Micro Focus Security
ArcSight ESM CIP for PCI DSS

Compliance Insight Package for the Payment Card Industry Data Security Standard

Legal Notices

Copyright Notice

Trademark Notices

Support

Contact Information

Phone	A list of phone numbers is available on the Technical Support Page: https://softwaresupport.softwaregrp.com/support-contact-information
Support Web Site	https://softwaresupport.softwaregrp.com/
ArcSight Product Documentation	https://www.microfocus.com/documentation/arcsight/

Contents

What's New

Delete this text and replace it with your own content.

Active Lists

The following table lists all the active lists in Compliance Insight Package for the Payment Card Industry Data Security Standard.

Active Lists Resources

Resource	Description	URI
Administrative Accounts	Contains the usernames that have administrative privileges in your domain. The administrator in charge of managing users with administrative privileges must populate this list manually when a new administrator is added to your environment. PCI Reports utilize this active list to track administrators and administrator activity. **Note:** Entries in this list should be in all lower case. For example, user "Administrator" should be added as "administrator."	/All Dashboards/ArcSight Solutions/PCI DSS/Requirement 1-Install and Maintain Network Security Controls
Allowed Ports	Contains all permissible destination ports (all permissible services). This active list should be manually populated according to your policy. If all ports are specified on the Allowed Ports active list (using the * character), the policy allows all ports (except those specified explicitly in the Disallowed Ports active list).	/All Active Lists/ArcSight Solutions/PCI DSS
Compliance Risk Score	Contains the compliance risk score for each regulation section. The compliance risk score is calculated based on the triggered rules in the solution package. You can manually change the score as required. This change will be reflected in the Compliance Risk Score dashboard.	/All Active Lists/ArcSight Solutions/PCI DSS
Default Vendor Accounts	Contains default user account names for various vendors. This list should be configured at set-up time with existing vendor user account names, and updated as necessary on an ongoing basis.	/All Active Lists/ArcSight Solutions/PCI DSS
Disallowed Ports	Contains all disallowed destination ports. This active list should be manually populated according to your policy. Explicit port entries on the Disallowed Ports active list always take precedence over entries in the Allowed Ports active list. Conditions are located in the Disallowed Ports Access filter.	/All Active Lists/ArcSight Solutions/PCI DSS

Active Lists Resources, continued

Resource	Description	URI
Insecure Ports	Contains ports that are used for insecure communication.	/All Active Lists/ArcSight Solutions/PCI DSS
Insecure Processes	Contains the names of processes that provide unencrypted and thus insecure communications.	/All Active Lists/ArcSight Solutions/PCI DSS
PCI Violations	Contains PCI violations.	/All Active Lists/ArcSight Solutions/PCI DSS

Dashboards

The following table lists all the dashboards in Compliance Insight Package for the Payment Card Industry Data Security Standard.

Dashboards Resources

Resource	Description	URI
Compliance Risk Score Overview	Displays information about the compliance risk score for each PCI Requirement. If you need to override the risk score status of a specific article, just right click on the article and choose the Override Status option. **Note:** Enable and deploy the following rules: • Compliance Score Update • Manual Status Change	/All Dashboards/ArcSight Solutions/PCI DSS/Overview
Inbound Data Flow to Cardholder Data Environment	Displays an overview of data flow from non cardholder data environments to cardholder data environments.	/All Dashboards/ArcSight Solutions/PCI DSS/Requirement 1-Install and Maintain Network Security Controls/ PCI Requirement 1
Malware Overview PCI 5.2	Displays an overview of malware activity in the organization.	/All Dashboards/ArcSight Solutions/PCI DSS/Requirement 5-Protect All Systems and Networks from Malicious Software/
Outbound Data Flow from Cardholder Data Environment	Displays an overview of data flow from cardholder data environments to non cardholder data environments.	/All Dashboards/ArcSight Solutions/PCI DSS/Requirement 1-Install and Maintain Network Security Controls/ PCI Requirement 1
Worm Activity	Displays a real-time overview of worm activity in your environment.	/All Dashboards/Real-time Rules/PCI DSS/Requirement 5-Protect All Systems and Networks from Malicious Software

Data Monitors

The following table lists all the data monitors in Compliance Insight Package for the Payment Card Industry Data Security Standard.

Data Monitors Resources

Resource	Description	URI
Activity per 10 Minutes	Shows a moving average of inbound traffic to CDE, It displays data for the last hour and will generate a correlation event if the moving average is increased by 500%.	/All Data Monitors/ArcSight Solutions/PCI DSS/Requirement 1-Install and Maintain Network Security Controls/Data Flow from non-CDE to CDE
Compliance Risk Score Overview	Shows an icon indicating the compliance risk score for each regulation section. The compliance score is maintained in the Compliance Score active list, and is calculated based on the severity of the rules that were triggered in the solution package.	/All Data Monitors/ArcSight Solutions/PCI DSS/Overview
Last Reported Events	Shows the last five data flow events from non-cardholder data environment to cardholder data environment.	/All Data Monitors/ArcSight Solutions/PCI DSS/Requirement 1-Install and Maintain Network Security Controls/Data Flow from non-CDE to CDE
Last 10 Worm Events	Shows the last ten worm events.	/All Data Monitors/Real-time Rules/PCI DSS/Requirement 5-Protect All Systems and Networks from Malicious Software
Top Source IPs	Shows the top five source IPs involved on data flow from cardholder data environment to non-cardholder data environment.	/All Data Monitors/ArcSight Solutions/PCI DSS/Requirement 1-Install and Maintain Network Security Controls/Data Flow from CDE to non-CDE
Top Source IPs	Shows the top five source IPs involved on data flow from non-cardholder data environment to cardholder data environment.	/All Data Monitors/ArcSight Solutions/PCI DSS/Requirement 1-Install and Maintain Network Security Controls/Data Flow from non-CDE to CDE
Top Target IPs	Shows the top five target IPs involved on data flow from cardholder data environment to non-cardholder data environment.	/All Data Monitors/ArcSight Solutions/PCI DSS/Requirement 1-Install and Maintain Network Security Controls/Data Flow from CDE to non-CDE

Data Monitors Resources, continued

Resource	Description	URI
Top Target IPs	Shows the top five target IPs involved on data flow from non-cardholder data environment to cardholder data environment.	/All Data Monitors/ArcSight Solutions/PCI DSS/Requirement 1-Install and Maintain Network Security Controls/Data Flow from non-CDE to CDE
Top Target Ports	Shows the top five target ports involved on data flow from cardholder data environment to non-cardholder data environment.	/All Data Monitors/ArcSight Solutions/PCI DSS/Requirement 1-Install and Maintain Network Security Controls/Data Flow from CDE to non-CDE
Top Target Ports	Shows the top five target ports involved on data flow from non-cardholder data environment to cardholder data environment.	/All Data Monitors/ArcSight Solutions/PCI DSS/Requirement 1-Install and Maintain Network Security Controls/Data Flow from non-CDE to CDE
Top 5 Target IPs	Shows the top five target IPs for the Worm Activity dashboard.	/All Data Monitors/Real-time Rules/PCI DSS/Requirement 5-Protect All Systems and Networks from Malicious Software
Worm Activity per 10 Minutes	Shows real-time worm activity over the last ten minutes.	/All Data Monitors/Real-time Rules/PCI DSS/Requirement 5-Protect All Systems and Networks from Malicious Software
Worm Propagation	Shows worm propagation in your environment.	/All Data Monitors/Real-time Rules/PCI DSS/Requirement 5-Protect All Systems and Networks from Malicious Software

Field Sets

The following table lists all the field sets in Compliance Insight Package for the Payment Card Industry Data Security Standard.

Field Set Resources

Resource	Description	URI
Data Flow Events	Shows data flow event fields.	/All Field Sets/ArcSight Solutions/PCI DSS

Filters

The following table lists all the filters in Compliance Insight Package for the Payment Card Industry Data Security Standard.

Filters Resources

Resource	Description	URI
Anti-Virus Clean or Quarantine Attempt	Identifies anti-virus events that indicate a quarantine or cleaning attempt of a detected malware instance.	/All Filters/ArcSight Solutions/PCI DSS/Requirement 5-Protect All Systems and Networks from Malicious Software
Attacker Host or Address Present	Identifies events that have either the Attacker Host Name or Attacker Address event fields populated.	/All Filters/ArcSight Solutions/PCI DSS/General Filters
Attacks and Suspicious Activity	Identifies events which indicate compromise, reconnaissance, hostile, or suspicious activity.	/All Filters/ArcSight Solutions/PCI DSS/General Filters
Cardholder Data Environment Inbound Events	Identifies all the cardholder data environment inbound traffic.	/All Filters/ArcSight Solutions/PCI DSS/General Filters/Data Flow
Cardholder Data Environment Outbound Events	Identifies all the cardholder data environment outbound traffic.	/All Filters/ArcSight Solutions/PCI DSS/General Filters/Data Flow
Compliance Score Updates	Identifies events that are generated when values in the Compliance Score active list are changed.	/All Filters/ArcSight Solutions/PCI DSS/General Filters/Overview/Risk Score Dashboard Overview
Default Vendor Account Credential Observed	Identifies events where system access with vendor-supplied accounts is observed.	/All Filters/ArcSight Solutions/PCI DSS/Requirement 2-Apply Secure Configurations to All System Components
Default Vendor Account Detected	Identifies default accounts reported by vulnerability scans.	/All Filters/ArcSight Solutions/PCI DSS/Requirement 2-Apply Secure Configurations to All System Components
Destination Asset is CDE	Identifies events with destination in the cardholder data environment.	/All Filters/ArcSight Solutions/PCI DSS/General Filters/Assets
Firewall Configuration Modifications	Identifies events when the configuration of a firewall is changed.	/All Filters/ArcSight Solutions/PCI DSS/General Filters/Configuration Changes
Limit Regulation	Ensures that the solution only processes events that are addressed by the regulation.	/All Filters/ArcSight Solutions/PCI DSS/My Filters

Filters Resources, continued

Resource	Description	URI
Malicious Traffic to Cardholder Data Environment	Identifies malicious inbound traffic to the cardholder data environment.	/All Filters/ArcSight Solutions/PCI DSS/Requirement 1-Install and Maintain Network Security ControlsRequirement 1-Install and Maintain Network Security Controls
Malware Activity	Identifies events where malware activity is detected.	/All Filters/ArcSight Solutions/PCI DSS/Requirement 5-Protect All Systems and Networks from Malicious Software
Network Device Configuration Modifications	Identifies events when the configuration of an infrastructural equipment (router, switch) is changed.	/All Filters/ArcSight Solutions/PCI DSS/General Filters/Configuration Changes
Network IDS Configuration Modifications	Identifies events when the configuration of NIDS equipment is changed.	/All Filters/ArcSight Solutions/PCI DSS/General Filters/Configuration Changes
Network Routing Configuration Modifications	Identifies events when a modification to the routing table of infrastructure equipment (router, switch) is made.	/All Filters/ArcSight Solutions/PCI DSS/General Filters/Configuration Changes
PCI Rule Firing	Identifies all PCI-DSS rules firing events.	/All Filters/ArcSight Solutions/PCI DSS/General Filters/Overview/Risk Score Dashboard Overview
Personal Records Information Leak	Identifies information leaks with regard to personal information.	/All Filters/ArcSight Solutions/PCI DSS/General Filters/Information Leakage
Security Software Stopped or Paused	Identifies indicating security software stopped or paused.	/All Filters/ArcSight Solutions/PCI DSS/General Filters
Source Asset is CDE	Identifies events with source in the cardholder data environment.	/All Filters/ArcSight Solutions/PCI DSS/General Filters/Assets
Spyware Activity	Identifies spyware activity events reported by either an Intrusion Detection System (IDS) or an anti-virus application.	/All Filters/ArcSight Solutions/PCI DSS/Requirement 5-Protect All Systems and Networks from Malicious Software
Target Host or Address Present	Identifies events that have either the Target Host Name or Target Address event fields populated.	/All Filters/ArcSight Solutions/PCI DSS/General Filters
Target User Present	Identifies if the Target User Name field is populated.	/All Filters/ArcSight Solutions/PCI DSS/General Filters
Trojan Activity	Identifies trojan activity.	/All Filters/ArcSight Solutions/PCI DSS/Requirement 5-Protect All Systems and Networks from Malicious Software

Filters Resources, continued

Resource	Description	URI
Virus Activity	Identifies virus activity events reported by either an Intrusion Detection System (IDS) or an anti-virus application.	/All Filters/ArcSight Solutions/PCI DSS/Requirement 5-Protect All Systems and Networks from Malicious Software
VPN Configuration Modifications	Identifies events indicating that a VPN configuration change has occurred.	/All Filters/ArcSight Solutions/PCI DSS/General Filters/Configuration Changes
Vulnerability Events	Identifies vulnerability related events.	/All Filters/ArcSight Solutions/PCI DSS/General Filters/Vulnerabilities
Wireless Related Events	Identifies wireless events reported from those products AirDefense, AirPatrolCorp, AirMagnet or events related to assets which categorized as/All Asset Categories/Industrial Control Systems/Wireless Network.	/All Filters/ArcSight Solutions/PCI DSS/General Filters/Wireless
Wireless Vulnerability or Misconfiguration Detected	Identifies wireless-related vulnerabilities and misconfigurations reported by vulnerability scans.	/All Filters/ArcSight Solutions/PCI DSS/Requirement 2-Apply Secure Configurations to All System Components
Worm Activity	Identifies events where worm activity is detected based on both correlation and base events reported by ArcSight Connectors.	/All Filters/ArcSight Solutions/PCI DSS/Requirement 5-Protect All Systems and Networks from Malicious Software
Worm Reported Events	Identifies events where worm activity is reported by ArcSight Connectors.	/All Filters/ArcSight Solutions/PCI DSS/Requirement 5-Protect All Systems and Networks from Malicious Software

Queries

The following table lists all the queries in Compliance Insight Package for the Payment Card Industry Data Security Standard.

Queries Resources

Resources	Description	URI
Cardholder Data Environment Inbound Traffic	Shows cardholder data environment inbound traffic.	/All Queries/ArcSight Solutions/PCI DSS/Requirement 1-Install and Maintain Network Security Controls
Cardholder Data Environment Outbound Traffic	Shows cardholder data environment outbound traffic.	/All Queries/ArcSight Solutions/PCI DSS/Requirement 1-Install and Maintain Network Security Controls

Queries Resources, continued

Resources	Description	URI
Firewall Configuration Modifications	Shows any configuration modifications of any firewall. Default time window: Last 24 hours.	/All Queries/ArcSight Solutions/PCI DSS/Requirement 1-Install and Maintain Network Security Controls
Firewall Configuration Modifications by Name	Shows the top configuration modifications of any firewall.	/All Queries/ArcSight Solutions/PCI DSS/Requirement 1-Install and Maintain Network Security Controls
IDS Configuration Modifications	Shows any configuration modifications of any network IDS. Default time window: Last 24 hours.	/All Queries/ArcSight Solutions/PCI DSS/Requirement 1-Install and Maintain Network Security Controls
IDS Configuration Modifications by Name	Shows the top configuration modifications of any network IDS.	/All Queries/ArcSight Solutions/PCI DSS/Requirement 1-Install and Maintain Network Security Controls
List of Default Vendor Account Used	Shows a list of default vendor account used. Default time window: Last 24 hours.	/All Queries/ArcSight Solutions/PCI DSS/Requirement 2-Apply Secure Configurations to All System Components
List of Wireless Vulnerabilities and Misconfigurations	Shows a list of wireless vulnerabilities and misconfigurations reported by vulnerability scanner devices. Default time window: Last 24 hours.	/All Queries/ArcSight Solutions/PCI DSS/Requirement 2-Apply Secure Configurations to All System Components
Network Routing Configuration Modifications	Shows any configuration modifications of any network routing. Default time window: Last 24 hours.	/All Queries/ArcSight Solutions/PCI DSS/Requirement 1-Install and Maintain Network Security Controls
Network Routing Configuration Modifications by Name	Shows the top configuration modifications of any network routing.	/All Queries/ArcSight Solutions/PCI DSS/Requirement 1-Install and Maintain Network Security Controls
PCI Rule Firing Events	Shows triggered PCI rules.	/All Queries/ArcSight Solutions/PCI DSS/Overview
Security Software Stopped or Paused	Shows security software stopped or paused.	/All Queries/ArcSight Solutions/PCI DSS/Requirement 1-Install and Maintain Network Security Controls
Top Default Vendor Accounts	Shows the top default vendor accounts.	/All Queries/ArcSight Solutions/PCI DSS/Requirement 2-Apply Secure Configurations to All System Components

Queries Resources, continued

Resources	Description	URI
Unmasked Primary Account Numbers	Shows data of stored or transmitted unmasked PAN.	/All Queries/ArcSight Solutions/PCI DSS/Requirement 3-Protect Stored Account Data/
VPN Configuration Modifications	Shows any configuration modifications of any vpn device. Default time window: Last 24 hours.	/All Queries/ArcSight Solutions/PCI DSS/Requirement 1-Install and Maintain Network Security Controls
VPN Configuration Modifications by Name	Shows the top configuration modifications of any vpn device.	/All Queries/ArcSight Solutions/PCI DSS/Requirement 1-Install and Maintain Network Security Controls

Query Viewers

The following table lists all the query viewers in Compliance Insight Package for the Payment Card Industry Data Security Standard.

Query Viewers Resources

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

Reports

The following table lists all the reports in Compliance Insight Package for the Payment Card Industry Data Security Standard.

Reports Resources

Resource	Description	URI
Cardholder Data Environment Inbound Traffic	Reports cardholder data environment inbound traffic.	/All Reports/ArcSight Solutions/PCI DSS/Requirement 1-Install and Maintain Network Security ControlsRequirement 1-Install and Maintain Network Security Controls
Cardholder Data Environment Outbound Traffic	Reports cardholder data environment inbound traffic.	/All Reports/ArcSight Solutions/PCI DSS/Requirement 1-Install and Maintain Network Security ControlsRequirement 1-Install and Maintain Network Security Controls

Reports Resources, continued

Resource	Description	URI
Firewall Configuration Modifications	Reports any configuration modifications of any firewall.	/All Reports/ArcSight Solutions/PCI DSS/Requirement 1-Install and Maintain Network Security ControlsRequirement 1-Install and Maintain Network Security Controls
IDS Configuration Modifications	Reports any configuration modifications of any network IDS.	/All Reports/ArcSight Solutions/PCI DSS/Requirement 1-Install and Maintain Network Security ControlsRequirement 1-Install and Maintain Network Security Controls
Malware Summary	Provides a chart and tabular view of malware activity. This report features prominent malware types, threats, and malware event information.	/All Reports/Real-time Rules/PCI DSS/Requirement 5-Protect All Systems and Networks from Malicious Software
Network Routing Configuration Modifications	Reports any configuration modifications of any network routing.	/All Reports/ArcSight Solutions/PCI DSS/Requirement 1-Install and Maintain Network Security ControlsRequirement 1-Install and Maintain Network Security Controls/
Security Software Stopped or Paused	Reports security software stopped or paused events.	/All Reports/ArcSight Solutions/PCI DSS/Requirement 1-Install and Maintain Network Security ControlsRequirement 1-Install and Maintain Network Security Controls
Summary of Wireless Vulnerabilities and Misconfigurations	Reports wireless vulnerabilities and misconfigurations.	/All Reports/ArcSight Solutions/PCI DSS/Requirement 2-Apply Secure Configurations to All System Components/
Summary of Vendor Default Accounts	Reports the list of default vendor accounts used.	/All Reports/ArcSight Solutions/PCI DSS/Requirement 2-Apply Secure Configurations to All System Component
Unmasked PAN Summary	Reports the data of unmasked plain text Primary Account Numbers like bank, credit cards, and others stored or transmitted in the network on an hourly basis.	/All Reports/ArcSight Solutions/PCI DSS/Requirement 3-Protect Stored Account Data/
VPN Configuration Modifications	Reports any configuration modifications of any vpn device.	/All Reports/ArcSight Solutions/PCI DSS/Requirement 1-Install and Maintain Network Security ControlsRequirement 1-Install and Maintain Network Security Controls/

Rules

The following table lists all the rules in Compliance Insight Package for the Payment Card Industry Data Security Standard.

Rules Resources

Resource	Description	URI
Anonymous Key Exchange Detected PCI 4.2.1	Triggers when there is an anonymous key exchange that happens in the network.	/All Rules/ArcSight Solutions/PCI DSS/Requirement 4-Protect Cardholder Data with Strong Cryptography During Transmission Over Open, Public Networks
Compliance Score Update	Detects other PCI rules and updates the Compliance Risk Score active list.	/All Rules/ArcSight Solutions/PCI DSS/Overview
Critical Configuration Change to NSC device	Detects changes in the configuration of NSC Devices that are classified with a “very-high” agent severity. Devices include Firewalls, VPNs, Network Equipment, Network Routings, and Network Intrusion Detection Systems.	/All Rules/ArcSight Solutions/PCI DSS/Requirement 1-Install and Maintain Network Security Controls
Database Reachable for Internet	Detects events coming from outside the organization network targeting database assets. Make sure the database assets are categorized under/All Assets Categories/ArcSight Solutions/Compliance Insight Package/Application/Type/Database.	/All Rules/ArcSight Solutions/PCI DSS/Requirement 1-Install and Maintain Network Security Controls
Default Password Detected PCI 2.2.2	Detects default passords via vulnerability scanners.	/All Rules/Real-time Rules/PCI DSS/Requirement 2-Apply Secure Configurations to All System Components/
Default Vendor Account Activity Detected	Detects authentication attempts made to accounts designated as default vendor accounts. Default vendor accounts are those listed in the active list:/All Active Lists/ArcSight Solutions/PCI DSS/Default Vendor Accounts. These accounts are typically associated with third-party vendors and may have elevated privileges or access levels. Detecting authentication attempts to these accounts is crucial for ensuring compliance with PCI DSS requirements and mitigating potential security risks associated with privileged access.	/All Rules/ArcSight Solutions/PCI DSS/Requirement 2-Apply Secure Configurations to All System Components

Rules Resources, continued

Resource	Description	URI
Default Vendor Account Detected	Detects default accounts via vulnerability scanners.	All Rules/ArcSight Solution/PCI DSS/Requirement 2-Apply Secure Configurations to All System Components
Default Wireless Password Detected PCI 2.2.2.	Triggers when a default password is detected on a Wireless asset. **Note:** In order for this rule to be triggered make sure of the following: 1. Ensure that wireless assets are added to the following Asset Category: /All Assets Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/Wireless. 2. The Default Password Detected rule should be enabled and deployed.	/All Rules/Real-time Rules/PCI DSS/Requirement 2-Apply Secure Configurations to All System Components
Deprecated TLS Protocol Version Detected PCI 4.2.1	Triggers when a deprecated version of TLS protocol is used.	/All Rules/ArcSight Solutions/PCI DSS/Requirement 4-Protect Cardholder Data with Strong Cryptography During Transmission Over Open, Public Networks
Insecure Communication Detected PCI 4.2.1.	Detects when there is an insecure communication in the network.	/All Rules/ArcSight Solutions/PCI DSS/Requirement 4-Protect Cardholder Data with Strong Cryptography During Transmission Over Open, Public Networks
Insecure Cryptographic Implementation Detected PCI 6.4.2	Detects when there is a weak cryptographic implementation.	/All Rules/ArcSight Solutions/PCI DSS/Requirement 6-Develop and Maintain Secure Systems and Software
Invalid or Expired Certificate Detected PCI 4.2.1.	Detects expired or invalid certificates.	/All Rules/ArcSight Solutions/PCI DSS/Requirement 4-Protect Cardholder Data with Strong Cryptography During Transmission Over Open, Public Networks

Rules Resources, continued

Resource	Description	URI
Malicious Traffic to Cardholder Data Environment	Detects malicious inbound traffic to the cardholder data environment.	/All Rules/ArcSight Solutions/PCI DSS/Requirement 1-Install and Maintain Network Security Controls
Malware Detected PCI 5.2	Detects potential malware activity in the environment.	/All Rules/Real-time Rules/PCI DSS/Requirement 5-Protect All Systems and Networks from Malicious Software
Manual Status Change	Detects when a section's status on the Compliance Risk Score dashboard is changed manually.	/All Rules/ArcSight Solutions/PCI DSS/Overview
Multiple Functions Implemented on a Server PCI 2.2.3.	Triggers when both a web server and a database are installed on the same machine, indicating multiple functionalities on a single asset. **Note:** Make sure the database assets should are categorized with the /All Assets Categories/ArcSight Solutions/Compliance Insight Package/Application/Type/Database.	/All Rules/Real-time Rules/PCI DSS/Requirement 2-Apply Secure Configurations to All System Components
Personal Information Leakage	Detects personal information leakage.	/All Rules/ArcSight Solutions/PCI DSS/Requirement 1-Install and Maintain Network Security Controls
Personal Information Leakage from Database	Detects personal Information Leakage from Database on Cardholder Data Environment. Make sure the database assets are categorized under/All Assets Categories/ArcSight Solutions/Compliance Insight Package/Application/Type/Database.	/All Rules/ArcSight Solutions/PCI DSS/Requirement 1-Install and Maintain Network Security Controls
Rogue Wireless Device Detected PCI 11.2.1 and 11.2.2	Detects rogue devices based on events reported from AirDefense, AirPatrolCorp, AirMagnet or events related to assets categorized under/All Asset Categories/Industrial Control Systems/Wireless Network.	/All Rules/ArcSight Solutions/PCI DSS/Requirement 11-Test Security of Systems and Networks Regularly
Security Software Stopped or Paused	Detects when a security software service has been disabled. Refer to the condition tab of this rule for the list of services.	/All Rules/ArcSight Solutions/PCI DSS/Requirement 1-Install and Maintain Network Security Controls

Rules Resources, continued

Resource	Description	URI
Spyware Detected PCI 5.2	Triggers when a spyware is reported by either an Intrusion Detection System (IDS) or an anti-virus application. **Note:** In order for this rule to be triggered, make sure the Malware Detected rule is enabled and deployed.	/All Rules/Real-time Rules/PCI DSS/Requirement 5-Protect All Systems and Networks from Malicious Software
SSH Weak Algorithm Detected PCI 4.2.1	Detects when a weak ssh algorithm is used in the network.	/All Rules/ArcSight Solutions/PCI DSS/Requirement 4-Protect Cardholder Data with Strong Cryptography During Transmission Over Open, Public Networks
SSL Protocol Detected PCI 4.2.1	Detects SSL protocols.	/All Rules/Real-time Rules/PCI DSS/Requirement 4-Protect Cardholder Data with Strong Cryptography During Transmission Over Open, Public Networks
Unauthorized Traffic from Cardholder Data Environment	Detects unauthorized outbound traffic from the cardholder data environment. Make sure the cardholder data environment assets are categorized under Asset Categories/ArcSight Solutions/Compliance Insight Package/Regulations/PCI/Cardholder Data.	/All Rules/ArcSight Solutions/PCI DSS/Requirement 1-Install and Maintain Network Security Controls
Unauthorized Traffic from Cardholder Data Environment to DMZ	Detects unauthorized outbound traffic from the cardholder data environment to DMZ. Make sure of the following: 1. The DMZ assets are categorized under/All Assets Categories/ArcSight Solutions/Compliance Insight Package/Address Spaces/DMZ. 2. Enable and deploy the rule: Unauthorized Traffic from Cardholder Data Environment.	/All Rules/ArcSight Solutions/PCI DSS/Requirement 1-Install and Maintain Network Security Controls
Unauthorized Traffic to Cardholder Data Environment from Wireless Environment	Detects unauthorized outbound traffic to the cardholder data environment from the wireless environment. Make sure of the following: 1. 1. The wireless assets are categorized under/All Assets Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/Wireless. 2. Enable and deploy Unauthorized Traffic to Cardholder Data Environment should be enabled and deployed.	/All Rules/ArcSight Solutions/PCI DSS/Requirement 1-Install and Maintain Network Security Controls

Rules Resources, continued

Resource	Description	URI
Unauthorized Traffic from Cardholder Data Environment to Third Party Asset	Detects unauthorized outbound traffic from the cardholder data environment to third-party assets. Make sure of the following: 1. The third-party assets are categorized under/All Assets Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/Third Party. 2. Enable and deploy the rule: Unauthorized Traffic from Cardholder Data Environment.	/All Rules/ArcSight Solutions/PCI DSS/Requirement 1-Install and Maintain Network Security Controls
Unauthorized Traffic from Cardholder Data Environment to Wireless Environment	Detects unauthorized outbound traffic from the cardholder data environment to the wireless environment. Make sure of the following: 1. The wireless assets are categorized under/All Assets Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/Wireless. 2. Enable and deploy rule: Unauthorized Traffic from Cardholder Data Environment.	/All Rules/ArcSight Solutions/PCI DSS/Requirement 1-Install and Maintain Network Security Controls
Unauthorized Traffic to Cardholder Data Environment	Detects unauthorized inbound traffic to the cardholder data environment. Make sure the cardholder data environment assets are categorized under/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Regulations/PCI/Cardholder Data.	/All Rules/ArcSight Solutions/PCI DSS/Requirement 1-Install and Maintain Network Security Controls
Unauthorized Traffic to Cardholder Data Environment from DMZ	Detects unauthorized outbound traffic to the cardholder data environment from DMZ. Make sure of the following: 1. The DMZ assets are categorized under/All Assets Categories/ArcSight Solutions/Compliance Insight Package/Address Spaces/DMZ. 2. Enable and deploy the rule: Unauthorized Traffic to Cardholder Data Environment.	/All Rules/ArcSight Solutions/PCI DSS/Requirement 1-Install and Maintain Network Security Controls
Unauthorized Traffic to Cardholder Data Environment from Third Party Asset	Detects unauthorized outbound traffic to the cardholder data environment from third-party assets. Make sure of the following: 1. The third-party Assets are categorized under/All Assets Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/Third Party. 2. Enable and deploy rule: Unauthorized Traffic to Cardholder Data Environment.	/All Rules/ArcSight Solutions/PCI DSS/Requirement 1-Install and Maintain Network Security Controls

Rules Resources, continued

Resource	Description	URI
Unmasked Primary Account Numbers Detected PCI 3.4.1 and 3.4.2	Detects when sensitive information such as credit card account numbers is stored or transmitted as plain text.	/All Rules/ArcSight Solutions/PCI DSS/Requirement 3-Protect Stored Account Data
Vulnerability Detected on Cryptographic Protocol PCI 4.2.1	Detects when a vulnerability is detected in a cryptographic algorithm that is being used.	/All Rules/ArcSight Solutions/PCI DSS/Requirement 4-Protect Cardholder Data with Strong Cryptography During Transmission Over Open, Public Networks
Weak Key Exchange Detected PCI 3.7.5	Detects weak key algorithms in the environment.	/All Rules/Real-time Rules/PCI DSS/Requirement 3-Protect Stored Account Data
Wireless Malicious Traffic Detected	Detects wireless malicious traffic based on events reported from AirDefense, AirPatrolCorp, AirMagnet or events related to assets categorized under/All Asset Categories/Industrial Control Systems/Wireless Network.	/All Rules/ArcSight Solutions/PCI DSS/Requirement 1-Install and Maintain Network Security Controls
Wireless Vulnerability or Misconfiguration Detected	Detects wireless vulnerabilities or misconfigurations.	All Rules/ArcSight Solution/PCI DSS/Requirement 2-Apply Secure Configurations to All System Components
Worm Detected PCI 5.2	Triggers when a worm is reported by either an Intrusion Detection System (IDS) or an anti-virus application. **Note:** In order for this rule to be triggered, make sure the Malware Detected rule is enabled and deployed.	/All Rules/Real-time Rules/PCI DSS/Requirement 5-Protect All Systems and Networks from Malicious Software

Use Cases

The following table lists all the use cases in Compliance Insight Package for the Payment Card Industry Data Security Standard.

Use Cases Resources

Resource	Description	URI
Critical Configuration Change to NSC device PCI 1.2, 1.2.1, 1.2.2	Provides resources that monitor critical configuration changes to NSC devices.	All Use Cases/ArcSight Solutions/PCI DSS
Database Reachable for Internet	Provides resources that monitor if the database can be reached by the internet.	All Use Cases/ArcSight Solutions/PCI DSS
Default Accounts	Provides resources to monitor default accounts.	All Use Cases/ArcSight Solutions/PCI DSS
Firewall Configuration Modifications PCI 1.2.1, 1.2.2, 1.2.7, 1.2.8	Provides resources that monitor firewall configuration changes.	All Use Cases/ArcSight Solutions/PCI DSS
IDS Configuration Modifications	Provides resources that monitor IDS configuration changes.	All Use Cases/ArcSight Solutions/PCI DSS
Inbound Traffic to CDE PCI 1.3.1, 1.4.1, 1.4.2	Providess resources that monitor inbound traffic to CDE.	/All Use Cases/ArcSight Solutions/PCI DSS/
Insecure Communication Detected	Provides resources that monitor insecure communications.	/All Use Cases/ArcSight Solutions/PCI DSS/

Use Cases Resources, continued

Resource	Description	URI
Invalid or Expired Certificate Detected PCI 4.2.1	Provides resources that monitor invalid or expired certificates.	/All Use Cases/ArcSight Solutions/PCI DSS/
Malware Monitoring PCI 5.2	Provides a high-level overview of resources that monitor and analyze malware events and devices in real-time.	All Use Cases/ArcSight Solutions/PCI DSS
Malicious Traffic to Cardholder Data Environment PCI 1.5.1	Provides Resources that monitor malicious traffic to cardholder data environments.	All Use Cases/ArcSight Solutions/PCI DSS
Network Routing Configuration Changes PCI 1.21, 1.2.2, 1.2.7, 1.2.8	Provides resources that monitor network routing configuration changes.	All Use Cases/ArcSight Solutions/PCI DSS
Outbound Traffic from CDE	Provides resources to monitor outbound traffic from CDE.	All Use Cases/ArcSight Solutions/PCI DSS
Personal Information Leakage from Database 1.4.4	Provides resources that monitor personal information leakages from your databases.	All Use Cases/ArcSight Solutions/PCI DSS
Security Software Stopped or Paused PCI 1.5.1	Provides resources that monitor security software stoppages or pauses.	All Use Cases/ArcSight Solutions/PCI DSS
Unauthorized Traffic from Cardholder Data Environment PCI 1.3.1, 1.4.1, 1.4.2	Provides resources that monitor unauthorized traffic from cardholder data environments with a specific focus on port-connection monitoring. By default, all connection types and ports are allowed. Disallowed ports are either ports entered into the Disallowed Ports active list or any port that is not entered into the Allowed Ports Active list. Explicit port entries on the Disallowed Ports active list always take precedence over entries on the Allowed Ports active list. Conditions are located in the Disallowed Ports Access filter.	All Use Cases/ArcSight Solutions/PCI DSS

Use Cases Resources, continued

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

Publication Status

Released: August 31, 2019

Updated: Thursday, July 18, 2024

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 system, click the link above and an email window opens with the following information in the subject line:

Feedback on ArcSight Administration and ArcSight System Standard Content Guide (ESM CIP for PCI DSS 4.0)

Just add your feedback to the email and click send.

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

We appreciate your feedback!