Maturity Model for Event Log Management

Whitepaper

Maturity Model Memorandum M-21-31

This memorandum was developed in accordance with and addresses the requirements in section 8 of the Executive Order for logging, log retention, and log management, with a focus on ensuring centralized access and visibility for the highest-level enterprise security operations center (SOC) of each agency. In addition, this memorandum establishes requirements for agencies to increase the sharing of such information, as needed and appropriate, to accelerate incident response efforts and to enable more effective defense of Federal information and executive branch departments and agencies.

Executive order 14028 - provides new guidance for improving the US federal governments investigative and remediation capabilities related to cybersecurity incidents.

Section 8 of the memorandum deals specifically with logging, log retention and log management, and focuses on ensuring centralized access and visibility for the highest level enterprise security operations center (SOC) of each agency.

The memorandum defines four levels of maturity, with a view to identifying and improving the handling of event log management within federal agencies.

Event	Logging Tiers	Rating Description
EL0	Not Effective	Logging requirements of highest criticality are either not met or are only partially met
EL1	Basic	Only logging requirements of highest criticality are met
EL2	Intermediate	Logging requirements of highest and intermediate criticality are met
EL3	Advanced	Logging requirements at all criticality levels are met

Full details of the Memorandum can be found here: https://www.whitehouse.gov/wp-content/uploads/2021/08/M-21-31-Improving-the-Federal-Governments-Investigative-and-Remediation-Capabilities-Related-to-Cybersecurity-Incidents.pdf

How Snare Can Help with Memorandum M-21-31

How Snare Can Help with Memorandum M-21-31

Centralized Access via Snare Central – Snare's centralized logging solution Snare Central was designed and developed to provide the type of centralized access called out in the Memorandum M-21-31.The latest version of Snare

Central features:

- Snare Management Center (SMC) – A centralized management view of multiple Snare Central systems, eliminating the need to visit each system on-site.
- Enhanced automated alerting to improve threat hunting speed
- New log types to expand coverage and enhance investigation capabilities
- Cloud-based log management and reports to support cloud or hybrid environments

How can Snare help you meet the requirements of executive order 14028?

Tier Level

Tier EL0,Rating – Not Effective

Requirements

The agency, or one or more of its components, have not implemented the requirement specified in "Logging Needs"

Logging Needs

The agency, or one or more of its components, have not implemented the requirement specified in "Logging Needs"

How Snare can help

Implementing Snare Central for secure centralized management and storage of all log data will help an agency to exit tier EL0. Snare Agents can be deployed across the environment to collect Criticality Level 0 logs from all host systems. Snare Central can also receive or actively collect syslog data from all internal and external syslog-capable devices, appliances and cloud based SaaS systems like firewalls, routers, switches, wireless access points, IPS/IDS sensors, malware tools, email gateways, and so on.

Tier EL1, Rating – Basic

Requirements

The agency and all of its components meet the requirement detailed in Table 2 (EL1 Basic Requirements) within Appendix A (Implementation and Centralized Access Requirements)

Logging Needs

- Basic Logging Categories
- Minimum Logging Data
- Time Standard
- Event Forwarding
- Protecting and Validating Log Information
- Passive DNS
- Cybersecurity Infrastructure Security Agency (CISA) and Federal Bureau of Investigations (FBI) Access Requirements
- Logging Orchestration, Automation, and Response – Planning
- User Behavior Monitoring – Planning
- Basic Centralized Access

How Snare can help

Snare Agents facilitate the collection of log data from desktop and server systems running a variety of operating systems and applications; including but not limited to Windows, Linux, MacOS and Database Activity Monitoring (DAM) for MSSQL Server and Oracle environments. Critical application text logs such as DHCP, DNS, IIS, Apache, Proxy logs, Java and other application logs can also be collected. All logs include the system timestamp, which as per memorandum guidance, should be based on a trusted NTP synchronized time source.

Snare agents allow logs to be sent to one or more destinations in near real time using various methods including TCP and TCP/TLS for reliable and secure encrypted transportation, and UDP for transit over data diodes between networks of controlled connectivity. Logs from Snare agents include a sequence number, and can also include checksum details for added tamper detection. Snare agents provide out-of-the-box policies that collect 90-95% of a systems significant administrative events. These policies can be tuned to collect additional events, filter for particular user activity, scan for specific application events, or generate and report on FIM, FAM, RIM and RAM requirements. Agents can generate heartbeat information to facilitate the detection of inactive systems. The Snare Agent Manager and Snare Central Server can provide alerts and reports of endpoint collection problems if a client system goes offline, or reporting volume drops significantly. For container-based or virtual environments, hypervisor and host monitoring can be facilitated by using Snare agents, syslog, and capturing container/hypervisor application log data. Virtual machines and in-container operating systems and applications can also be monitored subject to the installation of an appropriate agent on the container or by configuring the contained application to push data out to the centralized monitoring solution. Snare Central can be used to collect and store log data in a centralized, restricted-access environment under the control of the security team, away from the system that generated them. Snare Central is a software appliance; subject to appropriate resource allocation, it can store and provide

access to logs for an extended period. Snare Central provides role based access controls to manage who can access the system and what they can do. The data is kept in a portable format, suitable for export to third party forensic analysis tools used by CISA, FBI, CERT and NSA teams.

The whole process of log collection is fully automated. Log data is received, and broken up into fields of critical security relevance in order to facilitate rapid analysis using the event search functionality, or through the embedded intelligence of the dynamic query threat identification reports. Real time alerts and threshold reporting are also available to ensure that specific events trigger an alert based on the detection of identifiable user, system or network activities. Alerts can be sent via email or SNMP Trap depending on what alerting methods are available.

Systems policies can be implemented to purge unwanted data after designated periods of time to be in compliance with the defined logging retention needs.

Snare Central has over 650 out-of-the-box reports that cover a variety of system and user actions. Additional information is available in a related paper:

https://www.snaresolutions.com/portfolio-item/nist-zero-trust/.

Snare Central provides a range of "User Behavior Monitoring" reporting objectives within those default templates including, but not limited to:

- ✓ Login failures
- ✓ Login failures locked accounts
- ✓ Out of hours logins
- ✓ User interactive login logoff activity including type3 and type 10
- ✓ Accounts Added or removed
- ✓ Audit logs being cleared
- ✓ Audit policy changes
- ✓ Group Changes
- ✓ Group Member changes, users being added to administrators groups

- ✓ Changes to local Administrators group
- ✓ Groups added or removed
- ✓ User account changes
- ✓ Access to Sensitive file
- ✓ USB device usage and access
- ✓ Process monitoring, commands run and usage, running of special applications.
- ✓ Privilege escalation
- ✓ Scheduled tasks being created
- ✓ Services being installed
- ✓ Start-up run tasks being created
- ✓ For windows platforms: 25 reports covering sysmon log alerting types.

Activities such as lateral movement, compromised hosts, compromised user credentials, privileged account compromise, and unauthorized asset access, can be detected and reported on using the standard reporting and alerting capabilities. The system can be configured to generate regular scheduled reports as well as real time/threshold alerts for specific events of interest and/or specific systems and user classes. Scheduled reports can be a mix of hourly, daily, weekly, monthly, quarterly, yearly or at a custom interval.

Snare Central is designed as a central log management platform to collect, store and protect the log data for forensic analysis and reporting. The logs are stored and never altered. The system performs internal health checks and creates cryptographic checksums of the stored data and operating system components. If the operating system or log data is subject to tampering, the system can be configured to alert when the change is detected.

Snare agent log data utilizes sequence numbers on a per-event basis to facilitate the detection of missing data. Snare Agents support delivery of event log data over UDP, TCP or TCP/TLS. For reliable delivery it is recommended that TCP or TCP/TLS be used wherever possible. When additional data privacy is required, TLS is recommended. The Snare Central health checker can also send an alert when an agent or syslog source has

stopped sending logs or starts to send logs at a significantly higher or lower rate than normal.

The Snare Central environment has full role based access controls along with local user authentication. The Web UI allows local or external authentication using Windows Active Directory or LDAP. This ensures that only staff with a job related role have access at either view, access or adjust the reporting on data or can access the backend system. Backups of the data can also be created for export purposes, and data can be archived to other media or storage locations (ie DVD, USB, NAS).

Tier EL2,Rating – Intermediate

Requirements

The agency and all of its components meet the requirements detailed in Table 3 (EL2 Intermediate Requirements) within Appendix A (Implementation and Centralized Access Requirements)

Logging Needs

Meeting EL1 maturity level

- Intermediate Logging Categories
- Publication of Standardized Log Structure
- Inspection of Encrypted Data
- Intermediate Centralized Access

How Snare can help

As per EL1 capabilities, Snare Central has a built in log parser for a wide range of common log types. Bleeding edge and custom formats, will also be collected and stored by Snare Central in a generic log table in a format suited to reporting, follow-on analysis and custom data parsing. Snare Central can collect logs from any syslog source. New log types are added on a regular

basis. The log structure of the logs are detailed in our user guide documentation.

https://prophecyinternational.atlassian.net/wiki/spaces/SCV8/pages/742129903/Log+Types

Tier EL3,Rating – Advanced

Requirements

The agency and all its components meet the requirements detailed in in Table 4 (EL3 Advanced Requirements) within Appendix A (Implementation and Centralized Access Requirements)

Logging Needs

Meeting EL2 maturity level

- Advanced Logging Categories
- Logging Orchestration, Automation, & Response – Finalizing Implementation
- User Behaviour Monitoring – Finalizing Implementation
- Application Container Security, Operations, and Management
- Advanced Centralized

Snare can help

As per EL1 and EL2 levels. For EL3 environments where customers require a specialist third party analysis, SOAR, or machine learning pipeline, the Snare Central Server includes a built-in event reflector. The reflector includes advanced event selection, tagging, enhancement and multiplexing capabilities to selectivity send logs to collaborative processing tools in near real-time.

The reflector is network-aware, and can function as a data cache in the event of destination server downtime.

Where additional segmentation of data is required to meet the principles of need-to-know, the Snare Reflector can selectively divert data to one or more Snare Centrals or other SIEMs, based on advanced content filtering rules. Advanced centralized log storage and access controls is provided with Snare Central.

The Snare solution can help an agency to quickly attain EL2 levels of compliance with executive order 14028, and will facilitate the progression to EL3 as resourcing and funding allow. A variety of architectures can be implemented to facilitate the collection, storage and forwarding of the required log data to various levels of agencies as needed, and shared with other agencies as needed.

Snare also has broad coverage with the Mitre Att&ck framework that helps the security teams with detecting known APT threat actors using standard out of the box capabilities.

https://www.snaresolutions.com/portfolio-item/mitre-attack/

Ask us about Snare today

Learn More About Snare Can Help You Improve Your Log Management Maturity as Defined in Memorandum M-21-31

www.snaresolutions.com