

# **Regulatory Compliance: PCI/DSS V4.0**

### Whitepaper

Payment Card Industry Data Security Standard (PCI / DSS)





© Intersect Alliance International Pty Ltd. All rights reserved worldwide.

Intersect Alliance Pty Ltd shall not be liable for errors contained herein or for direct, or indirect damages in connection with the use of this material. No part of this work may be reproduced or transmitted in any form or by any means except as expressly permitted by Intersect Alliance International Pty Ltd. This does not include those documents and software developed under the terms of the open source General Public Licence, which covers the Snare agents and some other software.

The Intersect Alliance logo and Snare logo are registered trademarks of Intersect Alliance International Pty Ltd. Other trademarks and trade names are marks' and names of their owners as may or may not be indicated. All trademarks are the property of their respective owners and are used here in an editorial context without intent of infringement. Specifications and content are subject to change without notice.

About this document

The PCI/DSS documentation provides guidance on a set of baseline security measures that are designed to reduce fraud relating to credit cards, and to encourage the adoption of consistent security countermeasures across a range of businesses that are linked by the need to store or process payment card data.

This document discusses the role of audit log data in meeting PCI/DSS requirements.

# **Security Standard Overview**

The latest iteration of the PCI/DSS documentation (version 4.0), was released in March 2022. The security standard highlights a wide range of security practices that are designed to enhance the security of credit card information and client details. PCI/DSS requirements should be considered a baseline requirement, and can be enhanced with additional controls to further mitigate risk. A full copy of the standard can be found at <u>https://www.pcisecuritystandards.org</u> From the document:

"PCI DSS requirements apply to entities with environments where account data (cardholder data and/or sensitive authentication data) is stored, processed, or transmitted, and entities with environments that can impact the security of the CDE (**Cardholder Data Environment**). Some PCI/DSS requirements may also apply to entities with environments that do not store, process, or transmit account data – for example, entities that outsource payment operations or management of their CDE 1. Entities that outsource



their payment environments or payment operations to third parties remain responsible for ensuring that the account data is protected by the third party per applicable PCI/DSS requirements. The **primary account number** (PAN) is the defining factor for cardholder data. The term account data therefore covers the following: the full PAN, any other elements of cardholder data that are present with the PAN, and any elements of sensitive authentication data.."

If cardholder name, service code, and/or expiration date are stored, processed, or transmitted with the PAN, or are otherwise present in the Cardholder Data Envrionment (CDE), they **must** be protected in accordance with applicable PCI/DSS requirements.

If the entity does not store or process PAN data, but holds sensitive application data (SAD), or related sensitive cardholder data, some PCI/DSS requirements **may** still apply.

Consider the following:

- If the entity stores SAD, requirements specifically related to SAD storage in Requirement 3 will be applicable.
- If the entity engages third-party service providers to store, process or transmit PAN on its behalf, requirements related to the management of service providers in Requirement 12 will be applicable.
- If the entity can impact the security of a CDE because the security of an entity's infrastructure can affect how cardholder data is processed (for example, via a web server that controls the generation of a payment form or page) some requirements will be applicable.
- If cardholder data is only present on physical media (for example paper), requirements relating to the security and disposal of physical media in Requirement 9 will be applicable.
- Requirements related to an incident response plan are applicable to all entities, to ensure that there are procedures to follow in the event of a suspected or actual breach of the confidentiality of cardholder data.

Audit logging capabilities underpin a range of security measures within PCI/DSS, however section 10 of the document specifically addresses logging and auditing. Requirement 10 is reproduced below for reference:

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

Logging mechanisms and the ability to track user activities are critical in preventing, detecting, or minimizing the impact of a data compromise. The presence of logs on all system components and in the cardholder data environment (CDE) allows thorough tracking, alerting, and analysis when something does go wrong. Determining the cause of a compromise is difficult, if not impossible, without system activity logs. This requirement applies to user activities, including those by employees, contractors, consultants, and internal and external vendors, and other third parties (for example,



those providing support or maintenance services). These requirements do not apply to user activity of consumers (cardholders)

10.1 Processes and mechanisms for logging and monitoring all access to system components and cardholder data are defined and documented.

10.1.1 All security policies and operational procedures that are identified in Requirement 10 are, documented, kept up to date, in use, and known to all affected parties.

10.1.2 Roles and responsibilities for performing activities in Requirement 10 are documented, assigned, and understood

10.2 Audit logs are implemented to support the detection of anomalies and suspicious activity, and the forensic analysis of events (use Snare Agents to collect this data from host systems, Use Snare Central to collect this log data from syslog network devices)

10.2.1 Audit logs are enabled and active for all system components and cardholder data.

- 10.2.1.1 Audit logs capture all individual user access to cardholder data
- 10.2.1.2 Audit logs capture all actions taken by any individual with administrative access, including any interactive use of application or system accounts (Snare agents default policies help collect most of this information out of the box)
- 10.2.1.3 Audit logs capture all access to audit logs (Snare agents default policies help collect most of this information out of the box)



- 10.2.1.4 Audit logs capture all invalid logical access attempts (Snare agents default policies help collect most of this information out of the box)
- 10.2.1.5 Audit logs capture all changes to identification and authentication credentials including, but not limited to (Snare agents default policies help collect most of this information out of the box, Snare Central reports help with compliance and reporting of these activities)
- □ Creation of new accounts.
- □ Elevation of privileges.
- All changes, additions, or deletions to accounts with administrative access.

10.2.1.6 Audit logs capture the following: - (Snare agents default policies help collect most of this information out of the box)

- □ All initialization of new audit logs, and
- □ All starting, stopping, or pausing of the existing audit logs.

10.2.1.7 Audit logs capture all creation and deletion of system-level objects - (Snare agents default policies help collect most of this information out of the box, FIM,FAM,RIM and RAM extend the coverage to include other operating system and application areas)

10.2.2 Audit logs record the following details for each auditable event: - This is part of the structure of the Snare agent event that collect all this information for each event)

- □ User identification.
- □ Type of event.
- Date and time.
- □ Success and failure indication.
- □ Origination of event.



6

snaresolutions.com - Identity or name of affected data, system component, resource, or service (for example, name and protocol).

10.3 Audit logs are protected from destruction and unauthorized modifications. - (Snare Central is used to collect and store this information with the retention period that can be defined for 12 months or more if needed. Role based access controls are used to manage access to the systems and any admin levels of the system and data.)

- 10.3.1 Read access to audit logs files is limited to those with a job-related need
- 10.3.2 Audit log files are protected to prevent modifications by individuals
- 10.3.3 Audit log files, including those for external facing technologies, are promptly backed up to a secure, central, internal log server(s) or other media that is difficult to modify.
- 10.3.4 File integrity monitoring or change-detection mechanisms is used on audit logs to ensure that existing log data cannot be changed without generating alerts

10.4 Audit logs are reviewed to identify anomalies or suspicious activity - (Snare Central reports and event search options are available for compliance reporting as well as any incident investigation.)

10.4.1 The following audit logs are reviewed at least once daily:

- □ All security events.
- Logs of all system components that store, process, or transmit CHD and/or SAD.
- Logs of all critical system components.
- Logs of all servers and system components that perform security functions (for example, network security controls, intrusiondetection systems/intrusion-prevention systems (IDS/IPS), authentication servers)

10.4.2 Logs of all other system components (those not specified in Requirement 10.4.1) are reviewed periodically.

10.4.2.1 The frequency of periodic log reviews for all other system components (not defined in Requirement 10.4.1) is defined in the entity's



targeted risk analysis, which is performed according to all elements specified in Requirement 12.3.1

10.4.3 Exceptions and anomalies identified during the review process are addressed.

10.5 Audit log history is retained and available for analysis. (Snare Central can store the logs securely for as long as needed to meet the compliance needs)

10.5.1 Retain audit log history for at least 12 months, with at least the most recent three months immediately available for analysis

10.6 Time-synchronization mechanisms support consistent time settings across all systems. - ( Snare Agents will obtain the local system time for events, Snare Central will use any trusted NTP source on the customers network to ensure that the local logs and system time is correct.)

10.6.1 System clocks and time are synchronized using time-synchronization technology.

10.6.2 Systems are configured to the correct and consistent time as follows:

- One or more designated time servers are in use.
- Only the designated central time server(s) receives time from external sources.
- Time received from external sources is based on International Atomic Time or Coordinated Universal Time (UTC).
- □ The designated time server(s) accept time updates only from specific industry-accepted external sources.
- □ Where there is more than one designated time server, the time servers peer with one another to keep accurate time.
- Internal systems receive time information only from designated central time server(s).

10.6.3 3 Time synchronization settings and data are protected as follows:

- □ Access to time data is restricted to only personnel with a business nee
- Any changes to time settings on critical systems are logged, monitored, and reviewed.

10.7 Failures of critical security control systems are detected, reported, and responded to promptly. - (Snare Central real time alerts and threshold reporting can be used to alert on specific critical events to systems or access to sensitive data)

10.7.1 Additional requirement for service providers only: Failures of critical security control systems are detected, alerted, and addressed promptly, including but not limited to failure of the following critical security control systems:

- □ Network security controls.
- D IDS/IPS.
- D FIM.
- □ Anti-malware solutions.
- D Physical access controls.
- □ Logical access controls.
- Audit logging mechanisms.
- □ Segmentation controls (if used)

10.7.2 Failures of critical security control systems are detected, alerted, and addressed promptly, including but not limited to failure of the following critical security control systems:

- Network security controls.
- D IDS/IPS.
- Change-detection mechanisms.
- Anti-malware solutions.
- D Physical access controls.
- □ Logical access controls.
- Audit logging mechanisms.
- □ Segmentation controls (if used).
- □ Audit log review mechanisms.
- D Automated security testing tools (if used).

10.7,3 Failures of any critical security controls systems are responded to promptly, including but not limited to:

- Restoring security functions.
- □ Identifying and documenting the duration (date and time from start to end) of the security failure.

- □ Identifying and documenting the cause(s) of failure and documenting required remediation.
- Identifying and addressing any security issues that arose during the failure.
- Determining whether further actions are required as a result of the security failure.
- Implementing controls to prevent the cause of failure from reoccurring.
   Resuming monitoring of security controls.

The Snare solution covering Snare Agents and Snare Central Server are capable of supporting organisational PCI/DSS security strategies, and particularly focuses on meeting the requirements of section 10 of the security standard.

As a centralised log management, collection and analysis engine the Snare Central Server provides a repository of the systems and network audit log data to facilitate compliance for PCI/DSS. It includes reporting functionality suited to the daily, weekly and monthly review of security events, and it is capable of collecting, storing and processing large volumes of data on reasonably variable sized hardware depending ( from small that collect a few gigabytes per day to larger enterprise systems with terabyte collection) on the size of the customers environment and logging needs, in order to meet the requirements of 10.5.1 to keep log data for at least 12 months.

## **Audit Collection**

The following recommendations highlight strategies that can be implemented on the Snare Agents and Snare Central Server, to meet event collection, analysis and reporting requirements for systems, devices and applications that store or process data covered by PCI/DSS. It is strongly recommended that any recommendations below be considered in the light of an organisational risk assessment and security policy.

#### **Network Devices**

Collect management and security events, and failed connections. The management events should include events such as general reconfiguration, policies, reboots and password changes. Usually, events produced by these devices are sent out via SYSLOG, but SNMP Traps may also be used

as a communications medium. Although not directly related to the protection of PAN and related payment card information, successful attacks against network infrastructure can lead to organisational information leakage or enable further attacks against systems that may store and process PAN data. As a general practice all network devices such as firewalls, routers, switches and wireless devices should have their logs collected and stored on a centralized logging server.

The logs will contain valuable information relating to user logins, changes to configuration and policy as well as security-relevant details of network traffic.

If available in the configuration options for your device, the time on the device should be synchronised to a trusted central time server for log consistency.

#### **General Workstations and Servers**

All management and security events, logins and logouts both failed and successful, accounts created and deleted, policy changes should be logged from workstations and servers that do not directly store or process cardholder information, but form part of the CDE. The Snare Agents used for collection of such events should be configured to collect only those events to support this requirement, in order to reduce the flood of information that would otherwise be sent back to a central collection server for analysis and processing. The default Snare agent policies are created with these basic controls in mind and will collect 95% of the administrative type events a systems will create in normal circumstances.

Process monitoring or file access auditing on these servers and workstations is considered important and the general audit strategy should be to collect event log data that may indicate that these systems are used as a jumping-off-point to access other systems that host cardholder information.

In situations where general workstations are used as a transitory storage location for cardholder information (for example, spreadsheets), file auditing on the directories or files containing cardholder information that is used for transitory storage may be required. Snare Agents have several capabilities suited to this area, including.

- FIM File Integrity Monitoring can be configured to monitor sensitive operating system and application log files. This will provide the checksum details and highlight ownership and permission changes on files. These can run on a schedule.
- FAM File Activity Monitoring can be configured to monitor sensitive operating system and application log file. This will provide details on who access files, what program they used to edit the file and when the access occurred.
- RIM Registry Integrity Monitoring can be configured to monitor sensitive registry settings for the operating system and application settings. This will provide the checksum details and highlight ownership and permission changes on configured registry locations. These can run on a schedule.
- RAM Registry Activity Monitoring can be configured to monitor sensitive registry settings for the operating system and application settings. These will provide the information on who changed the registry keys, values before and after the change, who did the changes, and when the change occurred.
- USB USB and removable storage usage should be tracked for either leakage of sensitive data or loading up other unauthorised or potentially malicious files or software.

We have a detailed white paper on some recommended FIM, FAM, RIM and RAM settings can be set for various operating systems here. <u>https://www.snaresolutions.com/portfolio-item/howsnare-makes-fim-easier/</u>

All systems should be time-synchronised to a central time source for log timestamp consistency.

#### **Browsers and Proxies**

If the primary interface to your cardholder information store is via a web browser, browser and proxy log data may provide additional information on attacks against your user base.

Monitoring proxy log data for web sites that are accessed concurrently with your internal content, searching for known external problem sites that have poor reputation, or scanning logs for cross site scripting signatures, may provide indications of attempts to breach your cardholder data.

Snare Agents can collect logs from proxy servers such as ISA or Squid, to provide contextual information relating to internal web-based application access.

#### Web Servers

If the primary interface to your cardholder information store is via a web server, log data from the web server that hosts the user interface as well as operating system log files, may provide valuable information on attacks or attempts to scan the server for vulnerabilities.

Using Snare Agents to collect web logs from platforms such as IIS and Apache can facilitate historical forensics analysis. Monitoring the log data for URL access attempts outside a known authorised subset, can highlight attacks against the server itself. Scanning the logs for unexpected data content within 'GET/POST' requests, may alert administrators to 'fuzzing' attacks against the web-based application itself and areas that are being targeted for SQL Injection, Command Injection, buffer overflows or Cross Site Scripting attacks.

All systems should be time-synchronised to a central time source for log timestamp consistency.

#### Servers used to host/process cardholder information





- all management and security events
- logins and logouts (both failed and successful)
- accounts created and deleted, and
- events pertaining directly to the event/audit log.

File event monitoring should be considered on those directories that store cardholder or sensitive information (as detailed above) as well as critical operating system files and settings. Care should be taken in employing file auditing, since it generally results in a large number of system events being generated. File auditing should therefore be configured to monitor only those directories or files that store cardholder information. In situations where cardholder information is stored within a database, or are managed exclusively by a custom application, database and/or application logs may be used to either supplement or supplant file related audit data, assuming:

- Appropriate file level access controls are in place.
- Membership of groups that provide unrestricted access to the underlying data used by the database or application are monitored, and
- The organisational risk assessment deems the risk acceptable.

Applications and databases, in general, write audit log data to:

- An operating system log facility (eg: Windows Application log) Snare operating system agents
- An append-only, rotating, text-format log Snare operating system agents
- A database auditing log file Snare for MSSQL server
- A local or remote syslog server Snare Central native collection

The PCI Standard also requires that "all actions taken by any individual with root or administrative privileges" are logged, on any system that processes cardholder information. Unfortunately, older operating systems are generally less capable of auditing at this level of granularity - particularly for file-related events. Most modern operating systems such as Windows and Unix can track user activities to a granular level. However care should be taken with the Audit policy settings to avoid unnecessary load on the systems.

All systems should be time-synchronised to a central time source for log timestamp consistency.

#### **Security Infrastructure**

Third party security servers and software may provide security-critical functionality in an organisation, and may generate their own log data.

Authentication Authorization and Accounting (AAA) services such as RADIUS/TACACS authentication servers, remote VPN access, network intrusion/prevention detection systems, Antivirus system logs and related components are a valuable source of user information and will



potentially highlight the actions of malicious software. They will generally APR produce log data relating to user access, failed logon attempts, privileged account usage, and other event information. Data log volumes from these systems can potentially be very significant, and it is recommended that the data be passed back to the Snare Central Server where it can be filtered and analysed for events of interest.

#### **Cloud Based Systems**

Where cloud based systems such as Microsoft 365( Office 365) environments are used to store cardholder data then the access logs from emails, SharePoint, OneDrive, and teams should be collected from the cloud platform to provide the additional forensics from those platforms. Snare Central has cloud adapters to facilitate the collection of these logs from those platforms along with many out of the box reports to help with regular review and compliance needs.

#### **Custom Applications**

Where a custom application provides access to cardholder information, log data from the underlying operating system, or web server in the case of http-based applications, may not provide adequate granularity to meet PCI requirements.

In situations where the application manages user authentication internally, and/or uses a mechanism to access data that would not be tracked or adequately segregated at the operating system level (eg: a database, or a related amalgamated storage mechanism), It is recommend that the application generates log information that ties authenticated users directly to the activity being performed.

# Audit Analysis and Reporting

The following recommendations highlight some specific reports on the Snare Central Server that may assist in meeting PCI/DSS requirements. It is strongly recommended that any recommendations below be considered in the light of an organization's risk assessment and security policy.

The settings are the initial recommended settings, and should be fine-tuned once the Snare Central Server has been in operation for some time.



#### **Administrative Actions and Account Management**

snare		histrator 023, 15:34 GMT+9:	30		Configure /	Control Sc	nodule Q	E   B	nh Attachme	it
Cyber Network Map	Rep	rts > Operating f	Systems > Administrative Activi	ty > Windows Snare V2				90	0 0	(
Dashboard	B	ccounts Added o	or Removed							
C Events Search	~	udit Log Cleared								
		udit Policy Chan								
Reports		iroup Changes								
Agent Management	>	iroup Member C	hanges							
Status		roups Added or	Removed							
System	>	lser Account Cha	anges							
Jystein										
	5	indows and ACI	F2 Administration							
		L4								
A Provide States and the second						-	ŧ	2		
snare	📥 🏯 Adminis				<b>\$</b> °				-	
SNARE	May 16, 202	15:38 GMT+9:30	tems > Administrative Activity	> Windows > Accounts Added Or Remo	Configure Access (		Queue	Regenerate	Attachment	
Cyber Network Map Dashboard	Report:	<ul> <li>15:38 GMT+9:30</li> <li>&gt; Operating Sys</li> </ul>	leys Windows accounts (in specified o		Configure Access t	Control Schedule	Queue	Regenerate	Attachment	
Cyber Network Map	May 16. 202 Report:	<ul> <li>15:38 GMT+9:30</li> <li>&gt; Operating Sys</li> <li>This objective displayed by the state of the system of the</li></ul>	lays Windows accounts (in specified o	<ul> <li>Windows &gt; Accounts Added Or Remo emails) that have been recently created at dat</li> </ul>	Configure Access t	Control Schedule	Queue	Regenerate		
Cyber Network Map Dashboard Events Search	Report:	<ul> <li>15:38 GMT+9:30</li> <li>&gt; Operating Sys</li> <li>This objective displayment</li> </ul>	leys Windows accounts (in specified o	<ul> <li>Windows &gt; Accounts Added Or Remo emails) that have been recently created at dat</li> </ul>	Configure Access t	Control Schedule	Queue	Regenerate		
Cyber Network Map Dashboard	Reports		lays Windows accounts (in specified of source of the second sec	<ul> <li>Windows &gt; Accounts Added Or Remo emails) But have been recently created or del adaption of the second second</li></ul>	oved Leter Vices 0	Control Schedule G SOURCETYPE N/A	Queue merated: 16 M DESTAG Adminis	Regenerate ay 2023 00:03:4 COUNT trator	() [Duration: 00:0] RETURN Information	
Cyber Network Map Dashboard Events Search Reports	May 16, 202 Report	1 5:38 GWT-9:30     Operating Sys     This objective displ     Total 0     Table     Table     Table     1 2 3 4     Table     15 12:00:01	lays Windows accounts (in specified of mail Pa Gram 5 (active) 9 10 matter la SYSTEM WOMPOO WOMPOO	Windows > Accounts Added or Remo anality) but have been recently created as de at as     EVENTD     EVENTD     EVENTD     478 (A pass account was delated)     478 (A pass account was delated)	user N/A N/A	Control Schedule G SOURCETYPE N/A N/A	Queue merated: 16 M DESTAG Adminis Adminis	Regenerate uy 2023 00:03:4 CCOUNT trator trator	ff [Duration: 00:0] RETURN Information	
Cyber Network Map Dashboard Events Search	May 16. 2022           Report           Parent Nac           eff East 2           2023 66           2023 65           2023 265		In the second to	Windows > Accounts Added Or Remo emains) But have been recently created and of the second	oved USER NAA NAA NAA MARed	Control Schedule G SOURCETYPE NA NA User	Queue merated: 16 M DESTAG Adminis Adminis MrWhite	Regenerate uy 2023 00-03-4 CCOUNT trator trator 2	11 [Duration: 00:0] RETURN Information Information Success Audit	
Cyber Network Map Dashboard Events Search Reports	Kay 16. 2022           Report:           Prese file:           COLOR:           DATE           2023-66           2023-66           2023-66           2023-66           2023-66           2023-66		In the second to	Windows > Accounts Added or Remote anality) but have been recertly created as de EVENTD     EVENTD     EVENTD     EVENTD     EVENTD     A726 (A lease account was deleted)     50 (User Account Pued deleted)     50 (User Account Pued deleted)     50 (User Account Pued deleted)	oved Access of A	G SOURCETYPE NA NA User NA	Queue enerated: 16 M DESTAC Adminis Adminis Adminis	Regenerate Iny 2023 00:03:4 COUNT COUNT Trator 2 trator trator	Ef (Duration: 00-0. RETURN Information Information Success Audit Information	
Cyber Network Map Dashboard Events Search Reports Agent Management	Kay 16.202           Report           Preve file           Preve file           202.96           202.96           202.26           202.26           202.26           202.26           202.26           202.26           202.26	1538 GMT+9:30     Operating Sys     This objective displ     Toke 0     Toke 0     Take     Take     1 2 3 4     Take     15 07:00.01     15 07:00.01     15 07:00.01     15 08:00.01	In the second to	Vindows > Accounts Added or Remo analys) But have been recently created and Account and added or Remo Account and added Account and added Ar25 (Auser account was deleted) Ar26 (Auser account was deleted) Action	oved USER NAA NAA NAA MARed	Control Schedule G SOURCETYPE NA NA User	Queue merated: 16 M DESTAG Adminis Adminis MrWhite	Regenerate ay 2023 00:03:4 COUINT trator trator 2 Crockent 2 Coulor 3 Coulo	11 [Duration: 00:0] RETURN Information Information Success Audit	
Cyber Network Map Dashboard Events Search Reports	Upy 16.202           Report           Plane Mar           Other Mar           202366           202366           202366           202366           202366           202366           202366           202366	<ul> <li>&gt; Operating Sys</li> <li>This objective displayed in the o</li></ul>	lay Windows accounts (in specified to see Fe Sear 5 (January 9 12) matta la SYSTEM WOMPOO CURLEY CURLEY CURLEY CURLEY CURLEY	Windows > Accounts Added Or Remain analis) that have been recently created as do EVENTO 4726 (Answar account was deleted) 4726 (Answar account was	Leaning Access of Access o	SourceType NA NA NA User NA NA User NA	DESTAC Adminis Adminis MrWhite Adminis Adminis	Regenerate Iny 2023 00:03:4 CCOUNT Tration Tration Tration Tration Trator 2 Trator 2 Trator 2 Trator 2 Trator 2 Trator 2 Trator 4	Ef [Duration: 00:0] RETURN Information Information Success Audit Information Success Audit	
Cyber Network Map Dashboard Events Search Reports Agent Management	Kay 16.202           Report           Preve file           Preve file           202.96           202.96           202.26           202.26           202.26           202.26           202.26           202.26           202.26	L 1538 GMT-9630     Sys     Operating Sys     This objective digits     This objective digi	lays Wintows accounts (in specified of the Search of the	Vindows > Accounts Added or Remo analys) But have been recently created and Account and added or Remo Account and added Account and added Ar25 (Auser account was deleted) Ar26 (Auser account was deleted) Action	oved USER N/A N/A MiRed N/A MiGrey	Control Schedule G SOURCETYPE N/A N/A User N/A User User	Queue merated: 16 M DESTAC Adminis MrWhite Adminis MrBlack	Regenerate Inv 2023 00:03-4 CCOUNT Trailor Tra	ff [Duration: 00:0] RETURN Information Information Success Audit Information Success Audit	
Cyber Network Map Dashboard Events Search Reports Agent Management Status	Up 16.202           Report           Image: Image State           Image S	<ul> <li>&gt; Operating System</li> <li>&gt; This adjective depl</li> <li>Take</li> <li>1 2 3 4</li> <li>Take</li> <li>15 270011</li> <li>15 270011</li> <li>15 44001</li> <li>15 44001</li> <li>15 420011</li> <li>15 420011</li> <li>15 420011</li> <li>15 420011</li> <li>15 100021</li> <li>15 100021</li> </ul>	Inst Windows accounts (in specified of the Sear SYSTEM WOAPPOO CURLEW CURLEW CURLEW CURLEW FALCON MYORG COMAU	Windows > Accounts Added Or Remain analist) that have been recently created at data EVENTO 4726 (A user account was deleted) 4726 (A user account w	LoonTigure Access of Access of NA NA MARed NA MaGrey NA MeBlack	Control Schedule SOURCETYPE NVA NVA User NVA User NVA User User	Queue Proerated: 16 M DESTAG Adminis Adminis MrWhite Adminis MrSlisch Adminis MrSlisch MrWhite MrWhite Adminis	Regenerate any 2023 00:03:4	RETURN Information Information Success Audit Information Success Audit	
Cyber Network Map Dashboard Events Search Reports Agent Management	Bay         Report           Prepert         Prepert           Pare-time         Pare-time           Pare-time	<ul> <li>b) Operating Sys</li> <li>b) Operating Sys</li> <li>c) Operating Sys</li></ul>	by Windows accounts (in specified on	<ul> <li>Viindows &gt; Accounts Added Or Remainship Stat have been recently created as definition of the second state of the</li></ul>	Loofigure Access of aved USER N/A N/A MiRed N/A MiRed N/A MiRed N/A MiRed MiRack MisTagenee	SourceType NA NA NA User NA User NA User User User	Queue merated: 16 M DESTAC Adminis Adminis Mubliac Adminis Mubliac Adminis Mubliac Adminis	Regenerate wy 2023 00:03:4 COUNT trator 2 trator 2 trator 2 trator trator	RETURN Information Information Information Success Audit Information Success Audit	
Cyber Network Map Dashbaard Events Search Reports Agent Management Status	Usy 14.000           Report           Image: Start	<ul> <li>Issa GMT-9:00</li> <li>Operating Sys</li> <li>Operating Sys</li> <li>This sheether sheether</li> <li>This sheether</li> <li>This sheether sheether</li> <li>This sheether sheether</li> <li>This sheether sheether</li> <li>This sheether</li> <li>This sheether sheether sheether</li> <li>This sheether</li> <li>This sheether sheether</li> <li>This sheether</li> <li< td=""><td>Inst Windows accounts (in specified of second second seco</td><td>&gt; Windows &gt; Accounts Added Or Reme analyt) that have been recently created as def match EVENTDD 4726 (Asses account was deleted) 4726 (Asses account was deleted)</td><td>Loofigure Access of aved USER NA NA MiRed MiRed NA MaGrey NA MaGrey NA</td><td>Control Schedule SOURCETYPE NA NA User NA User NA User NA User NA User NA</td><td>Queue exercated: 16 M DESTAG Adminis MrWhite Adminis MrWhite Adminis MrBlub Adminis</td><td>Regenerate ary 2023 00:03:4 COULNT Trator 2 COULNT Trator 2 trator 2 trator 2 trator 2 trator 3 trator 4 trator</td><td>RETURN Information Information Success Audit Information Success Audit Information Success Audit Information</td><td></td></li<></ul>	Inst Windows accounts (in specified of second second seco	> Windows > Accounts Added Or Reme analyt) that have been recently created as def match EVENTDD 4726 (Asses account was deleted) 4726 (Asses account was deleted)	Loofigure Access of aved USER NA NA MiRed MiRed NA MaGrey NA MaGrey NA	Control Schedule SOURCETYPE NA NA User NA User NA User NA User NA User NA	Queue exercated: 16 M DESTAG Adminis MrWhite Adminis MrWhite Adminis MrBlub Adminis	Regenerate ary 2023 00:03:4 COULNT Trator 2 COULNT Trator 2 trator 2 trator 2 trator 2 trator 3 trator 4 trator	RETURN Information Information Success Audit Information Success Audit Information Success Audit Information	
Cyber Network Map Dashboard Events Search Reports Agent Management Status	Bay 16, 202           Report           Participant           Control	<ul> <li>&gt; Operating Sys</li> <li>This objective dept</li> <li>This objective dept</li> <li>Take 1</li> <li>2</li> <li>3</li> <li>4</li> <li>7</li> <li>4</li> <li>5</li> <li>4</li> <li>4</li> <li>5</li> <li>2</li> <li>1</li> <li>3</li> <li>4</li> <li>1</li> <li>5</li> <li>2</li> <li>1</li> <li>3</li> <li>4</li> <li>1</li> <li>1</li> <li>4</li> <li>1</li> <li>5</li> <li>2</li> <li>1</li> <li>3</li> <li>4</li> <l< td=""><td>Inst Wanters accounts (in specified of re-search (in specified of re-search (in specified of womenoo womenoo cure, Ew cure, Ew Cu</td><td>Vindows &gt; Accounts Added Or Remain analis) flat have been recertly created at data EVENTO 4726 (Answar account was deleted) 4726 (Answar account wa</td><td>Lonfigure Access of aved USER NAA NAA Maffaed NAA Maffaed NAA Maffaed NAA Maffaed NAA Maffaed NAA Maffaed NAA</td><td>Control Schedule</td><td>Queue enerated: 16 M DESTA( Adminis Adminis MsBlack Adminis McNiba McNiba Adminis</td><td>Regenerate Regenerate Regenerate</td><td>RETURN Information Success Audit Information Success Audit Information Success Audit Information</td><td></td></l<></ul>	Inst Wanters accounts (in specified of re-search (in specified of re-search (in specified of womenoo womenoo cure, Ew cure, Ew Cu	Vindows > Accounts Added Or Remain analis) flat have been recertly created at data EVENTO 4726 (Answar account was deleted) 4726 (Answar account wa	Lonfigure Access of aved USER NAA NAA Maffaed NAA Maffaed NAA Maffaed NAA Maffaed NAA Maffaed NAA Maffaed NAA	Control Schedule	Queue enerated: 16 M DESTA( Adminis Adminis MsBlack Adminis McNiba McNiba Adminis	Regenerate	RETURN Information Success Audit Information Success Audit Information Success Audit Information	
Cyber Network Map Dashbaard Events Search Reports Agent Management Status	Key 14. 202     Report     Key 14. 202     Report     Report	<ul> <li>&gt; Operating Sys</li> <li>&gt; Operating Sys</li> <li>This sheetly dependence of the system</li> <li>1 2 3 4</li> <li>&gt; 3 40001</li> <li>&gt; 15 50001</li> <li>&gt; 15 50001</li> <li>&gt; 15 600002</li> <li>&gt; 16 60002</li> </ul>	Inst Windows accounts (in specified of the Small Pro-Small Pro-Small Pro- Small Pro-Small Pro- Small Pro- WOMPOO CURLEW CORLEW CURLEW CORLEW PACON MYORG COM,AU PRACON MYORG COM,AU ENU ENU ENU ENU ENU ENU ENU EN	> Windows > Accounts Added Or Reme analytic) that have been recently created and data EVENTED 4726 (Asser account was deleted) 4726 (Asser account was deleted) 47	USER NAA NAA NAA NAA NAA NAA NAA NAA NAA NA	SourceTryPE NA NA User NA User NA NA NA NA NA NA NA NA NA NA	DESTAC DESTAC Adminis Adminis MrVhite Adminis MrNhite Adminis Adminis Adminis Adminis	Regenerate iny 2023 00:03:4	FETURN Information Information Success Audit Success Audit Success Audit Success Audit Information Information Information	
Cyber Network Map Dashbaard Events Search Reports Agent Management Status	Bay 16, 202           Report           Bay 202           Parameter           Control           Data	<ul> <li>&gt; Operating Sys</li> <li>&gt; Operating Sys</li> <li>&gt; Operating Sys</li> <li>This objective depth</li> <li>1 2 3 4</li> <li>7 2 4</li></ul>	Inst Wanters accounts (in specified of re-search (in specified of re-search (in specified of (in specified of womenoo curlet w curlet w curl	Vindows > Accounts Added Or Remain analis) flat have been recertly created at data EVENTO 4726 (Asser account was deleted) 4726 (Asse	USER Azzes of version of NA Azzes of NA A NA Media NA Manager NA Manager NA Manager NA NA NA NA NA	Goursell Schedule GOURCETYPE NA NA NA User NA NA User NA NA NA NA NA NA	Queue enerated: 18 M DESTAC Adminis Adminis Adminis MrVMits Adminis MrVMits Adminis Adminis Adminis Adminis Adminis	Regenerate ury 2023 00:03:4 COUNT COUNT Tration 2 crotunt crator 2 rator 2 rator rat	FETURN Information Information Information Success Audt Information Success Audt Information Information Information Information	
Cyber Network Map Dashboard Events Search Reports Agent Management Status	Key 14. 202     Report     Key 14. 202     Report     Report	<ul> <li>&gt; Operating Sys</li> <li>&gt; Operating Sys</li> <li>This sheetly dupt</li> <li>This sheetly dupt</li></ul>	by Wheles seconds (in specified of second second (in specified of second second se	> Windows > Accounts Added Or Reme annular) that have been recently created at del match EXECUTED 4726 (Assess account was deleted) 500 (User Account was deleted) 5126 (Asses account	USER USER NA NA NA NA NA NA NA NA NA NA NA NA NA	Sounce Type Sounce Type NA NA NA NA NA Var NA Var Var User User User Var NA NA NA NA NA NA	Queue DESTAC Adminis Adminis MrWhite Adminis MrWhite Adminis Adminis Adminis Adminis Adminis Adminis	Regenerate any 2023 00-03-4	FI [Duristion: 00:07 RETURN Information Information Success Audit Information Success Audit Information Information Information Information Information	
Cyber Network Map Dashboard Events Search Reports Agent Management Status	Usy 14.202           Report           Image: Image of the state of the st	<ul> <li>&gt; Operating Sys</li> <li>&gt; Operating Sys</li> <li>This objective display</li> <li>This objective display</li> <li>This objective display</li> <li>1 2 3 4</li> <li>7 200</li> <li>1 5 120001</li> <li>1 5 120001</li> <li>1 5 020001</li> <li>1 5 00001</li> <li>1 5 00000</li> <li>1 5 140001</li> <li>1 7 10000</li> <li>1 5 1700000</li> <li>1 5 1700000</li> <li>1 5 1400001</li> <li>1 1 100000</li> </ul>	Inst Wanters accounts (in specified of re-search (in specified of re-search (in specified of womenoo womenoo culture) womenoo culture) cul		USER Access to vere USER NA Access to vere NA Acc	Gourdel Schedule Gourdeeryee NA NA NA NA NA User NA NA NA NA NA NA NA NA NA NA NA NA NA	Queue DESTAC Adminis Admini	Regenerate ary 2023 00:03-4 COUNT Trator Trator 2 Count Trator 2 Trator 2 Trator 2 Trator 1 T	RETURN Information Information Information Success Audit Information Success Audit Information Information Information Information Information	
Cyber Network Map Dashboard Events Search Reports Agent Management Status	Key 14. 202     Report     Key 14. 202     Report     Report	<ul> <li>Operating Sys</li> <li>Operating Sys</li> <li>Operating Sys</li> <li>This adjective depth</li> </ul>	bys Windows second (in specified of the second se	> Windows > Accounts Added Or Reme analytic) But have been recently created and data EVENTD 4726 (Assess account was deleted) 500 (User Account was deleted) 4726 (Asses a	USER USER NA NA NA NA NA NA NA NA NA NA NA NA NA	Outreat Schedule	DESTAC DESTAC Adminis Mr/Mille Adminis Mr/Mille Adminis Adminis Adminis Adminis Adminis Adminis Adminis Adminis Adminis	Regerierate ay 2023 00:03:4	FETURN Information Soccess Audit Information Soccess Audit Information Soccess Audit Information Information Information Information Information Information	
Cyber Network Map Dashboard Events Search Reports Agent Management Status	Usy 16.202           Report           Image: State of the st	<ul> <li>Depending Systems</li> <li>Operating Systems</li> <li>This subjective display</li> <li>The subjective display<td>Inst Wanters accounts (in specified of re-search (in specified of s) (in account (in specified of womenoo currents) womenoo currents womenoo currents womenoo currents reaccon arronge com au reaccon arronge com</td><td>Vinidous &gt; Accounts Added Or Remain analisi) flat have laser recently created at data EVENTD EVENTD EVENTD EVENTD EVENTD T25 (A user account was deleted) A726 (A user acco</td><td>Access of Access of Access</td><td>SourceTryE SOURCETryE NA NA Uter NA Uter NA NA NA NA NA NA NA NA NA NA NA NA NA</td><td>Queue reverated: 16 M DESTAG Adminis Adminis McNita Adminis</td><td>Regerierate ary 2023 00:03-4 COUNT trator trator 2 COUNT trator t</td><td>RETURN Information Information Success Audit Information Success Audit Information Information Information Information Information Information Information</td><td></td></li></ul>	Inst Wanters accounts (in specified of re-search (in specified of s) (in account (in specified of womenoo currents) womenoo currents womenoo currents womenoo currents reaccon arronge com au reaccon arronge com	Vinidous > Accounts Added Or Remain analisi) flat have laser recently created at data EVENTD EVENTD EVENTD EVENTD EVENTD T25 (A user account was deleted) A726 (A user acco	Access of Access	SourceTryE SOURCETryE NA NA Uter NA Uter NA NA NA NA NA NA NA NA NA NA NA NA NA	Queue reverated: 16 M DESTAG Adminis Adminis McNita Adminis	Regerierate ary 2023 00:03-4 COUNT trator trator 2 COUNT trator t	RETURN Information Information Success Audit Information Success Audit Information Information Information Information Information Information Information	
Cyber Network Map Dashboard Events Search Reports Agent Management Status	Exp(16.202     Fepertin     Exp(16.202     Fepertin	Comparing Systems	by Wheles second (in specified of	> Windows > Accounts Added Or Reme annular) But have been recently created at def attract P278 (Assess account reas delated) 4728 (Asses account reas delated) 620 (Daw Account Assess delated) 620 (Daw Account Assess delated) 620 (Daw Account Assess 620 (Daw Account Asses 620 (Daw Account Asse	USER NAA NAA NAA NAA NAA NAA NAA NAA NAA NA	SourceTryPe Co SourceTryPe NA NA User NA Dar NA NA NA NA NA NA NA NA NA NA NA NA	DESTAA Adminis Adminis Mobile Adminis Adminis Adminis Adminis Adminis Adminis Adminis Adminis Adminis Adminis Adminis Adminis Adminis Adminis Adminis Adminis Adminis	Regenerate auy 2023 00:03:4 COUNT Tration 2 Trator 2 Trator 2 Trator 2 Trator 1 Trat	FE TURN RETURN Information Information Information Information Information Information Information Information Information Information Information Information Information Information Information Information Information	
Cyber Network Map Dashboard Events Search Reports Agent Management Status	Up         16.202           Report         Image: Control of the control o	<ul> <li>Deprating Systems</li> <li>Operating Systems</li> <li>This shipeshow ships</li> <li>The shipeshow ships</li> <li>The ships of the ships of the ships</li> <li>The ships of the ship</li></ul>	Inst Wanters accounts (in specified of re-search (in specified of s) (in account) (in specified of womenoo curlet w curlet w cockaroo (in conta) cockaroo cockaro cockaroo cockaroo cockaroo cockaroo cocka	> Windows > Accounts Added Or Remo enable) But have learn reportly created a de multi- EVENTID 4728 (I) learn account was deleted) 4728 (I) learn account was deleted) 4729 (I) learn account was deleted) 4720	Access of Access	SourceTryse SOURCETryse NA NA Uter NA NA Uter NA NA NA NA NA NA NA NA NA NA NA NA NA	DESTAC DESTAC	Regenerate iny 2023 00:03:4 COUNT Co	FETURN Information Information Success Audit Information Success Audit Information Information Information Information Information Information Information Information Information Information Information	
Cyber Network Map Dashboard Events Search Reports Agent Management Status	Exp(4.202     Former Mar     Fo	Itead GMT-H030           > Operating Sys           This indextwo shape           Thextwo shape <td>by Wheles second (in specified 0</td> <td>&gt; Windows &gt; Accounts Added Or Rems analytic) But have been recently created at def attract PCPU (Name Account was deleted) 4728 (Name Account was deleted) 4729 (Name Account was deleted) 4720 (Name Account was deleted)</td> <td>USER NAA NAA NAA NAA NAA NAA NAA NAA NAA NA</td> <td>SourceTryPe Co SourceTryPe Co NA NA User NA User NA NA NA NA NA NA NA NA NA NA NA NA NA</td> <td>Queue DESTA Adminis</td> <td>Regenerate any 2023 00:02:4</td> <td>RETURN RETURN Information</td> <td></td>	by Wheles second (in specified 0	> Windows > Accounts Added Or Rems analytic) But have been recently created at def attract PCPU (Name Account was deleted) 4728 (Name Account was deleted) 4729 (Name Account was deleted) 4720 (Name Account was deleted)	USER NAA NAA NAA NAA NAA NAA NAA NAA NAA NA	SourceTryPe Co SourceTryPe Co NA NA User NA User NA NA NA NA NA NA NA NA NA NA NA NA NA	Queue DESTA Adminis	Regenerate any 2023 00:02:4	RETURN RETURN Information	
Dashboard Events Search Reports Agent Management Status	Up         16.202           Report         0           Image: Image and the i	1538 GMT-930           > Operating Sys           Take adjective digit           Take adjective digit      <	Inst Wanters accounts (in specified of re-search (in specified of s) (in the second of (int the s	> Windows > Accounts Added Or Remo enable) But have been reportly credited at de multi- mutable EVENTID 4728 (I) have account was deleted) 4728 (I) have account was deleted) 4729 (I) have account was deleted) 4728 (I) have account was deleted) 4729 (I) have account was deleted) 4729 (I) have account was deleted) 4729 (I) have account was deleted) 472 (I) have account was deleted) 472 (I) have account was deleted) 472 (I) have account was deleted) 473 (I) have account was deleted) 474 (I) have account was deleted) 475 (I) I/ have account was deleted) 476 (I) I/ have account was deleted) 477 (I) I/ have account was deleted) 478 (I) I/ have account was deleted) 479 (I) I/ have account was deleted) 470 (I	Access of Access	Source Tryse Source Tryse NA NA Uter NA Uter NA NA NA NA NA NA NA NA NA NA NA NA NA	Queste DESTAL Adminis Adminis MrWhite Adminis	Regenerate any 2022 00:02:4 COUNT Columnt Count	AT [Durother: 00:02 RETURN Information	

10.2 Audit logs are implemented to support the detection of anomalies and suspicious activity, and the forensic analysis of events

10.2.1 Audit logs are enabled and active for all system components and cardholder data.

10.2.1.1 Audit logs capture all individual user access to cardholder data

10.2.1.2 Audit logs capture all actions taken by any individual with administrative access, including any interactive use of application or system accounts

10.2.1.3 Audit logs capture all access to audit logs

10.2.1.4 Audit logs capture all invalid logical access attempts

10.2.1.5 Audit logs capture all changes to identification and authentication credentials including, but not limited to

- □ Creation of new accounts.
- □ Elevation of privileges.



□ All changes, additions, or deletions to accounts with administrative access.

#### 10.2.1.6 Audit logs capture the following:

- □ All initialization of new audit logs, and
- □ All starting, stopping, or pausing of the existing audit logs.

10.2.1.7 Audit logs capture all creation and deletion of systemlevel objects

10.2.2 Audit logs record the following details for each auditable event:

- □ User identification.
- □ Type of event.
- Date and time.
- □ Success and failure indication.
- Origination of event.
- □ Identity or name of affected data, system component, resource, or service (for example, name and protocol).

In most organisations, group permissions and/or logical system access controls, are used to control access to sensitive data. These are also known as role based access controls or RBAC. The Snare Central Server can be used to scan for modifications to groups that control access to cardholder information, or additions and alterations to system accounts on servers that host cardholder information. It is recommended that reports related to the groups in question, be delegated to and reviewed by, the organisational users who are responsible for controlling the data.

- Monitor account-related activity for Windows, Unix, and Mainframe systems. The objectives should be checked daily as per PCI/DSS recommendations, to ensure that only authorized staff have been creating, deleting or otherwise changing accounts, and this activity can be linked back to approved activity.
- Monitor reports related to group modifications for those groups that are used to control access to cardholder data, or are used to gain access to administrator level functionality.
- Monitor group snapshot reports for unauthorised additions to sensitive groups that are used to control access to cardholder data, or are used to gain access to administrator level functionality.

Some operating systems generate events when the logging subsystem is modified and/or restarted. It is very important that such logs be sent off-server as soon as they are generated, to a central log collection server, using an application with functionality similar to the Snare agents.

• Examine objectives relating to the audit/eventlog infrastructure



#### Login Activity

snare	📥 💄 Administra	tor		<b>\$</b> \$		<b>≢</b> Ø	*
Share	May 16, 2023, 15				Control Schedule	Queue Refresh A	ttachment
Cyber Network Map							-
cyber network map	Reports >	Operating Sys	stems > Login Activity			0 0 B	
	202000		13				
Dashboard							
	ACF2						
Events Search	AIX B						
	0.000						
	Irix						
Reports	(TT) 1991						
	En Linux						
Agent Management	>						
.0	En Linux	Spare v2					
Status	> MacO	-					
	MacO	2					
System	MacO	5 Snare v2					
	RACF						
	Solari	5					
	Tru64						
	Windo	ws.					
		ws Snare v2					
snare	Administra	tor 1:39 GMT+9:30		Configure Access Co	ntrol Schedule	Cueue Regenerate A	La hument
snare	Administra	tor 139 GMT+9:30		Configure Access Co	ntrol Schedule	효 않. Queue Regenerate A	* sttachment
SINAIT P	Administra	i:39 GMT+9:30			ntrol Schedule	글 Cueve Regenerate A	<b>t</b> achment
	Administra	i:39 GMT+9:30	; stems > Login Activity > Winnie		ntrol Schedule	고 Cueue Regenerate A	stachment .
Cyber Network Map	Administra	i:39 GMT+9:30			ntrol Schedule	Tegenerate	* ttachment
	Administra May 16/2023. 11 Reports >	639 GMT+9:30 Operating Sys	stems > Login Activity > Wini				ttachment
Cyber Network Map	Administra May 16/2023. 11 Reports >	639 GMT+9:30 Operating Sys				Queue Regenerate A	station: 00:03:5
Cyber Network Map	Administra May 16/2023. 11 Reports >	639 GMT+9:30 Operating Sys	stems > Login Activity > Wini				stachment
Cyber Network Map Dashboard	Administra May 16: 2225. 1 Reports > Quantum Control (Control (Contro) (Control (Con	0perating Sys operating Sys way Windows S	stems > Login Activity > Win incurty logs for events of interest means Case	dows > Login Failures			stachment
Cyber Network Map Dashboard Events Search	■ Administra May 18,202,11 Reports >	Coperating Systems Windows S	stems > Login Activity > Wini locutly logs for events of interest meaning meaning bags determ 2 8 9 10 notice	dows > Login failures	Gene	ratod: 16 May 2023 00:04:27 [De	stachment
Cyber Network Map Dashboard	Administra May 16, 2023, 1 Reports > Free for c for 4 for Date	Operating Sys	stems > Login Activity > Winn locurity logs for events of interest means in the second	dows > Lopin Failures Lin Sue Balaz EXENTD	Gene	rated: 16 May 2023 00:04:27 [De FARREASON	
Cyber Network Map Dashboard Events Search	■ Administra May 18, 2023 11 3 Reports >	Coperating Sys every Windows S 1 2 3 4 TIME 12 00 01	stems > Login Activity > Win locarly logs for events of interest memory reserve Date article 2 (8 9 18 00d2 SYSTEM EAGLE	dows > Login failures in time texts EVENID 27 Experime An unspected error secured during legan)	Gene	rated: 16 May 2021 00-04-27 [De FALREASON An error occurred during logg	n
Cyber Network Map Dashboard Events Search Reports		Coperating Systems Coperating Systems Copera	stems > Login Activity > Win lecarly logs for events of Interest means of the second second system 1 and 1 a	dows > Login Failures  in the  VeryTio  VeryTio Very	Gene DESTUSER MrsBue -	FALREASON An error occurred during logg	n assword.
Cyber Network Map Dashboard Events Search		Coperating Sys every Windows S 1 2 3 4 TIME 12 00 01	stems > Login Activity > Win locarly logs for events of laterast research logs system EAGLE TORHOUT SHORE COM SWITT	dows > Login failures in two Interes I	Gene DESTUSER MisBite - david mahr	FALREASON An error socured during logg Unknown username or bad p Unknown username or bad p	n assword, nassword
Cyber Network Map Dashboard Events Search Reports	■ Administra May 16: 2023. 1 Reports > Percente OCT 20234515 20234515	Coperating Systems Coperating Systems Copera	stems > Login Activity > Wini lecarly logs for events of interest events / logs for events of interest events / log log log SYSTEM EAGLE SYSTEM EAGLE SYSTEM EAGLE SWIFT SWIFT	dows > Login Failures  I to 84e  Extex  EVENTO  S77 (Logar Failure -An unexpected error socured during logan)  455 (Apar Failure -An unexpected error socured during logan)  559 (Logar Failure -An unexpected error coccured during logan)  559 (Logar Failure -An unexpected error coccured during logan)	Gene DESTUSER MrsBue -	FALREASON An entor occurred during logo Unknown usiensame or bad p Unknown usiensame or bad p	n assword aasword n
Cyber Network Map Dashboard Events Search Reports Agent Management	■ Administra May 10, 2023, 11 Reports >	Coperating Systems Sys	stems > Login Activity > Win locarly logs for events of laterast research logs system EAGLE TORHOUT SHORE COM SWITT		Gene DESTUSER MisBite - david mahr	FALREASON An error occurred during logo Unknown user aran or bad p Unknown user aran or bad p An error occurred during logo Unknown user area or bad p Unknown user area or bad p Unknown user area or bad p	n assword nasword n
Cyber Network Map Dashboard Events Search Reports	■ Administra koy 16: 2023. 1 Reports > Pere tai Pere tai 202345-15 202345-15 202345-15	Coperating Systems Sys	stems > Login Activity > Win lacety logs for events of lateral revenue liket SYSTEM EAGLE TOPHOLY INFO SCOM SWWT SWWT	dows > Login Failures  I in Sva  Extra  EVENTO  S27 (Logan Failure An unexpected arts excurred during logan) 425 (on account failed in log on  S29 (Logan Failure An unexpected mean rans on bad passwell) 425 (on account failed in log on) 425 (on account failed in log on) 425 (on account failed in log on)	Gene DESTUSER MrsBke - devid mahr MeBlack -	FALREASON An error occurred during logg Unknown user name or bad p Unknown user name or bad p	n assword nasword n
Cyber Network Map Dashboard Events Search Reports Agent Management	■ Administra May 10, 2023, 11 Reports >	Coperating Systems Sys	stems > Login Activity > Wink licently logs for events of interest events of interest events for events of interest events for events for an event for events events for events for events even		Gene DESTUSER MisBite - david mahr	FALREASON FALREASON An error document during loga Unitianse uname to bad Unitianse uname marke to bad Unitianse una erran er bad	n assword, assword n assword assword,
Cyber Network Map Dashboard Events Search Reports Agent Management Status	■ Administra May 16, 222, 11 Reports >	Coperating Sys Coperating Sys any Windows S 1 2 3 4 TIME 12 00 01 1600 02 06 00 01 07 00 01 1100 02 09 00 01	stems > Login Activity > Wini lecarly Jogs for events of interest revenue load array of a state of a state system System Swert Swert Swert CORLEW CORLEW CORLEW	dows > Login Failures  I in Sva  Extra  EVENTO  S27 (Logan Failure An unexpected arts excurred during logan) 425 (on account failed in log on  S29 (Logan Failure An unexpected mean rans on bad passwell) 425 (on account failed in log on) 425 (on account failed in log on) 425 (on account failed in log on)	Gene DESTUSER MrsBke - devid mahr MeBlack -	FALREASON An error occurred during logg Unknown user name or bad p Unknown user name or bad p	n assword, assword n assword assword,
Cyber Network Map Dashboard Events Search Reports Agent Management	■ Administra koy 16: 2023. 1 Percent 20234515       Image: Control of the second	Coperating Systems Coperating Systems Copera	stems > Login Activity > Wink leactly logs for events of Interest executly logs for events of Interest executly logs for events bas executly log for events bas executly log for events bas executly log for events swift T sw	down > Login Failures I with the EXERCISE E	Gene DESTUSER Meißbe - devid mohr Maßback - - MesTangerine -	FALREASON FALREASON An error document during loga Unitianse uname to bad Unitianse uname marke to bad Unitianse una erran er bad	n assword, assword n assword assword,
Cyber Network Map Dashboard Events Search Reports Agent Management Status	■ Administra May 16, 2023, 11 Reports >	Coperating Systems Coperating Systems Copera	stems > Login Activity > Wini lecarly Jogs for events of interest research (Jogs for events of interest events (Jogs for events of interest events (Jogs for events of events SWFT SWFT SWFT SWFT CUREEW CUREEW CUREEW FALCON MYORG COM AU MAGPIE		Gene DESTUSER MrsBke - david mahr MrsBlack - MrsTangerise - MrsTangerise - MrsTangerise	FALREASON FALREASON An error document during loga Unitianse uname to bad Unitianse uname marke to bad Unitianse una erran er bad	n assword assword n assword assword assword
Cyber Network Map Dashboard Events Search Reports Agent Management Status	■ Administration to the second se	Operating Sy: Provide State S	stems > Login Activity > Wink leactly logs for events of Interest executly logs for events executly logs for ev	down > Login Failures I with the second sec	Gene DESTUSER MitBlue - david mater MaBlack  MasTangerine  Martine MasTangerine  Martine MasTangerine	FAREAON FAREAON An error counter during lago United and the second during	n assword assword n assword assword assword
Cyber Network Map Dashboard Events Search Reports Agent Management Status	■ Administra May 16, 222, 11 Reports >	Coperating Systems S Coperating S Copera	stems > Login Activity > Wini locarly logis for events of Interest events of Interest events of Interest System Swort		Gene DESTUSER MitBlue - david mater MaBlack  MasTangerine  Martine MasTangerine  Martine MasTangerine	FAREAON FAREAON An error counter during lago United and the second during	n assword assword assword assword assword
Cyber Network Map Dashboard Events Search Reports Agent Management Status	■ Addiministra buy 16: 2023. 1 Reports >	Contracting Systems Contracting Systems Contracti	stems > Login Activity > Wine eachty logis for events of Interest executy logis for events of Interest executy 2 (8 5 18) central execute 2 (8 5 18) execute 2 (8 5		DESTUBER Mittlew - - dear mark Mittlew - - Mittlew - - Mittlew - - Mittlew - - Mittlew - - - - Mittlew - - - - - - - - - - - - - - - - - - -	PADJEASON PADJEASON United and a second dating loga United and United and Second dating loga United and United and Second dating loga United and United and Second dating loga	n assword asstvord m assword assword n assword
Cyber Network Map Dashboard Events Search Reports Agent Management Status	■ Administers May 16, 2023 11 Reports >	Coperating Sys Coperating Sys ary Windows S TIME 1 2 3 4 TIME 1 2 0 01 1 600 02 0 500 01 0 700 01 1 100 05 0 90 001 1 300 01 0 600 02 0 600 02 0 600 01 1 500 01 1 300 01 0 600 02 0 600 01 1 500 01 1 400 01 1 700 02	stems > Login Activity > Wini locarly logis for events of Interest events of Interest events of Interest System Swort	down > Login Failures     down > Login + Lo	Gene DESTUSER MoDue - deal muh MoDas - MoTangerine - MoTangerine - MoTangerine - - MoTangerine - - - MoTangerine - - - - - - - - - - - - - - - - - - -	FALPEASON A error occurred Adres tops Uninen uner anne to bad Uninen uner anne to bad	n assword assword assword assword n assword
Cyber Network Map Dashbaard Events Search Reports Agent Management Status	■ Addiministra buy 16: 2023. 1 Reports >	Contracting Systems Contracting Systems Contracti	stems > Login Activity > Wine eachty logis for events of Interest executy logis for events of Interest executy 2 (8 5 18) central execute 2 (8 5 18) execute 2 (8 5	Login Failures     Login Failures     Login Failures     Login     Logi	DESTUBER Mittlew - - dear mark Mittlew - - Mittlew - - Mittlew - - Mittlew - - Mittlew - - - - Mittlew - - - - - - - - - - - - - - - - - - -	PADJEASON PADJEASON United and a second dating loga United and United and Second dating loga United and United and Second dating loga United and United and Second dating loga	n assword assword assword assword assword assword assword assword a
Cyber Network Map Dashboard Events Search Reports Agent Management Status	■ Administra May 16, 2028, 1 Reports >	Coperating Systems S Coperating S	stems > Login Activity > Wini locarly high for events of Interest events of the sector of the sector of the sector events of the sector of the sector of the sector events of the sector of the sector of the sector of the sector events of the sector	down > Login Failures     down > Login	Correl DESTURER MODA - - - - - MoTagene MoTagene MoTagene MoTagene MoTagene MoTagene MoTagene	FALPEASON A error account d Aring logo Uninou un uner anne to bad Uninou uner anne to bad A error accounted during logo A count tobel out	n assword assword assword assword n assword assword n assword
Cyber Network Map Dashboard Events Search Reports Agent Management Status	■ Addminister buy (6, 2023, 5) (0, 2023,	Control 20	Stems > Login Activity > Wint lacethy hops for events of interest events of interest events of a set of the SWFT SWFT SWFT SWFT SWFT SWFT ALCOR MYORG COM AU MAGNE SWFT SWFT CORELW CORELW CORELW CORELW CORELW CORELW CORELW CORELW CORELW CORELW CORELW CORELW CORELW CORELW CORELW		Centre DESTUDER MinDuta - - - MinDangeline MinDangeline MinDangeline MinDan MinDan MinDan MinDan MinDan MinDan	FALPEASON A nerve occurred Adving logo Urbinom uner anne or balg Dollhern uner anne or balg	n assword assword assword assword n assword assword n assword
Cyber Network Map Dashboard Events Search Reports Agent Management Status	■ Administra May 16, 2028, 1	Coperating Systems S Coperating S	stems > Login Activity > Wink locarly high for events of Interest locarly interest in the Interest SWIT SWIT SWIT SWIT URLEW CORALW CORALEL COCATEL COCA		Correl DESTUREF MODA - - - - - - - - - - - - - - - - - - -	FALPEASON A nerro scoursed Adres tops Uninen uncernance to Adres Uninen uncernance to Adres	n assword. a assword assword assword assword assword assword.
Cyber Network Map Dashboard Events Search Reports Agent Management Status	■ Administrative Control of the second s	Operating Sys ary Windows S 1 2 2 3 1 1 2 2 3 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	stems > Login Activity > Wint lacenty hops for events of interest events of interest events of interest events of interest events of interest SWFT SWFT SWFT SWFT SWFT SWFT CORE,EW	down > Login Failures     via Sam	Gener DESTUDER MitDus - - - - MitDus	FALREASON     An error occurred Adving loga     Unitions user anne on bag     An error occurred Adving loga     Unitions user anne on bag     An error occurred Adving loga     Unitions user anne on bag     Dollenen user anne on bag     Locked OU     Menor user anne on bag     An error occurred Adving loga     Unitions user anne on bag     An error occurred Adving loga     Unitions user anne on bag     An error occurred Adving loga     Unitions     Locked OU     Manor user anne on bag     An error occurred Adving loga     Locked OU     Manor user anne on bag     Locked OU     An error occurred Adving loga     Locked OU     Manor user anne on bag     Locked OU	n assword a assword as as as as as as as as as a a a a a a
Cyber Network Map Dashboard Events Search Reports Agent Management Status	■ Administra May 16: 2228-11 Reports > Per ter 20234-15 20234	Coperating Syn Coperating Syn Pry Windows S THE 1 2 3 1 THE 1 2 3 1 1 4 2 3 1 1 4 2 3 1 1 5 00 02 0 5 00 01 1 100 02 0 5 00 01 1 100 02 0 6 00 01 1 100 02 0 6 00 01 1 5 00 01 1 5 00 01 1 5 00 02 0 6 00 02 0 7 00 01 0 7 00 02 0 7 00 00 02 0	stems > Login Activity > Wink locarly high for events of interest		Correl DESTUREF MODA - - - - - - - - - - - - - - - - - - -	FALPEASON A nerro scoursed Adres tops Uninen uncernance to Adres Uninen uncernance to Adres	n assword a assword as as as as as as as as as a a a a a a
Cyber Network Map Dashboard Events Search Reports Agent Management Status	■ Administration (1997) Reports > Repor	Coperating Synthesis Coperating Synthesis	stems > Login Activity > Wint lacentry logs for events of interest	down > Login Failures     via Sea	Gener DESTURER MinButa - - - - MinTangerina - - MinTangerina - - MinTangerina - - MinTangerina - - MinTangerina - - MinBusk decla mint - - - - - - - - - - - - - - - - - - -	FALPEASON A nerro accounted Adring logo Utilinom una remaine to bad p Utilinom una remaine to bad p An entro accounted Adring logo Utilinom una remaine to bad p An entro accounted Adring logo Utilinom una remaine to bad p Linken of America accounted Adring logo Utilinom una remaine to bad Utilinom una remaine to bad	n session d. session d
Cyber Network Map Dashboard Dashboard Reports Reports Status Status	■ Administra May 16: 2228-11 Reports > Per ter 20234-15 20234	Coperating Syn Coperating Syn Pry Windows S THE 1 2 3 1 THE 1 2 3 1 1 4 2 3 1 1 4 2 3 1 1 5 00 02 0 5 00 01 1 100 02 0 5 00 01 1 100 02 0 6 00 01 1 100 02 0 6 00 01 1 5 00 01 1 5 00 01 1 5 00 02 0 6 00 02 0 7 00 01 0 7 00 02 0 7 00 00 02 0	stems > Login Activity > Wink locarly high for events of interest		Gener DESTUDER MitDus - - - - MitDus	FALREASON     An error occurred Adving loga     Unitions user anne on bag     An error occurred Adving loga     Unitions user anne on bag     An error occurred Adving loga     Unitions user anne on bag     Dollenen user anne on bag     Locked OU     Menor user anne on bag     An error occurred Adving loga     Unitions user anne on bag     An error occurred Adving loga     Unitions user anne on bag     An error occurred Adving loga     Unitions     Locked OU     Manor user anne on bag     An error occurred Adving loga     Locked OU     Manor user anne on bag     Locked OU     An error occurred Adving loga     Locked OU     Manor occurred Adving loga     Locked OU	n session d. session d

Unusual login activity can be a potential sign that an internal user is attempting to escalate their privileges, or an external attacker is trying to gain access to information that they are not authorised to view. It is recommended that failed login activity, and successful login activity outside of normal work hours, be monitored for abnormalities on systems that control access to, or host cardholder information.

- Scan for failed logins to your systems, network devices, and web-based application servers:
  - □ For example, 10 failed logins within a 1 hour period.
  - Over a threshold value
  - D To Locked Accounts (in the case of Windows accounts).
- Scan for successful or failed logins after normal working hours.
- Scan for logins to high privilege accounts (eg: Domain administrator, root or other power users), or attempts to increase privilege for administrative activity (eg: "Run as Administrator", sudo, /bin/su)



#### File or Resource Access

snare	Administrator May 16, 2023, 16:47	GMT+9:30		Configure Access Control	and the second second second second	enerate Attachment	2
Cyber Network Map	Reports > Ope	erating Systems >	File And Resource Access > Windo	ws > Sensitive Files			
Dashboard	Monito on Re	r access to Re and accesses	directories that are considered to be sens	live. Note that to use this objective, the Snare agents must be config	pared to report Generated: 1	16 May 2023 15:43:02 [Dura 00:01	
Events Search	Patart Nap	Talutar Datala	Pie Graph Pattern Map	8			_
	<= first < prev 1	2 3 4 5 5	Z 8 9 10 next> last>>				
Reports	DATE	TIME	SYSTEM	EVENTID	FILENAME	RETURN	
Reports	2023-05-16	12:00:01	WOMPOO	560 (Object Open)		Success Audit	
	2023-05-16	02:00:01	SWIFT	4656 (A handle to an object was requested)	2	Success Audit	
Agent Management	2023-05-16	12:00:01	SWIFT	4656 (A handle to an object was requested)		Success Audit	
-Bene management	2023-05-16	13:00:01	MAGPIE	560 (Object Open)		Success Audit	
	2023-05-16	07:00:01	CURRAWONG	4656 (A handle to an object was requested)		Success Audit	
Status	2023-05-16	10:00:01	GULL	4656 (A handle to an object was requested)		Success Audit	
	2023-05-16	12.00.01	LYREBIRD	4656 (A handle to an object was requested)		Success Audit	
	2023-05-15	09:00:01	GALAH	4656 (A handle to an object was requested)		Success Audit	
System	2023-05-15	17:00:02	CURLEW	4656 (A handle to an object was requested)		Success Audit	
	2023-05-15	11:00:02	FALCON	560 (Object Open)	-	Success Audit	
	2023-05-15	16:00:02	FALCON	560 (Object Open)	(4)	Success Audit	
	2023-05-15	02:00:02	LORIKEET MYORG COM	560 (Object Open)		Success Audit	
	2023-05-15	14:00:01	LORIKEET.MYORG.COM	560 (Object Open)	-	Success Audit	
	2023-05-15	04:00:01	WOMPOO	4656 (A handle to an object was requested)		Success Audit	
	2023-05-15	14:00:01	WOMPOO	560 (Object Open)		Success Audit	
	2023-05-15	10:00:01	LYREBIRD	560 (Object Open)		Success Audit	
	2023-05-15	12:00:01	KITE	4656 (A handle to an object was requested)	-	Success Audit	
	2023-05-15	00:00:02	TOPKNOT MYORG COM	4656 (A handle to an object was requested)		Success Audit	
	2023-05-15	05:00:01	EAGLE	560 (Object Open)		Success Audit	
	2023-05-15	03:00:01	COCKATOO	560 (Object Open)		Success Audit	
	2023-05-15	23:00:02	SWIFT	560 (Object Open)		Success Audit	
	2023-05-15	00.00.02	FROGMOUTH	4656 (A handle to an object was requested)		Success Audit	
	2023-05-15	10:00:01	FROGMOUTH	560 (Object Open)		Success Audit	
	2023-05-14	11:00:01	FROGMOUTH	560 (Object Open)		Success Audit	

For systems that store cardholder information, file auditing may be an important addition to the organisational monitoring plan.

Enabling file auditing on most operating systems, can result in very large volumes of data, and can adversely affect CPU resources to a degree, so care should be taken to restrict the paths to monitor to only those of critical value.

The term "system level object" in PCI DSS, is deliberately vague, and is designed to be flexible enough to include a wide range of different devices and systems. It can be generally defined as anything that is required for a system, device, or application to operate; including but not limited to executables, DLLs and configuration files.

On Unix systems, for example, monitoring the binary (/usr/sbin, /usr/bin), library (/usr/lib) and configuration (/etc, /boot) directories may be appropriate. Windows systems may wish to monitor the \Windows directory. Logging for web-based applications could focus on any backend components of the application that are not normally visible or accessible by regular users such as user administration or metadata update functionality.

**Network Devices** 



I	Administrator May 17, 2023, 17:06 GMT+9:30							NG	Lecess Control	Schedule Que		Luchment 1	U Log out
۲	Reports > Network									e	900	00	
	Cisco												1
Q	FortiGate												
•	ASA PIX Authentication												
	ASA PIX Firewall												
	Checkpoint Firewall 1												
E	CISCO Routers												
	CyberGuard Firewalls												
	F5 Violations per Server												
	Gauntlet Emails												
	Gauntlet Firewall												
	IPTables Firewall												
	ISA Firewall												
	Netgear Firewall												
<b>V</b>	-												•
	nare $\equiv$ Cyber Network Map		3, 16:49 GMT	+9:30 k > ASA PIX1	Firewall		Config			till televise hedule Queux	Regenerate	Attachment .	U Log out
Φ		May 16. 202 Reports	3. 16:49 GMT 5 > Network	k > ASA PIX I	Firewall A logs for events of	triesd				hedule Queue		Attuchment	Log out
•	Cyber Network Map	Reports	3, 16:49 GMT 5 > Network Query the C	K > ASA PIX I ISCO PIXIASJ Taxiar Cenas	A logs for events of Une Grayn	Cestination Fort Map	Config			hedule Queue	Regenerate	Attuchment	Log out
() () () () () () () () () () () () () (	Cyber Network Map Dashboard Events Search	Reports	3, 16:49 GMT 5 > Network Query the C	K > ASA PIX I ISCO PIXIASJ Taxiar Cenas	A logs for events of	Cestination Fort Map	Config			hedule Queue	Regenerate	Attuchment	Log out
() () () () () () () () () () () () () (	Cyber Network Map Dashboard	May 16.202 Reports Fatter May << Ent < DATE 2023. 2025	3, 16:49 GMT 5 > Network Query the C prev 1 2	<ul> <li>x &gt; ASA PIX I</li> <li>rsco POUASA</li> <li>rscalar Cenes</li> <li>3 4 5 5</li> </ul>	A logs for events of une Grayn 2   Z   8   9   19	Comment For Var	Config	ure Acc	ess Control 5cl	Generated: 11 DSTADDR 10.0	Regenerate 2	Attachment aration: 00:01:14	Log out
0 0 0	Cyber Network Map Dashboard Events Search	May 16, 202 Reports	3, 16:49 GMT Duery the C prev 1 2 04:00 02	<ul> <li>x &gt; ASA PIX I</li> <li>ISCO PRUASA</li> <li>ISCO P</li></ul>	A logs for events of une Grayn 2   Z   8   9   19	Desires Points         Sevenan May           Rest2         EVENTID           106001 (Indexing Connection denied)         394001 (rentropicames, address, Accessed (JANA, URL, URL), dest_address url)	Config	PROTO	SRCADDR 139-162 202 one register 10.0	Generated: 11 DSTADDR	Begenerate A Bay 2023 16:49:22 [D DSTPORT 162 (SNAPTRAP) 60 (Vibb Server)	uration: 00:01:14	Log out
0 0 0 0	Cyber Network Map Dashboard Events Search Reports Agent Management	May 16.202 Reports Fatar Nau << Erst < DATE 2023- 05-16 2023- 05-16	2, 16:49 GMT 5 > Network Duery the C TIME 04:00:02 04:00:02	<ul> <li>x &gt; ASA PIX I</li> <li>ISCO PRUASI</li> <li>SUSTEM</li> <li>127.0.0.1</li> <li>127.0.0.1</li> </ul>	Alogo for events of Une Gaun 2 Z R 9 12 CRITICALITY 2 5 6	Seman For tay     Seman For tay     Seman For tay      EVENTID      196001 (Industry TCP connection device)      304001 (insurgitource_address Accessed     (JANU URL, URL), least, address of      196015 (Davy TCP (ino connection))	ACTION drop Map drop	PROTO TCP TCP TCP	SRCADDR 139-16 SRCADDR 139-16 SRCADDR 199-16 SRCADDR 199-16 SRCADDR 199-16 SRCADDR 199-16 SRCADDR 199-16 SRCADDR 199-16 SRCADDR 199-16 SRCADDR	Generated: 11 DSTADOR 10 0 74 23 Work Date 10.1	Begenerate         J           Bay 2023 16:49:22 [Di           DSTPORT           162 (SNMPTRAP)           60 (Web Server)           61 (HOST2 Name Server)           51 (HOST2 Name Server)	Unation: 00:01:14	Log out
0 0 0 0	Cyber Network Map Dashboard Events Search Reports	May 16, 202 Reports Preser No. Control Control Control Preser No. Control Contrel Control Control Control Control	3, 16:49 GMT 6 > Network 0uery the C 0uery the C 12 TIME 04:00:02 04:00:02 04:00:02	x > ASA PIX I           ISCO POUAS/           SIGO POUAS/           3 4 5 5           SYSTEM           127.0.1           127.0.1           127.0.1           127.0.1	A legs for events of Une dean 2 Z 8 9 120 CRITICALITY 2 5 6	Semen for two Sement for two Sement for two Sement for two Sement for two Sements for the Sement Sement Sements Sement SementSement Sement Sement Sement Sement Sement Sement Sement Sem	ACTION Map drop sccept	PROTO TCP TCP TCP	SRCADDR 139 16. 139 16. 139 16. 130 16. 1423 11. 10. 10. 10. 10. 10. 10. 10. 10. 10.	Generated: 11 DSTADDR 10.0 DSTADDR 10.0 DSTADDR 10.0 DSTADDR 10.0 DSTADDR 10.0 DSTADDR 10.1 DSTA	Begenerate         J           Begenerate         J           May 2023 16:49:22 (D)         D           DSTPORT         162 (SNMPTRAP)           60 (Web Server)         60 (Web Server)           61 (HOST2X Name Server)         Server)           443 (Web Server)         Server)           Modely         Server)	DIRECTION Inbound - outbound	Log out
0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	Cyber Network Map Dashboard Events Search Reports Agent Management	May 16, 202 Report Faster vite 2023 05-16 2023 05-16 2023 05-16 2023 05-16 2023 05-16 2023 05-16 2023	2, 16:49 GMT Duery the C Duery the C 04:00:02 04:00:02 04:00:02 04:00:02 04:00:02	x > ASA PIX I           ISCO POUAS/           2         4         5         5           SYSTEM           127.0.1           127.0.1           127.0.1           127.0.1           127.0.1           127.0.1           127.0.1	A logs for events of Une Gran 5 Z S 9 12 CRITICALITY 2 5 5 6 6 2	Benner Hoteg      Benner	ACTION Map drop accept drop	PROTO TCP TCP TCP TCP TCP	SRCADDR 139 52 300 min 2000 7423 10 - 10 7423 10 7423 10 76 10 10 10 10 10 10 10 10 10 10 10 10 10 1	Generated: 10 DSTADDR 10.0 12.13 West Inne 10.1 12.13 West Inne 10.1	Engenerate / / DSTPORT 192 (SNMPTRAP) 60 (Web Server) 10 (POSTS 2017) 41 (POSTS 2017) 60 (Web Server) 10 (POSTS 2017) 10 (POSTS 2017)	Unation: 00:01:14	Log out
0 0 0 0 0	Cyber Network Map Dashboard Events Search Reports Agent Management Status	May 16, 202 Reports Terms War et Ent < 0273 05-16 05-16 0	3. 16.49 GMT 6 > Network 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	x > ASA PIX I           ISCO POUAS/           2         4           5         5           SYSTEM           127.0.1           127.0.1           127.0.1           127.0.1           127.0.1           127.0.1           127.0.1           127.0.1           127.0.1	A logs for events of Use See 2 Z 8 9 5 50 CRITICALITY 2 5 6 6 6 6 6 6 6 6 6 6 6 6 6 6 6 6 6 6	Descent Porting     Descent Porting     Descent Port     Descent D     DescentD     Descent D     Descent D     Descent D	ACTION drop drop eccept drop drop	PROTO TCP TCP TCP TCP TCP TCP	SRCADDR 133 fd 10 State 10 Sta	Operation         Operation           DSTADDR         10.0           10.0         12.13           10.0         10.0           10.0         10.0           10.0         10.0           10.0         10.0           10.0         10.0	Begenerate     Any 2023 16-49-22 (2)     DSTPORT     102 (INNMPTRAP)     00 (Web Server)     41 (INDSTS2 Name     Server)     42 (INNMPTRAP)     26 (Simple Mail	DIRECTION Inbound - outbound	Log out
0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	Cyber Network Map Dashboard Events Search Reports Agent Management Status	May 16, 202 Reports Preservite Control (10, 10, 10, 10, 10, 10, 10, 10, 10, 10,	2, 16:49 GMT Duery the C Duery the C 04:00:02 04:00:02 04:00:02 04:00:02 04:00:02	x > ASA PIX I           ISCO POUAS/           2         4         5         5           SYSTEM           127.0.1           127.0.1           127.0.1           127.0.1           127.0.1           127.0.1           127.0.1	A logs for events of Une Gran 5 Z S 9 12 CRITICALITY 2 5 5 6 6 2	Benner Hoteg      Benner	ACTION Map drop accept drop	PROTO TCP TCP TCP TCP TCP	SRCADDR 139 52 300 min 2000 7423 10 - 10 7423 10 7423 10 76 10 10 10 10 10 10 10 10 10 10 10 10 10 1	Operation         Operation           0         0         0           10         0         0           12         10         0           12         10         0           12         10         0           12         10         0           12         10         0           12         10         0           12         10         0	Engenerate / / DSTPORT 192 (SNMPTRAP) 60 (Web Server) 10 (POSTS 2017) 41 (POSTS 2017) 60 (Web Server) 10 (POSTS 2017) 10 (POSTS 2017)	DIRECTION Inbound - outbound	Log out
0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	Cyber Network Map Dashboard Events Search Reports Agent Management Status	May 16, 202 Reports File that 4 2023 001 002 002 002 002 002 002 002	3. 16.49 GMT 5. > Network 0	x > ASA PIX           ISCO POUASY           IZT 0.01           IZT 0.01           IZT 0.01           IZT 0.01	A logs for events of Use See 2 Z 8 9 5 50 CRITICALITY 2 5 6 6 6 6 6 6 6 6 6 6 6 6 6 6 6 6 6 6	Berner Hotey     Berner Hotey      Berner      Berner Hotey      Berner      Berner      Berner	ACTION drop drop accept drop drop drop	PROTO TCP TCP TCP TCP TCP TCP TCP	SRCADDR SRCADDR 133 14 10 200 000 000 10 200 000 000 10 200 000 000 25 512 25 52 26 000 000 25 50 000 000 25 50 000 20 000 2000 20 000 20 0000 20 000 20 000 20 000 20 000 20 0	Operation         Operation           DSTADOR         10.0           10.0         12.1           10.0         12.1           10.0         12.1           10.0         10.0	Begenerate // May 2021 16-69-22 (DC BSTPORT 162 (DNMTTMAP) 60 (Theb Server) 61 (FIOSTS2 Name Server) 63 (Strong Server) 64 (Str	DIRECTION Inheund - outbound - inheund -	Log out
0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	Cyber Network Map Dashboard Events Search Reports Agent Management Status	May 16, 2022 Reports File 100 File 100 Fil	2. 16.49 GMT	L > ASA PIX I           ISCO POUASI           3         4         5         5           SVSTEM           127.0.1           127.0.1           127.0.1           127.0.1           127.0.1           127.0.1           127.0.1           127.0.1           127.0.1           127.0.1           127.0.1	A logs for events of Unit from CRETICALITY	Senser Mritis     Bezarrie     Bezarr      Bezarr      Deterr	ACTION drop brop ccept drop drop drop drop drop	PROTO TCP TCP TCP TCP TCP TCP TCP TCP TCP	SRCADDR SRCADDR 139 5C Sing region 10.5 Sing region 25 5C Sing region 26 5C Sing reg	Cemerated:         II           DSTADDR         10.0           10.0         10.0           12.13         10.0           10.0         10.0           10.1         10.0           10.1         10.0           10.1         10.0           10.1         10.0           10.1         10.0           10.2         10.0           10.0         10.0           10.0         10.0	Bagenerate         J           DSTPORT         DSTPORT           142 (INAM*TRAP)         DSTPORT           432 (INAM*TRAP)         DSTPORT           433 (INAM*TRAP)         DSTPORT           443 (INAM*TRAP)         DSTPORT           442 (INAM*TRAP)         DSTPORT	DIRECTION Inheund - outbound - inheund -	Log out
0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	Cyber Network Map Dashboard Events Search Reports Agent Management Status	May 16, 2022 Reports Parent dia 2023 06-16 2025 06-16 2025 06-16 2025 06-16 2025 06-16 2025 06-16 2025 06-16 2025 06-16 2025 06-16 07 07 07 07 07 07 07 07 07 07	2. 16.49 GMT	x > ASA PIX I           HSCO PROASH           1         4         5         5           SVSTEM           127.0.1         127.0.1           127.0.1         127.0.1           127.0.1         127.0.1           127.0.1         127.0.1           127.0.1         127.0.1           127.0.1         127.0.1	A logs for events of Unit from CRETICALITY	Senser Mritis     Senser Mritis     Senser Mritis     Senser Mritis     Senser	ACTION drop drop accept drop drop drop drop drop drop drop drop	PROTO           TCP           TCP	SRCADDR     SRCADDR     SRCADDR     SRCADDR     SSRCADDR     SSRCADR     SSRCARR	Distriction         Operating           Distriction         10	Begenerate May 2021 16-49-22 (D DSTPCHT 162 (DMMTTRAP) 60 (DMB Server) 8 (DMB Server) 8 (DMB Server) 8 (DMB Server) 14 (DMB Server) 14 (DMB Server) 16 (DMB Se	DIRECTION Inheund - - - - - - - - - - - - - - - -	Log out

A range of network and firewall events can be monitored via the objectives in this category.

It is recommended that failed connections be monitored for patterns that may indicate attempts to compromise internally protected resources. Where supported by the source firewall, router or switch, management events such as login, or rule creation/removal, should be checked for anomalies also.

Proxy Server Logs



 nare		Administr May 16. 2023.		9:30				Configure A	cess Contr	el Schedule Queue Regenerate	Attachment Log out
Cyber Network Map		Reports :	> Applicatio	on Audit > Wet	Servers > URL S	Scanner					
Dashboard		0	Query web-re	lated logs for ever	its of interest					Generated: 16 May 2023 17:05:35	[Duration: 00:00:36]
Events Search		Paten Nag		tabe Details	Live Graph						
		DATE	TIME	SYSTEM	HOSTNAME	USERNAME	PROTOCOL	URL	BYTES	REFERRER	RETURNCODE
Reports		2023-05- 16	03.00.02	FROGMOUTH	69.251.22.1	MrRed	GET	/stuffy/severe/pieman.html	0	http://www.pieman.com.au/severe/heaped.html	200 (OK)
Agent Management	>	2023-05- 16	03:00:02	FROGMOUTH	98.191.195.92	MrsTangerine	GET	/pieman/unlike/simple.html	0		200 ( <b>OK</b> )
		2023-05- 16	03:00:02	FROGMOUTH	87.248.77.159	DrOrange	GET	/slalom/simple/stuffy.html	0	http://www.twiggy.com.au/angler/twiggy.html	200 ( <b>OK</b> )
Status	>	2023-05- 16	03.00.02	FROGMOUTH	202.142.47.78		GET	/twiggy/bistro/forest.html		http://www.dryads.com.au/slider/inbred.html	200 ( <b>OK</b> )
	~	2023-05- 16	03:00:02	FROGMOUTH	119.18.8.51 Australia	MsGrey	GET	/unlike/inbred/califs.html	0	2	200 ( <b>OK</b> )
System	>	2023-05- 16	03 00 02	FROGMOUTH	15.16.17.18 Mill United States	MsGrey	GET	/severe/lander/califs.html	0		200 ( <b>OK</b> )
		2023-05- 16	03.00.02	FROGMOUTH	66.220.110.56	×	GET	/rounds/forest/slalom.html		http://www.uncles.com.au/lander/inbred.html	200 ( <b>OK</b> )
		2023-05- 16	03.00.02	FROGMOUTH	202.142.47.78	MrsTangerine	GET	/severe/primes/rounds.html	0	(*)	200 ( <b>OK</b> )
		2023-05- 16	03:00:02	FROGMOUTH	18.19.20.21	MrGreen	GET	/angler/grange/frowsy.html	0	http://www.twiggy.com.au/califs/uncles.html	200 ( <b>OK</b> )
		2023-05- 16	03:00:02	FROGMOUTH	87.248.77.159		GET	/lander/califs/willer.html		http://www.twiggy.com.au/primes/simple.html	200 ( <b>OK</b> )
		2023-05- 16	03 00 02	FROGMOUTH	69.251.22.1	MrsBlue	GET	/heaped/dryads/grange.html	0	http://www.heaped.com.au/dryads/rounds.html	200 ( <b>OK</b> )
		2023-05- 16	03.00.02	FROGMOUTH	66.220.110.56	MrGreen	GET	/stuffy/willer/angler.html	0		200 ( <b>OK</b> )
		2023-05- 16	03:00:02	FROGMOUTH	69.251.22.1	MrGreen	GET	/califs/delays/slider.html	0	http://www.cellfs.com.au/lander/cellfs.html	200 ( <b>OK</b> )
		2023-05- 16	03:00:02	FROGMOUTH	98.191.195.92		GET	/heaped/califs/bistro.html		http://www.califs.com.au/heaped/dryads.html	200 ( <b>OK</b> )
		2023-05-			207 68 223 75	1005121	0.000		685		10.0222 M

Modern web browsers are complex tools that hold significant quantities of identifying information, or are used as a gateway to resources that are valued by attackers such as bank account details, information that can be sold to marketing firms, and data that can be used for identity theft.

As such, the browser is a significant potential attack vector for your payment card information data store; particularly if the attackers know the configuration of the internal web-based application that hosts your cardholder data, or if you are using an off-the-shelf application to host cardholder data that has known attack vectors or consistent URL paths to the data store.

To provide a level of audit information relating to browser based attack vectors, logs can be retrieved either directly from a proxy server or firewall, in order to attempt to detect cross site scripting attacks, or related browser probes.

Although it is also possible to use browser logs to gather data on application logins, or attempts by an internal attacker to circumvent access controls, in general, such information is available from the web server that hosts the application that provides access to cardholder data.

Web Server Logs



snare	=	Administr May 16. 2023.		9:30				Configure A	2A ccess Contr	ol Schedule	Queue Regenerate	Attachment	U Log out
Cyber Network Map		Reports :	> Application	on Audit > Web	Servers > URL	Scanner							
Dashboard		0	Query web-re	lated logs for ever	its of interest					Gene	rated: 16 May 2023 17:05:35	[Duration: 00:00:2	67
Events Search		Patient Map		öxler Details	Line Graph								
		<< first < pr				<u>12 (ast 22</u>							
Reports		DATE 2023-05-	TIME	SYSTEM	HOSTNAME 69.251	USERNAME	PROTOCOL	URL	BYTES	REFERRER		RETURNCODE	
		16	03:00:02	FROGMOUTH	09.20 Crited States	MrRed	GET	/stuffy/severe/pieman.html	0	http://www.pieman	com au/severe/heaped.html	200 (OK)	
Agent Management	>	2023-05- 16	03:00:02	FROGMOUTH	98.191.	MrsTangerine	GET	/pieman/unlike/simple.html	0			200 ( <b>OK</b> )	
		2023-05- 16	03:00:02	FROGMOUTH	87.248.	DrOrange	GET	Islalom/simple/stuffy.html	0	http://www.twiggy.c	com.au/angler/twiggy.html	200 ( <b>OK</b> )	
Status	>	2023-05- 16	03:00:02	FROGMOUTH	202.142.		GET	/twiggy/bistro/forest.html	-	http://www.dryads	com.au/slider/inbred.html	209 ( <b>OK</b> )	
		2023-05-	03:00:02	FROGMOUTH	119.18	MsGrey	GET	/unlike/inbred/califs.html	0	223		200 ( <b>OK</b> )	
System	>	2023-05- 16	03:00:02	FROGMOUTH	15.16	MsGrey	GET	/severe/lander/callfs.html	0			200 ( <b>OK</b> )	
		2023-05- 16	03:00:02	FROGMOUTH	66.220.	i k	GET	/rounds/forest/slalom.html	59 	http://www.uncles.c	com.au/lander/inbred.html	200 ( <b>OK</b> )	
		2023-05- 16	03:00:02	FROGMOUTH	202.142	MrsTangerine	GET	/severe/primes/rounds.html	0			200 ( <b>OK</b> )	
		2023-05- 16	03:00:02	FROGMOUTH	18.19.	MrGreen	GET	/angler/grange/frowsy.html	0	http://www.twiggy.c	com au/califs/uncles.html	200 ( <b>OK</b> )	
		2023-05- 16	03:00:02	FROGMOUTH	87.248.		GET	/lander/califs/willer.html		http://www.twiggy.c	com aulprimes/simple.html	200 ( <b>OK</b> )	
		2023-05- 16	03:00:02	FROGMOUTH	69.251	MrsBlue	GET	/heaped/dryads/grange.html	0	http://www.heaped	com au/dryads/rounds.html	200 ( <b>OK</b> )	
		2023-05- 16	03.00.02	FROGMOUTH	66.220	MrGreen	GET	/stuffy/willer/angler.html	0			200 ( <b>OK</b> )	
		2023-05- 16	03:00:02	FROGMOUTH	69.251.2000	MrGreen	GET	/califs/delays/slider.html	0	http://www.califs.co	om auflander/califs.html	200 ( <b>OK</b> )	
		2023-05- 16	03:00:02	FROGMOUTH	98.191		GET	/heaped/califs/bistro.html		http://www.califs.co	om au/heaped/dryads.html	200 ( <b>OK</b> )	
		2023-05-			207 68 2	1000 20 100	0000						*

As applications continue to migrate away from host-based binaries, to web based user interfaces, log data from web servers that host applications which store and process cardholder data, contributes more and more to the baseline security profile of an organisation.

Authentication and user administration may be handled internally within the application, or may be delegated to authentication services and servers. Other, related application tuning and management options, such as data backup or administration, may also be handled internally by the application. If handled internally, the subset of URLs that provide access to authentication management or administration functionality, should be checked for access by users outside an authorised subset.

Attempts to access URLs that are not specifically part of the application that hosts the cardholder data, should be investigated

Web server log data may or may not include information that specifically identifies an individual. Source IP address information, potentially correlated with workstation login information, may be able to facilitate user correlation with a reasonable level of confidence.

In situations where an application handles authentication internally, it is recommended that log data be generated directly by the application in order to facilitate positive user identification. Log data generated by custom applications can generally be collected by the Snare agents.

Security Infrastructure





Network intrusion detection products, such as the 'Snort', CISCO Sourcefire, and other firewalls that include IPS/IDS/NIDS, can be configured to send log data back to the Snare Central Server.

As noted above, such devices can produce an enormous volume of log data. If logs are to be reviewed daily, it is recommended that either the source system be configured to send only those events that are critical indicators of security-related issues, or that the Snare Central Server is configured to scan the verbose log events of critical of interest only.

#### **Custom Applications**

The Snare Central Server is capable of receiving log data from a wide variety of sources, including arbitrary applications that generate text-based log files or network events. If the organisation uses a custom application to store and process cardholder information, the log data generated by this application can be forwarded to the Snare Central Server for analysis and reporting, either by sending the data directly to the Snare Central Server using TCP or UDP (potentially as a syslog packet), or by writing the log data to an appendable local text file, which can be collected and pushed to the Snare Central Server by the Snare agents.

The Snare Central Server will capture log data from arbitrary custom sources, and include the information within a category known as 'Generic Log'. Snare's powerful substring matching and extraction functionality (or "Tokens"), provides the ability to pull embedded data out into useful fields, and use those fields as a basis for data searches and graphs.

#### **Health Checker**

The Snare Central Server health checker provides you with information relating to the health of your Snare Central Server collection, analysis and reporting environment. It is recommended that this facility be monitored daily to ensure that all system components are working correctly and the file system does not fill up and valuable log information is lost. It can also alert on when a device or system/Snare Agent is no longer sending logs that are expected so it can alert that something is not working correctly and needs investigation.