LiveAction®

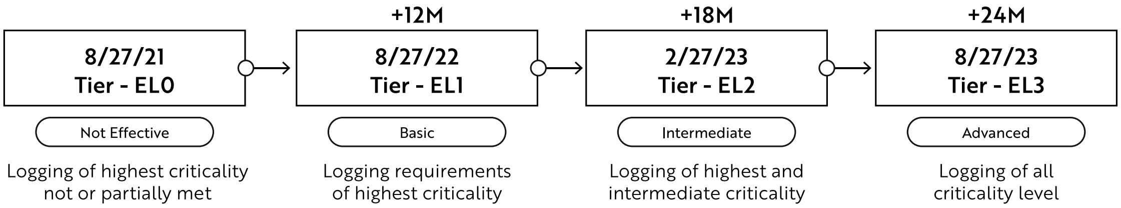
How LiveAction Supports the US Federal Government in Addressing OMB M-21-31

The Office of Management and Budget (OMB) issued Memorandum 21-31 (M-21-31) in August 2021 for the heads of executive departments and agencies of the federal government. The purpose of OMB M-21-31 is to support the logging, log retention, and log management requirements of Executive Order 14028 (Improving the Nation's Cybersecurity), with a focus on ensuring centralized access and visibility for the highest-level enterprise security operation center (SOC) of each agency.

This document outlines how LiveAction helps federal agencies support the maturity model outlined in OMB M-21-31 (see Figure 1), which guides the implementation and requirements across four Event Logging tiers and mandates adherence timelines. These tiers will help federal agencies prioritize their efforts and resources so they can achieve full compliance with requirements for implementation, log categories, and centralized access.

Summary of Event Logging Tiers and Timeline

Figure 1: Summary of Event Logging Tiers in OMB M-21-31



8/27/21
Tier - EL0
Not Effective
Logging of highest criticality not or partially met

+12M
8/27/22
Tier - EL1
Basic
Logging requirements of highest criticality

+18M
2/27/23
Tier - EL2
Intermediate
Logging of highest and intermediate criticality

+24M
8/27/23
Tier - EL3
Advanced
Logging of all criticality level

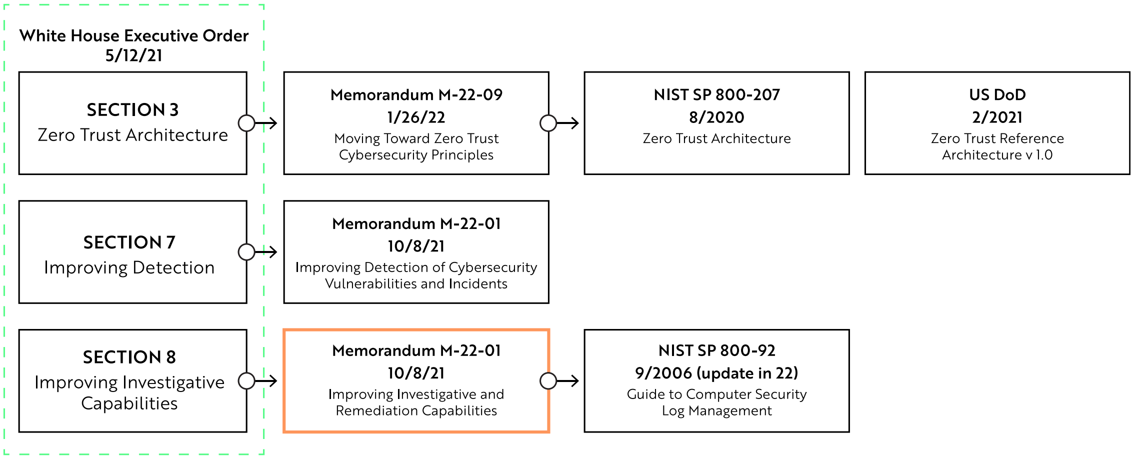
How LiveAction Helps with the OMB M-21-31 Maturity Model

LiveAction offers solutions for network performance monitoring (LiveNX), packet capture and forensic analysis (LiveWire), and network detection and response (ThreatEye). In short, LiveAction delivers real-time network intelligence to monitor, troubleshoot, and help secure enterprise networks and applications no matter where they are, including on-premises, hybrid, SD-WAN, and cloud operations.

For the OMB M-21-31 Event Logging Tiers, LiveAction helps federal agencies address the logging requirements for section 8 of Executive Order 14028 as related to the event logging tiers, detailed in Figure 2.

White House Executive Order and Memorandum

Figure 2: How LiveAction supports White House Executive Order 14028



White House Executive Order
5/12/21

SECTION 3
Zero Trust Architecture
→ Memorandum M-22-09
1/26/22
Moving Toward Zero Trust Cybersecurity Principles
→ NIST SP 800-207
8/2020
Zero Trust Architecture
US DoD
2/2021
Zero Trust Reference Architecture v 1.0

SECTION 7
Improving Detection
→ Memorandum M-22-01
10/8/21
Improving Detection of Cybersecurity Vulnerabilities and Incidents

SECTION 8
Improving Investigative Capabilities
→ Memorandum M-22-01
10/8/21
Improving Investigative and Remediation Capabilities
→ NIST SP 800-92
9/2006 (update in 22)
Guide to Computer Security Log Management

LiveAction Capabilities that Assist with Meeting EL1 Basic, EL2 Intermediate, and EL3 Advanced Requirements

○ **Packet Capture & Storage**

Packet capture data, in general, must be stored for a minimum of 72 hours and, depending on the category, up to 18 months to meet EL1 Basic Certification. LiveAction can provide solutions cost-effectively supporting very high sustained levels of network traffic, delivering up to 100Gbps of lossless full packet capture with the industry's most powerful and dense footprint. Customers requiring weeks to months of full PCAP duration are easily designed with our extremely dense storage platform purpose-built for Cyber Security Operations Center (SOC) teams. The solution interoperates with the security stack via a RESTful API and currently supports many solutions, including but not limited to SIEM (Splunk, Elastic, etc.).

○ **Tool Unification**

LiveAction supports, analyzes, and reports on diverse data types and offers a centralized platform (LiveNX) that requires fewer steps in meeting a centralized data access requirement. With LiveAction, users simply create a custom report and export a log file. In addition, LiveNX delivers a unified device management service (DMS) with a dashboard that shows packet-level visibility into network devices enabled through LiveWire.

○ **Playback Ability**

LiveNX offers a DVR-like playback ability to easily review network security incidents and disruptions by date and time for forensic analysis. And LiveWire extends playback capabilities to deep packet inspection for packet-level visibility into security incidents.

○ **Encrypted Traffic Analysis**

A requirement of EL1 certification is visibility into DNS traffic, encrypted or otherwise. EL2 requires inspection of encrypted data. The most resource-efficient, accurate way to inspect network traffic is through Encrypted Traffic Analysis (ETA), which allows users to see into traffic without requiring decryption. ThreatEye uses Deep Packet Dynamics (DPD), a highly effective, non- invasive method that allows admins to profile traffic characteristics and anomalies for risk.

○ **User Behavior Monitoring**

To receive EL1 certification, agencies must complete the planning state of User Behavior Monitoring. LiveAction offers behavior-based malware detection based on Machine Learning (ML) to improve accuracy and prediction capabilities over time. To receive EL3, User Behavior Monitoring needs to be implemented.

For more information on how LiveAction supports federal agencies for OMB M-21-31, please contact LiveAction Federal Sales via email FED@liveaction.com or call 425-239-8186.