TLP: CLEAR

IT Security | Supply Chain | OT Security | Insider Threat | Physical Security | Interoperable Communications

Guidance for Implementing M-21-31: Improving the Federal Government's Investigative and Remediation Capabilities

December 2022

Overview

The Office of Management and Budget (OMB) issued Memorandum 21-31, *Improving the Federal Government's Investigative and Remediation Capabilities Related to Cybersecurity Incidents,*[1] on August 27, 2021, in accordance with Executive Order 14028, *Improving the Nation's Cybersecurity*. The memorandum established federal agency[2] requirements to increase the government's visibility "before, during, and after a cybersecurity incident."[3] M-21-31 describes logs that agencies must capture as well as any required retention times. It also establishes a maturity model to track agency implementation. This document provides operational guidance to assist agencies with implementation of the M-21-31 requirements.

Purpose

The purpose of this operational guidance is to:

- Provide additional information to aid agencies in prioritizing their implementation of the policy requirements outlined in M-21-31.
- Answer frequently asked questions that CISA has received during its engagements with agencies.

This guidance intends to complement and clarify the requirements within M-21-31 and does not supersede or conflict with the policy. This is a non-binding document, and agencies can use an alternative approach if it satisfies the requirements of M-21-31. However, OMB and CISA may leverage this prioritization schema to track agency progress in achieving Event Logging tier 1 (EL1) of the M-21-31 maturity model in future performance metrics.

Definition of Key Terms

This guidance leverages several key terms that align to definitions in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-92 Guide to Computer Security Log Management:

Log: A record of the events occurring within an organization's systems and networks. Logs consist of log entries; each entry contains information related to a specific event that has occurred within a system or network.

Event: Something that occurs within a system or network.

Event Type: The category of an occurrence within a system or network.

Event Filtering: The suppression of log entries from analysis, reporting, or long-term storage because their characteristics indicate that they are unlikely to contain information of interest.

Prioritizing Implementation

Across its three maturity levels, M-21-31 requires many different event types to be logged. Agencies that are struggling to meet the lowest maturity level should prioritize their logging capability, deployment, log collection, and storage decisions based on system impact and by event type. The prioritization below provides a framework for deciding the systems to collect logs from and the event types to prioritize.

[1] 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
[2] "Agency" and "Agencies" is defined in 44 U.S.C. § 3502.
[3] M-21-31, page 1

How to Prioritize Deployment

Agencies should make risk-informed decisions about where log collection is most beneficial for improving cybersecurity incident detection and investigation. CISA recommends that agencies prioritize high value asset (HVA) systems, high impact systems, and the enterprise IT network (specifically identity providers like Azure Active Directory or Active Directory). Additionally, agencies should prioritize internet-accessible systems (e.g., web applications) and systems that interact with the internet regularly (e.g., devices from which users access email or browse the internet and DMZ network).

How to Prioritize Collection and Storage

CISA acknowledges that agencies may encounter challenges in collecting and storing all event types across their environments within the EL tier timeframes. CISA recommends agencies prioritize the following event types—listed in order of priority—for collection and storage as they work to achieve full EL1 compliance:

1. Identity, Credential, and Access Management (ICAM); Privileged ICAM (PICAM) event types, specifically:
    a. Manage/track changes in attributes and credentials[4]
    b. Track usage of credentials[5]
2. Operating systems (Windows/Linux/Mac where applicable) event types:
    a. Process creation
    b. Remote terminal or equivalent access and log off (success/failure)
    c. System access and logoff (success/failure)
    d. Scheduled task changes
    e. Service status changes (start, stop, fail, restart, etc.)
    f. Active network communication with other hosts
    g. Command-line interface (CLI)
    h. PowerShell execution commands
    i. Windows Management Instrumentation (WMI) Events
    j. Installation or removal of storage volumes or removeable media
3. Network device infrastructure event types:
    a. Domain Name System (DNS) query/response logs
    b. Dynamic Host Configuration Protocol (DHCP) lease information including media access control (MAC) address, IP address
    c. Firewall logs
4. Cloud environments (general logging):
    a. Any activity on breakglass account(s) (which should never have to be used)
5. Amazon Web service (AWS) event types:
    a. AWS CloudTrail
6. Cloud Azure
    a. Azure Active Directory logs
    b. Azure Activity
7. Microsoft 365
    a. Unified audit log (with advanced audit features)
8. Google Cloud Platform (GCP)
    a. Admin audit

Note: Agencies must still collect all Criticality 0 log types to be EL1 compliant.

[4] Examples include changes (create, update, delete) to identity objects (user, group, role, device, etc.).
[5] Examples include sign-in events (successful/unsuccessful) (e.g., Azure Active Directory sign-in logs, Active Directory sign-in logs)

Frequently Asked Questions

These questions will be added to the CyberStat Logging Requirements FAQ, wherein questions and answers on this topic are stored and continuously updated.

Does an agency need to "break and inspect" encrypted network traffic to meet EL2?

No, agencies do not need to implement a "break and inspect" solution to meet EL2. While maturity level 2 requires "full packet capture data: decrypted plaintext and clear text,"[6] the *Inspection of Encrypted Data* section of Table 3 states, "if agencies do not perform full traffic inspection, they should log the metadata available to them."[7] If an agency implements a decryption capability, they need to log decrypted packet capture (PCAP).

Can an agency drop events which it deems irrelevant to incident detection or response?

Yes, agencies may filter events they deem irrelevant "before, during, or after a cybersecurity incident." However, determining filterable events requires cybersecurity expertise and an understanding of the potential for an event to provide unique insight during an investigation.

Examples include filtering out encrypted packets from PCAP and certain Windows Service Host (svchost) process events from Process Create events.[8]

Collecting and storing 72 hours of PCAP is both challenging and expensive. How can agencies accomplish this requirement?

Due to the technical and operational obstacles to collecting and storing 72 hours of PCAP, CISA recommends that agencies allocate resources towards the priorities outlined in the Prioritizing Implementation section above. Additionally, agencies can minimize the size of collected PCAP by filtering out encrypted traffic (Transport Layer Security, etc.) and collecting PCAP only at central points (e.g., first hop in/out of an agency-managed network).

The memo repeatedly references an "agency and all of its components" and "component-level" capabilities. How is the term "component" defined for the purposes of the policy?

The term "component" is used in the memo to refer to the organizational unit below the agency enterprise level. Agencies across the FCEB have different designations and terminology for these organizational units, including component, bureau, administration, office, operating division, agency, sub-agency, etc. The policy recognizes that many agencies conduct security operations and have security operations centers and capabilities at both the enterprise and component levels. The memo calls these out explicitly to clarify that agencies must meet logging requirements across the entire organization to achieve the designated maturity level. Further, CISA's expectation is that agencies will provide all requested logs or information—from any level or entity within the agency—upon request.

How will CISA and the FBI access the data when a security incident occurs?

When a security incident occurs, CIOs will provision accounts within an agency environment and provide CISA and FBI officials credentials granting access to data by the same means as agency employees. In the long term, CISA will continue to explore approaches to allow queries of the data from outside the agency, or approaches that will allow agencies to send data continuously to CISA. These approaches would be designed to efficiently capture log data without impeding network performance. For more information contact: cyberstat@cisa.dhs.gov.

[6] M-21-31, page 39
[7] Ibid., page 9
[8] sysmon-config/sysmonconfig-export.xml at master · SwiftOnSecurity/sysmon-config · GitHub

DISCLAIMER: The Department of Homeland Security (DHS) does not provide any warranties of any kind regarding any information contained within. The DHS does not endorse any commercial product or service, referenced in this document or otherwise. This document is TLP: CLEAR: Recipients can spread this to the world, there is no limit on disclosure. Sources may use TLP: CLEAR when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. For more information on the Traffic Light Protocol, see http://www.us-cert.gov/tlp.