MeriTalk
Improving the Outcomes of Government IT

AXONIUS
FEDERAL SYSTEMS LLC

MEETING ZERO TRUST LOGGING REQUIREMENTS WITH AXONIUS

Building on the May 2021 cybersecurity executive order, the August 2021 Office of Management and Budget (OMB) memo M-21-31, "Improving the Federal Government's Investigative and Remediation Capabilities Related to Cybersecurity Incidents," requires Federal agencies to implement a four-tier system for event logging (EL) as part of the move to zero trust.

"Information from logs on Federal information systems (for both on-premises systems and connections hosted by third parties, such as cloud services providers) is invaluable in the detection, investigation, and remediation of cyber threats," said Shalanda Young, director of OMB.

M-21-31 Requirements

The first maturity model tier, EL0, indicates that agencies do not fully meet requirements for the most critical logging events. EL1 designates that the requirements for logging the highest criticality events are met. EL2 means the highest and intermediate criticality events are logged, and EL3 means the requirements for all levels of criticality are met. Levels EL1-EL3 must be implemented at six-month intervals so agencies can reach full logging maturity within two years.

When agencies are in full compliance, capabilities will include:

- Logging orchestration, automation, and response
- User behavior monitoring
- Application container security, operations, and management
- Advanced centralized access

M-21-31 notes, "These tiers will help agencies prioritize their efforts and resources so that, over time, they will achieve full compliance with requirements for implementation, log categories, and centralized access."

Logging underpins all cyber defense. Strong logging and visibility into agency systems are at the root of effective detection, investigation, and remediation. Logging enables agencies to monitor the effectiveness of responses, share information, and comply with regulations. Without effective logging, agencies struggle to detect incursions, run analytics on events, and understand incidents. Ineffective logging hinders evidence gathering after an attack and prevents agencies from establishing a baseline to help detect abnormal activity.

A Government Accountability Office report cited insufficient logging as an enabler of the SolarWinds breach, one of the most widespread and sophisticated cyberattacks targeting the Federal government: "varying levels of data log preservation among agencies and a lack of data collection tools limited evidence collection for the incidents." M-21-31 also noted, "Recent events, including the SolarWinds incident, underscore the importance of increased government visibility before, during, and after a cybersecurity incident."

Although the M-21-31 requirements are stringent, many agencies welcome the opportunity to improve logging procedures. FEMA CISO Gregory Edwards observed, "Our own experiences indicated that we needed to improve the investigative and remediation capabilities related to cybersecurity incidents … This is really a good push in the right direction for us."

Challenges for Agencies

However, implementing the provisions of M-21-31 will not be easy for all Federal agencies. They must move away from a reactive, tactical process of closing out alerts in a security information and event management (SIEM) system, searching for indicators of compromise, and conducting incident response investigations. Instead, agencies must take a proactive approach: trust nothing and verify everything. This foundational concept of a zero trust framework is outlined in the May 2021 executive order.

The combination of zero trust and proactive security will steeply increase the amount of logged information and necessitate enhanced logging capabilities – requiring petabytes of data and storage capacity. Agencies will also grapple with greater IT complexity as they collect and manage log data from on-premises, hybrid, and multiple cloud systems – and navigate dependencies across services.

They also face increased costs for licensing, storage, and infrastructure as well as employees' time and labor. However, agencies do not have a choice; M-21-31 is an unfunded mandate, so organizations must find ways to comply using existing budgets.

The first step to meeting these requirements is understanding the scope of the cyberattack surface; agencies must understand all assets in their purview, internal and external, as well as possible risks within the digital supply chain. This necessitates establishing a common, scalable cybersecurity asset management (CAM) platform that allows an agency to view all assets and confirm that logging capabilities are present, configured correctly, and functioning properly. Such an approach cannot be accomplished with siloed and/or legacy systems, which create an information patchwork that is inefficient and hinders productivity.

How Axonius Can Help

Fortunately, agencies don't have to start from scratch as they pursue an enterprise-wide view of their logging coverage. That is because CAM platforms connect to all security and IT management products in an organization's environment, providing a continuous view of devices, users, and security product coverage – and validating each against the organization's security policy. Instead of installing an agent, scanning, or sniffing traffic, a CAM platform uses adapters to connect to the SIEM solutions an agency already uses.

Axonius CAM represents a critical foundation for agencies to meet and maintain the M-21-31 requirements. Its capabilities include:

- Integration with existing security and IT management solutions
- Full accounting of all enterprise assets, including sensors
- Continuous verification that all tools and sensors are in place, configured correctly, and functioning properly
- Historic accounting of the daily state of all tools, sensors, and users, available for immediate reporting
- Notification if an asset or a sensor falls out of operational or security policy
- Operational platform for initiating and facilitating incident response actions

Axonius CAM offers aggregated asset intelligence, correlating data from numerous sources to provide rich, contextualized information on all deployed assets – in one place, from a single point of view, within a single management console. No more chasing data silos to identify asset-based vulnerabilities or exploits. No more manual data correlation. With Axonius, agencies can:

- Identify every location where an agency is not logging
- Find all agency assets missing logging coverage
- Reveal inconsistencies or misconfigurations in tool coverage and functionality
- Continually validate every asset's adherence to the overall security policy
- Create automatic, triggered actions when an asset deviates from policy

Axonius gives agencies the comprehensive asset visibility they need to control IT complexity, adopt zero trust principles, simplify incident response, and reduce manual work for the security team. This industry-leading solution offers the capability to ensure that all assets are accounted for and that all tools are functioning properly – so that all logging sources achieve EL2/EL3 maturity.

The M-21-31 requirements are substantial, time sensitive, and critical to zero trust architectures. Let Axonius smooth the path to M-21-31 compliance and zero trust with a solution that provides unprecedented visibility into agency environments.

To learn more, visit
https://www.axonius.com/company/axonius-federal-systems