Regulatory Compliance: PCI/DSS V4.0

Payment Card Industry
Data Security Standard (PCI / DSS)

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 https://www.pcisecuritystandards.org

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.

- 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, intrusion-detection 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.
- IDS/IPS.
- FIM.
- Anti-malware solutions.
- 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.
- IDS/IPS.
- Change-detection mechanisms.
- Anti-malware solutions.
- Physical access controls.
- Logical access controls.
- Audit logging mechanisms.
- Segmentation controls (if used).
- Audit log review mechanisms.
- 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. https://www.snaresolutions.com/portfolio-item/how-snare-makes-fim-easier/

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

In general, the following core event categories should be enabled:

- 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 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.

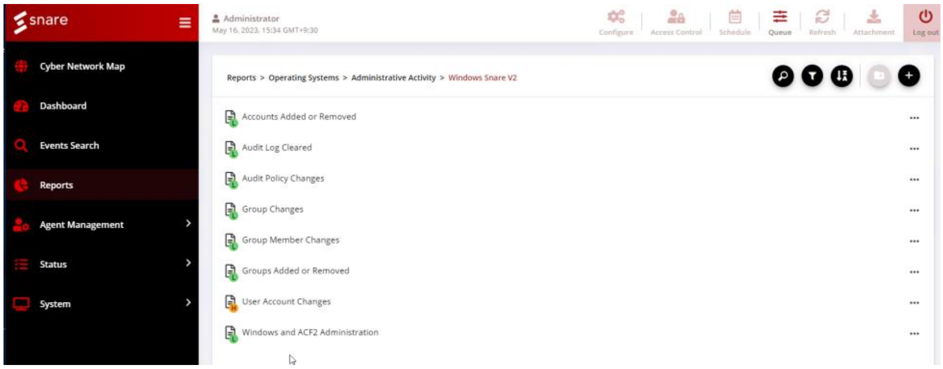
In situations where the application manages user authentication internally, and/or uses a mechanism to access data that would not be tracked or adequately segregated at the operating system level (eg: a database, or a related amalgamated storage mechanism), It is recommend that the application generates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

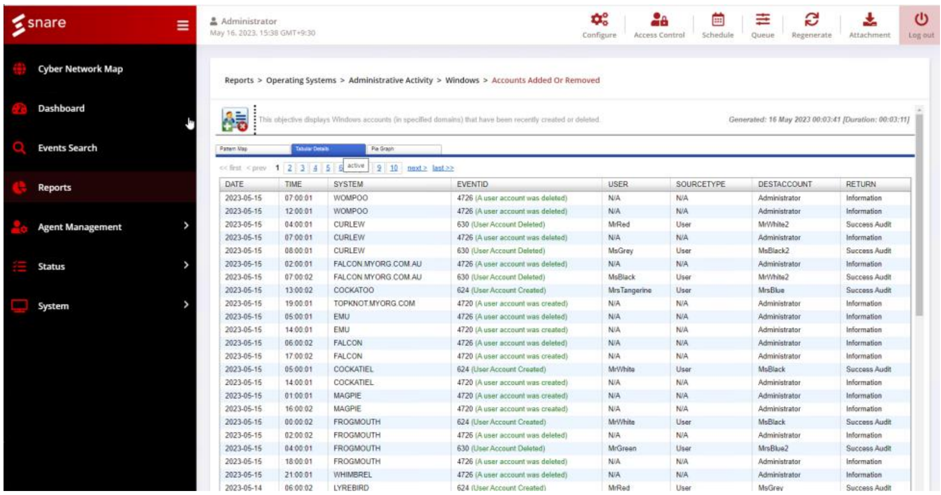
Administrative Actions and Account Management



Administrator
May 16, 2023, 15:34 GMT+9:30

Reports > Operating Systems > Administrative Activity > Windows Snare V2

- Accounts Added or Removed
- Audit Log Cleared
- Audit Policy Changes
- Group Changes
- Group Member Changes
- Groups Added or Removed
- User Account Changes
- Windows and ACF2 Administration



Administrator
May 16, 2023, 15:38 GMT+9:30

Reports > Operating Systems > Administrative Activity > Windows > Accounts Added Or Removed

This objective displays Windows accounts (in specified domains) that have been recently created or deleted.

Generated: 16 May 2023 00:03:41 [Duration: 00:03:11]

DATE	TIME	SYSTEM	EVENTID	USER	SOURCETYPE	DESTACCOUNT	RETURN
2023-05-15	07:00:01	WOMPOO	4726 (A user account was deleted)	N/A	N/A	Administrator	Information
2023-05-15	12:00:01	WOMPOO	4726 (A user account was deleted)	N/A	N/A	Administrator	Information
2023-05-15	04:00:01	CURLEW	630 (User Account Deleted)	MrRed	User	MrWhite2	Success Audit
2023-05-15	07:00:01	CURLEW	4726 (A user account was deleted)	N/A	N/A	Administrator	Information
2023-05-15	08:00:01	CURLEW	630 (User Account Deleted)	MsGrey	User	MsBlack2	Success Audit
2023-05-15	02:00:01	FALCON.MYORG.COM.AU	4726 (A user account was deleted)	N/A	N/A	Administrator	Information
2023-05-15	07:00:02	FALCON.MYORG.COM.AU	630 (User Account Deleted)	MsBlack	User	MrWhite2	Success Audit
2023-05-15	13:00:02	COCKATOO	624 (User Account Created)	MrsTangerine	User	MrsBlue	Success Audit
2023-05-15	19:00:01	TOPKNOT.MYORG.COM	4720 (A user account was created)	N/A	N/A	Administrator	Information
2023-05-15	05:00:01	EMU	4726 (A user account was deleted)	N/A	N/A	Administrator	Information
2023-05-15	14:00:01	EMU	4720 (A user account was created)	N/A	N/A	Administrator	Information
2023-05-15	06:00:02	FALCON	4726 (A user account was deleted)	N/A	N/A	Administrator	Information
2023-05-15	17:00:02	FALCON	4720 (A user account was created)	N/A	N/A	Administrator	Information
2023-05-15	05:00:01	COCKATIEL	624 (User Account Created)	MrWhite	User	MsBlack	Success Audit
2023-05-15	14:00:01	COCKATIEL	4720 (A user account was created)	N/A	N/A	Administrator	Information
2023-05-15	01:00:01	MAGPIE	4720 (A user account was created)	N/A	N/A	Administrator	Information
2023-05-15	16:00:02	MAGPIE	4720 (A user account was created)	N/A	N/A	Administrator	Information
2023-05-15	00:00:02	FROGMOUTH	624 (User Account Created)	MrWhite	User	MsBlack	Success Audit
2023-05-15	02:00:02	FROGMOUTH	4726 (A user account was deleted)	N/A	N/A	Administrator	Information
2023-05-15	04:00:01	FROGMOUTH	630 (User Account Deleted)	MrGreen	User	MrsBlue2	Success Audit
2023-05-15	18:00:01	FROGMOUTH	4726 (A user account was deleted)	N/A	N/A	Administrator	Information
2023-05-15	21:00:01	WHIMBREL	4726 (A user account was deleted)	N/A	N/A	Administrator	Information
2023-05-14	06:00:02	LYREBIRD	624 (User Account Created)	MrRed	User	MsGrey	Success Audit

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 system-level 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.

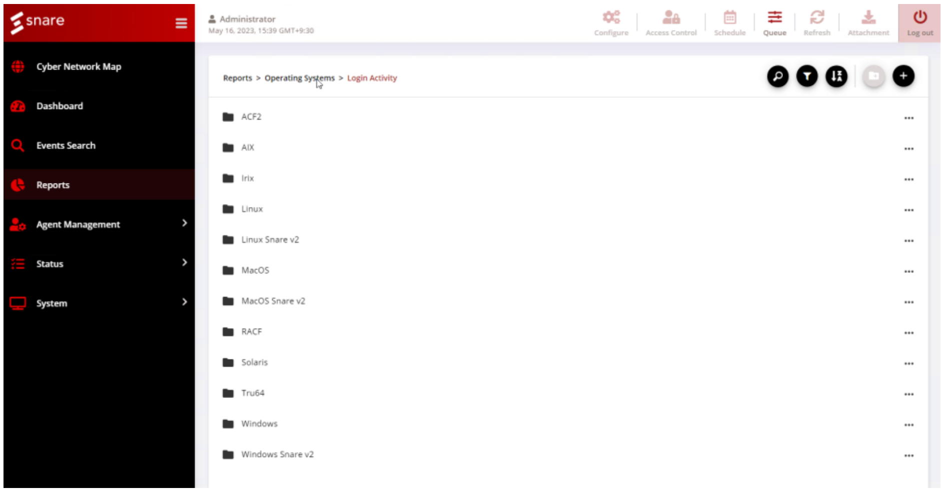
- Monitor account-related activity for Windows, Unix, and Mainframe systems. The objectives should be checked daily as per PCI/DSS recommendations, to ensure that only authorized staff have been creating, deleting or otherwise changing accounts, and this activity can be linked back to approved activity.

- 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

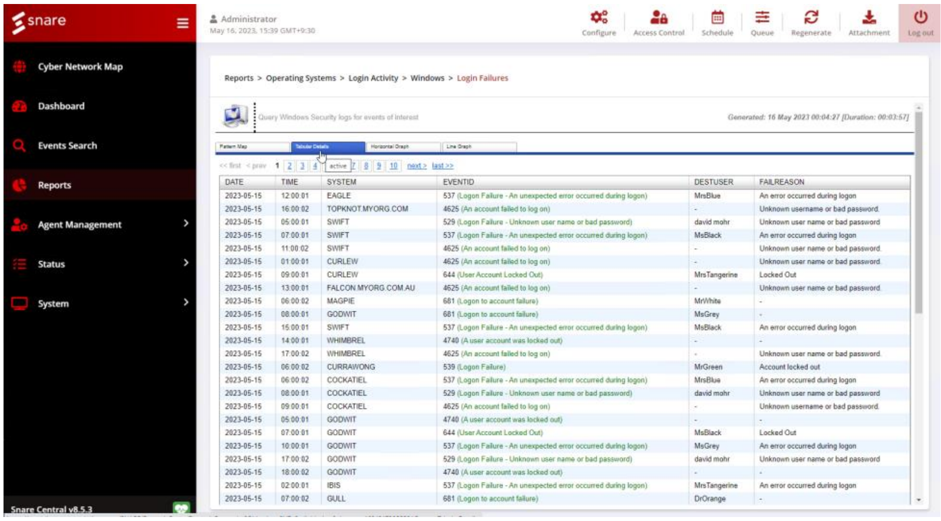
Login Activity



Administrator
May 16, 2023, 15:39 GMT+9:30

Reports > Operating Systems > Login Activity

- ACF2
- AIX
- Irix
- Linux
- Linux Snare v2
- MacOS
- MacOS Snare v2
- RACF
- Solaris
- Tru64
- Windows
- Windows Snare v2



Administrator
May 16, 2023, 15:39 GMT+9:30

Reports > Operating Systems > Login Activity > Windows > Login Failures

Query Windows Security logs for events of interest

Generated: 16 May 2023 00:04:27 [Duration: 00:03:57]

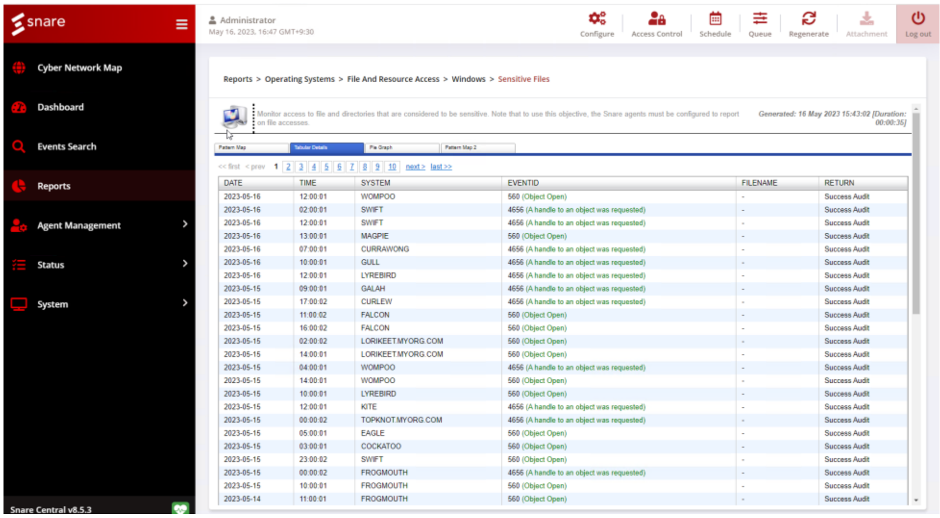
DATE	TIME	SYSTEM	EVENTID	DESTUSER	FAILREASON
2023-05-15	12:00:01	EAGLE	537 (Logon Failure - An unexpected error occurred during logon)	MrsBlue	An error occurred during logon
2023-05-15	16:00:02	TOPKNOT.MYORG.COM	4625 (An account failed to log on)	-	Unknown username or bad password.
2023-05-15	05:00:01	SWIFT	529 (Logon Failure - Unknown user name or bad password)	david mohr	Unknown user name or bad password
2023-05-15	07:00:01	SWIFT	537 (Logon Failure - An unexpected error occurred during logon)	MsBlack	An error occurred during logon
2023-05-15	11:00:02	SWIFT	4625 (An account failed to log on)	-	Unknown user name or bad password.
2023-05-15	01:00:01	CURLEW	4625 (An account failed to log on)	-	Unknown user name or bad password.
2023-05-15	09:00:01	CURLEW	644 (User Account Locked Out)	MrsTangerine	Locked Out
2023-05-15	13:00:01	FALCON.MYORG.COM.AU	4625 (An account failed to log on)	-	Unknown user name or bad password.
2023-05-15	06:00:02	MAGPIE	681 (Logon to account failure)	MrWhite	-
2023-05-15	08:00:01	GODWIT	681 (Logon to account failure)	MsGrey	-
2023-05-15	15:00:01	SWIFT	537 (Logon Failure - An unexpected error occurred during logon)	MsBlack	An error occurred during logon
2023-05-15	14:00:01	WHIMBREL	4740 (A user account was locked out)	-	-
2023-05-15	17:00:02	WHIMBREL	4625 (An account failed to log on)	-	Unknown user name or bad password.
2023-05-15	06:00:02	CURRAWONG	539 (Logon Failure)	MrGreen	Account locked out
2023-05-15	06:00:02	COCKATIEL	537 (Logon Failure - An unexpected error occurred during logon)	MrsBlue	An error occurred during logon
2023-05-15	08:00:01	COCKATIEL	529 (Logon Failure - Unknown user name or bad password)	david mohr	Unknown user name or bad password
2023-05-15	09:00:01	COCKATIEL	4625 (An account failed to log on)	-	Unknown username or bad password.
2023-05-15	05:00:01	GODWIT	4740 (A user account was locked out)	-	-
2023-05-15	07:00:01	GODWIT	644 (User Account Locked Out)	MsBlack	Locked Out
2023-05-15	10:00:01	GODWIT	537 (Logon Failure - An unexpected error occurred during logon)	MsGrey	An error occurred during logon
2023-05-15	17:00:02	GODWIT	529 (Logon Failure - Unknown user name or bad password)	david mohr	Unknown user name or bad password
2023-05-15	18:00:02	GODWIT	4740 (A user account was locked out)	-	-
2023-05-15	02:00:01	IBIS	537 (Logon Failure - An unexpected error occurred during logon)	MrsTangerine	An error occurred during logon
2023-05-15	07:00:02	GULL	681 (Logon to account failure)	DrOrange	-

Snare Central v8.5.3

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
  - 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



Reports > Operating Systems > File And Resource Access > Windows > Sensitive Files

Monitor access to file and directories that are considered to be sensitive. Note that to use this objective, the Snare agents must be configured to report on file accesses.

Generated: 16 May 2023 15:43:02 [Duration: 00:00:35]

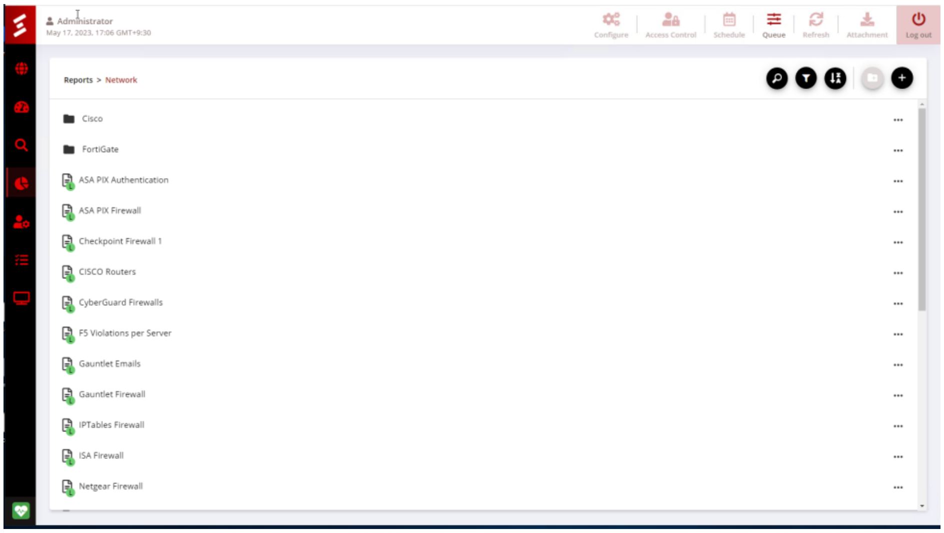
DATE	TIME	SYSTEM	EVENTID	FILENAME	RETURN
2023-05-16	12:00:01	WOMPOO	560 (Object Open)	-	Success Audit
2023-05-16	02:00:01	SWIFT	4656 (A handle to an object was requested)	-	Success Audit
2023-05-16	12:00:01	SWIFT	4656 (A handle to an object was requested)	-	Success Audit
2023-05-16	13:00:01	MAGPIE	560 (Object Open)	-	Success Audit
2023-05-16	07:00:01	CURRAWONG	4656 (A handle to an object was requested)	-	Success Audit
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
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)	-	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.

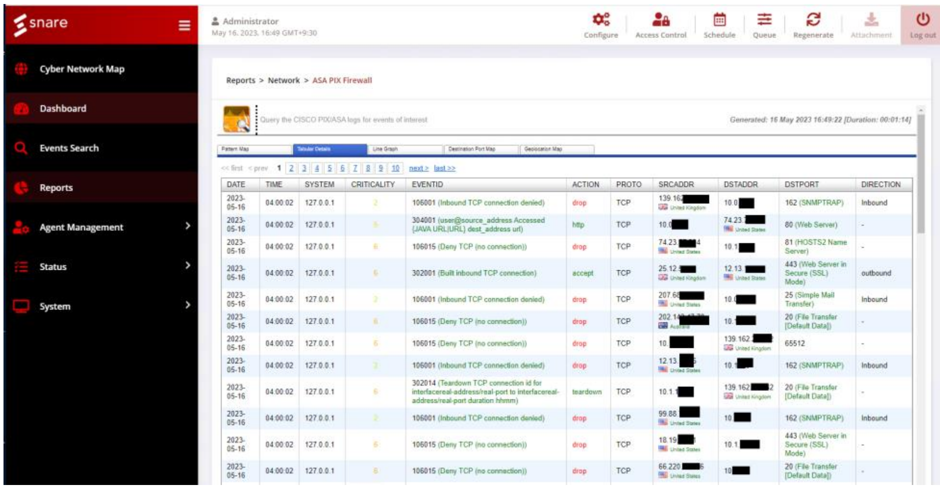
On Unix systems, for example, monitoring the binary (/usr/sbin, /usr/bin), library (/usr/lib) and configuration (/etc, /boot) directories may be appropriate. Windows systems may wish to monitor the \Windows directory. Logging for web-based applications could focus on any back-end components of the application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

Network Devices



Reports > Network

- Cisco
- FortiGate
- ASA PIX Authentication
- ASA PIX Firewall
- Checkpoint Firewall 1
- CISCO Routers
- CyberGuard Firewalls
- F5 Violations per Server
- Gauntlet Emails
- Gauntlet Firewall
- IPTables Firewall
- ISA Firewall
- Netgear Firewall



Reports > Network > ASA PIX Firewall

Query the CISCO PIX/ASA logs for events of interest

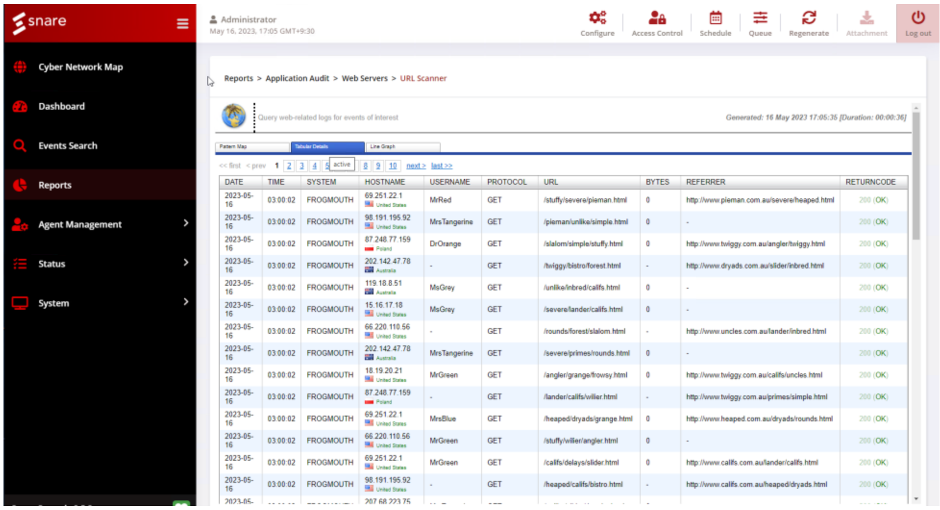
Generated: 16 May 2023 16:49:22 [Duration: 00:01:14]

DATE	TIME	SYSTEM	CRITICALITY	EVENTID	ACTION	PROTO	SRCADDR	DSTADDR	DSTPORT	DIRECTION
2023-05-16	04:00:02	127.0.0.1	2	106001 (Inbound TCP connection denied)	drop	TCP	139.162[redacted] United Kingdom	10.0[redacted]	162 (SNMPTRAP)	Inbound
2023-05-16	04:00:02	127.0.0.1	5	304001 (user@source_address Accessed {JAVA URL|URL} dest_address url)	http	TCP	10.0[redacted]	74.23.[redacted] United States	80 (Web Server)	-
2023-05-16	04:00:02	127.0.0.1	6	106015 (Deny TCP (no connection))	drop	TCP	74.23.[redacted]4 United States	10.1[redacted]	81 (HOSTS2 Name Server)	-
2023-05-16	04:00:02	127.0.0.1	6	302001 (Built inbound TCP connection)	accept	TCP	25.12.[redacted] United Kingdom	12.13.[redacted] United States	443 (Web Server in Secure (SSL) Mode)	outbound
2023-05-16	04:00:02	127.0.0.1	2	106001 (Inbound TCP connection denied)	drop	TCP	207.6[redacted] United States	10.0[redacted]	25 (Simple Mail Transfer)	Inbound
2023-05-16	04:00:02	127.0.0.1	6	106015 (Deny TCP (no connection))	drop	TCP	202.14[redacted] Australia	10.1[redacted]	20 (File Transfer [Default Data])	-
2023-05-16	04:00:02	127.0.0.1	6	106015 (Deny TCP (no connection))	drop	TCP	10.[redacted]	139.162.[redacted] United Kingdom	65512	-
2023-05-16	04:00:02	127.0.0.1	2	106001 (Inbound TCP connection denied)	drop	TCP	12.13.[redacted]5 United States	10.1[redacted]	162 (SNMPTRAP)	Inbound
2023-05-16	04:00:02	127.0.0.1	6	302014 (Teardown TCP connection id for interfacereal-address/real-port to interfacereal-address/real-port duration hhmm)	teardown	TCP	10.1.1[redacted]	139.162[redacted]2 United Kingdom	20 (File Transfer [Default Data])	-
2023-05-16	04:00:02	127.0.0.1	2	106001 (Inbound TCP connection denied)	drop	TCP	99.88.[redacted] United States	10.[redacted]	162 (SNMPTRAP)	Inbound
2023-05-16	04:00:02	127.0.0.1	6	106015 (Deny TCP (no connection))	drop	TCP	18.19.[redacted] United States	10.1.[redacted]	443 (Web Server in Secure (SSL) Mode)	-
2023-05-16	04:00:02	127.0.0.1	6	106015 (Deny TCP (no connection))	drop	TCP	66.220.[redacted]6 United States	10[redacted]	20 (File Transfer [Default Data])	-

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



Administrator
May 16, 2023, 17:05 GMT+9:30

Reports > Application Audit > Web Servers > URL Scanner

Query web-related logs for events of interest

Generated: 16 May 2023 17:05:35 [Duration: 00:00:36]

DATE	TIME	SYSTEM	HOSTNAME	USERNAME	PROTOCOL	URL	BYTES	REFERRER	RETURNCODE
2023-05-16	03:00:02	FROGMOUTH	69.251.22.1 United States	MrRed	GET	/stuffy/severe/pieman.html	0	http://www.pieman.com.au/severe/heaped.html	200 (OK)
2023-05-16	03:00:02	FROGMOUTH	98.191.195.92 United States	MrsTangerine	GET	/pieman/unlike/simple.html	0	-	200 (OK)
2023-05-16	03:00:02	FROGMOUTH	87.248.77.159 Poland	DrOrange	GET	/slalom/simple/stuffy.html	0	http://www.twiggy.com.au/angler/twiggy.html	200 (OK)
2023-05-16	03:00:02	FROGMOUTH	202.142.47.78 Australia	-	GET	/twiggy/bistro/forest.html	-	http://www.dryads.com.au/slider/inbred.html	200 (OK)
2023-05-16	03:00:02	FROGMOUTH	119.18.8.51 Australia	MsGrey	GET	/unlike/inbred/califs.html	0	-	200 (OK)
2023-05-16	03:00:02	FROGMOUTH	15.16.17.18 United States	MsGrey	GET	/severe/lander/califs.html	0	-	200 (OK)
2023-05-16	03:00:02	FROGMOUTH	66.220.110.56 United States	-	GET	/rounds/forest/slalom.html	-	http://www.uncles.com.au/lander/inbred.html	200 (OK)
2023-05-16	03:00:02	FROGMOUTH	202.142.47.78 Australia	MrsTangerine	GET	/severe/primes/rounds.html	0	-	200 (OK)
2023-05-16	03:00:02	FROGMOUTH	18.19.20.21 United States	MrGreen	GET	/angler/grange/frowsy.html	0	http://www.twiggy.com.au/califs/uncles.html	200 (OK)
2023-05-16	03:00:02	FROGMOUTH	87.248.77.159 Poland	-	GET	/lander/califs/wilier.html	-	http://www.twiggy.com.au/primes/simple.html	200 (OK)
2023-05-16	03:00:02	FROGMOUTH	69.251.22.1 United States	MrsBlue	GET	/heaped/dryads/grange.html	0	http://www.heaped.com.au/dryads/rounds.html	200 (OK)
2023-05-16	03:00:02	FROGMOUTH	66.220.110.56 United States	MrGreen	GET	/stuffy/wilier/angler.html	0	-	200 (OK)
2023-05-16	03:00:02	FROGMOUTH	69.251.22.1 United States	MrGreen	GET	/califs/delays/slider.html	0	http://www.califs.com.au/lander/califs.html	200 (OK)
2023-05-16	03:00:02	FROGMOUTH	98.191.195.92 United States	-	GET	/heaped/califs/bistro.html	-	http://www.califs.com.au/heaped/dryads.html	200 (OK)
2023-05-			207.68.223.75						

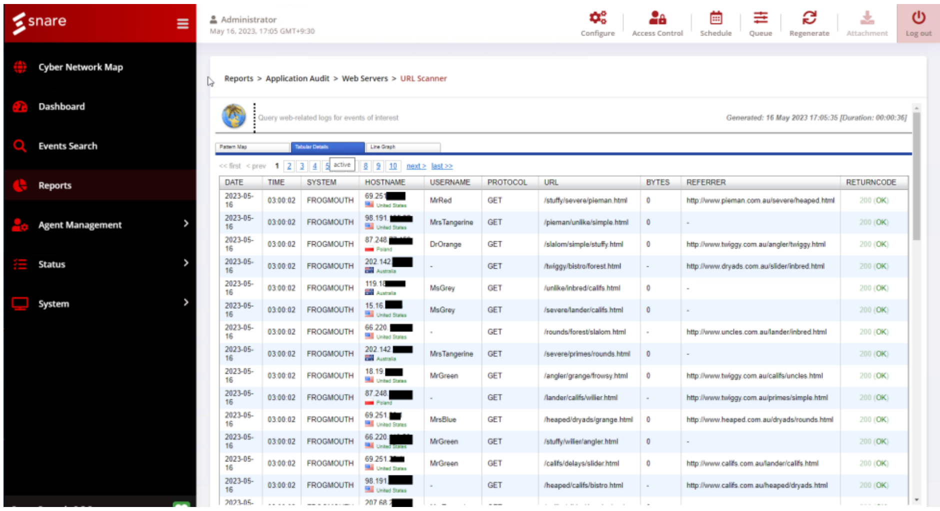
Modern web browsers are complex tools that hold significant quantities of identifying information, or are used as a gateway to resources that are valued by attackers such as bank account details, information that can be sold to marketing firms, and data that can be used for identity theft.

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



Reports > Application Audit > Web Servers > URL Scanner

Query web-related logs for events of interest

Generated: 16 May 2023 17:05:35 [Duration: 00:00:36]

DATE	TIME	SYSTEM	HOSTNAME	USERNAME	PROTOCOL	URL	BYTES	REFERRER	RETURNCODE
2023-05-16	03:00:02	FROGMOUTH	69.251[redacted] United States	MrRed	GET	/stuffy/severe/pieman.html	0	http://www.pieman.com.au/severe/heaped.html	200 (OK)
2023-05-16	03:00:02	FROGMOUTH	98.191.[redacted] United States	MrsTangerine	GET	/pieman/unlike/simple.html	0	-	200 (OK)
2023-05-16	03:00:02	FROGMOUTH	87.248.[redacted] Poland	DrOrange	GET	/slalom/simple/stuffy.html	0	http://www.twiggy.com.au/angler/twiggy.html	200 (OK)
2023-05-16	03:00:02	FROGMOUTH	202.142.[redacted] Australia	-	GET	/twiggy/bistro/forest.html	-	http://www.dryads.com.au/slider/inbred.html	200 (OK)
2023-05-16	03:00:02	FROGMOUTH	119.18[redacted] Australia	MsGrey	GET	/unlike/inbred/califs.html	0	-	200 (OK)
2023-05-16	03:00:02	FROGMOUTH	15.16.[redacted] United States	MsGrey	GET	/severe/lander/califs.html	0	-	200 (OK)
2023-05-16	03:00:02	FROGMOUTH	66.220.[redacted] United States	-	GET	/rounds/forest/slalom.html	-	http://www.uncles.com.au/lander/inbred.html	200 (OK)
2023-05-16	03:00:02	FROGMOUTH	202.142.[redacted] Australia	MrsTangerine	GET	/severe/primes/rounds.html	0	-	200 (OK)
2023-05-16	03:00:02	FROGMOUTH	18.19.[redacted] United States	MrGreen	GET	/angler/grange/frowsy.html	0	http://www.twiggy.com.au/califs/uncles.html	200 (OK)
2023-05-16	03:00:02	FROGMOUTH	87.248.[redacted] Poland	-	GET	/lander/califs/wilier.html	-	http://www.twiggy.com.au/primes/simple.html	200 (OK)
2023-05-16	03:00:02	FROGMOUTH	69.251.[redacted] United States	MrsBlue	GET	/heaped/dryads/grange.html	0	http://www.heaped.com.au/dryads/rounds.html	200 (OK)
2023-05-16	03:00:02	FROGMOUTH	66.220.[redacted] United States	MrGreen	GET	/stuffy/wilier/angler.html	0	-	200 (OK)
2023-05-16	03:00:02	FROGMOUTH	69.251.2[redacted] United States	MrGreen	GET	/califs/delays/slider.html	0	http://www.califs.com.au/lander/califs.html	200 (OK)
2023-05-16	03:00:02	FROGMOUTH	98.191[redacted] United States	-	GET	/heaped/califs/bistro.html	-	http://www.califs.com.au/heaped/dryads.html	200 (OK)
2023-05-			207.68.2[redacted]						

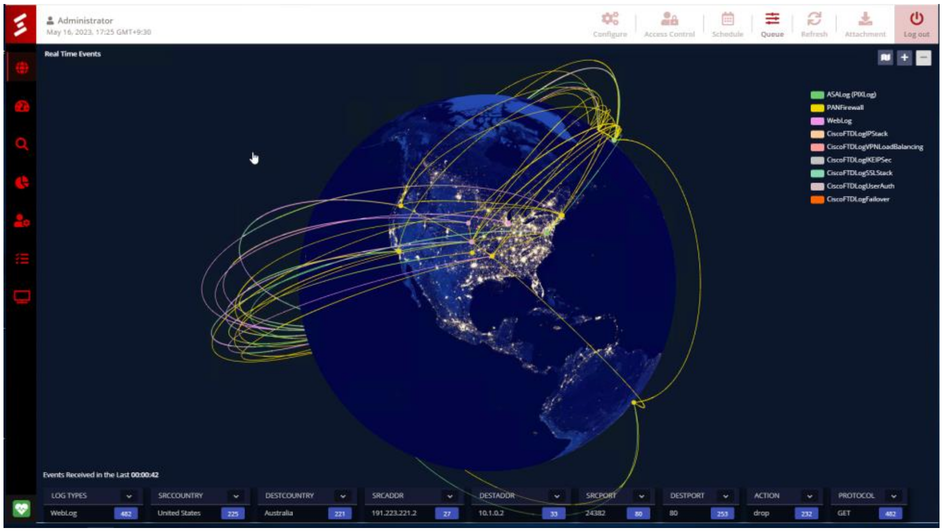
As applications continue to migrate away from host-based binaries, to web based user interfaces, log data from web servers that host applications which store and process cardholder data, contributes more and more to the baseline security profile of an organisation.

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.



Events Received in the Last 00:00:42

LOG TYPES		SRCCOUNTRY		DESTCOUNTRY		SRCADDR		DESTADDR		SRCPORT		DESTPORT		ACTION		PROTOCOL	
WebLog	482	United States	225	Australia	221	191.223.221.2	27	10.1.0.2	33	24382	80	80	253	drop	232	GET	482

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.