac Address ,Destination Zone URI, device event class ID , device product, device vendor ,name ,message, flex string1, device custom string6 Label, device custom String6, device custom string2 Label, device custom string2, Agent Severity.

Out of the box	Query	Time Range	Fields
Proxy Events	categoryDeviceGroup=/Proxy	$Now ,$Now -2h	Normalized Event Time, Source Address,Source Port, Destination Address Destination Zone URI, Destination Port, Destination Host Name, Request URL, Request URL File Name ,Request Method, Request Client Application ,Request Cookies, device event class ID, Device Product, Device Vendor, Category Behavior, Category Outcome.

Out of the box	Query	Time Range	Fields
Firewall Events	categoryDeviceGroup=/Firewall	$Now ,$Now -2h	Normalized Event Time, DeviceProduct, Name, DeviceEventClassId, SourceAddress, SourceTranslatedAddress, SourceHostName, SourcePort, sourceTranslatedPort, DestinationAddress, DestinationTranslatedAddress, DestinationHostName, DestinationPort, DestinationTranslatedPort, TransportProtocol, DeviceAction, DeviceSeverity, DeviceAddress, DeviceHostName, DeviceCustomNumber1Label, DeviceCustomNumber1, DeviceCustomNumber2, DeviceCustomNumber3, DeviceCustomString1, DeviceCustomString2, DeviceCustomString3, DeviceCustomString4, DeviceCustomString5Label, DeviceCustomString5, DeviceCustomString6Label, DeviceCustomString6, DeviceInboundInterface, DeviceOutboundInterface, BytesIn, BytesOut, CategoryDeviceGroup, CategoryBehavior, CategoryObject, CategoryOutcome, CategorySignificance

Out of the box	Query	Time Range	Fields
DGA Events	deviceCustomNumber1 >=1 and deviceCustomNumber1Label contains DNS	$Now,$Now-1d	Normalized Event Time, Source Address Source Port ,Source Zone URI, Destination Address, Destination Port, Destination Hostname, Destination Zone URI, Destination Geo Country Code, Device Custom Number1, Device Custom Number1Label, Request Url, Transport Protocol, Bytes In, Bytes Out, Category Behavior, Category Outcome , Device Event Category, Device Event Class ID, Device Direction, Request Url File Name

Create and Save a Search Criteria

You must have the **Manage Search Criteria** *permission.*

Creating search criteria will enable you to quickly refine your search results. You can easily create a search criteria that will display special results thanks to specific parameters such as time and fieldsets. Once the search criteria is saved, it can be easily accessed and loaded as many times as needed.

Recon has available system search criteria by default. However, you can also set your own search criteria.

- Use the Search Criteria Tab to Create and Save Criteria
- Use the Search Page to Create and Save Criteria

Use the Search Criteria Tab to Create and Save Criteria

1. Select Search > Search Criteria.
2. Click **+** .
3. For Search query and metadata, specify the query or type # to choose a saved query or critiera.
4. Specify the start and end time, as well as the timestamp.
   - The timestamp, by default, is **Normalized Event Time** or your custom preference.
   - The time range, by default, is **Last 30 minutes** or your custom preference.
5. Select a fieldset.

6. Specify a name for the new criteria.
   - Each search criteria must have a unique name.
   - We do not recommend using the same names for saved search queries, criteria, and results.
7. Click Save.

Use the Search Page to Create and Save Criteria

1. Select Search.
2. Enter the search criteria: query, time, and fieldset.
3. Click Save.
4. Select Search Criteria as the save type.
5. Specify a name for the search.
6. Click Save.

Delete a Search Criteria

You must have the **Manage Search Criteria** *permission.*

IMPORTANT: The deleting option will be disabled (gray out) for system searches as these cannot be deleted. For more details on the pre-defined items, see "Understand the System Search Criteria " on page 45.

1. Select Search > Search Criteria.
2. Select one or more criteria to delete.
3. Click the delete icon.
4. Click Yes to acknowledge the deletion.

Modify Search Criteria

You must have the **Manage Search Criteria** *permission.*

If a private search includes a query with default parameters, you have the option to modify or remove any parameter at any time.

IMPORTANT: The modifying option will be disabled (gray out) for system searches as these cannot be edited.

1. Select the criteria that you want to edit.
2. Click the modify icon (pencil).

3. Edit the query and parameters as needed.
4. Save the changes. Otherwise, click Cancel.

View and Load Search Criteria

*You must have the **Manage Search Criteria** permission.*

You can view all the search criteria (system and private) from one single window. Load the search to retrieve the query and correspondent settings.

- "View a Search Criteria" below
- "Load the Search Criteria" below

View a Search Criteria

By default, search criteria are sorted alphabetically by name, followed by sharing type. Date columns are displayed according to your user preferences.

Load the Search Criteria

Load the criteria with the predefined start and end date, timestamp, and fields. Search will load the saved query and its correspondent details.

The system discards any updates that you make after loading unless you click **save** and **Overwrite**.

From the Search Criteria main table

1. Select Search > Search Criteria.
2. Click the box next to the search criteria you want to load.
3. Click Load. The search criteria will be loaded in the main search page.

   If a maximum of 10 searches in the search navigation bar has been reached, the system displays an error message.

From the Main Search Page

1. Select Search.
2. Click Load.

   If a search query and search criteria are saved under the same name, only one will be displayed in the search box.
3. Select the search criteria that you want to load.
4. Click Load.

   The maximum search result is based on the hit limit configured in the User Preferences.

Scheduling Regular Runs of a Search

*You must have the **Manage Scheduled Searches** permission to schedule runs of a search.*

Select Search > Scheduled Searches > Schedule.

A **scheduled search** is a search that runs on a regular interval. Whereas a saved search is saved, but does not run automatically.

Each time a scheduled search runs, search adds the results to the list of completed search runs.

Manage Scheduled Searches

*You must have the **Manage Scheduled Searches** permission to schedule runs of a search.*

Select Search > Scheduled Searches > Scheduled.

- "Create a Scheduled Search" on the next page
- "Clone a Scheduled Search" on page 55
- "Edit a Scheduled Search" on page 56
- "Delete a Scheduled Search" on page 56
- "Enable and Disable a Scheduled Search" on page 56

For your scheduled searches, you can perform the following actions:

View and edit all details for a schedule search
To view specific scheduled search details, in the Name column, locate the search name and select it. Click Edit at the top of the table.

Sort the data in columns
To change the sort order, click the column heading to toggle between ascending and descending order.

Reorder columns
To rearrange the order of the columns, drag each column header to a new position.

Search for a search keyword
To find a keyword, click the field next to the Magnifying Glass icon (Search Keyword), enter a value, and the system displays your results automatically.

Hide and display columns

To hide and display a column, in the far right-corner of the window, click the Wrench icon (Manage Columns), and then select and clear the column name checkboxes.

Filter the data in columns

You can filter scheduled searches based on Status, Timestamp, and Fieldset. To filter the data for more specific results, in the far-right corner of the window, click the Funnel icon (Filters), and then select and clear the filter options.

Create a Scheduled Search

*You must have the **Manage Scheduled Searches** permission to schedule runs of a search.*

For every scheduled search, enter the query, fieldset, or time range for the search events or leave the defined values for the saved search. Just as for a saved search, the following considerations apply to a scheduled search:

- The search is case sensitive.
- The query input determines the search type (full text, natural language, or contextual).
- The system treats a comma (,) between search items and values as an OR operator.
- As you specify the search criteria, the system suggests search items and operators based on a schema data dictionary. To view the predefined queries, type # in the query field.
- To search for a field without data, enter [field_name] = *Null*.

To create a scheduled search:

1. (Conditional) To schedule a search that you are currently viewing, select Schedule.
2. (Conditional) To schedule a search without currently viewing one, complete the following steps:
   a. Select Search > Scheduled Searches.
   b. Select +.
   c. Specify the search settings.
3. Specify a Name that is 5 to 255 character long.
4. To enable the scheduled search, select enable. You can enable and disable scheduled searches at any time in the Scheduled tab.
5. To indicate how frequently you want the search to run, specify one of the following options:
   - Hourly
   - Daily

- Weekly
- Monthly

6. Depending on the frequency that you specified in Step 5, configure the settings for the dates and times of each run.

   NOTE: For Starting from, if you select end after, the maximum number of instances is 1000.

7. (Conditional) To schedule an existing search, type # to reveal the list of available saved searches.
8. (Conditional) To create a query, specify the query parameters, fieldset, or time range.

   For example:

   `Source Address = 192.10.11.12` and `Destination Address less than 192.10.11.12`

9. Under Result Retention and Limitations, configure how long you want to keep each completed run of the scheduled search.
   - Your choice of values for each setting might be confined to limits set by your product administrator.
   - For Delete results after, you can specify a value that overrides how you configured Search Expires In for your search preferences.

     For example, your prefer that searches expire within five days. But you want the results for this scheduled search to expire after 10 days.
   - If you select Keep only the most recent run, then, when a run completes successfully, Search deletes the results of the previous run.
10. For Retrieve up to, specify the number of results that you want to receive.
11. Select Schedule.

Clone a Scheduled Search

*You must have the **Manage Scheduled Searches** permission to schedule runs of a search.*

Select Search > Scheduled Searches > Scheduled.

After creating a scheduled search, you can clone it at any time.

1. Select the scheduled searches that you want to clone.
2. Click the clone icon.

Edit a Scheduled Search

*You must have the **Manage Scheduled Searches** permission to schedule runs of a search.*

After creating a scheduled search, you can edit it at any time. After you modify a schedule, the first completed run will have a flag to indicate that the modification occurred.

If you change the Pattern values, please be aware that Search counts any and all completed runs before you made the change. For example, your scheduled search uses the repeat forever option and Search has performed three runs. If you update the ending option to end after eight occurrences, Search counts the three previous completed runs; therefore, you would only have five occurrences of the eight occurrences left to run. Should you want eight occurrences, you would need to change your ending option to 11 occurrences.

1. Select **Search** > **Scheduled Searches**.
2. Select the scheduled searches that you want to edit.
3. Click the **edit** icon.

Delete a Scheduled Search

*You must have the **Manage Scheduled Searches** permission to schedule runs of a search.*

Select Search > Scheduled Searches > Scheduled.

You can delete a scheduled search at any time. After selecting **Delete**, the system prompts you to keep or delete the completed runs associated with the scheduled search.

NOTE: To cancel the deletion process, select the **X** that closes the dialog box, instead of selecting **Yes** or **No**.

Enable and Disable a Scheduled Search

*You must have the **Manage Scheduled Searches** permission to schedule runs of a search.*

Select Search > Scheduled Searches > Scheduled.

After creating a scheduled search, you can enable and disable it at any time.

1. Select the searches that you want to enable or disable.
2. Select **Enable** or **Disable**.

The **Status** column, which you can add with the *Manage Columns* option, displays the status of either **Enabled** (green) or **Disabled** (red).

Manage Completed Runs of a Scheduled Search

*You must have the **Manage Scheduled Searches** permission to schedule runs of a search.*

Select **Search** > **Scheduled Searches** > **Completed**.

After creating a scheduled search, you can view, delete, export, and filter the **completed runs** of that search. The results of a completed run are immutable. That is, if you edit the settings or query of a completed run, your changes do not affect the original results stored in the Completed list of scheduled searches.

View a Completed Run of a Scheduled Search

*You must have the **Manage Scheduled Searches** permission to schedule runs of a search.*

Select **Search** > **Scheduled Searches** > **Completed**.

The name of a completed run represents the name of the scheduled search name plus its start date and time.

When a run is in progress, Search displays the number of events received thus far and when the last chunk of data was received. Also, a flag beside the name of a completed run indicates that the settings for that scheduled search were changed before this run.

In the **Completed** tab, you can perform the following actions:

View all details for a completed schedule search

To view completed search results, click the Eye icon beside the search name.

Sort the data in columns

To change the sort order, click the column heading.

Reorder columns

To rearrange the order of the columns, drag each column to new position.

Search for a search keyword

To find a keyword, click in the field next to the Magnifying Glass icon (Search Keyword), enter a value, and the system displays your results automatically.

Hide and display columns

To hide and display a column, in the far right-corner of the window, click the Wrench icon (Manage Columns), and then select and clear the column name checkboxes.

Filter the data in columns

To filter scheduled searches based on *Status* and *Fieldset*, select the corresponding filter parameter. You can also filter completed scheduled searches based on a time range (custom and preset).

To filter the data for more specific results, in the far right-corner of the window, click the Funnel icon (Filters), and then select and clear the filter options. To filter the results based on execution time, set the date picker filter in the far right corner.

Create a report based on the run results

Each completed run has a unique Search Results ID, which allows you to create a report based on the search results.

To copy the ID, view the search results. Then either copy the ID from the URL or select the Copy icon above the Events table. To complete the process, follow the steps in Build a Report Using Search Results.

Delete Completed Runs of a Scheduled Search

*You must have the **Manage Scheduled Searches** permission to schedule runs of a search.*

Select **Search** > **Scheduled Searches** > **Completed**.

You can delete a completed run of a scheduled search at any time.

1. Select the completed runs that you want to delete.
2. Click the delete icon.

Export Completed Runs of a Scheduled Search

*You must have the **Manage Scheduled Searches** permission to schedule runs of a search.*

Select **Search** > **Scheduled Searches** > **Completed**.

You can export the completed run of a scheduled search to CSV format.

1. Click the CSV icon next to the name of the scheduled search that you want to export.
2. Alternatively, view the search, then select the CSV icon to export the results.

II Checking the Integrity of Event Data

*You must have the **Perform Event Integrity Check** permission to run a check.*

Select Admin > Event Integrity.

When investigating a security incident or hunting for threats, users expect that the search results provide valid and accurate data. However, the data that analysts rely on could be compromised by users who want to hide their activities or who maliciously change content. Data also is vulnerable to human errors, transfer errors, or loss and corruption caused by hardware or software issues.

NOTE: At this time, the Event Integrity Check searches Recon events only and does not include events migrated from Logger at this time.

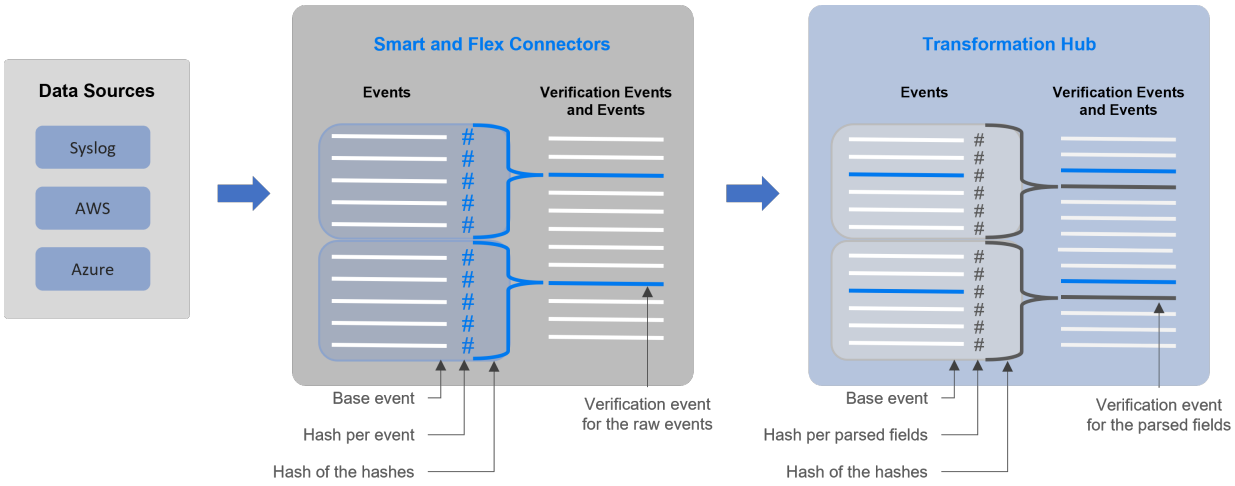
To validate that the event information in your database matches the content sent from SmartConnectors, run an **Event Integrity Check**. When you run the check, Recon searches the database for verification events received within the specified date range, then runs a series of checks to compare content in the database with information supplied by the verification events. The results of an Event Integrity Check help you identify whether event data might be compromised or incomplete. The event integrity checks can involve two different types of verification events: generated for *raw events* from SmartConnectors or for *parsed fields* from Transformation Hub. Both types of verification events can be used in the same environment for increased visibility into the integrity of the events in the database.

Understand the Event Integrity Check

Depending on how you have configured your SmartConnectors and Transformation Hub, the Event Integrity Check can verify raw event data and the parsed fields within an event, respectively. The check looks for events referenced by verification events in the database. The SmartConnectors group several events and compute a hash for each raw event in the batch. If you use Transformation Hub as a destination, it also groups events then generates a hash for the parsed fields within each event. The SmartConnector and Transformation Hub each generates a *hash of the individual hashes* to create a **verification event**. The number of events in a batch depends on how you configure the batch size setting for each connector. Note that SmartConnectors do not store the hashes for individual events.

Figure 1 (below) shows how events flow from your data sources to the SmartConnectors, which generate the verification events for the raw events. Then Transformation Hub generates verification events for parsed fields within each event.

Figure 1. *Process for generating verification events for an Event Integrity Check*



Each verification event includes the following items:

- a group of events with raw data or events with parsed fields
- an ordered list of the event IDs within the batch
- a crypto signature field representing the computed hash for that batch (the hash of hashes)

When you **run an Event Integrity Check**, the system performs the following actions for each verification event in the specified time range:

- Looks for the globally unique event ID (GEID) of each event referenced with the verification event.
- Generates hashes for the events within the base event.
- Generates a hash to represent the base events' hashes in the sequence provided by the verification event. You might call this the *generated hash of hashes*.
- Compares the generated hash of hashes to the hash of hashes in the crypto signature field that the SmartConnector or Transformation Hub created for the verification event.

Some base events could have been deleted on purpose to comply with data retention policies, depending on storage group configuration. When performing an event integrity check, the system reports these deleted events as missing base events.

Run an Event Integrity Check

An Event Integrity Check looks for verification events received within the specified date range. To reduce the chance of false-negative results, the check also searches for base events outside of the specified date range. For example, you specify a date range of 29 May to 5 June. The check finds several verification events within the date range; however, Verification Event A was created on 29 May and includes base events that occurred on 28 May. To prevent the verification event from failing, Recon will expand the search for base events beyond the specified dates.

NOTE: The check process can take a long time if it includes large amounts of data. Therefore you should run the check during off-peak hours, and limit the date range to include only the data that you are interested in.

1. Select Admin > Event Integrity.
2. Specify the Start Date and End Date for the range of data that you want to check.
   The *Start Time* for the check corresponds to the time when you select Run. For example, 5:29 pm.

   If the start and end dates encompass a time when the database is receiving events, it's possible to get a Missing Events notification. This occurs because the integrity check finds the verification events before ingesting their associated base events. We recommend that you avoid running the check against events currently being ingested by the database.
3. Select the timestamp type.
4. Click Run.

   If the Run button is disabled, a check is running currently. You can run one check at a time only. The check provides a Status update, as well as a showing when the check began and its specified date range.
5. (Optional) To cancel the check, click Cancel.

   Run as needed.
6. View the results.

View Event Integrity Check Results

To view the status and results, select Admin > Event Integrity.

The **Event Integrity Check** feature provides the following status and results:

- "View the Event Integrity Check Status" below
- "View Last Event Integrity Check Results Table" on the next page

View the Event Integrity Check Status

The **Event Integrity Check status** displays the date range from which the results are currently being checked, as well as the current status, including:

Note that, if the Recon system is busy, it might take a moment for the interface to indicate whether a check is running or has been canceled.

New
Indicates that you have never performed an Event Integrity Check; therefore, no results display.

In Progress
Indicates that an Event Integrity Check is running. If Run is disabled, a check is running currently. You can run one check at a time only.

Canceled
Indicates that you canceled an Event Integrity Check, and the system has completed the cancel task.

Canceling the check might take time to end the tasks that had been in progress.

Completed
Indicates that the Event Integrity Check has completed successfully. The results display in the results table.

Failed
Indicates that the Event Integrity Check failed to complete due to an error. The following table lists the failure categories and recommended remediation.

For this error...	Which indicates that...	You might want to...
No Data Found	The check did not find verification events in the selected date range	Enable Event Integrity in the SmartConnector or Transformation Hub
Insufficient Disk Space	The system does not have enough disk space to run the check	Reduce the Event Integrity Task Count setting in the CDF Management Portal Run the check when the system is less busy Change the Use Event Integrity Resource Pool setting to TRUE in the CDF Management Portal

Insufficient Resources	The system does not have enough memory to run the check	Reduce the Event Integrity Chunk Size setting in the CDF Management Portal Run the check when the system is less busy Change the Use Event Integrity Resource Pool setting to TRUE in the CDF Management Portal
Event Integrity Running	An Event Integrity Check is already running	Wait for the current check to finish or cancel the check in progress
Other errors	Depends on the situation	Review the details of the error in the Search Engine log

View Last Event Integrity Check Results Table

The **Last Event Integrity Check Results table** displays the date range from the last check as well as the details of the last check, including the following information:

NOTE: The Event Integrity Check might display the last result from another user. The last result might also display after logging out.

Base events checked
Represents the number of base events referenced by verification events found in the specified date range.

Intact events
Represents the number of base events referenced by verification events that passed the Event Integrity check.

Missing events
Represents the number of base events referenced by verification events where missing base events exist.

You might see this result when the integrity check finds the verification events before ingesting their associated base events. Try adjusting the start or end date for the check.

Tampering has been detected
Represents the number of base events referenced by verification events where the Event Integrity check failed to match the information provided by the verification events, such as due to a change in the data in the base event.

Missing hashes, incorrect hashes, or base events being out of sequence usually indicates that the data has been deliberately changed in an attempt to hide a user's activities.

Duplicate base event IDs

Represents the number of base events referenced by verification events where the Event Integrity check failed because more than one base event has the same globally unique event ID. This situation results in the Event Integrity check of the referenced base events to fail.

Duplicate verification events IDs

Represents the number of base events referenced by verification events where the Event Integrity check failed because more than one verification event has a globally unique event ID.

Configure Data Collection to Support Event Integrity Checks

An Event Integrity Check can review both raw event data and the parsed fields within an event, depending on how you configure SmartConnectors and Transformation Hub, respectively.

Configure a SmartConnector to Generate a Verification Event

The Event Integrity Check can verify the raw data received from a SmartConnector. You must configure the connector to generate a verification event for batches of events. This configuration allows you to verify that the raw data in the database matches the event captured at the moment that it occurred in your environment.

To configure SmartConnectors, see "Configuring a SmartConnector to Include a Verification Event for Raw Events" in the *Administrator's Guide for ArcSight Platform*.

Enable Transformation Hub to Generate Verification Events for Parsed Fields

The Event Integrity Check can verify the integrity of multiple parsed fields within an event that Transformation Hub received from a SmartConnector. For example, it verifies the *deviceProduct* and *sourceHostName* fields if they exist in an event. You might want to check these types of parsed fields as an alternative to verifying the raw event data. For example, your environment might not have the disk space, processing power, or network capacity to manage large amounts of raw event data forwarded from SmartConnectors.

You can configure this setting as you deploy Transformation Hub or at any time after deployment. For more information, see "Enabling Transformation Hub to Generate Verification Events for Parsed Fields" in the *Administrator's Guide for ArcSight Platform*.

III Analyzing Anomalous Data with Outlier Analytics

Select Insights > Outliers.

To help you identify anomalous behavior, the **Outlier Analytics** feature allows you to compare incoming *EventCount*, *BytesIn*, and *BytesOut* values to typical values for your environment. The EventCount, BytesIn and BytesOut values are aggregations over certain time periods for each host/IP address. Outlier Analytics can create and persist a baseline of host behavior. To derive outliers, you compare this baseline with aggregations over new time periods. Basically, the lower the anomaly score, the more likely the event is anomalous.

The analytics process allows you to define and build a model that identifies typical behavior for your environment, and then start a scoring process that evaluates incoming events against the model. The scoring process assigns a score that indicates the degree to which the incoming data varies from the typical behavior. Outlier Analytics displays the results of the scoring process in a table that shows the top anomalous hosts. From the table, you can generate charts that provide additional information about the anomaly.

The model specifies a subset of data from the Events table that represents typical behavior on your network. When you define the model, you can specify criteria that identify which device behaviors you want to model. For example, you might want to look for anomalous values in events that you receive from a specific device vendor or in systems on a specific subnet.

- "Generating Models to View Anomalous Data " below
- "Viewing Anomalous Data in a Model" on page 71

Generating Models to View Anomalous Data

*You must have the **Manage Outlier Models and Scoring** permission to define and build models.*

The model for Outlier Analytics defines typical *EventCount*, *BytesIn*, and *BytesOut* behavior for a set of IP addresses over a specified date range. You can define the criteria that identify which device behaviors you want to model. If you want a different model, you must define and build a new one.

- "Considerations for Generating Models" on the next page
- "Define and Build a Model" on the next page
- "Score a Model" on page 69
- "Delete a Model" on page 70

Considerations for Generating Models

Before defining and building a model, review the following considerations:

- You can create and delete models, but you cannot modify them.
- You can define as many models as you want, but you can only build one model at a time.
- When you define the model, you should set the date range wide enough (more than 168 hours) so that the model includes a variety of device behaviors, including cyclical patterns.
- Because the scoring algorithm is based on peer group analysis, Micro Focus recommends that you include similar devices in a model, based on activity. For example, you might want to create separate models for scoring endpoints, scoring DNS servers, and scoring databases.
- Each model definition applies a filter where Source Address != NULL.
- When you build a model, Outlier Analytics adds a lookup list of the same name to Configuration > Lookup Lists. You cannot view or edit this list. When you delete the model, the lookup list also gets deleted.
- The auto-complete functionality is temporarily unavailable in search input. The following columns are available for outliers filtering in the Search feature:

  - Source Address of *<Model_Name>*
  - Base Event Count Score of *<Model_Name>*
  - Bytes Out of *<Model_Name>*
  - Bytes In of *<Model_Name>*

    <Model_Name> corresponds to the model name being scored.

Define and Build a Model

When you build the model, the feature aggregates events from the Events table by IP address, day of week, and hour of day for each five-minute time increment.

The feature then calculates a sum for:

- *EventCount*
- *BytesIn*
- *BytesOut*

Outlier Analytics then creates conditional probability tables for sum of *EventCount*, sum of *BytesIn*, and sum of *BytesOut*.

To build a model:

1. Review the considerations for building a model.
2. Select Configuration > Outlier.
3. From the **Create Model Configuration** section, specify the criteria that you want to use for building the model.

   For example:

   - To define a specific subnet that represents a specific class of equipment (like server or data center), specify criteria similar to the following:

     `sourceAddress in subnet 10.1.1.0/24`.

   - To model outbound HTTP/HTTPS traffic, specify criteria similar to the following:

     `destinationPort = 80,443`
4. To more easily find the model later, give the model a name by typing over the Model Name.

   The model name can contain letters, numbers, and underscores only. The name must start with an alpha character and cannot exceed 19 characters.
5. For the time range, perform **one** of the following actions:

   - Accept the default time (Last 14 days)
   - From the drop-down menu, select a pre-defined value under Quick Ranges
   - From the drop-down menu, use the Custom Range fields to specify a time range
   - From the drop-down menu, select Dynamic, and then enter a dynamic date value

   Because of assumptions about the hours and days that comprise a model, do not specify a range that includes a shift in Daylight Savings Time. Also, the timestamp for events always represents the Normalized Event Time.
6. Click Create.

   The created model displays in the **Available Models** table with a status of Created.
7. From the **Available Models** table, select the model that you want to build.

   You can build only one model at a time.
8. Click Build.
9. To evaluate incoming events against the model, you must start the scoring process.

Score a Model

*You must have the **Manage Outlier Models and Scoring** permission to score a model.*

Select Insights > Outliers.

After you build a model, you can start a **scoring process** that evaluates incoming events against the model. The process assigns a score that indicates the degree to which the incoming data varies from typical behavior. By default, Outlier Analytics selects the current date as the scoring start date. You can only score one model at a time, but you can build another model while a different model is being scored.

To start the scoring process:

1. Select Configuration > Outlier.
2. From the **Available Models** table, select the model that you want to score.

   The model must be in Build Complete status before you can score it.
3. Select Score.
4. Select the date for which you want to start the scoring process, then click Start.

   Because of assumptions about the hours and days that comprise a model, do not use a model that you built with Daylight Savings Time data to score non-Daylight Savings Time data. Conversely, do not use a model that you built with non-Daylight Savings Time data to score Daylight Savings Time data.
5. (Conditional) To pause scoring because of performance or ingestion issues, select Pause.

   If you selected a date in the past to start the scoring process, the scoring job runs frequently to catch up to the current date. To allow any running scoring jobs to complete, wait 15 minutes before performing any other action such as deleting a model or resetting scoring.
6. (Conditional) To resume the scoring process from the point at which you paused it, select Resume.

   Alternatively, to restart the scoring process, select Reset.
7. To view the scored data when scoring completes, select Insights > Outliers.

Delete a Model

*You must have the **Manage Outlier Models and Scoring** permission to delete a model.*

When you delete a model, Outlier Analytics deletes the model definition and all scores that are based on that model.

1. Select Configuration > Outlier.
2. From the **Available Models** table, select the model that you want to delete.
3. Click Delete.

Viewing Anomalous Data in a Model

Select Insights > Outliers.

After you specify search criteria for the data that you want to view in the model, Outlier Analytics displays the top anomalous hosts that meet the criteria. When you select a host from the **Top Anomalous Hosts** table, the feature generates charts that provide more information about the anomaly scores.

The scores are calculated for five-minute chunks, so each source address can have multiple outlier scores each hour. When listing the top anomalous hosts, Outlier Analytics shows the maximum scores for each source address for each hour. If the specified search criteria included a filter, the scores represent results after being filtered.

- "Understand the Provided Analytics Charts" below
- "Investigate Anomalies Further" on the next page
- "View a Scored Model" on the next page

Understand the Provided Analytics Charts

Each Outlier Analytics model includes the following charts:

Outlier Scores History

Compares anomaly scores of the top anomalous hosts for one week from the specified End time.

Use this chart if you suspect a lateral attack. To view details about the score for a specific date and hour, hover over the corresponding area in the chart.

Selected Anomalous IP

Shows the anomaly score for the host that you selected for two weeks from the specified End time.

If you suspect that a host is under attack (for example, from ex-filtration malware), use this chart to study the behavior of the IP address over time and identify anomalous patterns. To view details about a data point, hover over it.

Selected Anomaly Hour

Compares the anomaly score for the host that you selected to the top 30 hosts for the anomaly hour.

If you suspect that a network is under attack (for example, a denial of service attack), use this chart to study the behavior of other top 30 hosts during the anomaly hour. To view more details, hover over a bar in the chart, click and drag to move within the chart, and double-click to reset it to its default view.

Investigate Anomalies Further

After you view the outlier data, you can use the action available from the grid rows in the **Top Anomalous Hosts** table to further investigate anomalies:

Search for <IP_Address>

Searches events for the host and time range for which you selected to view scoring data and displays the results on the **Search** page.

View a Scored Model

1. Select Insights > Outliers.
2. Specify the outlier metric that you want to view: EventCount, BytesIn, or BytesOut.
3. For the search query, specify any of the following criteria that you want to apply to the data:
   - Base Event Count Score of
   - Bytes In Score of *<Model_Name>*
   - Bytes Out Score of *<Model_Name>*
   - Source Address of *<Model_Name>*
   - Start Time of *<Model_Name>*
4. Click Detect.
5. Specify a valid time range to view the scored data.

   The time range selector displays the valid date range in the date selection area to ensure that you specify a valid date range. Scoring data is performed hourly so the time range for detection is in an hourly format (YYYY-MM-DD HH). End time hour is inclusive. If the end time is 2019-05-21 05, the scoring data from 2019-05-21 05:00-06:00 will be included. To help you select time range for detection, the time range selector displays Score Available Range.
6. Wait while Outlier Analytics processes the request and generates the **Top Anomalous Hosts** table and the **Outlier Scores History** table.

CAUTION: If Outlier Analytics retrieves a large amount of data, the search might pause. You must allow the feature to populate the **Top Anomalous Hosts** table before you click Play to resume the search. Otherwise, the table will not be displayed.

7. (Optional) To generate the remaining charts, select a row in the **Top Anomalous Hosts** table.
8. (Optional) To use the filter action in your investigation, complete the following steps:
   a. Right-click a row in the grid.
   b. Select Search for <IP_Address>.

IV Managing the Quality of Your Data

Select Insights > Data Quality.

Data Quality Dashboard provides detailed information about the gap between Device Receipt Time from the raw event itself versus the Normalized Event Time and Database Receipt Time. Data Quality Dashboard identifies the sources that cause issues with the data. Based on the information analyzed through the Data Quality Dashboard, you can accurately mitigate the problem. This feature also provides history of your data over time.

- "Understanding the Data Quality Insights" below
- "Understanding How Data Quality is Calculated" on the next page
- "Analyzing Data Quality" on page 76

Understanding the Data Quality Insights

Content in the Data Quality Dashboard is divided into the following categories that represent how big the gaps are among Database Receipt Time (dBRT), Device Receipt Time (DRT), and Normalized Event Time (NET):

- Active Events
- Future Events
- Past Events

Active Events

Indicates that your events have a timestamp within the database's active time frame where `NET - DRT = 0`. The Data Quality Dashboard presents active events in sub-categories based on the following time gaps between DRT and dBRT:

Sub-category	Description	Formula
Within 1 Minute	Data received in the ArcSight database with less than a one-minute gap	`dBRT- DRT = values between -60000 and 60000` milliseconds
Hour Ahead	Data received between one minute and an hour before DRT	`dBRT- DRT = a value between -3600000 and -60001` milliseconds
Hour Behind	Data received between one minute and an hour after DRT	`dBRT- DRT = a value between 60001 and 3600000` milliseconds

Sub-category	Description	Formula
Day Ahead	Data received between one and 24 hours before DRT	`dBRT- DRT = a value between -86400000 and -3600001` milliseconds
Day Behind	Data received between one and 24 hour after DRT	`dBRT - DRT = a value between 3600001 and 86400000` milliseconds
Week Behind	Data received between one and seven days after DRT	`dBRT - DRT = a value between 86400001 and 604800000` milliseconds

Future Events

Indicates that your events have a future timestamp where `NET - DRT < 0`. The Data Quality Dashboard presents future events in sub-categories based on the following time gaps between DRT and dBRT:

Sub-category	Description	Formula
Week Ahead	Data received between one and seven days before DRT	`dBRT - DRT = a value between -604800000 and -86400001` milliseconds
Far Future	Data received more than a week before DRT	`dBRT - DRT < -604800001` milliseconds

The **Far Future** critical category helps identify events that fall well outside the most accepted variance range.

Past Events

Indicates that events have a past timestamp where `NET - DRT > 0`. The Data Quality Dashboard presents past events in a sub-category based on the following time gap between DRT and dBRT:

Sub-category	Description	Formula
Distant Past	Data received more than a week after DRT	`dBRT - DRT > -604800001` milliseconds

The **Distant Past** critical category helps identify events that fall well outside the most accepted variance range.

Understanding How Data Quality is Calculated

Data Quality is calculated and aggregated every one hour, including all events that arrive in the database within the same hour. For example, the aggregated information at 10:00 AM includes all data from 10:00:00.000 to 10:59:59.999, inclusively. The time of the aggregation process depends on when the ArcSight Database was installed or upgraded:

- During a fresh installation, the process creates a new table to store Data Quality overtime with source information. The feature schedules the aggregation process at the tenth minute of every hour. For example, if a fresh install was performed at 9:15:00 AM, the aggregation would be scheduled to execute at 10:10:00 AM and every one hour after that.
- After an upgrade, previous data will be dropped because they are no longer relevant to new categories. For example, if an upgrade was performed at 9:15:00 AM, the aggregation would be scheduled to execute at 10:10:00 AM to aggregate all events from 9:00:00.000 to 9:59:59.999 AM, inclusive. Then it will run every one hour after that.

If you switch to a different database, you would need to wait for a few minutes before accessing the Data Quality page again.

Analyzing Data Quality

Select Insights > Data Quality.

The Dashboard provides the following visualizations to help you gain insight into quality of your data.

Date Picker Filter

Provides options to filter the time range for the entire Data Quality Dashboard page, including built-in Custom Range and Quick Ranges. By default, the Dashboard displays data per the Last 7 days setting. If the Cron Job has not been run yet, the charts would display no data.

Data Timeseries

Represents, in a stacked area chart, how data is distributed among the Categories by percentage over time.

Source Agents

This visualization group consists of the following components:

- **Category Selector**

  Displays data sources in each of the 12 Data Categories. *Far Future* is the default selection.

- **Top 10 Agents from Future Events**

  Represents the percentages of up to 10 top agents with the greatest amount of events under the selected Data Categories. To see the IP address, host name, and number of events of each source, hover over each donut piece. If you click a donut piece, the Hourly Event Volume chart displays more values.

- **Hourly Event Volume**

  Shows, in a bar chart, the number of events from a source that contributed to the selected Data Categories. If available, the source with the highest number of events will be displayed by default.

V Managing and Importing Stored Data

*You must have the **Manage Storage Groups** permission to use this feature.*

Search performance can be affected by your environment's set up and the way that your data is organized. To enable faster search times, you can configure Recon to organize data into storage groups, which represent partitions in the ArcSight database.

These storage groups can support compliance requirements for data retention policies, such as those for the Payment Card Industry Data Security Standard (PCI DSS). For example, you might be required to retain certain data for 12 to 24 months. You can instruct Recon to purge data that is older than a certain number of months. By deleting data, you reduce the amount of content within the database and improve search performance.

Managing Your Stored Data

*You must have the **Manage Storage Groups** permission to use this feature.*

Select Configuration > Storage.

The **Storage Information** list provides an overview of all available storage groups. You can have up to 10 storage groups, each with specific retention periods and query filters. To find a storage group, use the Search field.

Use Storage Groups to Organize and Retain Data

You can divide data into **storage groups**, which allows you to partition the incoming events data and provide different retention periods, based on the query filter. Because you can set data retention policies per storage group, you can retain certain high volume events for a short time period and other important events for longer time period.

The **query filter** enables you to associate a storage group with specific compliance requirements, business needs, or search activities. Your specified query filters direct events to the correct storage group. For example, one group might have a filter for categoryDeviceGroup =/ Firewall and another for severity >= 7. If an event does not match any of the active filters, the event gets sent to the *Default Storage Group*. You cannot change the name, query, or rank of this built-in group.

By default, the maximum value for retaining events in the *Default Storage Group* is 12 months. However, the license for your deployed product might require a lower maximum value, such as 30 days. For more information about how deployed products affect data retention policies, see "Understanding License Keys" in the *ArcSight Platform Administrator's Guide*.

The Apply Changes to System option at the top of the Storage Groups page indicates that one or more groups have been modified but the changes need to be applied.

- "Create a Storage Group" below
- "Direct Events to the Correct Storage Group" below

Create a Storage Group

You can have up to **10 storage groups**, including the provided *Default Storage Group*.

1. Select **Configuration** > **Storage**.
2. Click the add icon +.
3. Enter a name for the storage group.

   CAUTION: You cannot change the name after you create the group.

   The name cannot include special characters other than a hyphen (-).
4. Enter a query with which to filter the incoming events into this storage group.

   For example: categoryDeviceGroup='/Firewall' or categoryDeviceGroup='/IDS'.

   The query can include parentheses, quotes, and single quotes.
5. For the storage group's status, indicate whether to activate the group.
6. (Optional) For **Delete Data Older than**, enter the age of data, in months, that you want to purge from the storage group in the database.
7. Click **Save**.
8. Apply your changes.

Direct Events to the Correct Storage Group

For efficient data retrieval, the system matches each incoming event with the query filter for a single, active storage group. However, an event could be associated with the rules of more than one group. When an event matches with multiple storage groups, the system **assigns the event to the highest ranked group**.

For example, *if Event_29* matches the query filter for the storage groups ranked 3, 5, and 6, then the system assigns the event to the group that is ranked 3. If an event does not match any of the active filters, the system sends the event to the *Default Storage Group*.

You can change the ranking of storage groups to ensure that the system places events in the best location.

1. Select **Configuration** > **Storage**.
2. From the **Storage Information** table, drag each storage group up or down to the preferred priority position.

   The system always places the *Default Storage Group* in the lowest ranked position.

Activate and Deactivate Storage Groups

Recon allows you to have up to **10 storage groups**, including the provided *Default Storage Group*. To inactive to prevent new events from being sent to the group, change a storage group's status. For example, you might no longer need a particular storage group or find that you have changed the filters and functionality of that group from its original purpose. Rather than continuing to modify an existing group, you can deactivate it. Alternatively, you might want to activate a storage group only during certain periods of time.

Although you deactivate a group, the deletion settings for that group remain in effect.

1. Select Configuration > Storage.
2. Select the storage group that you want to activate or deactivate.
3. To edit the group's settings, click the icon.
4. For Group Status, slide the indicator left or right.

   Activated groups display a status of Active.
5. Click Save.

Change the Settings of a Storage Group

After creating or modifying storage groups, you must apply the changes. You can modify multiple groups before applying your changes.

- "Modify a Storage Group" below
- "Apply Your Changes to a Storage Group" on the next page

Modify a Storage Group

You can modify a storage group at any time.

1. Select Configuration > Storage.
2. Select the storage group that you want to modify.
3. Click the pencil icon .
4. For Group Status, slide the indicator left or right.
5. Activated groups will display a status of Active.
6. Click Save.
7. "Apply Your Changes to a Storage Group" below.

Apply Your Changes to a Storage Group

Select Configuration > Storage > Apply Changes to System.

When you change the query filter, status, or rank of a storage group, your changes do not go into effect until you apply the changes. The following considerations affect how your changes are applied:

- If you modify the query filter, Recon will begin adding events that match the updated filter. However, the storage group retains all currently stored events associated with the previous filter. The retention policies continue to apply to all events within the group.
- If you do not want the storage group to have both sets of events, you can create a new storage group for the updated query filter, then deactivate the older storage group.
- On the first day of the month, Recon deletes events matching the retention policies of the storage groups. For example, on March 15, you change the deletion time to three months from four months. On April 1, Recon begins deleting all data older than three months.
- While changes are being applied, you cannot create or modify a storage group.

Use Storage Group Queries in a Search

Search allows you to include a storage group in a query. Rather than entering the query filter of a storage group again in Search, specify the following for your Search query: Storage Group = Firewall Events. By specifying the storage group, you limit the search to that storage group's partitions only, thus improving search performance.

Configure Retention Policies for Your Data

Events are stored in their assigned storage groups in the ArcSight database. Over time, the storage system can retain unneeded or outdated data. To preserve space in the database and improve data retrieval from storage groups, you can configure the database to remove events older than a certain number of months. For example, your data retention policy might expect your system to purge certain data, such as DNS logs that are older than 24 months.

When setting the policies for storage group retention and disk space utilization, do not allow your disk space utilization to increase above 90%. Running out of disk space can reduce the performance of searches due to increasing fragmentation. If such a situation continues to where there is no space left, then the database cannot ingest new data.

Delete Old Data from Storage Groups

Events are stored in their assigned storage groups in the ArcSight Database. Over time, the storage system can retain unneeded or outdated data. To preserve space in the database and improve data retrieval from storage groups, you can configure the database to remove events older than a certain number of months. For example, the data retention policy for your organization might expect data older than 24 months to be purged. This process **deletes data from the database**.

The system automatically applies all deletion settings on the first day of the month at 2:10 a.m.

1. Create or modify a storage group.
2. For Delete Data Older Than, enter the age of data, in months, when you want old events to be deleted.

   By default, the maximum value for retaining events in the Default Storage Group is 12 months. However, the license for your deployed product might require a lower maximum value, such as one month. In Recon, you can choose Never Expire for a long-term storage option.

   Ensure that your retention policy takes into consideration the maximum size of your storage groups and database. Also, consider that, in deleting events, the policy might affect results of an Event Integrity Check.
3. Click Save.
4. Apply your changes.

Set the Retention Policies for Imported Logger Data

You can have up to 10 storage groups overall (including the Recon and Logger migrated). Exceeding this quantity will likely affect the performance.

To manage the storage and expiration of the recently imported data from Logger to Recon, the retention policy will be automatically enabled for the logger event data. You will not need to manually direct events to a certain storage group and implement additional retention policies, but rather take advantage of the same storage rules set in Logger. You can update and view the

retention policy strictly from the Logger UI. Likewise, Recon will reflect the information added prior to the import.

Once the logger metadata is imported to Recon from one or more logger nodes, an storage logger table is populated. Recon will only consider the values added in the maximum archives age. These values are converted from days to months (30 days equal to 1 month) unless the process is disabled (value of -1). To align with Recon's retention cycle, the decimal values are disregarded, and instead, the integer (rounded to the highest number) is set as the maximum period for archiving.

Logger event data with more than one month old will be considered for the retention cycle. The retention process is done periodically causing some events to not be deleted immediately after reaching the maximum period. If Logger processes remain active, the retention will be managed by Logger based on the storage configuration. For further details on how storage groups are handled in Logger, see the Storage Groups section in Chapter 5 of the *Logger Administrator's Guide*. Otherwise, if Logger services have been shut down, the ArcSight Database will manage and execute the retention policy in the ArcSight Database.

Importing Event Data From Logger

Not available in a SaaS environment.

You can view ArcSight Logger event data collected over time. If you have ArcSight Logger and Recon in your network infrastructure, you can search logger data using Recon capabilities. To do so, you must import the Logger events stored in Logger archives and live events. The process requires you to first import the metadata, then the event data. Before you begin searching Logger data, ensure that the data migrations have completed.

The following topics also provide information related searching and managing the imported Logger data:

- "Search Event Data from Logger" on page 7
- "Set the Retention Policies for Imported Logger Data" on the previous page

Checklist: Migrating Logger Data

Not available in a SaaS environment.

Use the following checklist to migrage event data from Logger for including in a Search. You must perform the tasks in the listed order.

	Task	See
❑	1. Review the prerequisites and considerations for migrating event data from Logger to the ArcSight Database	"Understand the Prerequisites for Importing Logger Data" below
❑	2. Archive all live data in Logger	"Archive Live Logger Data " on page 86
❑	3. Change the Maximum Live Data Age for each storage group	"Set the Maximum Age of the Live Data" on page 86
❑	4. Import the metadata	"Import Metadata for Logger Data" on page 86
❑	5. (Conditional) If credentials were changed after importing metadata, update the username and password information, and then update the Logger registration	"Update the Logger Registration" on page 87
❑	6. Import the Logger data that you want to search	"Import Logger Data" on page 88

Understand the Prerequisites for Importing Logger Data

Not available in a SaaS environment.

Make sure you comply with these requirements and considerations before importing the Logger data. Only archived events from the current Logger instance are imported to Recon. The system does not import configuration and logger peers data.

- "Logger " below
- "ArcSight Platform " on the next page
- "ArcSight Database " on the next page
- "Metadata Import" on the next page
- "Logger Data Import" on the next page

Logger

- Server power needs to be on for importing the metadata.
- Recon and Logger can be in different servers. However, the Logger server must have the VSQL Client driver. For more information, see the *Logger Administrator's Guide*.
- Admin user must have SSH credentials.
- Logger services will be disabled in the Logger installation after you migrate the metadata.

ArcSight Platform

You must have the *Logger Data Migration* permission. This is assigned by default to the System Admin role. Users with the default analyst role can execute searches after the data import completes.

ArcSight Database

- Logger and Recon (including the ArcSight Database) can be installed in the same machine.
- Run the `logger_migration_preconfig.sh` script located by default in the `/opt/arcsight-db-tools/scripts/` directory.

Metadata Import

- Before migrating the metadata, you must archive all live data in Logger.
- After archiving the live Logger data, change the maximum age of the live data for each storage group in Logger to 1 day.
- When you import the metadata, the Logger server must be accessible.

Logger Data Import

- Before you can migration Logger data, you must import the metadata that defines it.
- If you plan to import from several different Loggers, run the imports sequentially.
- The username and password you use to import Logger data must match the OS credentials set in Logger.
- If credentials have been changed after importing metadata, make sure to update the username and password information before importing data. Otherwise, an error message will be displayed. You will also need to update the Logger registration.
- Select a data-time range different than the one already imported. To confirm the host's start and end dates already available in Recon, see the migration table.

Prepare Live Logger Data

Not available in a SaaS environment.

Before you can migrate Logger data to the ArcSight Platform, you must archive the live data and set the maximum age for the data in each storage group that you archive.

- "Archive Live Logger Data " on the next page
- "Set the Maximum Age of the Live Data" on the next page

Archive Live Logger Data

You must archive all live data in Logger. You can manually add archives to a storage group that has a mount configured.

1. To configure an archive location in Logger, select Configuration > Storage > Archive Storage Settings.
2. To get the instructions for mounting the archives in the database, run the following command where you installed Logger:

```
wget PATH_NOT_DEFINE_YET
chmod +x ./loggerToReconConstructMounts
./loggerToReconConstructMounts.sh $<install_logger_path>
```

3. Run the instructions received from Step 2 to mount the archive in the following location:

   `/opt/LOGGER_<logger_IP_without_periods>`

   For example, if the Logger IP address is 12.345.67.890, then the directory should be `/opt/LOGGER_1234567890`.
4. Complete the instructions for ensuring that the database user can access the archive directory.

Set the Maximum Age of the Live Data

Although you might archive the live data, the system does not delete the events from the local storage until the events (and their related indexing information) age out due to the Maximum Live Data Age. You should configure the maximum age of the live data in the storage groups.

1. In Logger, select Configuration > Storage > Storage Groups.
2. For each storage group that you want to modify, select the Edit icon.
3. For **Maximum Live Data Age**, specify 1 day.

Import Metadata for Logger Data

Not available in a SaaS environment.

Select Configuration > Import Logger Data > Logger Metadata Import.

This topic applies only to Logger processes soon-to-be shut down

Ensure that you have reviewed the prerequisites and considerations.

The Logger **metadata** represents the detailed information that each event needs to be correctly scanned, allocated to the storage group of your selection, and consumed in Recon.

Metadata contains all the information of the archives from a particular Logger. You can migrate the Logger metadata to the ArcSight Database directly from the **Logger Metadata Import** page.

You import the metadata once for each Logger whose processes are soon to be shutdown. Make sure to import the metadata before importing the Logger data as this is the first step to view and consume logger events.

- "Register a Logger " below
- "Import the Metadata" below
- "Update the Logger Registration" below

Register a Logger

Before importing the metadata, make sure to add the Logger details for the import process.

1. Select **Configuration > Import Logger Data > Logger Metadata Import**.
2. Click the + icon.
3. Add the Logger details such as:
   a. Host: Logger IP address or host name
   For example, `12.345.67.890` or `logger6.extremelyfocused.com`
   b. Host Username: OS username
   c. Host Password: OS password
4. Click **Save**. Otherwise, click **Cancel**.

Note: You can remove Logger registration if no data has been imported. To delete the Logger registration, click the delete icon (trash can).

Import the Metadata

After successfully registering the Logger, check the box next to it and then click the import icon.

The system be imports and stores the metadata in Recon. However, ensure that you also import the Logger data so that you can view the events in Recon.

Update the Logger Registration

The Logger processes status, host username, and password can be updated after the Logger registration or metadata import. However, these values cannot be updated while an import is in progress.

1. Select **Configuration > Import Logger Data > Logger Data Import**
2. Check the box next to the Logger host and click the pencil icon.
3. Update the values accordingly.

   Ensure that the username and password that you use match the OS credentials set in Logger.
4. Click **Save**. Otherwise, click **Cancel**.

Import Logger Data

Not available in a SaaS environment.

Select Configuration > Import Logger Data > Data Import.

This option will allow you to bring events from a Logger instance to Recon and perform searches over the migrated data. Please consider to only migrate the time ranges needed since this is both time and resources consuming process.

- "Import Data" below
- "Review Migration Details" on the next page
- "Resume an Incomplete Migration" on page 90
- "Delete Incomplete or Failed Migrations" on page 90

Import Data

Before importing data, ensure that you have reviewed the prerequisites and considerations.

1. Select **Configuration** > **Import Logger Data** > **Logger Data Import**.
2. Click +.
3. Select the Logger host of your preference.

   You can choose only one host at a time.
4. Specify the time range that you want to import.
   - The time range is based on receipt time.
   - The migration only allows you to migrate a minimum time range of 1 day.
   - Specify a date in the past. You cannot import data for future dates as it will importno events and will cause issues when you try to import new data again.
   - Overlapping dates will cause an error message. If this is not the first import of this Logger instance, ensure to select a time range different than the one already imported.

5. Click Import.
6. To check the import progress, view the Import Status column.

   The import will take a considerable amount of time, based on the quantity of events that are present in the time range selected.
7. (Optional) If the import is interrupted, you can attempt to resume the process.

   Alternatively, you can delete an incomplete migration.

Review Migration Details

The migrations table will display the most relevant information of all the imports executed. For each migration, the system registers the following details:

Logger Host
Represents the Logger IP address or host name. For example, `12.345.67.890` or `logger6.extremelyfocused.com`.

Data Start Date
Indicates the absolute date of the earliest possible event.

Data End Date
Indicates the absolute date of the latest possible event.

Import Date
Indicates the migration date and time displayed in the ArcSight Database timezone.

Import Status
Indicates the status of the import process:

- **Start Migration**: Confirms the Logger is reachable and can properly communicate with Recon.
- **In progress**: Import is still in progress. PostgreSQL is downloaded to allow data to be extracted, read, and sent to the ArcSight Database.
- **Complete**: Successful import execution.
- **Failed**: Unavailable connections due to an unreachable Logger. Ensure that you review the prerequisites before importing data.

Event Count
Indicates the number of events migrated. This number increases automatically as the process continues.

Logger Host User Name
Indicates the OS username associated with the Logger host.

Data Import ID

Represents the unique identifier for the event migration. You must have this value to delete a migration.

To review details about the executed migration, see the logs in the `opt/vertica/udfs/datamigration/logs/` directory.

After events have been imported, the retention policy will be managed by Logger or Recon depending on the state of the Logger processes.

Resume an Incomplete Migration

You can resume an Incomplete migration. The process starts from the last point of migration so you do not lose the data previously migrated.

1. Select the migrations that you want to resume.
2. Click .

Delete Incomplete or Failed Migrations

It's possible that a migration might fail to complete. For example, the status is Failed or indicates that the migration is Complete but it contains no events. In these types of scenarios, you can delete the migration, then try again.

1. Select the migrations that you want to delete.
2. Click .

V Ensuring Data Compliance

Recon provides **Compliance Packs** that contain reports and dashboards to help you comply with a broad set of legal and governmental regulations that require your enterprise to organize and manage sensitive data and institute a strong IT governance program. Designed around industry best practices, these packages provide a comprehensive method for assessing and monitoring internal controls, such as access control changes, administrative activity, log-in monitoring, and change and risk management. The packages automatically map these technical checks to the relevant standard using policy and risk-relevant operational context so you can focus on key services and business processes and address critical audit points.

You must purchase, then import each Compliance Pack to the Reports Portal repository. For more information about the packs, see the Recon documentation site.

Ensuring Compliance with GDPR Standards

Select Reports > Portal > Repository > Standard Content > GDPR.

The European Union (EU) adopted the General Data Protection Regulation (GDPR) to ensure that businesses and organizations protect individuals' data privacy and security. If your enterprise processes the personal data of EU citizens or residents or offers goods and services to such individuals, then you must comply with the GDPR. The regulation sets out standards for any action, automatic or manual, that processes a person's data. These standards include requiring that data controllers and data processors – the individuals in your enterprise or third-party organizations who control, manage, or make decisions about data processing – must be able to demonstrate that they are GDPR compliant.

To help you comply or prove compliance with GDPR, Recon provides the **Compliance Pack for GDPR**. For more information about adding the pack to the Reports repository, see the *Solutions Guide for ArcSight Recon Compliance Pack for GDPR*. The guide includes information about identifying assets that must comply with GDPR.

This package includes the following dashboards and reports, organized by GDPR objectives:

Category	Dashboards	Reports
Access Activity - Access Activity	After Hours Access Activity on GDPR Systems Overview Authorization Changes on GDPR Systems Overview Failed Access Activity on GDPR Systems Overview Failed Access Relationship on GDPR Systems Overview Failed Access Activity by GDPR Asset Failed Access Activity on GDPR Systems by User	After Hours Access Activity on GDPR Systems Summary Authorization Changes Summary on GDPR Systems Failed Access Activity by GDPR Assets Failed Access Activity on GDPR Systems Summary Failed Access Activity on GDPR Systems by Users
Access Activity - Regulatory Exposure	n/a	Potential Regulatory Exposure on GDPR Systems
Access Activity - Threat User Analysis	n/a	Admin Activity from Compromised GDPR System Anti-Virus Disabled on GDPR Systems Summary Audit Log Cleared on GDPR Systems Summary Threats Executed against GDPR Systems Summary
Admin Activity	n/a	User Creations on GDPR Environment User Deletions on GDPR Environment Users Added to a Group on GDPR Environment Users Removed from a Group on GDPR Environment

Category	Dashboards	Reports
Attack Surface Analysis - Attack Surface Identification	High Risk Vulnerabilities on GDPR Systems Information Leakage Vulnerabilities on GDPR Systems Password and Authentication Weaknesses on GDPR Systems SQL Injection Vulnerabilities on GDPR Systems SSL or TLS Vulnerabilities on GDPR Systems Vulnerabilities on GDPR Systems Overview Vulnerable GDPR Assets by Vulnerability Type XSS Vulnerabilities on GDPR Systems	High Risk Vulnerabilities on GDPR Systems Information Leakage Vulnerabilities on GDPR Systems Password and Authentication Weaknesses on GDPR Systems SQL Injection Vulnerabilities on GDPR Systems SSL or TLS Vulnerabilities on GDPR Systems Unpatched GDPR Systems Vulnerability Summary by CVE ID Vulnerability Summary by GDPR Asset Vulnerability Summary on GDPR Systems XSS Vulnerabilities on GDPR Systems
Attack Surface Analysis - Security Controls Risk Identification	DoS Attacks Against GDPR Systems	DoS Attacks Against GDPR Systems
Corporate Governance	Access Activity on GDPR Systems Overview Geo Access Activity on GDPR Systems Overview Physical Access Activity on GDPR Systems Overview	Access Activity on GDPR Systems Summary After Work Hours Physical Access Activity on GDPR Systems Summary Physical Access Activity on GDPR Systems Summary

Category	Dashboards	Reports
Regulatory Exposure	Data Flow to GDPR Systems Data Flow from GDPR Systems Data Flow from GDPR Systems to non EU Data Flow from non EU to GDPR Systems GDPR Systems Communication with non EU Countries GDPR Systems Communication Overview High Risk Events on GDPR Systems Overview Policy Violations on GDPR Systems Overview Threat Relationship on GDPR Systems Overview Threats on GDPR Systems Overview	Data Flow from GDPR Systems Summary Data Flow from GDPR Systems to non EU Summary Data Flow from non EU to GDPR Systems Summary Data Flow to GDPR Systems Summary High Risk Events on GDPR Systems Summary Policy Violations on GDPR Systems Summary Threats on GDPR Systems Summary

Category	Dashboards	Reports
Threat Analysis - Data Store Risk	n/a	Attacks Against Databases on GDPR Systems Cassandra Vulnerabilities on GDPR Systems CRM and ERP Vulnerabilities on GDPR Systems Database Configuration Changes on GDPR Systems Database Weaknesses on GDPR Systems Elasticsearch Vulnerabilities on GDPR Systems IBM Db2 Vulnerabilities on GDPR Systems MariaDB Vulnerabilities on GDPR Systems Microsoft SQL Server Vulnerabilities on GDPR Systems MongoDB Vulnerabilities on GDPR Systems MySQL Vulnerabilities on GDPR Systems Oracle Vulnerabilities on GDPR Systems PostgreSQL Vulnerabilities on GDPR Systems Redis Vulnerabilities on GDPR Systems
Threat Analysis - Internet	Malware Found on GDPR Systems MITRE ATT&CK on GDPR Systems by GDPR Asset MITRE ATT&CK on GDPR Systems by MITRE ID MITRE ATT&CK on GDPR Systems Overview MITRE ATT&CK Relationship on GDPR Systems Overview	Firewall Blocked Events in GDPR Environment Information Leaks from GDPR Systems Malware Found on GDPR Systems

Access Activity

Select Reports > Portal > Repository > Standard Content > GDPR > *Reports* or *Dashboards* > GDPR Access Activity.

As a data controller or data processor, you need to track access to GDPR systems, which collect, store, transfer, use, and organize data related to EU citizens or residents.

Category	Dashboards	Reports
Access Activity	After Hours Access Activity on GDPR Systems Overview Authorization Changes on GDPR Systems Overview Failed Access Activity on GDPR Systems Overview Failed Access Relationship on GDPR Systems Overview Failed Access Activity by GDPR Asset Failed Access Activity on GDPR Systems by User	After Hours Access Activity on GDPR Systems Summary Authorization Changes Summary on GDPR Systems Failed Access Activity by GDPR Assets Failed Access Activity on GDPR Systems Summary Failed Access Activity on GDPR Systems by Users
Regulatory Exposure	n/a	Potential Regulatory Exposure on GDPR Systems
Threat User Analysis	n/a	Admin Activity from Compromised GDPR System Anti-Virus Disabled on GDPR Systems Summary Audit Log Cleared on GDPR Systems Summary Threats Executed against GDPR Systems Summary

Access Activity

Select Reports > Portal > Repository > Standard Content > GDPR > *Reports* or *Dashboards* > GDPR Access Activity > Access Activity.

To comply with GDPR, you might want to track accounts that have been accessing systems that store or process users' personal data. A high number of failed access attempts can indicate malicious activity. Also, to prevent a malicious user from accessing sensitive data, you should know when and what type of authorization changes occur on those systems.

After Hours Access Activity on GDPR Systems Summary

Reports the number of times and the accounts that accessed GDPR systems outside of regular hours, such as accessing a server on the weekend. The table provides results by the account and its associated server, and the target server accessed. This report relates to GDPR Articles 5 and 25 and Recital 49.

By default, the report uses the following time ranges to check for "after hours" access:

- 12 a.m. to 7 a.m. Monday through Friday
- 18 p.m. (6 p.m.) to 12 a.m. Monday through Friday
- All day on Saturday and Sunday

However, you can modify the time ranges by editing the filters for the report. The time range uses 24-hour values.

Authorization Changes Summary on GDPR Systems

Reports the number and type of authorization change events that occur on GDPR systems over time. The table provides results by the number of times each account made a change, the type of change, the affected GDPR system, and the outcome of the change such as 'success.' This report relates to GDPR Articles 5, 18, 24, 29, and 32 and Recital 39.

Authorization Changes Summary on GDPR Systems

Reports the number and type of authorization change events that occur on GDPR systems over time. The table provides results by the number of times each account made a change, the type of change, the affected GDPR system, and the outcome of the change such as 'success.' This report relates to GDPR Articles 5, 18, 24, 29, and 32 and Recital 39.

Failed Access Activity by GDPR Assets

Reports the number of times access to a GDPR asset failed. The chart shows the top GDPR assets with failed access attempts. For each GDPR asset, the table provides results by the number of failed events, user accounts with failed attempts, and the number of IP addresses associated with the failed events. This report relates to GDPR Articles 5 and 25 and Recital 49.

Failed Access Activity on GDPR Systems by Users

Reports the number of times users failed to access a GDPR system. The chart shows the users with the most failed access attempts. The table provides results by number of failed events, GDPR assets affected, and IP addresses associated with the failed events for each user with a failed attempt. This report relates to GDPR Articles 5 and 25 and Recital 49.

Failed Access Activity on GDPR Systems Summary

Reports the number attempts that failed to access a GDPR system over time. For each failed attempt, the table provides results by user account, the account's IP address and country, the target server's IP and host name, and the number of failed events. This report relates to GDPR Articles 5 and 25 and Recital 49.

After Hours Access Activity on GDPR Systems Overview

Provides, in charts and a table, an overview of accounts that access GDPR systems outside of regular hours, such as accessing a server on the weekend. You can view the targeted systems, users, and source IPs that generate the most events. This dashboard relates to GDPR Articles 25, 30, and 32 and Recital 82.

By default, the dashboard uses the following time ranges to check for "after hours" access:

- 12 a.m. to 7 a.m., Monday through Friday
- 18 p.m. to 12 a.m., Monday through Friday
- All day on Saturday and Sunday

Authorization Changes on GDPR Systems Overview

Provides an overview of events that indicate authorization change attempts on GDPR Systems. Relevant to GDPR Articles 5, 18, 24, and 32 and Recital 39.

Failed Access Activity by GDPR Asset

Provides, in charts and a table, an overview of failed access activity on the specified GDPR systems. This dashboard relates to GDPR Articles 5 and 25 and Recital 49.

You must specify at least one IP address, Mac address, or host name in lowercase.

Failed Access Activity on GDPR Systems by User

Provides, in charts and a table, an overview of failed access activity by user. This dashboard relates to GDPR Articles 5 and 25 and Recital 49.

You must specify at least one user account in lowercase.

Failed Access Activity on GDPR Systems Overview

Provides an overview of failed access activity on GDPR systems. This dashboard relates to GDPR Articles 5 and 25 and Recital 49.

Failed Access Relationship on GDPR Systems Overview

Provides an overview of the relationship between source and destination addresses and users on events that indicate a failure login activity on GDPR systems. This dashboard relates to GDPR Articles 5 and 25 and Recital 49.

Regulatory Exposure

Select Reports > Portal > Repository > Standard Content > GDPR > *Reports* or *Dashboards* > GDPR Access Activity > Regulatory Exposure.

As part of your compliance measures, you most likely track access events that might have compromised user data, thus breaching GDPR regulations.

Potential Regulatory Exposure on GDPR Systems

Reports the GDPR systems that might have been exposed to a regulatory infraction due to user access activities. The chart shows the systems with the most events. The table provides results by the event name and time by GDPR system. This report relates to GDPR Article 32 and Recital 49.

Threat User Analysis

Select Reports > Portal > Repository > Standard Content > GDPR > *Reports* or *Dashboards* > GDPR Access Activity > Threat User Analysis.

User activities such as changing authorizations or clearing audit logs often indicate malicious activities or potential vulnerabilities. Run the following reports to check for threat activities on your GDPR systems.

Admin Activity from Compromised GDPR System

Reports events associated with administrative activities that occur on GDPR systems. For example, users are executing commands or changing authorizations. The chart shows activity over time. The table provides results by time, user, affected GDPR asset, activity type, and the number of events. This report relates to GDPR Articles 30 and 32 and Recital 49.

Anti-Virus Disabled on GDPR Systems Summary

Reports how often anti-virus services have been stopped or paused on GDPR systems over time. A malicious user might pause an anti-virus service before running an illegal command or script or downloading or installing malicious programs. The table provides results by time, GDPR system, affected service, and number of events. This report relates to GDPR Article 32 and Recital 49.

Audit Log Cleared on GDPR Systems Summary

Reports the audit log has been cleared on GDPR systems. The chart shows the number of events over time. The table provides results by date, user, and host. This report relates to GDPR Articles 5 and 25 and Recital 49.

Threats Executed against GDPR Systems Summary

Reports how often GDPR systems have been threatened. The chart shows the number of events over time. The table provides results by date, system IP address, threat technique, event name, and number of events. This report relates to GDPR Article 32 and Recital 49.

Admin Activity

Select Reports > Portal > Repository > Standard Content > GDPR > *Reports* or *Dashboards* > GDPR Admin Activity > Provisioning Activity.

Administrators can create and remove users. These admins might inadvertently or deliberately add users to a system or group, giving users access to sensitive systems and information. Alternatively, a malicious user with access to an admin account might attempt to create users for later access or remove necessary accounts. To comply with GDPR, you should track administrator activities related to user creations, deletions, and group assignments.

Dashboards	Reports
n/a	User Creations on GDPR Environment User Deletions on GDPR Environment Users Added to a Group on GDPR Environment Users Removed from a Group on GDPR Environment

User Creations on GDPR Environment

Reports the number of user accounts created over time and by whom in the GDPR environment. The table provides results by date, created account, user creating the account, and their domains. This report relates to GDPR Articles 5, 6, and 7 and Recitals 78, 82, and 84.

User Deletions on GDPR Environment

Reports the number of user accounts deleted over time and by whom in the GDPR environment. The table provides results by date, the deleted account, user deleting the account, and their domains. This report relates to GDPR Article 17 and Recital 66.

Users Added to a Group on GDPR Environment

Reports the number of user accounts added to groups over time and by whom in the GDPR environment. The table provides results by date, subject, user adding the account, and affected group. This report relates to GDPR Articles 5, 6, 7, and 32 and Recitals 78, 82, and 84.

You must specify the name of a user group in lowercase.

Users Removed from a Group on GDPR Environment

Reports the number of user accounts removed from groups over time and by whom in the GDPR environment. The table provides results by date, subject, user removing the account,

and affected group. This report relates to GDPR Articles 17 and 32 and Recital 66.

You must specify the name of a user group in lowercase.

Attack Surface Analysis

Select Reports > Portal > Repository > Standard Content > GDPR > *Reports* or *Dashboards* > **GDPR Attack Surface Analysis**.

Each point entry in your environment, which unauthorized users or programs can exploit, increases the environment's attack surface. This package helps you analyze the extent of the environment's vulnerability.

Category	Dashboards	Reports
Attack Surface Identification	High Risk Vulnerabilities on GDPR Systems Information Leakage Vulnerabilities on GDPR Systems Password and Authentication Weaknesses on GDPR Systems SQL Injection Vulnerabilities on GDPR Systems SSL or TLS Vulnerabilities on GDPR Systems Vulnerable GDPR Assets by Vulnerability Type Vulnerabilities on GDPR Systems Overview XSS Vulnerabilities on GDPR Systems	High Risk Vulnerabilities on GDPR Systems Information Leakage Vulnerabilities on GDPR Systems Password and Authentication Weaknesses on GDPR Systems SQL Injection Vulnerabilities on GDPR Systems SSL or TLS Vulnerabilities on GDPR Systems Unpatched GDPR Systems Vulnerability Summary by CVE ID Vulnerability Summary by GDPR Asset Vulnerability Summary on GDPR Systems XSS Vulnerabilities on GDPR Systems
Security Controls Risk Identification	DoS Attacks Against GDPR Systems	DoS Attacks Against GDPR Systems

Attack Surface Identification

Select Reports > Portal > Repository > Standard Content > GDPR > *Reports* or *Dashboards* > **GDPR Attack Surface Analysis** > **Attack Surface Identification**.

To prevent data breaches, you need to know how much of your GDPR environment is vulnerable to attack. Use the following dashboards and reports to identify, and thus reduce, your environment's attack surface.

High Risk Vulnerabilities on GDPR Systems Dashboard

Provides an overview of high-risk vulnerabilities reported on GDPR systems. This dashboard relates to GDPR Articles 32, 35, and 83 and Recitals 76, 77, 78, and 83.

High Risk Vulnerabilities on GDPR Systems Report

Reports the high-risk vulnerabilities detected in the GDPR environment. The chart shows the systems with the most vulnerabilities. The table provides results by GDPR asset, signature ID, agent severity, description of the vulnerability, and date of the most recent event. This report relates to GDPR Articles 32, 35, and 83 and Recitals 76, 77, 78, and 83.

Information Leakage Vulnerabilities on GDPR Systems Dashboard

Provides an overview of information leakage vulnerabilities reported on GDPR systems. This dashboard relates to GDPR Articles 32, 35, and 83 and Recitals 76, 77, 78, and 83.

Information Leakage Vulnerabilities on GDPR Systems Report

Reports the information leakage vulnerabilities detected in the GDPR environment. The chart shows the systems with the most vulnerabilities. The table provides results by GDPR asset, signature ID, agent severity, description of the vulnerability, and date of the most recent event. This report relates to GDPR Articles 32, 35, and 83 and Recitals 76, 77, 78, and 83.

Password and Authentication Weaknesses on GDPR Systems Dashboard

Provides an overview of password and authentication Weaknesses reported on GDPR systems. This dashboard relates to GDPR Articles 32, 35, and 83 and Recitals 76, 77, 78, and 83.

Password and Authentication Weaknesses on GDPR Systems Report

Reports the password and authentication weaknesses detected in the GDPR environment. The chart shows the number of events over time. The table provides results by GDPR asset, signature ID, agent severity, description of the vulnerability, and date of the most recent event. This report relates to GDPR Articles 32, 35, and 83 and Recitals 76, 77, 78, and 83.

SQL Injection Vulnerabilities on GDPR Systems Dashboard

Provides an overview of SQL Injection vulnerabilities reported on GDPR systems. This dashboard relates to GDPR Articles 32, 35, and 83 and Recitals 76, 77, 78, and 83.

SQL Injection Vulnerabilities on GDPR Systems Report

Reports the SQL injection vulnerabilities detected in the GDPR Environment. The chart shows the systems with the most detected vulnerabilities. The table provides results by GDPR asset, signature ID, agent severity, description of the vulnerability, and date of the most recent event. This report relates to GDPR Articles 32, 35, and 83 and Recitals 76, 77, 78, and 83.

SSL and TLS Vulnerabilities on GDPR Systems Dashboard

Provides an overview of SSL and TLS vulnerabilities reported on GDPR systems. This dashboard relates to GDPR Articles 32, 35, and 83 and Recitals 76, 77, 78, and 83.

SSL or TLS Vulnerabilities on GDPR Systems Report

Reports the SSL and TLS vulnerabilities detected in the GDPR Environment. Malicious users can exploit vulnerabilities in SSL and TLS. For example, the Heartbleed Bug is a known SSL vulnerability. The chart shows the systems with the most detected vulnerabilities. The table provides results by GDPR asset, signature ID, agent severity, description of the vulnerability, and date of the most recent event. This report relates to GDPR Articles 32, 35, and 83 and Recitals 76, 77, 78, and 83.

Unpatched GDPR Systems

Reports the GDPR Systems with missing security patches. One of the most common ways to reduce your environment's attack surface is to ensure that all systems have the most recent security patches applied. The chart shows the systems with the most missing security patches. The table provides results by GDPR asset, signature ID, agent severity, description of the vulnerability, and date of the most recent event. This report relates to GDPR Articles 32, 35, and 83 and Recitals 76, 77, 78, and 83.

Vulnerable GDPR Assets by Vulnerability Type

Provides an overview of vulnerabilities reported on GDPR systems by Type. This dashboard relates to GDPR Articles 32, 35, and 83 and Recitals 76, 77, 78, and 83.

Vulnerabilities on GDPR Systems Overview

Provides an overview of vulnerabilities reported on GDPR systems. This dashboard relates to GDPR Articles 32, 35, and 83 and Recitals 76, 77, 78, and 83.

Vulnerability Summary by CVE ID

Reports the vulnerabilities detected in the GDPR environment by specific CVE ID. The chart shows the number of assets with the specified vulnerability over time. The table provides results by host name, IP address, Mac address, signature ID, description of the vulnerability, and date of the most recent event. This report relates to GDPR Articles 32, 35, and 83 and Recitals 76, 77, 78, and 83.

You must specify a CVE ID.

Vulnerability Summary by GDPR Asset

Reports the vulnerabilities detected on a specific GDPR asset. The chart shows the number of vulnerabilities detected over time. The table provides results by host name, IP address, Mac address, signature ID, description of the vulnerability, and date of the most recent event. This report relates to GDPR Articles 32, 35, and 83 and Recitals 76, 77, 78, and 83.

You must specify one GDPR asset by host name, IP address, or Mac address.

Vulnerability Summary on GDPR Systems

Reports the vulnerabilities detected in the GDPR environment. The chart shows the assets with the most detected vulnerabilities. The table provides results by asset, signature ID, agent severity, description of the vulnerability, and date of the most recent event. This report relates to GDPR Articles 32, 35, and 83 and Recitals 76, 77, 78, and 83.

XSS Vulnerabilities on GDPR Systems Dashboard

Provides an overview of XSS vulnerabilities reported on GDPR systems. This dashboard relates to GDPR Articles 32, 35, and 83 and Recitals 76, 77, 78, and 83.

XSS Vulnerabilities on GDPR Systems Report

Reports the cross-site scripting (XSS) vulnerabilities detected in the GDPR environment. Vulnerabilities associated with XSS enable malicious users to inject code in legitimate web pages or applications that executes harmful scripts in the user's web browser when the browser parses data. The chart shows the assets with the most detected vulnerabilities. The table provides results by asset, signature ID, agent severity, description of the vulnerability, and date of the most recent event. This report relates to GDPR Articles 32, 35, and 83 and Recitals 76, 77, 78, and 83.

Security Controls Risk Identification

Select Reports > Portal > Repository > Standard Content > GDPR > *Reports* or *Dashboards* > GDPR Attack Surface Analysis > Security Controls Risk Identification.

Not all malicious users want to breach your systems to access or manipulate data. Some might want to disrupt service and deny users access to information. However, a denial-of-service (DoS) attack might indicate a future threat to your environment.

DoS Attacks Against GDPR Systems

Reports potential DoS events against databases in the GDPR environment. The chart shows the number of attacks over time. The table provides results by the source IP and port, the target IP and port, name of the event, and number of events. This report relates to GDPR Article 32 and Recital 49.

DoS Attacks Against GDPR Systems

Provides a summary overview of DoS Attacks against GDPR Systems. This dashboard relates to GDPR Article 32 and Recital 49.

Corporate Governance

Select **Reports > Portal > Repository > Standard Content > GDPR** > *Reports* or *Dashboards* > **GDPR Corporate Governance** > **Record Keeping**.

In some environments, sensitive data is stored in file cabinets or archives. To ensure compliance with GDPR, your organization might control access to the physical environment where these records are kept. Use the following dashboards and reports to track access to these environments.

Dashboards	Reports
Access Activity on GDPR Systems Overview	Access Activity on GDPR Systems Summary
Geo Access Activity on GDPR Systems Overview	After Work Hours Physical Access Activity on GDPR Systems Summary
Physical Access Activity on GDPR Systems Overview	Physical Access Activity on GDPR Systems Summary

Access Activity on GDPR Systems Summary

Reports access events to GDPR systems. The chart shows access by country over time. The table provides results by user, source IP and country, target IP and host, and number of events. This report relates to GDPR Articles 30, 32, and 25, and Recital 82.

After Work Hours Physical Access Activity on GDPR Systems Summary

Reports access to physical GDPR systems, such as buildings, during after work hours. The chart shows both failed and successful access by user and building. The table provides results by date, user, building, result, and number of attempts. This report relates to GDPR Articles 24 and 32 and Recital 49.

By default, the report uses the following time ranges to check for "after hours" access:

- 12 a.m. to 7 a.m., Monday through Friday
- 18 p.m. (6 p.m.) to 12 a.m., Monday through Friday
- All day on Saturday and Sunday

However, you can modify the time ranges by editing the filters for the report. The time range uses 24-hour values.

Physical Access Activity on GDPR Systems Summary

Reports access to physical GDPR systems, such as building. The chart shows both failed and successful access by building over time. The table provides results by date, user, building, result, and number of attempts. This report relates to GDPR Articles 24 and 32 and Recital 49.

Access Activity on GDPR Systems Overview

Provides an overview of access events reported on GDPR systems. This dashboard relates to GDPR Articles 30, 32, and 25 and Recital 82.

Geo Access Activity on GDPR Systems Overview

Provides an overview of GEO access activity to GDPR systems. This dashboard relates to GDPR Articles 30, 32, and 25 and Recital 82.

Physical Access Activity on GDPR Systems Overview

Provides an overview of physical access events reported on GDPR systems, by default "after Work Hours" charts defined from 12 a.m. to 7 a.m. and 18 p.m. to 12 a.m every Monday to Friday and the whole days of Saturday and Sunday, those can be re-configured to different values using this dashboard charts components filter. This dashboard relates to GDPR Articles 24 and 32 and Recital 49.

Regulatory Exposure

Select Reports > Portal > Repository > Standard Content > GDPR > *Reports* or *Dashboards* > **GDPR Regulatory Exposure** > **Composite Regulatory Exposure**.

To comply with GDPR, you might need to track how data flows among GDPR system, and from systems in non-EU countries.

Dashboards	Reports
Data Flow from GDPR Systems	Data Flow from GDPR Systems Summary
Data Flow from GDPR Systems to non EU	Data Flow from GDPR Systems to non EU Summary
Data Flow from non EU to GDPR Systems	Data Flow from non EU to GDPR Systems Summary
Data Flow to GDPR Systems	Data Flow to GDPR Systems Summary
GDPR Systems Communication with non EU Countries	High Risk Events on GDPR Systems Summary
GDPR Systems Communication Overview	Policy Violations on GDPR Systems Summary
High Risk Events on GDPR Systems Overview	Threats on GDPR Systems Summary
Policy Violations on GDPR Systems Overview	
Threat Relationship on GDPR Systems Overview	
Threats on GDPR Systems Overview	

Data Flow from GDPR Systems

Provides a summary overview of data flow from GDPR Systems. This dashboard relates to GDPR Articles 30, 46, 32, 45, 46, and 49 and Recital 82.

Data Flow from GDPR Systems Summary

Reports events that detect the flow of data from GDPR systems. The chart shows the GDPR systems with the most data flowing outward. The table provides results by the IP address of the GDPR source system, the target IP address and host, and the number of events detected. This report relates to GDPR Articles 30, 32, 45, 46, and 49 and Recital 82.

Data Flow from GDPR Systems to non EU

Provides a summary overview of data flow from non EU to GDPR Systems. This dashboard relates to GDPR Articles 30, 46, 32, 45, 46, and 49 and Recital 82.

Data Flow from GDPR Systems to non EU Summary

Reports events that detect the flow of data from GDPR systems to systems in non-European Union countries. The chart shows the GDPR systems with the most data flowing outward by country. The table provides results by the IP address of the GDPR source system, the IP address of the non-EU system, the country code of the target system, and the number of events detected. This report relates to GDPR Articles 30, 32, 45, 46, and 49 and Recital 82.

Data Flow from non EU to GDPR Systems

Provides a summary overview of data flow from non EU to GDPR Systems. This dashboard relates to GDPR Articles 30, 46, 32, 45, 46, and 49 and Recital 82.

Data Flow from non EU to GDPR Systems Summary

Reports events that detect the flow of data to GDPR systems from systems in non-European Union countries. The chart shows the GDPR systems with the most data flowing in by country of origin. The table provides results by the IP address and country code of the source system, the IP address of the GDPR system, and the number of events detected. This report relates to GDPR Articles 30, 32, 45, 46, and 49 and Recital 82.

Data Flow to GDPR Systems

Provides a summary overview of data flow to GDPR Systems. This dashboard relates to GDPR Articles 30, 46, 32, 45, 46, and 49 and Recital 82.

Data Flow to GDPR Systems Summary

Reports events that detect the flow of data to GDPR systems. The chart shows the GDPR systems with the most data flowing into them. The table provides results by the IP address of the source system, the target (GDPR system) IP address and host, and the number of events detected. This report relates to GDPR Articles 30, 32, 45, 46, and 49 and Recital 82.

GDPR Systems Communication Overview

Provides an overview of GDPR Systems communications. This dashboard relates to GDPR Articles 30, 46, 32, 45, 46, and 49 and Recital 82.

GDPR Systems Communication with non EU Countries

Provides an overview of GDPR Systems communications with non EU Countries. This dashboard relates to GDPR Articles 30, 46, 32, 45, 46, and 49 and Recital 82.

High Risk Events on GDPR Systems Overview

Provides an overview of high risk events related to GDPR systems. This dashboard relates to GDPR Article 32 and Recital 49.

High Risk Events on GDPR Systems Summary

Reports high-risk events that involve GDPR systems. The chart shows the targeted GDPR systems with the most high-risk events. The table provides results by the source IP and host of the events, the targeted IP and host GDPR system, the user, and number of events detected. This report relates to GDPR Articles 32 and 83 and Recital 49.

Policy Violations on GDPR Systems Overview

Provides an overview of policy violation events related to GDPR systems. This dashboard relates to GDPR Articles 32 and 83 and Recital 49.

Policy Violations on GDPR Systems Summary

Reports the number of policy violation events on GDPR systems over time. The table provides results by source IP address, the IP address and host of the target GDPR system, user, and number of events. This report relates to GDPR Articles 32 and 83 and Recital 49.

Threat Relationship on GDPR Systems Overview

Provides an overview of relationship between source and destination addresses on events which indicate compromise, reconnaissance, hostile, or suspicious activity on GDPR systems. This dashboard relates to GDPR Article 32 and Recital 49.

Threats on GDPR Systems Overview

Provides an overview of events that indicate compromise, reconnaissance, hostile, or suspicious activity on GDPR systems. This dashboard relates to GDPR Article 32 and Recital 49.

Threats on GDPR Systems Summary

Reports the number of events that indicate compromise, reconnaissance, hostile, or suspicious activity on GDPR systems over time. The table provides results by IP and Mac address of the source system, the IP address and host of the target GDPR system, user, and number of events. This report relates to GDPR Articles 32 and Recital 49.

Threat Analysis

Select Reports > Portal > Repository > Standard Content > GDPR > *Reports* or *Dashboards* > GDPR Threat Analysis.

GDPR requires that your enterprise establish technical and organizational standards that ensure appropriate security-to-risk levels. To create appropriate security measures, you need to assess the risks and the severity of threats to sensitive data.

- "Threat Analysis - Data Store Risk" on the next page
- "Threat Analysis - Internet" on page 111

Threat Analysis - Data Store Risk

Select **Reports** > **Portal** > **Repository** > **Standard Content** > **GDPR** > *Reports* or *Dashboards* > **GDPR Threat Analysis** > **Data Store Risk**.

As part of your threat analysis, you should assess the vulnerability of data storage systems.

Dashboards	Reports
n/a	Attacks Against Databases on GDPR Systems Cassandra Vulnerabilities on GDPR Systems CRM and ERP Vulnerabilities on GDPR Systems Database Configuration Changes on GDPR Systems Database Weaknesses on GDPR Systems Elasticsearch Vulnerabilities on GDPR Systems IBM Db2 Vulnerabilities on GDPR Systems MariaDB Vulnerabilities on GDPR Systems Microsoft SQL Server Vulnerabilities on GDPR Systems MongoDB Vulnerabilities on GDPR Systems MySQL Vulnerabilities on GDPR Systems Oracle Vulnerabilities on GDPR Systems PostgreSQL Vulnerabilities on GDPR Systems Redis Vulnerabilities on GDPR Systems

Attacks Against Databases on GDPR System

Reports events that indicate compromise, reconnaissance, hostile, or suspicious activity against GDPR systems databases over time. The table provides results by the source GDPR IP address, IP address and host of the target system, name of the event, and number of events. This report relates to GDPR Article 32 and Recital 49.

Cassandra Vulnerabilities on GDPR Systems

Reports vulnerabilities related to Apache Cassandra on GDPR systems. Apache Cassandra is a free and open-source, distributed, wide-column store, NoSQL database management system. The chart shows the GDPRs reporting the most vulnerabilities. The table provides results by GDPR asset, signature ID, agent severity, description of the vulnerability, and date of the most recent event. This report relates to GDPR Articles 32, 35, and 83 and Recitals 76, 77, 78, and 83.

CRM and ERP Vulnerabilities on GDPR Systems

Reports vulnerabilities detected on GDPR systems related to CRM (Customer Relationship Management) and ERP (Enterprise Resource Planning) software. The chart shows the GDPR systems with the most vulnerabilities. The table provides results by GDPR asset, signature ID, agent severity, description of the vulnerability, and date of the most recent event. This report relates to GDPR Articles 32, 35, and 83 and Recitals 76, 77, 78, and 83.

Database Configuration Changes on GDPR Systems

Reports changes to the database configuration in the GDPR environment. The chart shows the GDPR systems with the most changes. The table provides results by host system, database change, the type of change, agent severity, and date of the most recent event. This report relates to GDPR Article 32.

Database Weaknesses on GDPR Systems

Reports vulnerabilities in databases detected in the GDPR environment over time and by severity. The table provides results by GDPR asset, signature ID, description of the vulnerability, agent severity, and date of the most recent event. This report relates to GDPR Articles 32, 35, and 83 and Recitals 76, 77, 78, and 83.

Elasticsearch Vulnerabilities on GDPR Systems

Reports vulnerabilities related to Elasticsearch on GDPR systems. The chart shows the GDPR systems with the most vulnerabilities. The table provides results by GDPR asset, signature ID, agent severity, description of the vulnerability, and date of the most recent event. This report relates to GDPR Articles 32, 35, and 83 and Recitals 76, 77, 78, and 83.

IBM Db2 Vulnerabilities on GDPR Systems

Reports vulnerabilities related to IBM Db2 on GDPR systems. The chart shows the GDPR systems with the most vulnerabilities. The table provides results by GDPR asset, signature ID, agent severity, description of the vulnerability, and date of the most recent event. This report relates to GDPR Articles 32, 35, and 83 and Recitals 76, 77, 78, and 83.

MariaDB Vulnerabilities on GDPR Systems

Reports vulnerabilities related to MariaDB on GDPR systems. The chart shows the GDPR systems with the most vulnerabilities. The table provides results by GDPR asset, signature ID, agent severity, description of the vulnerability, and date of the most recent event. This report relates to GDPR Articles 32, 35, and 83 and Recitals 76, 77, 78, and 83.

Microsoft SQL Server Vulnerabilities on GDPR Systems

Reports vulnerabilities related to Microsoft SQL Server on GDPR systems. The chart shows the GDPR systems with the most vulnerabilities. The table provides results by GDPR asset, signature ID, agent severity, description of the vulnerability, and date of the most recent event. This report relates to GDPR Articles 32, 35, and 83 and Recitals 76, 77, 78, and 83.

MongoDB Vulnerabilities on GDPR Systems

Reports vulnerabilities related to MongoDB on GDPR systems. The chart shows the GDPR systems with the most vulnerabilities. The table provides results by GDPR asset, signature ID, agent severity, description of the vulnerability, and date of the most recent event. This report relates to GDPR Articles 32, 35, and 83 and Recitals 76, 77, 78, and 83.

MySQL Vulnerabilities on GDPR Systems

Reports vulnerabilities related to MySQL on GDPR systems. The chart shows the GDPR systems with the most vulnerabilities. The table provides results by GDPR asset, signature ID, agent severity, description of the vulnerability, and date of the most recent event. This report relates to GDPR Articles 32, 35, and 83 and Recitals 76, 77, 78, and 83.

Oracle Vulnerabilities on GDPR Systems

Reports vulnerabilities related to Oracle on GDPR systems. The chart shows the GDPR systems with the most vulnerabilities. The table provides results by GDPR asset, signature ID, agent severity, description of the vulnerability, and date of the most recent event. This report relates to GDPR Articles 32, 35, and 83 and Recitals 76, 77, 78, and 83.

PostgreSQL Vulnerabilities on GDPR Systems

Reports vulnerabilities related to PostgreSQL on GDPR systems. The chart shows the GDPR systems with the most vulnerabilities. The table provides results by GDPR asset, signature ID, agent severity, description of the vulnerability, and date of the most recent event. This report relates to GDPR Articles 32, 35, and 83 and Recitals 76, 77, 78, and 83.

Redis Vulnerabilities on GDPR Systems

Reports vulnerabilities related to Redis on GDPR systems. The chart shows the GDPR systems with the most vulnerabilities. The table provides results by GDPR asset, signature ID, agent severity, description of the vulnerability, and date of the most recent event. This report relates to GDPR Articles 32, 35, and 83 and Recitals 76, 77, 78, and 83.

Threat Analysis - Internet

Select Reports > Portal > Repository > Standard Content > GDPR > *Reports* or *Dashboards* > **GDPR Threat Analysis** > **Internet Threat Analysis**.

As part of your threat analysis, you should assess the vulnerability of firewalls, places where information might leak, and existence of malware on your GDPR systems.

Dashboards	Reports
Malware Found on GDPR Systems MITRE ATT&CK on GDPR Systems by GDPR Asset MITRE ATT&CK on GDPR Systems by MITRE ID MITRE ATT&CK on GDPR Systems Overview MITRE ATT&CK Relationship on GDPR Systems Overview	Firewall Blocked Events in GDPR Environment Information Leaks from GDPR Systems Malware Found on GDPR Systems

Firewall Blocked Events in GDPR Environment

Reports firewall blocked events in the GDPR environment. The chart shows the number of events by time and target port. If you pro-actively monitor the firewalls in your enterprise, you can identify problems at an early stage and prevent network attacks. The table provides results by source IP address and port, the targeted GDPR IP address and port, and the number of events. This report relates to GDPR Article 32 and Recital 49.

Information Leaks from GDPR Systems

Reports events that indicate information leaks on GDPR systems over time. The table provides results by date, event name, source IP address and port, the targeted GDPR IP address and port, and the user. This report relates to GDPR Articles 32, 33, and 34 and Recitals 49, 85, and 86.

Malware Found on GDPR Systems Dashboard

Provides an overview of malware reported events on GDPR Systems. This dashboard relates to GDPR Articles 32, 33, and 34 and Recitals 49 and 83.

Malware Found on GDPR Systems Report

Reports malware found on GDPR systems. The chart shows the systems with the most malware activity. The table provides results by GDPR asset, malware program, name of the event, and date of the most recent event. This report relates to GDPR Articles 32, 35, and 83 and Recitals 76, 77, 78, and 83.

MITRE ATT&CK on GDPR Systems by GDPR Asset

Provides an overview of MITRE ATT&CK events by GDPR asset. This dashboard relates to GDPR Article 32 and Recital 49.

MITRE ATT&CK on GDPR Systems by MITRE ID

Provides an overview of MITRE ATT&CK events reported on GDPR Systems by MITRE IDs. This dashboard relates to GDPR Article 32 and Recital 49.

MITRE ATT&CK on GDPR Systems Overview

Provides an overview of MITRE ATT&CK events reported on GDPR Systems. This dashboard relates to GDPR Article 32 and Recital 49.

MITRE ATT&CK Relationship on GDPR Systems Overview

Provides an overview of the relationship between different event entities on MITRE ATT&CK events reported on GDPR systems. This dashboard relates to GDPR Article 32 and Recital 49.

Ensuring Compliance with IT Governance

Select Reports > Portal > Repository > Standard Content > IT GOV > ISO-27002.

To comply with the information security management controls as part of ISO 27002 guidelines, your enterprise needs to establish and follow information security standards and policies. The guidelines help you identify and implement the controls needed to secure data. You can check the security controls in your enterprise against one or more specific ISO 27002 control set, such as *Information Security Policies or Asset Management*.

Recon provides the **Compliance Pack for IT Governance** to help you comply with Controls 6, 8, 9, 10, 12, 13, 14, 16, and 17. For more information about adding the pack to the Reports repository, see the *Solutions Guide for ArcSight Recon Compliance Pack for IT Governance*.

This package includes dashboards and reports organized by the ISO-27002 requirements:

Category	Dashboards	Reports
"IT Governance – Executive Overview" on page 117	"Overall Risk Management" on page 117	n/a
"6 – Organization of Information Security" on page 118	n/a	"Suspicious Activity in Wireless Network" on page 118
"8 – Asset Management" on page 118	n/a	"Network Active Assets" on page 119 "New Hosts" on page 119 "New Services" on page 119

Category	Dashboards	Reports
"9 – Access Control" on page 119	"User Account Management" on page 121	"Account Lockouts by User" on page 120 "All Login Activity" on page 120 "Authentication with Null Sessions" on page 120 "Authorization Changes" on page 120 "Privileged Account Changes" on page 120 "Removal of Access Rights" on page 120 "Successful Brute Force Logins" on page 120 "Unauthorized User Access to Network Domain" on page 120 "User Account Creation" on page 121 "User Account Deletion" on page 121
"10 – Cryptography" on page 121	n/a	"Insecure Cryptographic Storage" on page 122 "Invalid Certificates" on page 122 "Systems Providing Unencrypted Services" on page 122

Category	Dashboards	Reports
"12 – Operations Security" on page 122	"Authentication Errors" on page 126 "Database Events" on page 126 "Events and Incidents that have Occurred" on page 127 "Malware Activity" on page 128 "Scans Overview" on page 129 "Vulnerabilities Management" on page 131 "Vulnerability Scans and Unauthorized Access" on page 131	"Account Activity Summary" on page 125 "Administrative Actions Events" on page 125 "Administrative Logins and Logouts" on page 125 "Application Configuration Modification" on page 125 "Audit Log Cleared" on page 125 "Authentication Logins with Insecure Ports" on page 125 "Blocked Firewall Traffic" on page 126 "Changes to Operating System" on page 126 "Covert Channel Activity" on page 126 "Device Configuration Changes" on page 126 "Device Logging Review" on page 126 "Exploit of Vulnerabilities" on page 127 "Failed Administrative User Logins" on page 127 "Failed Antivirus Updates" on page 127 "Failed File Access" on page 127 "Failed File Deletions" on page 127 "Failed User Logins" on page 127 "Fault Logs" on page 128 "File Changes in Production" on page 128 "Firewall Configuration Changes" on page 128 "Logins to Database Machines" on page 128 "Machines Conducting Policy Breaches" on page 128

Category	Dashboards	Reports
		"Malicious Code Sources" on page 128 "Network Device Configuration Changes" on page 129 "Policy Violations" on page 129 "Resource Exhaustion" on page 129 "Software Changes in Production" on page 129 "Successful Administrative User Logins" on page 129 "Successful File Deletions" on page 130 "Successful User Logins" on page 130 "Suspicious Activity" on page 130 "Trojan Code Activity" on page 130 "User Actions All Events" on page 130 "User Logins and Logouts" on page 130 "Virus Infected Machines" on page 130 "Vulnerabilities Scanner Results" on page 131
"13 – Communications Security" on page 131	"Email Activities" on page 132 "Peer to Peer Activity" on page 133 "Phishing Activities" on page 133	"Accessed Ports through Firewall" on page 132 "Firewall Open Port Review" on page 132 "Information Interception Events" on page 132 "Insecure Services" on page 132 "Interzone Traffic" on page 132 "Organizational Information Leaks" on page 132 "Personal Information Leaks" on page 133 "Processes by Asset" on page 133

Category	Dashboards	Reports
"14 – System Acquisition, Development, and Maintenance" on page 133	n/a	"Invalid Data Input" on page 134
"16 – Information Security Incident Management" on page 134	"Internal Reconnaissance" on page 135	"Confidential Breach Sources" on page 134 "Denial of Service" on page 134 "File Integrity Changes" on page 135 "Information Systems Failures" on page 135 "Integrity Breach Sources" on page 135 "Internal Reconnaissance by Event" on page 135 "Internal Reconnaissance by Source Address" on page 135 "Internal Reconnaissance by Target Address" on page 136
"17 – Information Security Aspects of Business Continuity Management" on page 136	n/a	"Availability Attacks" on page 136

IT Governance – Executive Overview

Select Reports > Portal > Repository > Standard Content > IT GOV > ISO-27002 > Dashboards > Overview.

To help individuals in management and C-suite positions to quickly understand the current state of your enterprise's compliance with ISO-27002 controls, you can view the following dashboard:

Dashboards	Reports
"Overall Risk Management" below	n/a

Overall Risk Management

Provides, in charts, the overall risk score of your IT environment. You can view the most assets at highest risk, risk score by ISO control, and the rules triggered by an ISO control.

6 – Organization of Information Security

Select Reports > Portal > Repository > Standard Content > IT GOV > ISO-27002 > Reports > ISO 6 – Organization of Information Security.

Control 6: *Organization of information security* of the ISO 27002 standard focuses on ensuring that your organization supports and maintains information security operations, both on- and off-site.

To assess your enterprise's compliance with this requirement, use the following reports:

Dashboards	Reports
n/a	"Suspicious Activity in Wireless Network" below

Suspicious Activity in Wireless Network

Reports events that indicate suspicious activity in the wireless network. For example, a malicious user might scan ports to discover open doors or weak points in the wireless network. The table provides results by the type of suspicious activity, details about the target and source systems, and the number of events.

In the logical model, use the iDestinationWirelessNetwork variable to specify wireless networks. For more information, see the *Solutions Guide for ArcSight Recon Compliance Pack for IT Governance*.

8 – Asset Management

Select Reports > Portal > Repository > Standard Content > IT GOV > ISO-27002 > Reports > ISO 8 – Asset Management.

Control 8: *Asset Management* of the ISO 27002 standard focuses on identifying the physical and information assets in your enterprise, and determining the appropriate level of protection necessary for each.

To assess your enterprise's compliance with this requirement, use the following reports:

Dashboards	Reports
n/a	"Network Active Assets" on the next page "New Hosts" on the next page "New Services" on the next page

Network Active Assets

Reports all hosts that have been included as the source address in logged events. The table provides results by the source IP address, user, and zone; the number of events; and when the event occurred.

New Hosts

Reports all new hosts on the network detected by traffic analysis systems. The table provides results by the host name, IP address, and zone of the target system and when the event occurred.

New Services

Reports all new services on the network detected by traffic analysis systems. The table provides results by the service name, IP address, and host name; the port used, the number of events, and when the most recent event occurred.

9 – Access Control

Select Reports > Portal > Repository > Standard Content > IT GOV > ISO-27002 > *Dashboards* or *Reports* > ISO 9 – Access Control.

Control 9: *Access Control* of the ISO 27002 standard focuses on preventing unauthorized user access to information and the facilities that process information.

To assess your enterprise's compliance with this requirement, use the following dashboard and reports:

Dashboards	Reports
"User Account Management" on page 121	"Account Lockouts by User" on the next page "All Login Activity" on the next page "Authentication with Null Sessions" on the next page "Authorization Changes" on the next page "Privileged Account Changes" on the next page "Removal of Access Rights" on the next page "Successful Brute Force Logins" on the next page "Unauthorized User Access to Network Domain" on the next page "User Account Creation" on page 121 "User Account Deletion" on page 121

Account Lockouts by User

Reports the accounts most often locked out. The table provides results about the locked out user, the target IP address and host name, the number of event, and when the most recent event occurred.

All Login Activity

Reports all successful, failed, and attended login activity by all users in the network. The table provides results by the IP address and name of the target system, the source IP address, the user involved, the outcome of the login attempt, the number of attempts, and when the most recent attempt occurred.

Authentication with Null Sessions

Reports possible null authentication sessions where the outcome is successful, failed, or an attempt. A null session attack exploits an authentication vulnerability for Windows Administrative Shares where a malicious user connects to a local or remote share without authentication. The table provides results by the target IP address and user, the source IP address and user, the outcome of the authentication attempt, the number of attempts, and when the most recent attempt occurred.

Authorization Changes

Reports authorization changes made on systems and the number of events per host. The table provides results by the target zone, IP address, and user; the source user, the type of event, the number of attempts, and when the most recent attempt occurred.

Privileged Account Changes

Reports all changes made to privileged accounts, such as password changes. The table provides results by the event, the name and IP address of the user who made the change, and when the change occurred.

Removal of Access Rights

Reports the access rights removed from user accounts. The table provides results by the access right that was removed, the IP address and host where the change was made, the user who made the change, the number of changes, and when the change occurred.

Successful Brute Force Logins

Reports the details of successful brute force logins. The table provides results by the user logging in, the IP address and host affected, the number of logins and when the event occurred.

Unauthorized User Access to Network Domain

Reports login sessions where the user is unauthorized for the specific network domain. The table provides results by the user attempted access, the target IP address and host, the source IP address for the user, the outcome of the attempt, the number of attempts, and when the event occurred.

To specify authorized users and network domains, update the variables isDestinationAuthorizeUser and isNetworkDomain. For more information, see the *Solutions Guide for ArcSight Recon Compliance Pack for IT Governance*.

User Account Creation

Reports all events that indicate a user account has been added to a system. The table provides results by the IP address and host where the event occurred, the user adding accounts, the number of events, and when the event occurred.

User Account Deletion

Reports all events that indicate a user account has been removed from a system. The table provides results by the IP address and host where the event occurred, the user removing accounts, the number of events, and when the event occurred.

User Account Management

Provides, in charts, details of scans, probes, and unauthorized access. You can view the number of accounts created and deleted by the user making the change, as well as the hosts that have been added or deleted.

10 – Cryptography

Select Reports > Portal > Repository > Standard Content > IT GOV > ISO-27002 > Reports > ISO 10 – Cryptography.

Control 10: *Cryptography* of the ISO 27002 standard focuses on using cryptographic keys to protect the confidentiality, integrity, and availability of information.

To assess your enterprise's compliance with this requirement, use the following reports:

Dashboards	Reports
n/a	"Insecure Cryptographic Storage" on the next page "Invalid Certificates" on the next page "Systems Providing Unencrypted Services" on the next page

Insecure Cryptographic Storage

Reports vulnerabilities associated with insecure cryptographic storage detected on your systems. The table provides results by IP address and name of the asset, the detected vulnerability, and when the most recent event occurred.

Invalid Certificates

Reports events that indicate an error with a server's certificate. The chart displays the number of such occurrences per host. The table provides results by the name of the event, the IP address and host name of the server, the user associated with event, the number of events, and when the event occurred.

Systems Providing Unencrypted Services

Reports the systems that provide unencrypted services. The table provides results by the port, process, service, IP address of the system, and the number of events.

12 – Operations Security

Select Reports > Portal > Repository > Standard Content > IT GOV > ISO-27002 > *Dashboards or Reports* > ISO 12 – Operations Security.

Control 12: *Operations security* of the ISO 27002 standard focuses on ensuring that the facilities that store and process information are protected from malware, data loss, and the exploitation of technical vulnerabilities. Use the following reports to check for compliance with the standard.

To assess your enterprise's compliance with this requirement, use the following dashboards and reports:

Dashboards	Reports

	"Trojan Code Activity" on page 130 "User Actions All Events" on page 130 "User Logins and Logouts" on page 130 "Virus Infected Machines" on page 130 "Vulnerabilities Scanner Results" on page 131

Account Activity Summary

Reports all account activities by type. The table provides results by the event name, the user associated with the event, the target IP address and host name, and number of events per user.

Administrative Actions Events

Reports the accounts that have performed the most administrative actions. The table provides results by admin account, destination IP address, the name and ID of the detected event, the affected product, the number of events, and when the most recent event occurred.

Administrative Logins and Logouts

Reports the hosts that have had the highest number of logins and logouts by administrative accounts. The table provides results by the name of the event, the admin account, the IP address and name of the affected host, the action taken, the number of events, and when most recent event occurred.

Application Configuration Modification

Reports the applications that have had the highest number of configuration changes. For example, a user might have updated a license file or a program setting. The table provides results by the product modified, the IP address and zone of the host system, and the date that the modification occurred.

Audit Log Cleared

Reports the indication that audit logs have been cleared over time. The table provides results by when the event occurred, the IP address and host of the affected system, the affected account, the source account that might have cleared the audit log, and the affected device.

Authentication Logins with Insecure Ports

Reports assets with authenticated logins that used insecure ports. This report is useful for auditors to track and identify assets that are not following the security standard. The table

provides results by the insecure port, the name of the source and target systems, the target user (if any), the type of event or user, the number of events, and the date of the most recent event.

Authentication Errors

Provides an overview of the authentication failure events in your enterprise. You can view a trend of failed authentication events over time, the different outcomes of the authentication events, and the failed logins by administrative and non-administrative users.

Blocked Firewall Traffic

Reports events generated by devices that have blocked traffic. The table provides results by the target port, the source and target IP address and host name, the type of event, and number of events.

Changes to Operating System

Reports the hosts with the most changes to the operating system. Detected modifications might be to the security options or OS accounts. The table provides results by the change made; the IP address, name, and zone of the affected host system; and the device product that was changed.

Covert Channel Activity

Reports events identified as covert channel activity. These events are generated by IDS devices and could indicate the use of different tools designed to establish an undetected channel to and from your enterprise. The table provides results by the type of event, the IP address and host name of the target and source systems, and when the event occurred.

Database Events

Provides, in charts and a table, an overview of the database events. You can view of trend of events over time, events by product, by the behavior of each event, and user names, IPs involved in the events. The table lists the name of the event; the target user and associated IP address; the source user and associated IP address; the outcome of the event; and the number of events.

Device Configuration Changes

Reports the type and number of modifications made to devices in the network. The table provides results by the date, time, event name, affected product, and the host where the changes occurred.

Device Logging Review

Reports the devices with the most logging events, such as a database. The table provides results by the device host name and address, a count of events received, and when the

device most recently received an event.

Because this report queries the logging activity from all devices, it will have a performance impact each time that you run it.

Events and Incidents that have Occurred

Provides, in charts, an overview of the different security incidents that might indicate that an systems or data in your enterprise have been compromised. You can view a trend of events by severity over time, as well as events by geographic location, the techniques used, severity, source IP address, and target IP address. You can also review the relationships between target and source IP addresses.

Exploit of Vulnerabilities

Reports the number of detected events where a user might have exploited a well-known vulnerability. For example, an IDS might report an event associated with a Unicode vulnerability. The table provides results by the vulnerability, the affected host, the source system, and the number of detected events.

Failed Administrative User Logins

Reports the number of failed logins by administrative accounts over time. A high number of failed access attempts can indicate malicious activity. The table provides results by account name, the name and IP address of the host where the login failed, the affected product or operating system, the number of failures detected, and when the most recent event occurred.

Failed Antivirus Updates

Reports number of failures in updating anti-virus software over time. The table provides results by the update that failed; the IP address, name, and zone of the target system; the type of event, and when the failure occurred.

Failed File Access

Reports the details of events that indicate failed attempts to access files. The table provides results by the targeted file, the IP address and name of the target system, the type of event, the number of attempts, and when the most recent attempt occurred.

Failed File Deletions

Reports information about files that failed to be deleted. The table provides results by the targeted file, the IP address and name of the target system, the type of event, the number of attempts, and when the most recent attempt occurred.

Failed User Logins

Reports the number of failed logins over time. A high number of failed access attempts can indicate malicious activity. The table provides results by account name, the name and IP address of the host where the login failed, the affected product or operating system, the number of failures detected, and when the most recent event occurred.

Fault Logs

Reports all events indicating that a system fault has occurred over time. The table provides results by the IP address and name of the host where the fault occurred, the name of the event, the number of events, and when the most recent event occurred.

File Changes in Production

Reports changes made to files in the production network. The table provides results by the target file, the IP address and name of the host of the file, the number of events, and when the most recent event occurred.

Before using this report, you must add the systems that reside in the production network to the variable isProductionNetwork. For more information, see the *Solutions Guide for ArcSight Recon Compliance Pack for IT Governance*.

Firewall Configuration Changes

Reports events by host that indicate changes to firewall configuration. The table provides results by the IP address and zone of the firewall, the firewall rule and configuration that was changed, the number of changes, and the time that the event occurred.

Logins to Database Machines

Reports the user accounts with the most attempts to log in to databases in your environment. The table provides results by the user account, the affected host, the number of attempts, whether the attempt was successful, and events per hour.

Machines Conducting Policy Breaches

Reports policy breaches by system, where the event matches the category technique of `/Policy/Breach`. The table provides results by the device group, affected vendor and product, the IP address and name of the host, and when the breach occurred.

Malicious Code Sources

Reports malicious code events by host system. The table provides results by the event name, the IP address and name of the affected device, the affected product, the category of the malicious code, and the outcome.

Malware Activity

Provides, in charts, an overview of the malware events that might indicate systems or data in your enterprise have been compromised. You can view a trend of malware events over

time, as well as events by geographic location, malware category and malicious event, the affected IP addresses and hosts, suspicious IP addresses and hosts names, and target IP addresses. You can also review the relationships between target and source IP addresses. You can also review the techniques used to exploit and launch further attacks.

Network Device Configuration Changes

Reports events that indicate configuration file changes on network equipment such as routers and switches. The table provides results by the change made, the device affected, the IP address where the change originated, the IP address and name of the host where the change occurred, and when the change occurred.

Policy Violations

Reports all policy breaches by source IP address. A policy breach could be IM use or the downloading of unauthorized content. The table provides results by the affected policy, the IP address and name of the source and target hosts, the number of breaches, and when the most recent breach occurred.

Resource Exhaustion

Reports events that indicate resource exhaustion on particular hosts. A malicious user can create or exploit resource exhaustion vulnerabilities by causing the programs to crash or falter, or by interfering with the programs such that the programs do not have enough resources to perform properly. If this occurs, the systems and programs become unavailable for use. The table provides results by the IP address and name of the host where the event occurred, the type of event, the number of events, and when the most recent event occurred.

Scans Overview

Provides an overview of scan results. You can view the signatures of potential vulnerabilities, the most active scanners, and the most scanned ports and assets.

Software Changes in Production

Reports events that indicate changes to daemons, access policies, and other software changes in the production environment. The table provides results by the event, the IP address and name of the target asset, and the target user.

Before using this report, you must add the systems that reside in the production network to the variable isProductionNetwork. For more information, see the *Solutions Guide for ArcSight Recon Compliance Pack for IT Governance*.

Successful Administrative User Logins

Reports the number of successful logins by administrative accounts over time. The table provides results by account name, the name and IP address of the host where the logins

occurred, the affected product or operating system, the number of successful logins, and the date of the most recent event.

Successful File Deletions

Reports events that indicate successful attempts to delete files by the target IP address. The table provides results by name of the deleted file, the IP address where the file was deleted, the number of files deleted, and when the deletion occurred.

Successful User Logins

Reports the number of successful logins over time. The table provides results by account name, the name and IP address of the host where the logins occurred, the affected product or operating system, the number of successful logins, and when the most recent event occurred.

Suspicious Activity

Reports suspicious events in your network. The table provides results by the event name, the IP address and name of the host where the event occurred, the number of events, and when the most recent event occurred.

Trojan Code Activity

Reports all the trojan activity detected by IP address in the environment. The table provides results by the type of activity, the IP address that originated the activity, the IP address and name of the target host, and when the event occurred.

User Actions All Events

Reports the actions taken by non-administrative accounts. For example, a user might delete an infected file. The report provides results by the source account, the affected account, the name of the event, the IP address where the action occurred, the affected product, the outcome of the user's action, the number of times that the action was detected, and the date of the most recent event.

Run this report with caution, as it can generate enormous amounts of data. This report will not include events in which both source and destination users are null.

User Logins and Logouts

Reports the user accounts that log in and out the most. The table provides results by the name of the login action and category, the user account, the IP address, name, and zone of the affected system, and the date of the event.

Virus Infected Machines

Reports the systems with the most detected viruses by affected product. The table provides results by the virus name, the affected system and product, and the date of the event.

Vulnerabilities Management

Provides an overview of the vulnerabilities detected per host. You can view a trend of vulnerabilities reported over time, the most reported vulnerabilties, the assets with the most vulnerabilities, and vulnerabilities by severity.

Vulnerabilities Scanner Results

Reports vulnerabilities by type as detected by vulnerability scanners. The table provides results by the vulnerability, the IP address and name of the affected host, and the quantity found.

Vulnerability Scans and Unauthorized Access

Provides an overview of the scans, probes, and unauthorized access reported in your environment. You can view results by the systems with the most unauthorized access attempts, severity of events, the most scanned ports, the vulnerabilities scanned, and the signature of the riskiest vulnerabilities.

13 – Communications Security

Select Reports > Portal > Repository > Standard Content > IT GOV > ISO-27002 > *Dashboards* or *Reports* > ISO 13 – Communications Security.

Control 13: *Communications Security* of the ISO 27002 standard focuses on using cryptographic keys to protect the confidentiality, integrity, and availability of information.

To assess your enterprise's compliance with this requirement, use the following reports:

Dashboards	Reports
"Email Activities" on the next page "Peer to Peer Activity" on page 133 "Phishing Activities" on page 133	"Accessed Ports through Firewall" on the next page "Firewall Open Port Review" on the next page "Information Interception Events" on the next page "Insecure Services" on the next page "Interzone Traffic" on the next page "Organizational Information Leaks" on the next page "Personal Information Leaks" on page 133 "Processes by Asset" on page 133

Accessed Ports through Firewall

Reports all ports accessed through a firewall by port and number of events. The table provides results by IP address of the firewall device, the type and vendor of the firewall, and the port used.

Email Activities

Provides an overview of email activities in your enterprise. You can view the accounts by quantity of emails received and sent, as well as by the size of emails received and sent.

Firewall Open Port Review

Reports the ports open in firewalls by the number of access events per port. The table provides results by IP address of the firewall device, the type of firewall, the open port, the number of events, and when the most recent event occurred.

Information Interception Events

Reports the traffic interception events that indicate spoofing and man-in-the-middle attacks. The table provides results by the type of event, the IP address of the target and source systems, the number of events, and when the most recent event occurred.

Insecure Services

Reports the events by port number and type of insecure service, such as FTP or Telnet. The table provides results by the target port, target process, target and source IP addresses, the target host name, the product that reported the insecure service, and the number of events.

Interzone Traffic

Reports the communications that pass between different zones over time. The table provides results by the IP address, name, and zone of the target host; the source zone, the protocol used; and when the most recent communication occurred.

Organizational Information Leaks

Reports events associated with information leaks as reported by IDSs over time. The table provides results by the event, the source and target users, the number of events, and when the most recent event occurred.

Peer to Peer Activity

Provides an overview of peer-to-peer communication events. You can view a trend of communications over time, the total number of communications, communications by source IP address, and the relationship of communications that occur between source and target IP address.

Personal Information Leaks

Reports events that are associated with personal information leaks as reported by IDSs over time. The table provides results by the event, the source and target users, the number of events, and when the most recent event occurred.

Phishing Activities

Provides an overview of phishing activity in your enterprise. You can view a trend of phishing events over time, events received from suspicious domains, and number of events by recipient email and sender's email.

Processes by Asset

Reports the processes running on assets in your environment. The table provides results by the IP address, name, and zone of the host where the processes are running, the process, the application protocol used, the service, the product, and the number of running processes.

14 – System Acquisition, Development, and Maintenance

Select Reports > Portal > Repository > Standard Content > IT GOV > ISO-27002 > Reports > ISO 14 – System acquisition development and maintenance.

Control 14: *System acquisition, development, and maintenance* of the ISO 27002 standard focuses on incorporating information security throughout the lifecycle of the data. Your enterprise is expected to ensure the security of data in both test/development and product environments.

To assess your enterprise's compliance with this requirement, use the following report:

Dashboards	Reports
n/a	"Invalid Data Input" on the next page

Invalid Data Input

Reports events that indicate corrupt data input such as exceptionally long URLs or SNMP requests that exceed the allowed buffer size.

The table provides results by the type of event, the IP address and name for both the target and source of the host, and the number of events.

16 – Information Security Incident Management

Select Reports > Portal > Repository > Standard Content > ITGov > *Reports* or *Dashboards* > ISO 16: Information security incident management

Control 16: *Information security incident management* of the ISO 27002 standard expects your enterprise to effectively and consistently manage information security incidents.

To assess your enterprise's compliance with this requirement, use the following reports:

Dashboards	Reports
"Internal Reconnaissance" on the next page	"Confidential Breach Sources" below "Denial of Service" below "File Integrity Changes" on the next page "Information Systems Failures" on the next page "Integrity Breach Sources" on the next page "Internal Reconnaissance by Event" on the next page "Internal Reconnaissance by Source Address" on the next page "Internal Reconnaissance by Target Address" on page 136

Confidential Breach Sources

Reports the number of confidentiality breach events by IP addresses of the source system. The table provides results by the IP address, name, and zone of the source; the number of events; and when the most recent event occurred.

Denial of Service

Reports the number of denial of service (DoS) events by IP addresses of the targeted system. The table provides results by the IP address , name, and zone of the targeted system; the

type of DoS activity; and the number of events.

File Integrity Changes

Reports changes to files where the modification might compromise the integrity of the file. The table provides results by the path to the modified file, the IP address and name of the targeted host, the number of modifications, and when the most recent event occurred.

Information Systems Failures

Reports the number of changes to monitored files by target IP address and type of change. The report includes only events where agent severity is High or Very-High. The table provides results by the type of event; the IP address, name, and zone of the targeted system; and the number of events.

Integrity Breach Sources

Reports the number of attacks associated with integrity breaches, by source IP and type of breach. The table provides results by the type of breach event; the IP address, name, and zone of the source system; the number of events; and when the most recent event occurred.

Internal Reconnaissance

Provides an overview of events that indicate internal reconnaissance, which are attacks that occur within your organization's network, systems, and premises.

Internal Reconnaissance by Event

Reports the top events by the source IP address associated with the specified internal reconnaissance events. The table provides results by the type of event, the IP address, name, and zone of the target and source hosts; and the number of events.

You must specify at least one event by type.

Internal Reconnaissance by Source Address

Reports the number of internal reconnaissance events associated with the specified source IP address. The table provides results by the type of event, the IP address, name, and zone of the target and source hosts; and the number of events.

You must specify at least one IP address.

Internal Reconnaissance by Target Address

Reports the number of internal reconnaissance events associated with the specified target IP address. The table provides results by the type of event, the IP address, name, and zone of the target and source hosts; and the number of events.

You must specify at least one IP address.

17 – Information Security Aspects of Business Continuity Management

Select Reports > Portal > Repository > Standard Content > IT GOV > ISO-27002 > Reports > ISO 17 – Information security aspects of business continuity management.

Control 17: *Information security aspects of business continuity management* of the ISO 27002 standard expects that your business practices include managing the continuity of information security.

To assess your enterprise's compliance with this requirement, use the following report:

Dashboards	Reports
n/a	"Availability Attacks" below

Availability Attacks

Reports the number of events by targeted zone that indicate attacks to limit or prevent the availability of systems, networks, devices, or services in your enterprise. The table provides results by the type of event; the IP address, name, and zone of the targeted host; the number of events; and when the most recent event occurred.

Ensuring Compliance with PCI DSS

Select Reports > Portal > Repository > Standard Content > PCI.

The PCI Security Standards Council has established standards to ensure the security of payment account data. To help you comply with the PCI Data Security Standards, Recon provides the **Compliance Pack for PCI**. For more information about adding the pack to the Reports repository, see the *Solutions Guide for ArcSight Recon Compliance Pack for PCI*.

This pack includes dashboard and reports organized by the following PCI requirements:

Category	Dashboards	Reports
"1 – Maintain Firewalls to Protect Cardholder Data" on page 144	"Overview of Communication Activity from CDE" on page 149 "Overview of Communication Activity to CDE" on page 149	"Accessed Ports Through Firewall" on page 147 "Blocked Inbound Traffic to Card Holder Data Environment" on page 147 "Blocked Outbound Traffic from Card Holder Data Environment" on page 147 "Cardholder Data in the DMZ" on page 148 "External to Internal PCI Systems" on page 148 "Firewall Configuration Changes" on page 148 "Inbound Traffic to the Card Holder Data Environment" on page 148 "Internal PCI Systems to External" on page 148 "Network Routing Configuration Changes" on page 148 "Outbound Traffic from the Card Holder Data Environment" on page 149 "Personal Firewall Installed" on page 149 "Private IP Addresses Disclosure" on page 149 "Unauthorized Access to Card Holder Data Environment" on page 149 "Unauthorized Inbound Traffic to Card Holder Data Environment" on page 149 "Unauthorized Inbound Traffic to DMZ" on page 150 "Unauthorized Outbound Traffic from Card Holder Data Environment" on page 150 "VPN Configuration Changes" on page 150

Category	Dashboards	Reports
"2 – Do Not Use Default Security Parameters" on page 150	"Default Vendor Accounts Overview" on page 151 "Insecure Services – Dashboard" on page 151	"Default Vendor Accounts" on page 151 "Insecure Services – Report" on page 151 "Misconfigured Systems" on page 151 "Multiple Functions Implemented on a Server" on page 151 "Software Inventory" on page 151 "Unencrypted Administrative Accesses" on page 152
"3 – Protect Stored Cardholder Data" on page 152	n/a	"Credit Cards in Clear Text" on page 152
"4 – Encrypt Transmission of Cardholder Data" on page 152	n/a	"Cryptographic Hash Algorithm Related Vulnerabilities" on page 153 "Cryptographic Public Key Related Vulnerability Detected" on page 153 "Cryptographic Symmetric Key Related Vulnerabilities" on page 153 "Cryptographic Weak Protocol Vulnerability Detected" on page 153 "SSL or TLS Vulnerabilities" on page 153 "TLS BREACH Vulnerabilities" on page 154 "TLS CRIME Vulnerabilities" on page 154 "Wireless Encryption Violations" on page 154

Category	Dashboards	Reports
"5 – Use and Regularly Update Antivirus Software or Programs" on page 154	" Antivirus Activity" on page 155 " Malware Activities Overview" on page 156	"Disabled Antivirus and EDR" on page 155 "Failed Antivirus and EDR Updates" on page 155 "Installed Antivirus and EDR" on page 155 "Malicious Code Activities from CDE" on page 155 "Malware Activity" on page 156 "Malware Activity by Host" on page 156 "Spyware and Adware Activity" on page 156

Category	Dashboards	Reports
"6 – Maintain Secure Systems and Applications" on page 156	n/a	"Broken Authentication and Session Management" on page 157 "Buffer Overflows" on page 157 "Configuration Modifications by Host" on page 158 "Cross Site Request Forgery" on page 158 "Cross Site Scripting" on page 158 "Database Configuration Changes" on page 158 "Improper Access Control" on page 158 "Improper Error Handling" on page 159 "Injection Flaws" on page 159 "Insecure Cryptographic Storage" on page 159 "Meltdown or Spectre Vulnerable Assets" on page 159 "Operating System Changes" on page 159 "Outbound Communication from Development to Production" on page 159 "Outbound Communication from Production to Development " on page 159 "Security Patch Missing" on page 160 "SQL Injection Vulnerabilities" on page 160 "Use of Custom Accounts in Production" on page 160
"7 – Restrict Access to Cardholder Data" on page 160	"User Access Activity to Card Holder Data Environment" on page 161	"All Accesses to Cardholder Data Environment" on page 161 "All Accesses to Cardholder Data Environment by User" on page 161

Category	Dashboards	Reports
"8 – Assign a Unique ID to Each User" on page 161	"Password Policy Changes Overview" on page 162 "Windows Account Lockout" on page 163	"Clear Text Password Transmission" on page 162 "Password Policy Changes" on page 162 "Password Policy Minimum Age Changed" on page 162 "Successful Password Changes" on page 162 "Terminated User Activity" on page 163 "Terminated Users" on page 163 "Windows Account Lockouts by System" on page 163 "Windows Account Lockouts by User" on page 163
"9 – Restrict Physical Access to Cardholder Data" on page 163	"Failed Physical Facility Access - Dashboard" on page 164 "Successful Physical Facility Access" on page 164	"Failed Physical Facility Access - Report" on page 164 "Physical Facility Access Attempts" on page 164

Category	Dashboards	Reports
"10 – Track and Monitor Access to Cardholder Data" on page 164	"Firewall Events" on page 167	"Account Creation" on page 165 "Account Deletion" on page 165 "Account Modification" on page 166 "Administrative Actions Events" on page 166 "Administrative Authorization Changes" on page 166 "Anonymous User Activity in CDE" on page 166 "Audit Logs Cleared" on page 166 "Clock Synchronization Problems" on page 166 "Empty Origination of Event" on page 167 "Failed Administrative Actions" on page 167 "Failed Administrative Logins" on page 167 "Failed Logins" on page 167 "File Creations Deletions Modifications" on page 167 "IDS Events" on page 167 "Information System Failures" on page 168 "Successful Administrative Logins" on page 168 "Successful Logins to CDE" on page 168 "Successful User Logins" on page 168 "Successful User Logins by Host" on page 168 "User Group Creation" on page 168 "User Group Deletion" on page 168

Category	Dashboards	Reports
"11 – Test Security Systems and Processes Regularly" on page 168	"Attacks and Suspicious Activities Overview" on page 169 "Vulnerabilities Scanning" on page 172 Vulnerability Summary Overview	"Drill Down Assets with Buffer Overflow Vulnerabilities" on page 169 "Drill Down Assets with High Risk Vulnerabilities" on page 170 "Drill Down Assets with SSL and TLS Vulnerabilities" on page 170 "Drill Down CSRF Vulnerable Assets" on page 170 "Drill Down SQL Injection Vulnerable Assets" on page 170 "Drill Down XSS Vulnerable Assets" on page 170 "Exploit of Vulnerability" on page 171 "File Integrity Events" on page 171 "High Risk Vulnerabilities" on page 171 "Information Interception Events" on page 171 "Rogue Wireless AP Detected" on page 171 "Traffic Anomaly on Application Layer" on page 171 "Traffic Anomaly on Network Layer" on page 172 "Traffic Anomaly on Transport Layer" on page 172 "Vulnerability Summary by CVE" on page 172 "Vulnerability Summary by Host" on page 172 "Ensuring Compliance with PCI DSS" on page 136
"12 – Maintain a Policy that Addresses Information Security " on page 173	"Policy Violations - Dashboard" on page 173	"All Reporting Devices" on page 173 "Policy Violations - Report" on page 173 "Windows Domain Policy Changes" on page 173

1 – Maintain Firewalls to Protect Cardholder Data

Select Reports > Portal > Repository > Standard Content > PCI > *Reports* or *Dashboards* > Requirement 1: Firewall Configuration.

PCI Requirement 1 requires that you install and maintain a firewall configuration to protect data in a cardholder data environment (CDE). **Firewalls** control computer traffic in and out of your network, as well as to and from sensitive areas within secure or sensitive internal networks. To prove compliance with PCI DSS, you must monitor the firewalls at Internet connections and between any demilitarized zones (DMZs). You must also monitor the devices that manage traffic.

Use the following dashboards and reports to check for potential firewall vulnerabilities in your environment.

Dashboards	Reports

"Overview of Communication Activity from CDE" on page 149

"Overview of Communication Activity to CDE" on page 149

"Accessed Ports Through Firewall" on the next page

"Blocked Inbound Traffic to Card Holder Data Environment" on the next page

"Blocked Outbound Traffic from Card Holder Data Environment" on the next page

"Cardholder Data in the DMZ" on page 148

"External to Internal PCI Systems" on page 148

"Firewall Configuration Changes" on page 148

"Inbound Traffic to the Card Holder Data Environment" on page 148

"Internal PCI Systems to External" on page 148

"Network Routing Configuration Changes" on page 148

"Outbound Traffic from the Card Holder Data Environment" on page 149

"Personal Firewall Installed" on page 149

"Private IP

	Addresses Disclosure" on page 149 "Unauthorized Access to Card Holder Data Environment" on page 149 "Unauthorized Inbound Traffic to Card Holder Data Environment" on page 149 "Unauthorized Inbound Traffic to DMZ" on page 150 "Unauthorized Outbound Traffic from Card Holder Data Environment" on page 150 "VPN Configuration Changes" on page 150

Accessed Ports Through Firewall

Reports the firewalls that allowed the most traffic by port number. The table provides results by IP addresses for the firewall, the source system, and the destination system; the destination port; number of events; and the firewall rule number that triggered the event.

Blocked Inbound Traffic to Card Holder Data Environment

Reports the destination ports with traffic to the CDE from non-CDE systems that has been blocked the most often. The table provides results by IP addresses for the firewall, the source system, and the destination system; the destination port; the protocol used, number of events; and when the most recent event occurred.

Blocked Outbound Traffic from Card Holder Data Environment

Reports an overview of blocked traffic from the CDE to non-CDE systems over time. The table provides results by blocked outbound traffic per firewall. It lists the IP addresses for the firewall, the source system, and the destination system; the source and destination zones; affected port; and when the most recent event occurred.

Cardholder Data in the DMZ

Reports the internal systems that send the most communications to a DMZ, or less secure environment, in the specified time range. The table provides results by IP address of the source and destination systems, the affected ports, when the events occurred, and the number of events.

External to Internal PCI Systems

Reports the external systems that are communicating directly with PCI internal systems most often. The table provides results by the IP addresses and zones of the source and destination systems, the affected port, protocol used, and the number of events.

Firewall Configuration Changes

Reports the firewalls and devices with the most changes to their configuration. The table provides results by the IP address, product, and vendor of the device that was changed; the name and rule related to the change; the number of changes detected; and when the most recent event occurred.

Inbound Traffic to the Card Holder Data Environment

Reports the systems that allowed the most traffic to the CDE from non-CDE systems by destination address and port. The table provides results by the IP addresses for the firewall, the source system, and the destination system; the affected port; the protocol used; the number of events; and when the most recent event occurred.

Internal PCI Systems to External

Reports the CDE systems that communicate directly with external systems. PCI standards expects that your enterprise can justify this type of traffic. The table provides results by the IP address of the source system, destination system, and the device; the destination port; the protocol used; and the number of events.

Network Routing Configuration Changes

Reports the network routing devices that have had the most configuration changes in the specified time range. The table provides results by the IP address for the device, the type of device; the event name; number of events; and when the most recent event occurred.

Outbound Traffic from the Card Holder Data Environment

Reports the systems that allowed traffic from the CDE to non-CDE systems by destination IP address. The table provides results by the IP addresses for the device, the source system, and the destination system; the affected port; the protocol used; number of events; and when the most recent event occurred.

Overview of Communication Activity from CDE

Provides, in charts and a table, an overview of communication going out from the CDE. You can view the target and source IP addresses, target ports, and the block source IP addresses.

Overview of Communication Activity to CDE

Provides, in charts and a table, an overview of communication coming into the CDE. You can view the target and source IP addresses, target ports, and the block source IP addresses.

Personal Firewall Installed

Reports the servers with a personal firewall installed. PCI standards require that users install personal firewall software on any device, such as a laptop, that is used to access the cardholder data environment and also might connect to the Internet when outside the PCI network. The table lists the IP address and name of the system hosting the personal firewall, as well as the more recent time that the firewall was detected.

Private IP Addresses Disclosure

Reports the RFC1918 IP addresses with the most communication with public IP addresses. The table provides results by IP address of the source and associated destination systems, the destination port, the protocol used, and the number of events.

Unauthorized Access to Card Holder Data Environment

Reports the accounts with the most unauthorized attempts to access the CDE. The table provides results by the user account, source and destination IP addresses, time the events occurred, and the number of events.

Unauthorized Inbound Traffic to Card Holder Data Environment

Reports the IP addresses in the cardholder environment that have experienced the most unauthorized traffic to the CDE from non-CDE systems. The table provides results by the source and destination IP addresses, the ports of the destination system, the protocol used, the number of events, and when the most recent event occurred.

Unauthorized Inbound Traffic to DMZ

Reports the systems with the highest amount of unauthorized traffic to the DMZ. The table provides results by the IP addresses for the device, the source system, and the destination system; the source zone; affected port; number of events; and when the most recent event occurred.

Unauthorized Outbound Traffic from Card Holder Data Environment

Reports the ports with the most unauthorized traffic from the CDE to non-CDE systems. The table provides results by the IP addresses for the device, the source system, and the destination system; the destination zone; the affected port; the protocol used; and number of events.

VPN Configuration Changes

Reports the VPN gateways with the most changes to their configuration. The table provides results by IP address of the VPN, the policies or configurations changed, the type of VPN, and number of events.

2 – Do Not Use Default Security Parameters

Select Reports > Portal > Repository > Standard Content > PCI > *Reports* or *Dashboards* > Requirement 2: Default Security Parameters.

PCI Requirement 2 addresses the use of vendor-supplied default settings, such as passwords and account names. These are known values and can be exploited by malicious users. While devices and firewalls installed by IT administrators might have strong security process, users who install software and add devices might not follow good security practices.

Use the following dashboards and reports to check for default security parameters in your environment.

Dashboards	Reports
"Default Vendor Accounts Overview" on the next page "Insecure Services – Dashboard" on the next page	"Default Vendor Accounts" on the next page "Insecure Services – Report" on the next page "Misconfigured Systems" on the next page "Multiple Functions Implemented on a Server" on the next page "Software Inventory" on the next page "Unencrypted Administrative Accesses" on page 152

Default Vendor Accounts

Reports default vendor accounts by username. The table provides results by the IP address and name of the device's address, the vendor's name, the account name, and quantity.

Default Vendor Accounts Overview

Provides, in several charts, an overview of default vendor accounts. You can view the accounts associated with the most events, account activity over time, the IP addresses associated with the accounts, and the most active vendors.

Insecure Services – Dashboard

Provides, in charts and table, insecure events by port number and IP address, activities by day, and the products that report insecure services in other systems.

Insecure Services – Report

Reports insecure events by port number. The table provides results by the target port, target process, target and source IP addresses, the target host name, the product that reported the insecure service, and the number of events.

Misconfigured Systems

Reports systems with the most misconfiguration events reported in your environment. In general, the most common vulnerability in your environment is misconfigured operating systems, frameworks, libraries, and applications. Misconfigurations include missing security patches or updates, incomplete or ad hoc configurations, use of insecure default configurations, poorly configured HTTP headers, and error messages that contain sensitive information. The table provides results by IP address and name of the misconfigured system, the name of the event, and number of events.

Multiple Functions Implemented on a Server

Reports the servers that have multiple functions installed on them. For example, a server might have functions such as DNS, a Web server, and a database.

Software Inventory

Reports the software found by IP address and host name.

Unencrypted Administrative Accesses

Reports the accounts that have had unencrypted administrative access events. The table provides results by the IP address and name of the host, the affected account, the port used, affected process, and number of events.

3 – Protect Stored Cardholder Data

Select Reports > Portal > Repository > Standard Content > PCI > Reports > Requirement 3: Protect Stored Cardholder Data.

PCI Requirement 3 ensures that cardholder data cannot be read or used by individuals who maliciously or unintentionally access encrypted data. You must have security measures to encrypt, truncate, mask, or hash critical components of the data.

To assess your enterprise's compliance with this requirement, use the following report:

Credit Cards in Clear Text

Reports the hosts where credit card data has been detected in clear text format. The table provides results by the affected host and reporting device IP addresses, the signature ID, and when the clear text was detected.

4 – Encrypt Transmission of Cardholder Data

Select Reports > Portal > Repository > Standard Content > Reports > Requirement 4: Encryption Transmission.

PCI Requirement 4 focuses on managing and maintaining the security of the card holder data when it is transmitted over open or public networks. Transmitted data should be encrypted. Malicious users can exploit vulnerabilities in cryptographic hashes and keys, as well as through SSL and TLS. For example, the Heartbleed Bug is a known SSL vulnerability.

To assess your enterprise's compliance with this requirement, use the following reports:

Dashboards	Reports
n/a	"Cryptographic Hash Algorithm Related Vulnerabilities" below "Cryptographic Public Key Related Vulnerability Detected" below "Cryptographic Symmetric Key Related Vulnerabilities" below "Cryptographic Weak Protocol Vulnerability Detected" below "SSL or TLS Vulnerabilities" below "TLS BREACH Vulnerabilities" on the next page "TLS CRIME Vulnerabilities" on the next page "Wireless Encryption Violations" on the next page

Cryptographic Hash Algorithm Related Vulnerabilities

Reports events by host name that indicate potential vulnerabilities related to hash algorithms. All cryptographic hashes that directly use the full output of a Merkle–Damgård construction are vulnerable to length extension attacks. The table provides results by name of the event, host and IP address, and number of events.

Cryptographic Public Key Related Vulnerability Detected

Reports flaws found in cryptographic public keys on hosts, as reported by vulnerability scanners in your environment. The table provides results by name of the event, host and IP address, and number of events.

Cryptographic Symmetric Key Related Vulnerabilities

Reports vulnerabilities related to cryptographic symmetric keys by the address or host name of the target asset. The table provides results by the target asset, the device vendor and product, the number of events, and when the most recent event occurred.

Cryptographic Weak Protocol Vulnerability Detected

Reports all vulnerabilities associated with weak cryptographic protocol. The table provides results by the vulnerability name, the affected assets, the number of events, and when the most recent event occurred.

SSL or TLS Vulnerabilities

Reports all SSL and TLS vulnerabilities detected by host name. The table provides results by name of the event, host and IP address, and number of events.

TLS BREACH Vulnerabilities

Reports TLS BREACH vulnerabilities detected by host name. A TLS BREACH attack is a form of the CRIME attack against HTTP compression. The table provides results by name of the event, host and IP address, and number of events.

TLS CRIME Vulnerabilities

Reports the hosts detected of having vulnerabilities to a TLS CRIME attack. In a CRIME attack, malicious users access the content of secret authentication cookies, so they can hijack sessions of an authenticated web session, then launch additional attacks. The table provides results by name of the event, host and IP address, and number of events.

Wireless Encryption Violations

Reports the hosts that have wireless encryption violations, as detected by vulnerability scanners. The table provides results by name of the event, host and IP address, and number of events.

5 – Use and Regularly Update Antivirus Software or Programs

Select Reports > Portal > Repository > Standard Content > PCI > *Reports* or *Dashboards* > Requirement 5: Antivirus.

PCI Requirement 5 focuses on preventing malware, such as worms, viruses, and trojans, from infecting the cardholder data environment (CDE). This type of malware can enter the network through common business activities and processes: employee email, Internet usage, cell phones, or storage devices. Malware can then damage systems by exploiting system security vulnerabilities or trying to steal confidential information. Your enterprise should install and maintain antivirus software on all devices frequently affected by malware to protect networks from existing and emerging threats.

To assess your enterprise's compliance with this requirement, use the following dashboards and reports:

Dashboards	Reports
" Antivirus Activity" below " Malware Activities Overview" on the next page	"Disabled Antivirus and EDR" below "Failed Antivirus and EDR Updates" below "Installed Antivirus and EDR" below "Malicious Code Activities from CDE" below "Malware Activity" on the next page "Malware Activity by Host" on the next page "Spyware and Adware Activity" on the next page

Antivirus Activity

Provides charts for an overview of antivirus activities in the CDE. You can view the trends of antivirus cleaning/quarantining attempts and failures over time, a trend of failed cleaning and the number of times antivirus has failed to update and the associated agent, and the number of events by device vendor.

Disabled Antivirus and EDR

Reports events associated with disabling antivirus and EDR programs by target host. The table provides results by the target host, the antivirus or EDR program affected, the user that disabled the program, the number of events, and when the event occurred.

Failed Antivirus and EDR Updates

Reports events where antivirus and EDR programs failed to update by target host. The table provides results by the target host, the antivirus or EDR program affected, the name and userID that disabled the program, the number of events, and when the event occurred.

Installed Antivirus and EDR

Reports events where antivirus and EDR programs are installed by type of program. The table provides results by the type of antivirus or EDR product, the location of the program, and the number of events.

Malicious Code Activities from CDE

Reports malicious code activity sent from the CDE. The table provides results by the source and target addresses, the type of event, the product, and the number of events.

Malware Activities Overview

Provides an overview of all malware activity in the CDE. You can view the trends of malware activities over time, top signature IDs, top affected systems, and the top reporting products.

Malware Activity

Reports the malware detected in the CDE. The table provides results by the type of malware, the target asset, the number of events, and the when the event occurred.

Malware Activity by Host

Reports the malware activity by target host. The table provides results by the type of malware, the target asset, the number of events, and the when the event occurred.

Spyware and Adware Activity

Reports target hosts where spyware or adware has been detected. The table provides results by the affected asset, the type of spyware or adware, the event class, the number of events, and the when the event occurred.

6 – Maintain Secure Systems and Applications

Select Reports > Portal > Repository > Standard Content > PCI > *Reports* or *Dashboards* > Requirement 6: Secure Systems and Applications.

PCI Requirement 6 sets the expectation that you apply security patches to all applications and systems in the cardholder data environment (CDE) to protect them from malicious and unintentional misuse. The patches should be evaluated to ensure that they do not conflict with current security configurations. You must also ensure that in-house development teams practice secure coding techniques. Applications that store sensitive data must be able to protect the data.

To assess your enterprise's compliance with this requirement, use the following reports:

Dashboards	Reports
n/a	"Broken Authentication and Session Management" below "Buffer Overflows" below "Configuration Modifications by Host" on the next page "Cross Site Request Forgery" on the next page "Cross Site Scripting" on the next page "Database Configuration Changes" on the next page "Improper Access Control" on the next page "Improper Error Handling" on page 159 "Injection Flaws" on page 159 "Insecure Cryptographic Storage" on page 159 "Meltdown or Spectre Vulnerable Assets" on page 159 "Operating System Changes" on page 159 "Outbound Communication from Development to Production" on page 159 "Outbound Communication from Production to Development " on page 159 "Security Patch Missing" on page 160 "SQL Injection Vulnerabilities" on page 160 "Use of Custom Accounts in Production" on page 160

Broken Authentication and Session Management

Reports events associated with broken authentication and session management over time. The table provides results by the target asset, name and signature ID of the vulnerability, and the number of events.

Buffer Overflows

Reports vulnerabilities associated with buffer overflows by CDE asset. This type of vulnerability occurs when a developer fails to appropriately manage memory for user-controlled data. A malicious user could put more data into a pre-allocated memory buffer than the buffer can hold, dramatically impacting the operation of a program. The table provides results by the affected asset, the detected vulnerability, the signature ID of the vulnerability, and when the most recent event occurred.

Configuration Modifications by Host

Reports modifications made to CDE assets. The table provides results by the affected asset, the type of modification, the user who made the change, the number of events, and when the most recent event occurred.

Cross Site Request Forgery

Reports assets that might be vulnerable to a cross-site request forgery (XSRF or CSRF) attack. In an CSRF attack, also known as a one-click attack or session riding, a malicious user submits unauthorized commands to a web application from a user account that the application trusts. The table provides results by the targeted asset and when the most recent event occurred.

Cross Site Scripting

Reports the signature ID of cross-site scripting (XSS) attacks by volume. Vulnerabilities associated with XSS enable malicious users to inject code in legitimate web pages or applications that executes harmful scripts in the user's web browser when the browser parses data. The scripts might hijack user sessions, deface web sites, or redirect users to harmful sites. A web application or web page becomes vulnerable when it includes untrusted data; data without proper validation or escaping; or data supplied by users through an API that can create HTML or Java-script. XSS attacks tend to occur in forums, message boards, and web pages that allow comments. Malicious users can execute XSS attacks in VPSCript, ActiveX, Flash, and CSS. However, this type of injection attack most commonly occurs in Java Script. The table provides results by the signature ID of the event, the target asset, the number of events, and when the most recent event occurred.

Database Configuration Changes

Reports changes to the database configuration by affected asset. The table provides results by the database host, the modification made, the user who made the change, the number of changes, and when the most recent change occurred.

Improper Access Control

Reports vulnerabilities associated with improper access controls. The table provides results by the signature ID of the event, the target asset, the number of events, and when the most recent event occurred.

Improper Error Handling

Reports vulnerabilities associated with improper handling of errors by affected assets. The table provides results by the signature ID of the event, the target asset, and when the most recent event occurred.

Injection Flaws

Reports the assets with the most injection flaws. The table provides results by the affected asset, the injection flaw and its signature ID, and when the event occurred.

Insecure Cryptographic Storage

Reports the IP addresses of systems where sensitive data is not stored securely. The table provides results by the affected asset, the event, the number of events, and when the most recent event occurred.

Meltdown or Spectre Vulnerable Assets

Reports the assets with the most Meltdown or Spectre vulnerabilities. The table provides results by the affected asset, the vulnerability and its signature ID, the number of events, and when the most recent event occurred.

Operating System Changes

Reports changes to operating systems. The table provides results by the target asset, the change, the outcome of the change, and the number of changes.

Outbound Communication from Development to Production

Reports all communication sent from the development environment to the production environment. The table provides results by the source and target addresses, the port used, the transportation protocol, and the number of events.

In the logical model, you must edit the `isSourceZonePCIDevelopment` and `isDestinationZonePCIProduction` variables to indicate the respective zones for development and production.

Outbound Communication from Production to Development

Reports all communication sent from the production environment to the development environment. The table provides results by the source and target addresses, the port used, the transportation protocol, and the number of events.

In the logical model, you must edit the `isSourceZonePCIProduction` and `isDestinationZonePCIDevelopment` variables to indicate the respective zones for production and development.

Security Patch Missing

Reports assets by IP address with missing security patches. One of the most common ways to reduce your environment's attack surface is to ensure that all systems have the most recent security patches applied. The table provides results by the affected asset, the vulnerability and signature ID associated with the missing patch, the number of events, and when the most recent event occurred.

SQL Injection Vulnerabilities

Reports SQL injection vulnerabilities by asset. In a SQL injection attack, a malicious user can interfere with the queries that an application makes to its database. The user could view delete, or modify data not usually available for retrieval. A malicious user could also use SQL injections to start a denial-of-service attack or compromise other services, servers, or infrastructure. The table provides results by the target assets, the vulnerability and its signature ID, the number of events, and when the most recent event occurred.

Use of Custom Accounts in Production

Reports events in the production environment associated with the specified list of accounts. The table provides results by the specified accounts, the target asset, the number of events, and when the most recent event occurred.

You must enter the accounts that you want to include in the report. Use commas to separate the values.

7 – Restrict Access to Cardholder Data

Select Reports > Portal > Repository > Standard Content > PCI > *Reports* or *Dashboards* > Requirement 7: Restrict Access By Business Need to Know.

PCI Requirement 7 focuses on controlling access to cardholder data, thus limiting access privileges only to users who need to know the data according to your enterprise's needs. Usually, enterprises apply the principle of least privilege when granting access rights in the cardholder data environment (CDE).

To assess your enterprise's compliance with this requirement, use the following dashboards and reports:

Dashboards	Reports
"User Access Activity to Card Holder Data Environment" below	"All Accesses to Cardholder Data Environment" below "All Accesses to Cardholder Data Environment by User" below

All Accesses to Cardholder Data Environment

Reports the most accessed hosts in the CDE. The table provides results by the target host name and IP address, the target user, the source user and address, and the number of events.

All Accesses to Cardholder Data Environment by User

Reports all access activity in the CDE by the user. By default, the report lists user activities. The table provides results by the target host name and address, the target user, the port used, the source address, and the number of events.

In the logical model, use the isDestinationUserPCI variable to specify the users in the CDE that you want to include in the reports. For more information, see the *Solutions Guide for ArcSight Recon Compliance Pack for PCI*.

User Access Activity to Card Holder Data Environment

Provides, in charts and a table, an overview of user access activities in the CDE. You can view a trend of activity over time, as well as events by target users, target IP address, and source IP address.

8 – Assign a Unique ID to Each User

Select Reports > Portal > Repository > Standard Content > PCI > *Reports* or *Dashboards* > Requirement 8: Unique User ID.

PCI Requirement 8 covers identification and authentication for all access to system components in the cardholder data environment (CDE). Basically, your enterprise must maintain and monitor changes to user accounts and password policies to prevent malicious users from gaining access to the CDE through weak passwords or by changing password policies. This requirements applies to all accounts with administrative features, including point-of-sale accounts; accounts used by vendors and third parties; and any account used to view cardholder data or access cardholder data or to access systems with cardholder data. This requirement does not apply to end-user accounts used by consumers.

To assess your enterprise's compliance with this requirement, use the following dashboards and reports:

Dashboards	Reports
"Password Policy Changes Overview" below "Windows Account Lockout" on the next page	"Clear Text Password Transmission" below "Password Policy Changes" below "Password Policy Minimum Age Changed" below "Successful Password Changes" below "Terminated User Activity" on the next page "Terminated Users" on the next page "Windows Account Lockouts by System" on the next page "Windows Account Lockouts by User" on the next page

Clear Text Password Transmission

Reports events by IP address where passwords were transmitted in clear text. The table provides results by the target host name and IP address, the port used, the number of events, and when the clear text password was detected.

Password Policy Changes Overview

Provides, in charts and a table, an overview of policy changes on CDE assets. You can view a trend of changes made over time, changes to target user accounts, changes to target IP addresses, and changes by type.

Password Policy Changes

Reports changes to the password policy over time in the CDE. The table provides results by the target IP address, the user who made the change, the change made, the number of events, and when the change occurred.

Password Policy Minimum Age Changed

Reports changes to the policy for the minimum password age over time in the CDE. The table provides results by the target IP address, the user who made the change, the change made, the number of events, and when the change occurred.

Successful Password Changes

Reports successful password changes over time in the CDE. The table provides results by the target IP address and host name, the affected user account, the number of events, and when the most recent event occurred.

Terminated User Activity

Reports user accounts that have been terminated but show successful authentication events after termination. The table provides results by the terminated account and when successful authentication occurred.

Terminated Users

Reports all user accounts terminated in the CDE by termination date. The table provides results by the terminated account and when the account was terminated.

Windows Account Lockout

Provides, in charts and a table, an overview of Windows accounts that have been locked out. You can view a trend of events over time, events by target IP address, and events by the accounts locked out.

Windows Account Lockouts by System

Reports, by host system, all Windows accounts that have been locked out. The table provides results by the target host name, IP address, domain, and user; the number of lockouts; and when the most recent event occurred.

Windows Account Lockouts by User

Reports, by user and domain, all Windows accounts that have been locked out. The table provides results by the target domain and user, the number of lockouts, and when the most recent event occurred.

9 – Restrict Physical Access to Cardholder Data

Select Reports > Portal > Repository > Standard Content > PCI > *Reports* or *Dashboards* > Requirement 9: Physical Access.

PCI Requirement 9 expects your organization to restrict access to devices that allow an individual physical access to the systems that store cardholder data, thus limiting the ability for malicious users to access or destroy the devices, data, systems, or hard copies.

By default, these reports and dashboards assume all assets are associated with physical access. To specify specific locations and buildings, update the isPCIBuilding variable in the data worksheet for each PCI Requirement 9 report or dashboard. For more information, see the *Solutions Guide for ArcSight Recon Compliance Pack for PCI*.

To assess your enterprise's compliance with this requirement, use the following dashboards and reports:

Dashboards	Reports
"Failed Physical Facility Access - Dashboard" below	"Failed Physical Facility Access - Report" below
"Successful Physical Facility Access" below	"Physical Facility Access Attempts" below

Failed Physical Facility Access - Dashboard

Provides, in charts and table, an overview of failed attempts to access physical facilities. You can view a trend of access activity over time, as well as activity by reporting device, location, and user.

Failed Physical Facility Access - Report

Reports the number of failed attempt to access physical facilities by location. The table provides results by the target location, the user involved, the number of attempts, and when the attempt occurred.

Physical Facility Access Attempts

Reports the number of attempts to access physical facilities by location and user. The table provides results by the target location, the user involved, the outcome of the attempt, the number of attempts, and when the most recent event occurred.

Successful Physical Facility Access

Provides, in charts and table, an overview of successful attempts to access physical facilities. You can view a trend of access activity over time, as well as activity by reporting device, location, and user.

10 – Track and Monitor Access to Cardholder Data

Select Reports > Portal > Repository > Standard Content > PCI > *Reports* or *Dashboards* > Requirement 10: Track and Monitor Data Access.

PCI Requirement 10 focuses on tracking changes to user accounts and groups to detect and prevent data breaches within the cardholder data environment (CDE). Malicious users might create groups or accounts to grant them access to sensitive data, then delete their changes to hide their activity.

To assess your enterprise's compliance with this requirement, use the following dashboard and reports:

Dashboards	Reports
"Firewall Events" on page 167	"Account Creation" below "Account Deletion" below "Account Modification" on the next page "Administrative Actions Events" on the next page "Administrative Authorization Changes" on the next page "Anonymous User Activity in CDE" on the next page "Audit Logs Cleared" on the next page "Clock Synchronization Problems" on the next page "Empty Origination of Event" on page 167 "Failed Administrative Actions" on page 167 "Failed Administrative Logins" on page 167 "Failed Logins" on page 167 "File Creations Deletions Modifications" on page 167 "IDS Events" on page 167 "Information System Failures" on page 168 "Successful Administrative Logins" on page 168 "Successful Logins to CDE" on page 168 "Successful User Logins" on page 168 "Successful User Logins by Host" on page 168 "User Group Creation" on page 168 "User Group Deletion" on page 168

Account Creation

Reports all user accounts created. The table provides results by IP address or host name of the system, as well as the name of the new account.

Account Deletion

Reports all user accounts that have been deleted. The table provides results by name of the account that made the change, IP address or host name of the system, and event name for the deleted account.

Account Modification

Reports all user accounts that have been modified. The table provides results by the type of modification, name of the changed account, the account that made the change, and the IP address or host name of the system.

Administrative Actions Events

Reports all actions, except logins, made by administrative users. The table provides results by the user name, device event class, number of events, and when the change occurred.

Administrative Authorization Changes

Reports all changes authorized by administrative users. The table provides results by the source and target user, the number of changes, and when the change occurred.

Anonymous User Activity in CDE

Reports all logins to the CDE by anonymous users. The table provides details about the user, the affected host, the number of attempted logins, and when the most recent event occurred.

By default, the report includes all users who log in to the CDE because the variable `isUserNameAnonymous` is set to *yes*. To make the report more specific, in the logical model, enter the list of anonymous users for the variable `isUserNameAnonymous`, as shown in the example. For more information, see the *Solutions Guide for ArcSight Recon Compliance Pack for PCI*.

Audit Logs Cleared

Reports the audit logs cleared by user. The table provides results by the user, the affected host, the number of events, and when the most recent event occurred.

Clock Synchronization Problems

Reports the number of assets with clock synchronization issues over time. In SSL, clocks are used for certificate validation. A malicious user could modify the server or client clock to disregard dates in certificates. Then that user will be able to impersonate the server forever even if the certificate expires. The table provides details about the affected asset and when the most recent event occurred.

Empty Origination of Event

Reports events in which the source, such as user, address, device or hostname, cannot be identified. The table provides results by the anomaly's name, the number of events, and when the most recent event occurred.

Failed Administrative Actions

Reports failed actions, except logins, by administrative users. The table provides results by the target user and host, device event class, the affected product, the number of failed attempts, and when the most recent event occurred.

Failed Administrative Logins

Reports the number of failed logins by administrative users. The table provides results by the target host, administrative user, and the number of failed attempts.

Failed Logins

Reports the number of failed logins by user. The table provides results by the target host, administrative user, and the number of failed attempts.

File Creations Deletions Modifications

Reports the file creations, deletions, and modifications by host. The table provides results by the asset, the type of activity, outcome of the activity, the number of events, and when the most recent event occurred.

Firewall Events

Provides, in charts and a table, an overview of firewall events. You can view a trend of firewall events overtime, the number of times a firewall rule has been hit, the firewalls by vendor, and products reporting the events.

IDS Events

Reports all events recorded by the IDSs in your enterprise. The table provides results by the IDS device, the type of event, the number of events, and when the most recent event occurred.

Information System Failures

Reports all failures associated with information systems. The table provides results by the target asset, the type of failure, the device vendor, and the number of failure events.

Successful Administrative Logins

Reports all successful logins by administrative users. The table provides results by the target asset, the user, and the number of logins.

Successful Logins to CDE

Reports all successful logins within the CDE. The table provides results by the target asset, the user, the number of logins, and when the most recent login occurred.

Successful User Logins

Reports all successful logins by user. The table provides results by the target asset, the user, the number of logins, and when the most recent login occurred.

Successful User Logins by Host

Reports all successful user logins by host. The table provides results by the target asset, the user, the number of logins, and when the most recent login occurred.

User Group Creation

Reports all user groups created. The table provides results by the event, the new user group, and the user who created the account.

User Group Deletion

Reports all user groups deleted. The table provides results by the event, the user group deleted, and the user who deleted the account.

11 – Test Security Systems and Processes Regularly

Select Reports > Portal > Repository > Standard Content > PCI > *Reports* or *Dashboards* > Requirement 11: Test Systems and Processes.

PCI Requirement 11 focuses on frequently testing your processes and the security system components of your cardholder data environment, such as performing regular vulnerability

scans. PCI expects your enterprise to keep your processes and systems current with evolving security issues.

To assess your enterprise's compliance with this requirement, use the following dashboards and reports:

Dashboards	Reports
"Attacks and Suspicious Activities Overview" below "Vulnerabilities Scanning" on page 172 "Vulnerability Type Overview" on page 172	"Drill Down Assets with Buffer Overflow Vulnerabilities" below "Drill Down Assets with High Risk Vulnerabilities" on the next page "Drill Down Assets with SSL and TLS Vulnerabilities" on the next page "Drill Down CSRF Vulnerable Assets" on the next page "Drill Down SQL Injection Vulnerable Assets" on the next page "Drill Down XSS Vulnerable Assets" on the next page "Exploit of Vulnerability" on page 171 "File Integrity Events" on page 171 "High Risk Vulnerabilities" on page 171 "Information Interception Events" on page 171 "Rogue Wireless AP Detected" on page 171 "Traffic Anomaly on Application Layer" on page 171 "Traffic Anomaly on Network Layer" on page 172 "Traffic Anomaly on Transport Layer" on page 172 "Vulnerability Summary by CVE" on page 172 "Vulnerability Summary by Host" on page 172 "Vulnerability Summary Overview" on page 172

Attacks and Suspicious Activities Overview

Provides, in charts and a table, an overview of attacks and suspicious events. You can view the IP addresses generating the most attacks, the systems that are the target of most attacks, a trend of attacks over time, and the top events.

Drill Down Assets with Buffer Overflow Vulnerabilities

Lists assets that might be vulnerable to buffer overflow. This type of vulnerability occurs when a developer fails to appropriately manage memory for user-controlled data. A

malicious user could put more data into a pre-allocated memory buffer than the buffer can hold, dramatically impacting the operation of a program.

Drill Down Assets with High Risk Vulnerabilities

Reports assets that might be vulnerable to listed high-risk security threats. High-risk vulnerabilities represent those that are relatively easy for attackers to exploit and gain control over system components. Many high-risk vulnerabilities can temporarily or permanently disrupt enterprise operations.

Drill Down Assets with SSL and TLS Vulnerabilities

Reports assets that might have the listed TLS or SSL vulnerability. For example, malicious users can exploit a known vulnerability in SSL with the Heartbleed Bug.

Drill Down CSRF Vulnerable Assets

Reports assets that might be vulnerable to the listed cross-site request forgery (XSRF or CSRF) attack. In a CSRF attack, also known as a one-click attack or session riding, a malicious user submits unauthorized commands to a web application from a user account that the application trusts.

Drill Down SQL Injection Vulnerable Assets

Reports assets that might be vulnerable to the listed SQL injection attacks. In a SQL injection attack, a malicious user can interfere with the queries that an application makes to its database. The user could view delete, or modify data not usually available for retrieval. A malicious user could also use SQL injections to start a denial-of-service attack or compromise other services, servers, or infrastructure.

Drill Down XSS Vulnerable Assets

Reports assets that might be vulnerable to the listed cross-site scripting (XSS) attacks. Vulnerabilities associated with XSS enable malicious users to inject code in legitimate web pages or applications that executes harmful scripts in the user's web browser when the browser parses data. The scripts might hijack user sessions, deface websites, or redirect users to harmful sites. A web application or web page becomes vulnerable when it includes untrusted data; data without proper validation or escaping; or data supplied by users through an API that can create HTML or Java-script. XSS attacks tend to occur in forums, message boards, and web pages that allow comments. Malicious users can execute XSS attacks in VBSCript, ActiveX, Flash, and CSS. However, this type of injection attack most commonly occurs in Java Script.

Exploit of Vulnerability

Reports events that indicate an attempt to exploit a given detected vulnerability. The table provides results by the vulnerability, IP address and name of the affected system, number of events associated with the vulnerability, and when the most recent event occurred.

File Integrity Events

Reports events that indicate file integrity might be compromised in your environment. File integrity monitoring, also known as change monitoring, checks operating system files, Windows registries, application software, Linux system files, and more, for changes that might indicate an attack. The table provides results by the signature ID, IP address and name of the affected system, the number of events, and when the most recent event occurred.

High Risk Vulnerabilities

Reports the systems with the greatest likelihood of being exploited based on the reported vulnerabilities. The table provides results by the vulnerability, the signature ID, name of the affected system, and when the most recent event occurred.

Information Interception Events

Reports traffic interception events that indicate spoofing or man-in-the-middle attacks. The table provides results by the signature ID, details of the source and destination addresses, the number of events, and when the most recent event occurred.

Rogue Wireless AP Detected

Reports rogue wireless access points (AP) found in your environment. A user might install a rogue AP unintentionally or maliciously in an office or data center without the knowledge or permission from the system administrator via the wired infrastructure. The chart shows rogue APs found over time. The table provides results by the device ID and name, when the event occurred, and the number of events.

Traffic Anomaly on Application Layer

Reports all the traffic anomalies found in the application layer. Malicious users attack the application layer of an application, which specifies the communication protocols and interface methods used by hots in the network, to disrupt processes and services on a web server or application. The table provides results by signature ID, details of the affected system or product, the number of events, and when the most recent event occurred.

Traffic Anomaly on Network Layer

Reports all the traffic anomalies found in the network layer. This layer supports communications by sending packets of data back and forth between different networks, and thus can be vulnerable to a large variety of attacks. The table provides results by the destination and source systems, the number of events, and when the most recent event occurred.

Traffic Anomaly on Transport Layer

Reports all the traffic anomalies found in the transport layer. In this layer, a malicious user might highjack session by taking control of a session between two nodes after the initial authentication process is complete. The table provides results by signature ID, the destination and source systems, the number of events, and when the most recent event occurred.

Vulnerability Summary by CVE

Reports vulnerabilities by CVE and severity. The table provides results by the CVE, its severity, the affected asset, and when the most recent event occurred.

Vulnerability Summary by Host

Reports vulnerabilities found by host. The table provides results by the CVE, its severity, the affected asset, and when the most recent event occurred.

Vulnerability Summary Overview

Reports all the vulnerabilities found in the PCI environment. The table provides results by the vulnerability name, CVE, the common vulnerability score (CVSS), signature ID, the affected asset, and when the most recent event occurred.

Vulnerabilities Scanning

Provides, in several charts, the details of reported vulnerabilities over time. You can view the assets with the most high-risk vulnerabilities, the most reported vulnerabilities, and the assets with vulnerabilities including the hostnames.

Vulnerability Type Overview

Provides charts for an overview of vulnerabilities by category: SQL, XSS, CSRF, SSL, high-risk, and buffer overflow. You can drill down in the charts to identify the affected assets.

12 – Maintain a Policy that Addresses Information Security

Select Reports > Portal > Repository > Standard Content > PCI > *Reports* or *Dashboards* > Requirement 12: Maintain Information Security Policy.

PCI Requirement 12 expects your enterprise to maintain a policy that addresses the information security for all personnel who are associated with your enterprise or have some form of access to the cardholder's data system. Personnel should know the enterprise's expectations for handling cardholder data, and should know their responsibilities for protecting the sensitivity of the data.

To assess your enterprise's compliance with this requirement, use the following dashboards and reports:

Dashboards	Reports
"Policy Violations - Dashboard" below	"All Reporting Devices" below "Policy Violations - Report" below "Windows Domain Policy Changes" below

All Reporting Devices

Lists all reporting devices in the environment by number of events. PCI expects that you maintain an inventory of devices and check for unapproved devices. The table lists device by product, vendor, IP address, and zone.

Policy Violations - Dashboard

Provides , in charts and a table, an overview of policy violations. You can view the number of violations by day, the IP addresses and signature IDs associated with violations, and the users with the most violations.

Policy Violations - Report

Reports policy violations by IP address. The table lists the details of the affected host system, the number of events, and when the events occurred.

Windows Domain Policy Changes

Reports changes to the Windows domain policy by associated IP address. The table lists the details of the affected host system and the number of changes.

Ensuring Compliance with SOX Standards

Select Reports > Portal > Repository > Data Compliance Content > SOX.

The Sarbanes-Oxley Act (SOX) is a United States federal law that was enacted in 2002. The stated purpose of the law is to protect investors by improving the accuracy and reliability of corporate disclosures made pursuant to the securities laws and for other purposes.

To help you comply or prove compliance with SOX, Recon provides the **Compliance Insight Package for SOX**. For more information about adding the package to the Reports repository, see the *Solutions Guide for ArcSight Insight Compliance Package for SOX*. The guide includes information about identifying assets that must comply with SOX.

This package includes the following dashboards and reports, organized by SOX objectives:

Category	Dashboards	Reports
Executive Summary	Control Overview Controls Risk Score Overview Executive Cyber Threat Overview	n/a
ISO 5 Information Security Policies	Policy Violations Overview	Policy Violations
ISO 6 Organization of Information Security	VPN Connection Overview Wireless Attacks and Suspicious Activity	Outbound Communication from Development to Production Environment Outbound Communication from Production to Development Environment VPN Connection Summary Wireless Attacks and Suspicious Activity
ISO 7 Human Resource Security	Activity by User	n/a
ISO 8 Asset Management	Removable Media Activity	n/a

Category	Dashboards	Reports
ISO 9 Access Control	n/a	Account Creations Account Deletions Account Lockouts by System Account Lockouts by User Insecure Ports Insecure Services Password Policy Changes Password Weaknesses User Group Account Creations User Group Account Deletions
ISO 10 Cryptography	n/a	SSH Vulnerabilities SSL or TLS Vulnerabilities VPN Vulnerabilities
ISO 11 Physical and Environmental Security	Failed Physical Physical Access Overview Successful Physical Physical Access Overview	Failed Building Physical Access Activity Summary Failed User Physical Access Activity Summary Successful Building Physical Access Activity Summary Successful User Physical Access Activity Summary

Category	Dashboards	Reports
ISO 12 Operations Security	Administrative Login Overview Application Vulnerabilities Overview Failed Login Overview Failed Login Relationship Firewall Configuration Changes Malware Overview Successful Login Overview Unpatched Systems Vulnerability Overview	Antivirus Stopped or Paused Audit Log Cleared Database Configuration Changes Database Vulnerabilities Failed Administrative Login Summary Failed Antivirus Updates Failed Login by SOX Asset Failed Login Summary Firewall Configuration Changes High Risk Vulnerabilities Malware Summary Network Device Configuration Changes Overflow Vulnerabilities SQL Injection Vulnerabilities Successful Administrative Login Summary Successful Login by SOX Asset Unpatched Systems Vulnerability Summary by CVE ID Vulnerability Summary by SOX Asset Vulnerability Summary on SOX Environment XSRF Vulnerabilities XSS Vulnerabilities
ISO 13 Communications Security	DoS Activity Firewall Blocked Events	Covert Channel Activity DoS Attacks Summary Firewall Blocked Events

Category	Dashboards	Reports
ISO 16 Information Security Incident Management	High Risk Events Overview MITRE ATT&CK Overview Reconnaissance Activity Threat Overview Threat Relationship	High Risk Events Summary MITRE ATT&CK Summary by MITRE Technique MITRE ATT&CK Summary by SOX Asset Reconnaissance Summary Threats Summary
ISO 17 Information Security Aspects of Business Continuity Management	n/a	Asset Shutdown Summary
ISO 18 Compliance	Information Disclosure Vulnerabilities Organization Information Leaks Personal Information Leakage Overview	Information Disclosure Vulnerabilities Organization Information Leaks Summary Personal Information Leakage Summary

Sarbanes-Oxley Executive Summary

Select Reports > Portal > Repository > Data Compliance Content > Sarbanes Oxley > Executive Summary.

This category is relevant to all ISO 27002:2013 controls. To assess your enterprise's compliance with this requirement, use the following dashboards:

Dashboards	Reports
Control Overview Controls Risk Score Overview Executive Cyber Threat Overview	n/a

Control Overview

Used as a drill-down dashboard by the Controls Risk Score Overview dashboard.

Controls Risk Score Overview

Provides an overview of ISO 27002:2013 controls based on correlation events reported from ESM.

Executive Cyber Threat Overview

Provides a cyber threat overview for executives. The dashboard shows the top 5:

- Vulnerabilities
- MITRE ATT&CK techniques
- ArcSight categorized attacks
- Attacked assets

5 – Information Security Policies

Select Reports > Portal > Repository > Data Compliance Content > Sarbanes Oxley > ISO 27002 > *Dashboards* or *Reports* > ISO 5 Information Security Policies.

To assess your enterprise's compliance with this requirement, use the following dashboard and report:

Dashboards	Reports
Policy Violations Overview	Policy Violations

Policy Violations Overview

Provides an overview of policy violation events that involve Sarbanes Oxley systems, relevant to ISO 27002:2013 Control 5.1.2.

Policy Violations

Provides a summary of policy violation events that involve Sarbanes Oxley systems, relevant to ISO 27002:2013 Control 5.1.2.

6 – Organization of Information Security

Select Reports > Portal > Repository > Data Compliance Content > Sarbanes Oxley > ISO 27002 > *Dashboards* or *Reports* > ISO 6 Organization of Information Security.

To assess your enterprise's compliance with this requirement, use the following dashboards and reports:

Dashboards	Reports
VPN Connection Overview Wireless Attacks and Suspicious Activity	Outbound Communication from Development to Production Environment Outbound Communication from Production to Development Environment VPN Connection Summary Wireless Attacks and Suspicious Activity

VPN Connection Overview

Provides an overview of VPN connection activity involving Sarbanes Oxley systems, relevant to ISO 27002:2013 Control 6.2.2.

Before using this dashboard, ensure that variables `isAgentZoneSOX` and `isAgentAddressSOX` are defined in the SOX logical model. For more information, see the *Solutions Guide for ArcSight Insight Compliance Package for SOX*.

Wireless Attacks and Suspicious Activity

Provides an overview of wireless attacks and suspicious activity involving Sarbanes Oxley systems, relevant to ISO 27002:2013 Control 6.2.1.

Outbound Communication from Development to Production Environment

Provides a summary of outbound communication events from development to production environments involving Sarbanes Oxley systems, relevant to ISO 27002:2013 Control 6.1.2.

Before using this report, ensure that variables `isSourceZoneSOXDevelopment` and `isDestinationZoneSOXProduction` are defined in the SOX logical model. For more information, see the *Solutions Guide for ArcSight Insight Compliance Package for SOX*.

Outbound Communication from Production to Development Environment

Provides a summary of outbound communication events from production to development environments involving Sarbanes Oxley systems, relevant to ISO 27002:2013 Control 6.1.2.

Before using this report, ensure that variables `isSourceZoneSOXProduction` and `isDestinationZoneSOXDevelopment` are defined in the SOX logical model. For more information, see the *Solutions Guide for ArcSight Insight Compliance Package for SOX*.

VPN Connection Summary

Provides a summary about VPN connection events which involving Sarbanes Oxley systems, relevant to ISO 27002:2013 Control 6.2.2.

Before using this report, ensure that variables `isAgentZoneSOX` and `isAgentAddressSOX` are defined in the SOX logical model. For more information, see the *Solutions Guide for ArcSight Insight Compliance Package for SOX*.

Wireless Attacks and Suspicious Activity

Provides a summary of wireless attack and suspicious activity events involving Sarbanes Oxley systems, relevant to ISO 27002:2013 Control 6.2.1.

7 – Human Resource Security

Select Reports > Portal > Repository > Data Compliance Content > Sarbanes Oxley > ISO 27002 > Reports > ISO 7 Human Resource Security.

Activity by User

Provides an overview of activity by specific users involving Sarbanes Oxley systems, relevant to ISO 27002:2013 Controls 7.1.1, 7.2.3 , and 7.3.1.

8 – Asset Management

Select Reports > Portal > Repository > Data Compliance Content > Sarbanes Oxley > ISO 27002 > Reports > ISO 8 Asset Management.

Removable Media Activity

Provides an overview of removable media activity involving Sarbanes Oxley systems, relevant to ISO 27002:2013 Control 8.3.1.

9 – Access Control

Select Reports > Portal > Repository > Data Compliance Content > Sarbanes Oxley > SOX Reports > ISO 9 Access Control.

To assess your enterprise's compliance with this requirement, use the following reports:

Dashboards	Reports
n/a	Account Creations Account Deletions Account Lockouts by System Account Lockouts by User Insecure Ports Insecure Services Password Policy Changes Password Weaknesses User Group Account Creations User Group Account Deletions

Account Creations

Provides a summary of account creation activity events involving Sarbanes Oxley systems, relevant to ISO 27002:2013 Control 9.2.1.

Account Deletions

Provides a summary of account deletion activity events involving Sarbanes Oxley systems, relevant to ISO 27002:2013 Control 9.2.1.

Account Lockouts by System

Provides a summary of account lockout activity events by system involving Sarbanes Oxley systems, relevant to ISO 27002:2013 Control 9.2.1.

Account Lockouts by User

Provides a summary of account lockout activity events by user involving Sarbanes Oxley systems, relevant to ISO 27002:2013 Control 9.2.1.

Insecure Ports

Provides a summary of insecure ports that are involved in communication with Sarbanes Oxley systems, relevant to ISO 27002:2013 Control 12.1.2.

Insecure Services

Provides a summary of insecure services that are involved in communication with Sarbanes Oxley systems, relevant to ISO 27002:2013 Control 12.1.2.

Password Policy Changes

Provides a summary of password policy change events involving Sarbanes Oxley systems, relevant to ISO 27002:2013 Control 9.4.3.

Password Weaknesses

Provides a summary of SQL vulnerabilities involving Sarbanes Oxley systems, relevant to ISO 27002:2013 Control 9.4.3.

User Group Account Creations

Provides a summary of user group account creation events involving Sarbanes Oxley systems, relevant to ISO 27002:2013 Control 9.2.1.

User Group Account Deletions

Provides a summary of user group account deletion events involving Sarbanes Oxley systems, relevant to ISO 27002:2013 Control 9.2.1.

10 – Cryptography

Select Reports > Portal > Repository > Data Compliance Content > Sarbanes Oxley > ISO 27002 > Reports > ISO 10 Cryptography.

To assess your enterprise's compliance with this requirement, use the following reports:

Dashboards	Reports
n/a	SSH Vulnerabilities SSL or TLS Vulnerabilities VPN Vulnerabilities

SSH Vulnerabilities

Provides a summary of SSH vulnerabilities involving Sarbanes Oxley systems, relevant to ISO 27002:2013 Control 10.1.1.

SSL or TLS Vulnerabilities

Provides a summary of SSL or TLS vulnerabilities involving Sarbanes Oxley systems, relevant to ISO 27002:2013 Control 10.1.1.

VPN Vulnerabilities

Provides a summary of VPN vulnerabilities involving Sarbanes Oxley systems, relevant to ISO 27002:2013 Control 10.1.1.

11 – Physical and Environmental Security

Select Reports > Portal > Repository > Data Compliance Content > Sarbanes Oxley > ISO 27002 > *Dashboards* or *Reports* > ISO 11 Physical and Environmental Security.

To assess your enterprise's compliance with this requirement, use the following dashboards and reports:

Dashboards	Reports
Failed Physical Physical Access Overview	Failed Building Physical Access Activity Summary
Successful Physical Physical Access Overview	Failed User Physical Access Activity Summary
	Successful Building Physical Access Activity Summary
	Successful User Physical Access Activity Summary

Failed Physical Physical Access Overview

Provides an overview of failed physical access activity events, relevant to ISO 27002:2013 Control 11.1.2.

Successful Physical Physical Access Overview

Provides an overview of successful physical access activity events, relevant to ISO 27002:2013 Control 11.1.2.

Failed Building Physical Access Activity Summary

Provides a summary of failed physical access activity events by building, relevant to ISO27002:2013 control 11.1.2.

Failed User Physical Access Activity Summary

Provides a summary of failed physical access activity events by user, relevant to ISO27002:2013 control 11.1.2.

Successful Building Physical Access Activity Summary

Provides a summary of successful physical access activity events by building, relevant to ISO27002:2013 control 11.1.2.

Successful User Physical Access Activity Summary

Provides a summary of successful physical access activity events by user, relevant to ISO27002:2013 control 11.1.2.

12 – Operations Security

Select Reports > Portal > Repository > Data Compliance Content > Sarbanes Oxley > ISO 27002 > *Dashboards* or *Reports* > ISO 12 Operations Security.

To assess your enterprise's compliance with this requirement, use the following dashboards and reports:

Dashboards	Reports
Administrative Login Overview	Antivirus Stopped or Paused
Application Vulnerabilities Overview	Audit Log Cleared
Failed Login Overview	Database Configuration Changes
Failed Login Relationship	Database Vulnerabilities
Firewall Configuration Changes	Failed Administrative Login Summary
Malware Overview	Failed Antivirus Updates
Successful Login Overview	Failed Login by SOX Asset
Unpatched Systems	Failed Login Summary
Vulnerability Overview	Firewall Configuration Changes
	High Risk Vulnerabilities
	Malware Summary
	Network Device Configuration Changes
	Overflow Vulnerabilities
	SQL Injection Vulnerabilities
	Successful Administrative Login Summary
	Successful Login by SOX Asset
	Unpatched Systems
	Vulnerability Summary by CVE ID
	Vulnerability Summary by SOX Asset
	Vulnerability Summary on SOX Environment
	XSRF Vulnerabilities
	XSS Vulnerabilities

Administrative Login Overview

Provides an overview of administrative login activity, relevant to ISO 27002:2013 Control 12.4.3.

To define administrative accounts, use the worksheet condition of this dashboard. Use lowercase to define the accounts. For example, add the user "Administrator" as "administrator."

Application Vulnerabilities Overview

Provides an overview of the following application vulnerabilities, relevant to ISO 27002:2013 Control 12.6.1:

- SQL injection
- XSS
- XSRF
- Overflow

Failed Login Overview

Provides an overview of failed login activity, relevant to ISO 27002:2013 Control 12.4.1.

Failed Login Relationship

Based on ArcSight categorization, provides an overview of failed login relationships involving Sarbanes Oxley systems, relevant to ISO 27002:2013 Control 12.4.1.

Firewall Configuration Changes

Provides an overview of firewall configuration change events, relevant to ISO 27002:2013 Control 12.1.2.

Malware Overview

Provides an overview of malware activity, relevant to ISO 27002:2013 Control 12.2.1.

Successful Login Overview

Provides an overview of successful login activity, relevant to ISO 27002:2013 Control 12.4.1.

Unpatched Systems

Provides an overview of missing security patches on Sarbanes Oxley systems, relevant to ISO 27002:2013 Control 12.5.1.

Vulnerability Overview

Provides an overview of vulnerability events involving Sarbanes Oxley systems, relevant to ISO 27002:2013 Control 12.6.1.

Antivirus Stopped or Paused

Provides a summary of antivirus services that were stopped or paused, relevant to ISO 27002:20213 Control 12.4.1.

Audit Log Cleared

Provides a summary of audit log cleared events involving Sarbanes Oxley systems, relevant to ISO 27002:2013 Control 12.4.2.

Database Configuration Changes

Provides a summary of database configuration changes, relevant to ISO 27002:2013 Control 12.1.2.

Database Vulnerabilities

Provides a summary of database vulnerabilities involving Sarbanes Oxley systems, relevant to ISO 27002:2013 Control 12.6.1.

Failed Administrative Login Summary

Provides a summary of failed administrative login events involving Sarbanes Oxley systems, relevant to ISO 27002:2013 Control 12.4.3.

To define administrative accounts, use the worksheet condition of this dashboard. Use lowercase to define the accounts. For example, add the user "Administrator" as "administrator."

Failed Antivirus Updates

Provides a summary of failed antivirus updates, relevant to ISO 27002:20213 Control 12.4.1.

Failed Login by SOX Asset

Provides a summary of failed logins detected on specific SOX assets , relevant to ISO 27002:2013 control 12.4.1.

When you run this report, specify the asset (host name, IP address, or MAC address) in lowercase.

Failed Login Summary

Provides a summary of failed login events involving Sarbanes Oxley systems, relevant to ISO 27002:2013 Control 12.4.1.

Firewall Configuration Changes

Provides a summary of firewall configuration change events, relevant to ISO 27002:2013 Control 12.1.2.

High Risk Vulnerabilities

Provides a summary of high-risk vulnerabilities involving Sarbanes Oxley systems, relevant to ISO 27002:2013 Control 12.6.1.

Malware Summary

Provides a summary of malware events on Sarbanes Oxley systems, relevant to ISO 27002:2013 Control 12.2.1.

Network Device Configuration Changes

Provides a summary of network device configuration change events involving Sarbanes Oxley systems, relevant to ISO 27002:2013 Control 12.1.2.

Overflow Vulnerabilities

Provides a summary of overflow vulnerabilities involving Sarbanes Oxley systems, relevant to ISO 27002:2013 Control 12.6.1.

SQL Injection Vulnerabilities

Provides a summary of SQL vulnerabilities involving Sarbanes Oxley systems, relevant to ISO 27002:2013 Control 12.6.1.

Successful Administrative Login Summary

Provides a summary of successful administrative login events involving Sarbanes Oxley systems, relevant to ISO 27002:2013 Control 12.4.3.

To define administrative accounts, use the worksheet condition of this dashboard. Use lowercase to define the accounts. For example, add the user "Administrator" as "administrator."

Successful Login by SOX Asset

Provides a summary of successful logins detected on specific SOX assets, relevant to ISO 27002:2013 control 12.4.1.

When you run this report, specify the asset (host name, IP address, or MAC address) in lowercase.

Unpatched Systems

Provides a summary of missing security patches involving Sarbanes Oxley systems, relevant to ISO 27002:2013 Control 12.5.1.

Vulnerability Summary by CVE ID

Provides a summary of vulnerabilities detected on SOX environments by specific CVE ID, relevant to ISO 2700:2013 Control 12.6.1.

When you run this report, specify the CVE ID in lowercase.

Vulnerability Summary by SOX Asset

Provides a summary of vulnerabilities detected on specific SOX assets, relevant to ISO 27002:2013 Control 12.6.1.

When you run this report, specify the asset (host name, IP address, or MAC address) in lowercase.

Vulnerability Summary on SOX Environment

Provides a summary of vulnerabilities involving Sarbanes Oxley systems, relevant to ISO 27002:2013 Control 12.6.1.

XSRF Vulnerabilities

Provides a summary of XSRF vulnerabilities involving Sarbanes Oxley systems, relevant to ISO 27002:2013 Control 12.6.1.

XSS Vulnerabilities

Provides a summary of XSS vulnerabilities involving Sarbanes Oxley systems, relevant to ISO 27002:2013 Control 12.6.1.

13 – Communications Security

Select Reports > Portal > Repository > Data Compliance Content > Sarbanes Oxley > ISO 27002 > *Dashboards* or *Reports* > ISO 13 Communications Security.

To assess your enterprise's compliance with this requirement, use the following dashboards and reports:

Dashboards	Reports
DoS Activity	Covert Channel Activity
Firewall Blocked Events	DoS Attacks Summary
	Firewall Blocked Events

DoS Activity

Based on ArcSight categorization, provides an overview of DoS activity involving Sarbanes Oxley systems, relevant to ISO 27002:2013 Control 13.2.3.

Firewall Blocked Events

Provides an overview of blocked firewall events, relevant to ISO 27002:2013 Control 13.2.1.

Covert Channel Activity

Displays covert channel activities, relevant to ISO 27002:2013 Control 13.2.1.

DoS Attacks Summary

Provides a summary of events that indicate DoS activity, relevant to ISO 27002:2013 Control 13.2.3.

Firewall Blocked Events

Provides a summary of blocked firewall events, relevant to ISO27002:2013 control 13.2.1

16 – Information Security Incident Management

Select Reports > Portal > Repository > Data Compliance Content > Sarbanes Oxley > ISO 27002 > *Dashboards* or *Reports* > ISO 16 Information Security Incident Management.

To assess your enterprise's compliance with this requirement, use the following dashboards and reports:

Dashboards	Reports
High Risk Events Overview	High Risk Events Summary
MITRE ATT&CK Overview	MITRE ATT&CK Summary by MITRE Technique
Reconnaissance Activity	MITRE ATT&CK Summary by SOX Asset
Threat Overview	Reconnaissance Summary
Threat Relationship	Threats Summary

High Risk Events Overview

Provides an overview of high-risk events involving Sarbanes Oxley systems, relevant to ISO 27002:2013 Control 16.1.2.

MITRE ATT&CK Overview

Provides an overview of MITRE ATT&CK events involving Sarbanes Oxley systems, relevant to ISO 27002:2013 Control 16.1.2.

Reconnaissance Activity

Based on ArcSight categorization, provides an overview of reconnaissance activity involving Sarbanes Oxley systems, relevant to ISO 27002:2013 Control 16.1.2.

Threat Overview

Based on ArcSight categorization, provides an overview of threat activity involving Sarbanes Oxley systems, relevant to ISO 27002:2013 Control 16.1.2.

Threat Relationship

Based on ArcSight categorization, provides overview of threat relationships involving Sarbanes Oxley systems, relevant to ISO 27002:2013 Control 16.1.2.

High Risk Events Summary

Provides a summary of high-risk events involving Sarbanes Oxley systems, relevant to ISO 27002:2013 Control 16.1.2.

MITRE ATT&CK Summary by MITRE Technique

Provides a summary of MITRE ATT&CK events involving Sarbanes Oxley systems by MITRE technique, relevant to ISO 27002:2013 Control 16.1.2.

MITRE ATT&CK Summary by SOX Asset

Provides a summary of MITRE ATT&CK events involving Sarbanes Oxley systems by target asset, relevant to ISO 27002:2013 Control 16.1.2.

Reconnaissance Summary

Provides a summary of reconnaissance events involving Sarbanes Oxley systems, relevant to ISO 27002:2013 Control 16.1.2.

Threats Summary

Provides a summary of threat events involving Sarbanes Oxley systems, relevant to ISO 27002:2013 Control 16.1.2.

17 – Information Security Aspects of Business Continuity Management

Select Reports > Portal > Repository > Data Compliance Content > Sarbanes Oxley > ISO 27002 > Reports > ISO 17 Information Security Aspects of Business Continuity Management.

Asset Shutdown Summary

Provides a summary of asset shutdown events involving Sarbanes Oxley systems, relevant to ISO 27002:2013 Control 17.1.3.

18 – Compliance

Select Reports > Portal > Repository > Data Compliance Content > Sarbanes Oxley > ISO 27002 > *Dashboards* or *Reports* > ISO 18 Compliance.

To assess your enterprise's compliance with this requirement, use the following dashboards and reports:

Dashboards	Reports
Information Disclosure Vulnerabilities	Information Disclosure Vulnerabilities
Organization Information Leaks	Organization Information Leaks Summary
Personal Information Leakage Overview	Personal Information Leakage Summary

Information Disclosure Vulnerabilities

Provides an overview of information disclosure vulnerability events involving Sarbanes Oxley systems, relevant to ISO 27002:2013 Controls 18.1.4, 13.2.4.

Organization Information Leaks

Based on ArcSight categorization, provides an overview of information leakage activity (for example, company data), relevant to ISO 27002:2013 Controls 18.1.3, 13.2.4.

Personal Information Leakage Overview

Based on ArcSight categorization, provides an overview of personal information leakage activity, relevant to ISO 27002:2013 Controls 18.1.4, 13.2.4.

Information Disclosure Vulnerabilities - Dashboard

Provides a summary of information disclosure vulnerabilities involving Sarbanes Oxley systems, relevant to ISO 27002:2013 Controls 18.1.4, 13.2.4.

Organization Information Leaks Summary - Dashboard

Provides a summary of information leakage events (for example, company data leaks), relevant to ISO 27002:2013 Controls 18.1.3, 13.2.4.

Personal Information Leakage Summary - Dashboard

Provides a summary of personal information leakage events, relevant to ISO 27002:2013 Controls 18.1.4, 13.2.4.

VIII Appendices

The appendices in this guide provide additional information or guidance for using the features and functions for this product.

A1 Mapping Database Names to their Appropriate Search Fields

When creating a fieldset, Search displays the coding-style name for the fields instead of the human-readable names that you see when creating a query. For example, in a query you can enter or select Agent Address. However, in the fieldsets selection, this same field appears as agentAddressBin. This issue also occurs when you're adding queries to a Report.

The following tables provide the coding-style names that appear in the fieldset and report configurations, so that you can easily map them to their human-readable names.

Agent Fields

Substitute the following labels in the agent category:

For the field that you want to add...	You should choose...
Agent Address	agentAddressBin
Agent DNS Domain	agentDnsDomain
Agent Hostname	agentHostName
Agent ID	agentId
Agent Mac Address	agentMacAddressBin
Agent NT Domain	agentNtDomain
Agent Receipt Time	agentReceiptTime
Agent Severity	agentSeverity
Agent Timezone	agentTimeZone
Agent Translated Address	agentTranslatedAddressBin
Agent Translated Zone External ID	agentTranslatedZoneExternalID
Agent Translated Zone URI	agentTranslatedZoneURI
Agent Type	agentType
Agent Version	agentVersion
Agent Zone External ID	agentZoneExternalID
Agent Zone URI	agentZoneURI

Category Fields

Substitute the following labels in the category:

Category Behavior	categoryBehavior
Category Device Group	categoryDeviceGroup
Category Device Type	categoryDeviceType
Category Object	categoryObject
Category Outcome	categoryOutcome
Category Significance	categorySignificance
Category Technique	categoryTechnique
Version	version

Correlation Fields

Substitute the following labels in the `correlation` category:

Substitute the following labels in the correlation category:	You should choose...
Base Event Ids	correlated_event_id
Correlated Event Id	generatorURI
Generator External ID	generatorExternalID
Generator URI	base_event_ids
Priority	priority

Destination Fields

Substitute the following labels in the `destination` category:

For the field that you want to add...	You should choose...
Destination Address	destinationAddressBin
Destination DNS Domain	destinationDnsDomain
Destination Geo Country Code	destinationGeoCountryCod
Destination Geo Latitude	destinationGeoLatitude
Destination Geo Longitude	destinationGeoLongitude
Destination Geo Postal Code	destinationGeoPostalCode
Destination Geo Region Code	destinationGeoRegionCode
Destination Geolocation Info	destinationGeoLocationInfo
Destination Hostname	destinationHostName
Destination Mac Address	destinationMacAddressBin
Destination NT Domain	destinationNtDomain
Destination Port	destinationPort
Destination Process ID	destinationProcessId
Destination Process Name	destinationProcessName
Destination Service Name	destinationServiceName
Destination Translated Address	destinationTranslatedAddressBin
Destination Translated Port	destinationTranslatedPort
Destination Translated Zone External ID	destinationTranslatedZoneExternalID
Destination Translated Zone URI	destinationTranslatedZoneURI
Destination User ID	destinationUserId
Destination User Privileges	destinationUser Privileges

Destination Username	destinationUserName
Destination Zone External ID	destinationZoneExternalID
Destination Zone URI	destinationZoneURI

Device Fields

Substitute the following labels in the device category:

For the field that you want to add...	You should choose...
Device Action	deviceAction
Device Event Class ID	deviceEventClassId
Device Address	deviceAddressBin
Device Asset ID	deviceAssetID
Device Direction	deviceDirection
Device DNS Domain	deviceDnsDomain
Device Domain	deviceDomain
Device Event Category	deviceEventCategory
Device Inbound Interface	deviceInboundInterface
Device Event Class ID	deviceEventClassId
Device External ID	deviceExternalId
Device Facility Hostname	deviceFacility
Device Hostname	deviceHostName
Device Mac Address	deviceMacAddressBin
Device NT Domain	deviceNtDomain
Device Outbound Interface	deviceOutboundInterface
Device Process ID	deviceProcessId
Device Process Name	deviceProcessName
Device Product	deviceProduct
Device Receipt Time	deviceReceiptTime
Device Severity	deviceSeverity
Device Timezone	deviceTimeZone
Device Translated Address	deviceTranslatedAddressBin
Device Translated Zone External ID	deviceTranslatedZoneExternalID

Device Translated Zone URI	deviceTranslatedZoneURI
Device Version	deviceVendor
Device Version	deviceVersion
Device Zone External ID	deviceZoneExternalID
Device Zone URI	deviceZoneURI
Normalized Event Time	normalizedEventTime

Device Custom Fields

Substitute the following labels in the `device custom` category:

For the field that you want to add...	You should choose...
Device Custom Date 1	deviceCustomDate1
Device Custom Date 1 Label	deviceCustomDate1Label
Device Custom Date 2	deviceCustomDate2
Device Custom Date 2 Label	deviceCustomDate2Label
Device Custom Descriptor ID	deviceCustomDescriptorId
Device Custom Floating Point 1	deviceCustomFloatingPoint1
Device Custom Floating Point 1 Label	deviceCustomFloatingPoint1Label
Device Custom Floating Point 2	deviceCustomFloatingPoint2
Device Custom Floating Point 2 Label	deviceCustomFloatingPoint2Label
Device Custom Floating Point 3	deviceCustomFloatingPoint3
Device Custom Floating Point 3 Label	deviceCustomFloatingPoint3Label
Device Custom Floating Point 4	deviceCustomFloatingPoint4
Device Custom Floating Point 4 Label	deviceCustomFloatingPoint4Label
Device Custom Number 1	deviceCustomNumber1
Device Custom Number 1 Label	deviceCustomNumber1Label
Device Custom Number 2	deviceCustomNumber2
Device Custom Number 2 Label	deviceCustomNumber2Label
Device Custom Number 3	deviceCustomNumber3
Device Custom Number 3 Label	deviceCustomNumber3Label
Device Custom String 1	deviceCustomString1
Device Custom String 1 Label	deviceCustomString1Label

For the field that you want to add...	You should choose...
Device Custom String 2	deviceCustomString2
Device Custom String 2 Label	deviceCustomString2Label
Device Custom String 3	deviceCustomString3
Device Custom String 3 Label	deviceCustomString3Label
Device Custom String 4	deviceCustomString4
Device Custom String 4 Label	deviceCustomString4Label
Device Custom String 5	deviceCustomString5
Device Custom String 5 Label	deviceCustomString5Label
Device Custom String 6	deviceCustomString6
Device Custom String 16 Label	deviceCustomString6Label
Device CustomIPv6 Address 1	deviceCustomIPv6Address1Bin
Device CustomIPv6 Address 1 Label	deviceCustomIPv6Address1Label
Device CustomIPv6 Address 2	deviceCustomIPv6Address2Bin
Device CustomIPv6 Address 2 Label	deviceCustomIPv6Address2Label
Device CustomIPv6 Address 3	deviceCustomIPv6Address3Bin
Device CustomIPv6 Address 3 Label	deviceCustomIPv6Address3Label
Device CustomIPv6 Address 4	deviceCustomIPv6Address4Bin
Device CustomIPv6 Address 4 Label	deviceCustomIPv6Address4Label

Event Fields

Substitute the following labels in the `event` category:

For the field that you want to add...	You should choose...
Application Protocol	applicationProtocol
Base Event Count	baseEventCount
Bytes In	bytesIn
Bytes Out	bytesOut
Crypto Signature	cryptoSignature
Customer External ID	customeExternalID
Customer URI	customerURI
End Time	endTime

For the field that you want to add...	You should choose...
Event ID	eventId
Event Outcome	eventOutcome
External Id	externalID
Locality	locality
Message	message
Name	name
Originator	originator
Reason	reason
Start Time	startTime
Transport Protocol	transportProtocol
Type	type

Extension Fields

Substitute the following labels in the `extension` category:

For the field that you want to add...	You should choose...
Extra Fields	extraFields
Storage Group	storageGroup

File Fields

Substitute the following labels in the `file` category:

For the field that you want to add...	You should choose...
File Create Time	fileCreateTime
File Hash	fileHash
File ID	fileId
File Modification Time	fileModificationTime
File Name	fileName
File Path	filePath
File Permission	filePermission
File Size	fileSize
File Type	fileType

Flex Fields

Substitute the following labels in the `flex` category:

For the field that you want to add...	You should choose...
Flex Date 1	flexDate1
Flex Date 1 Label	flexDate1Label
Flex Number 1	flexNumber1
Flex Number 1 Label	flexNumber1Label
Flex Number 2	flexNumber2
Flex Number 2 Label	flexNumber2Label
Flex String 1	flexString1
Flex String 1 Label	flexString1Label
Flex String 2	flexString2
Flex String 2 Label	flexString2Label

OldField Fields

Substitute the following labels in the `oldfield` category:

For the field that you want to add...	You should choose...
Old File Create Time	oldFileCreateTime

Old File Fields

Substitute the following labels in the `old file` category:

For the field that you want to add...	You should choose...
Old File Hash	oldFileHash
Old File ID	oldFileId
Old File Modification Time	oldFileModificationTime
Old File Name	oldFileName
Old File Path	oldFilePath
Old File Permission	oldFilePermission
Old File Size	oldFileSize
Old File Type	oldFileType

Request Fields

Substitute the following labels in the `request` category:

For the field that you want to add...	You should choose...
Request Client Application	requestClientApplication
Request Context	requestContext
Request Cookies	requestCookies
Request Method	requestMethod
Request URL	requestUrl
Request URL FileName	requestUrlFileName
Request URL Query	requestUrlQuery

Source Fields

Substitute the following labels in the `source` category:

For the field that you want to add...	You should choose...
Source Address	sourceAddressBin
Source DNS Domain	sourceDnsDomain
Source Geo Country Code	sourceGeoCountryCode
Source Geo Latitude	sourceGeoLatitude
Source Geo Longitude	sourceGeoLongitude
Source Geo Postal Code	sourceGeoPostalCode
Source Geo Region Code	sourceGeoRegionCode
Source Geolocation Info	sourceGeoLocationinfo
Source Hostname	sourceHostName
Source Mac Address	sourceMacAddressBin
Source NT Domain	sourceNtDomain
Source Port	sourcePort
Source Process ID	sourceProcessId
Source Process Name	sourceProcessName
Source Service Name	sourceServiceName
Source Translated Address	sourceTranslatedAddressBin

For the field that you want to add...	You should choose...
Source Translated Port	sourceTranslatedPort
Source Translated Zone External ID	sourceTranslatedZoneExternalID
Source Translated Zone URI	sourceTranslatedZoneURI
Source User ID	sourceUserId
Source User Privileges	sourceUser Privileges
Source Username	sourceUserName
Source Zone External ID	sourceZoneExternalID
Source Zone URI	sourceZoneURI

Legal Notice

of, and supersedes, any other FAR, DFARS, or other clause or provision that addresses government rights in computer software or technical data.

For additional information, such as certification-related notices and trademarks, see https://www.microfocus.com/en-us/about/legal.

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://www.microfocus.com/documentation/arcsight/

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 User's Guide to ArcSight Recon 1.4.1 (ArcSight Recon 1.4.1 1.4.1)

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!