Accelerating M-21-31 Logging Maturity with the Gigamon Deep Observability Pipeline

With the increasing sophistication of attackers and the criticality of their targets, the stakes for cybersecurity have never been higher, perhaps nowhere as much as in national security. To guide agencies and establish consistent standards, the U.S. government has issued cybersecurity requirements and direction. Gigamon is helping agencies meet these standards with deep observability across hybrid cloud infrastructure.

M-21-31 Requirements

To help the government detect, investigate, and remediate cyber threats as directed by Executive Order 14028, *Improving the Nation's Cybersecurity,* the Office of Management and Budget (OMB) issued Memorandum M-21-31, *Improving the Federal Government's Investigative and Remediation Capabilities Related to Cybersecurity Incidents*. M-21-31 requires each federal agency to collect, retain, and manage logs, focusing on centralized access and visibility for each agency's security operations center (SOC). It establishes a tier-based event logging (EL) maturity model that directs agencies to meet specific requirements, or levels, within a given timeline.

The goal of OMB M-21-31 is to establish a common level of logging, data retention, and reporting for Federal agencies. During operational and breach investigations it was concluded that organizations did not have a common level of logging, data retention, and reporting. This is an unfunded mandate, however, over time it should help lower risk and cost to the organization.

Why Deep Observability Matters

The Gigamon Deep Observability Pipeline provides capabilities that allow government agencies to implement current requirements of federal Zero Trust architecture initiatives such as M-21-31. At the same time, Gigamon helps public sector organizations simplify complex network architectures, consolidate tools, speed root-cause analysis of performance bottlenecks, lower operational overhead, and streamline workflow so teams can focus on mission-critical, high-priority objectives.

For more information on Gigamon M-21-31 and Zero Trust capabilities, please visit gigamon.com/campaigns/zero-trust.html.

How the Gigamon Deep Observability Pipeline Helps to Address These Requirements

Gigamon has a broad view of networks. This is a passive or external view. That means Gigamon can observe the behavior of workloads, network appliances and applications regardless of their state. When devices become overloaded or compromised, they may not log accurately. This can be seen as a second source of truth and more easily lends itself to logging in hybrid cloud scenarios and potentially reducing PCAP storage needs by 98 percent.

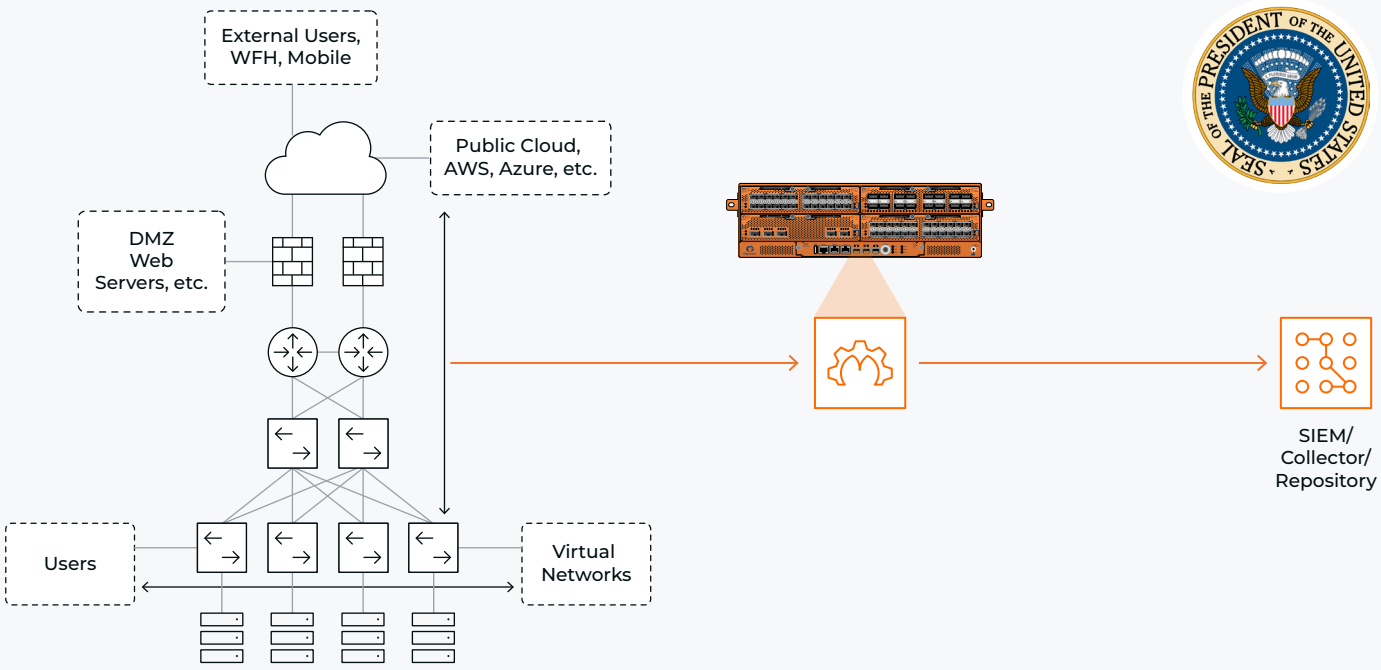

Figure 1. Three major ways Gigamon accelerates M-21-31 maturity across the hybrid network.

Most agencies will be operating in a hybrid cloud model for the foreseeable future, and one of the challenges of this model—one that seriously impacts M-21-31 compliance—is gaining visibility into the data-in-motion and logs across hybrid cloud infrastructure, including on-premises, private cloud, and public cloud. The Gigamon Deep Observability Pipeline, a solution already used extensively within leading Federal agencies, provides deep observability across hybrid cloud infrastructure and accelerates M-21-31 maturity by helping agencies meet requirements at each event logging level.

Tier Level	Difficulty	Requirements	How Gigamon Helps Aid or Meet Requirements
EL0	Not Effective	Does not meet or only partially meets requirements	
EL1	Basic Logging Categories	Requires detailed logs be maintained from every part of the network, including physical, cloud, and virtual environments	Minimum Logging Data, Time Standard, Event Forwarding, Protecting and Validating Log Information, Passive DNS For 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
EL2	Intermediate Logging Categories	Adds requirements, including the need to decrypt network traffic and data sharing capabilities so the DHS and FBI can more effectively detect threat patterns and investigate and remediate cyber threats	Publication of Standardized Log Structure, Inspection of Encrypted Data, Intermediate Centralized Access
EL3	Advanced Logging Categories	Enhances centralized access monitoring of data, adds user behavior monitoring and logging and monitoring of containerized services	Logging Orchestration, Automation, and Response – Finalizing Implementation, User Behavior Monitoring – Finalizing Implementation, Application Container Security, Operations, and Management, Advanced Centralized Access

Figure 2. Summary of M-21-31 event logging (EL) levels and requirements that Gigamon helps aid or meet.

EL1: Basic – Detailed logs from physical, virtual, and cloud networks

- Extends visibility into physical, virtual, and cloud environments with Application Metadata Intelligence, fulfilling the requirements in Network Flow Logs for the Network Device Infrastructure (General Logging) Category
- Increases the number of hours of data captured from physical, virtual, and cloud networks, enabling packet capture technologies to satisfy the Network Device Infrastructure (General Logging) Category
- Generates full-fidelity, non-sampled flow records. Given its inherently high demands on available bandwidth, NetFlow has a performance impact on the devices where it is implemented. To reduce that impact on performance, networking devices often rely on sampling packets (similar to sFlow) to generate NetFlow statistics. Low sampling rates—sometimes as few as one in 1,000 packets—dramatically reduce network visibility and could prevent teams from uncovering critical security threats or performance issues

Minimum Logging Data requirements can be challenging to satisfy even for the EL1 Basic level. Gigamon can assist with simplifying compliance from the network perspective. In addition to simplification, Gigamon can also ensure accuracy and completeness of logged data, mitigating the risk that an adversary will escape detection, whether before, during, or after a breach. Examples include:

- **Properly formatted and accurate timestamp**
  While traditional device-generated logs include their own timestamps, network traffic and network-based metadata relies on accurate and precise timestamping. Considering that a primary goal of M-21-31 is to assist with forensics, understanding the precise order of different events, especially data movement, is essential for success. Gigamon Timestamping can be applied in a non-disruptive manner to the network, timestamping upon ingress into the Deep Observability Pipeline, and optionally also on egress from the Gigamon software (whether appliance-based or virtualized). Gigamon utilizes Precision Time Protocol (PTP) in the TA200 device which can be configured globally and on a per-port basis, as desired. PTP timestamps can deliver nanosecond resolution, enabling evidentiary proof of not only time but also order of specific events viewed over the network.
- **Device Identifier (MAC address or other unique identifiers)**
  Logs will generally include its own device identifier, including the permanent identifier of MAC address and the network-defined identifier of IP address. However, there are several attack techniques that can obscure the true device involved. MITRE ATT&CK has identified ARP Cache Poisoning where an adversary "may poison Address Resolution Protocol (ARP) caches to position themselves between the communication of two or more networked devices." The networking device will from that point on log an adversary's MAC address as mapping to a legitimate IP address, instead of the true MAC address. While encryption can mitigate the Confidentiality risk, only intra-network inspection like "M1037 Filter Network Traffic" can correctly map IP address to MAC in a reliable fashion, thus achieving Integrity and Availability. Further, MITRE recommends "DS0029 Network Traffic Content" and "Network Traffic Flow" monitoring to identify unusual ARP traffic, gratuitous ARP replies, or other suspicious behavior.
- **Passive DNS**
  M-21-31 requires logging of DNS activities, which can be a burden on existing DNS servers. Gigamon can observe and record all DNS requests externally without placing burden on servers. By inspecting the network traffic Gigamon determines who initiated the request, which server responded, what was requested and the reply, as well as error codes and DNS over nonstandard ports, whether the workload resides on-premises or public cloud environments.

CISA has provided follow-on "Guidance for Implementing M-21-31" in a supplementary note from February 2023. In this guide, CISA advises "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." For all logging of network traffic including packet capture, Gigamon offers many core capabilities to help agencies prioritize exactly what information is logged, and where it can be stored. Major Gigamon capabilities for EL1 and beyond include:

- **Flow Mapping** specifies exactly which traffic will be sent to which tools or storage entities. Far more granular and scalable than connection- or ACL filter-based technologies, Flow Mapping can simultaneously guarantee that certain critical L4 traffic reaches high-inspection Security tools, while other low-risk/low-interest traffic may be dropped.
- **Application Filtering Intelligence** can filter out specific applications based on L4-7 criteria, for example eliminating any streaming media applications which are high-bandwidth but low-interest.
- **Application Metadata Intelligence** can replace packet capture entirely with application metadata derived from network traffic. Full packet capture (PCAP) may be onerous to maintain for 72 hours, so organizations can prioritize such that a small subset of mission-critical traffic is kept in its entirety, but most other traffic is processed for metadata extraction, which enables most key information to be maintained at a small fraction of the storage cost. A typical result would be 96-98% volume reduction, since the information kept is metadata of source, destination, port, application, application action, protocol, etc., but none of the actual payload.
- **Deduplication** can ensure no duplicate packets are stored, which would waste storage resources as well as risk incorrect analysis.

- **Advanced Flow Slicing** allows an organization to forward the first set of packets, then slice or drop the rest. In this way, all flows are logged and recorded, but a large/long flow which may have no useful insight or information beyond the initial flow set-up, will no longer fill costly storage. AFS alone can reduce traffic by more than 60% without impacting security and monitoring.

Planning for greater levels of maturity requires consideration of what foundational visibility is required to achieve later goals. User Behavior Monitoring which is an EL3 Advanced Requirement "allows for early detection of malicious behavior" by detecting "anomalous user actions." M-21-31 specifies that "Agencies at EL1 stage shall start planning on how to best implement a user behavior analytics capability in their environment." Most UBA (also called UEBA) solutions on the market require network traffic to baseline user behavior, after which the systems can detect anomalies which may be malicious activity. The Gigamon Deep Observability Pipeline is the most efficient way to deliver network traffic to UBA/UEBA tools and allows organizations to leverage the same infrastructure used for Network-based logging for this additional capability. UEBA needs to be fed by high-fidelity, complete telemetry to avoid both false positives and false negatives.

EL1/EL2: Basic/Intermediate – Packet capture, syslog and metadata requirements

- Most efficient mechanism to capture packets across the agency and its components. Not only physical but also virtualized and containerized networks can be "tapped" to capture packets sent from/to any system or application. The Gigamon Deep Observability Pipeline uses physical taps and aggregators to solve this problem for data center environments, without any expansion or new requirement on the production network. Further, Gigamon uses cloud-native, virtualized, and/or containerized methods to capture packets from any virtualized or cloud environment, such as AWS, Azure, Google, Red Hat Open Shift, Nutanix, and VMware. In this way, an organization can ensure the ability to capture packets from any or all networks, without changing the design or implementation of any existing infrastructure
- Provides the required network-derived syslog records and metadata to meet the data requirements of EL1 (10 fields) and EL2 (4 fields)

M-21-31 EL1	EL1 Basic Requirements
Basic logging categories	Ensure EL0 has been met and maintained
Minimum logging data	Specific technical details on additional network logging
Time standards	Consistent timestamp formats across all event logs
Event forwarding	Forward logs to centralized data lake or SIEM
Protecting and validating log information	Encrypt and monitor log access
Passive DNS	Implement DNS logging
CISA and FBI access	Make logs available as needed
Logging orchestration, automation and response – planning	Start to plan how to implement manual and automated responses
User behavior monitoring – planning	Start to plan how to implement manual and automated responses
Basic centralized access	Log aggregation of all the events above including DNS

Figure 3. M-21-31 EL2 requirements that Gigamon helps aid or meet.

Fast and cost-effective implementation. While M-21-31 prescribes specific requirements, the ability to implement these in a practical manner is important. The ability to leverage investments already made in existing infrastructure, tools, and knowledge helps achieve that goal. Gigamon Deep Observability is designed to feed existing tools.

Traffic decryption is a challenge in any context and more so in virtual environments. The goal of the control is to record encrypted traffic in plane text via any means. Classic forms of decryption are friction points especially in virtual environments. Gigamon Precrpytion™ technology is an industry leading approach to capturing traffic in virtual environments before it is encrypted with no key management or complicated configurations leading to faster and cost-effective implementations. This supplements classic decrypt solutions and is the first cloud-native solution to capture traffic without the legacy friction in virtual environments whether it be on-premises or in the public cloud.

EL2: Intermediate – Traffic decryption

- Sends and decrypts packet data to the packet capture solution
- Centrally performs a "break, inspect, and fix" on all data eligible for decryption and optimizes IDS, IPS, firewall, NDR, SIEM, and DLP data before delivering it to tools
- Acquire plaintext/cleartext communications from virtualized and containerized workloads without any break-and-inspect, via Gigamon Precryption technology that leverages eBPF to acquire traffic in a secure and efficient manner from within the workload itself
- Helps maintain compliance through techniques, such as PII Masking, setting Decrypt/Do Not Decrypt policy rules, and extracting metadata from the packets without exposing PII

Inspection of Encrypted Data is a specific requirement for EL2, such that "Federal agencies shall retain and store in cleartext form the data or metadata from Appendix C that is collected in their environment." Network Traffic is required to log "Full Packet Capture Data" including decrypted plaintext and cleartext. The Gigamon Deep Observability Pipeline is the most efficient method for decryption, by decrypting once, by policy, and then utilizing the resulting (subset of) plaintext and cleartext data for packet capture for M-21-31 compliance as well as to feed all security tools for threat detection, file inspection, and other use cases. Gigamon Fabric Health Analytics enables organizations to prove compliance by showing exact health and operation of the Decryption Infrastructure, efficiency of the decryption process, any anomalies or alerts of encrypted traffic flows that may attempt to bypass decryption, historical trending, and more. In parallel with satisfying this crucial M-21-31 logging requirement, organizations will also be able to identify any outdated TLS versions still in use, weak ciphers, encrypted web traffic of concern, and more.

EL2 M-21-31	EL2 Intermediate Requirements
All EL1 requirements	All requirements for EL1 must be met
Intermediate Logging Categories	Logs categorized as Criticality Level 1 and 2 must be retained
Publication of Standardized Log Structure	Provide a document detailing the structure (schema) for those logs to CISA
Inspection of Encrypted Data	Retain and store in cleartext form the data or Metadata
Intermediate Centralized Access	Required Logs categorized as Criticality Levels 0 and 1 are accessible and visible for the highest-level security operations at the head of each agency

Figure 4. M-21-31 EL2 requirements that Gigamon helps aid or meet.

EL3: Advanced – Logging and monitoring for containerized workloads

- Provides the same set of capabilities to containerized microservices-based workloads using the GigaVUE® Universal Cloud Tap (UCT) to gain access to container log data and direct that traffic to any destination, such as a SIEM or packet capture tools

Containerized workloads can be complex to monitor for data communications. In addition to the Container cluster/pod events and other logging specified in M-21-31, all overarching logging information is still required for these workloads, including packet capture and network traffic metadata. Kubernetes and other containerized environments typically have high volumes of inter-service/container-to-container traffic which is difficult to log for M-21-31 compliance, and difficult to analyze for security concerns. MITRE ATT&CK identifies many container-specific techniques for Persistence tactics (TA0003) such as External Remote Services (T1133) and Discovery tactics (TA0007) using Network Service Discovery techniques (T1046) that may be difficult to see with our monitoring actual traffic and embedded API calls. In general, the ephemerality of containers including ever-changing IP addresses will prove a major challenge to overall M-21-31 compliance as containerized environments grow. The Gigamon Deep Observability Pipeline utilizes a Universal Cloud Tap (UCT) as part of the Gigamon Cloud Suite to completely cover and automatically scale with any containerized environment, through automation of a UCT-Controller that can acquire any traffic from any workload, by policy, no matter how fast-moving or how big it may be.

Network traffic visibility plays a critical role in aligning security operations with the requirements indicated under OBM M-21-31 mandate. By leveraging Gigamon Deep Observability Pipeline organizations enhance visibility on all network traffic that support continuous monitoring while improving threat detection and response programs. Organizations can effectively meet the cybersecurity risk management, reporting requirements and ease operational costs and deployment friction ensuring compliance with government regulations and enhancing overall security posture.

Further Gigamon Benefits

In addition to meeting M-21-31 requirements, the Gigamon Deep Observability Pipeline provides many technical and commercial advantages, including:

Cost control and reduction

Gigamon can reduce the amount of network data sent to security and network management tools by 50 to 60 percent without compromising the logging and metadata necessary to meet M-21-31 requirements. In many cases, this may mean fewer instances of your most common tools.

Security

Gigamon advanced security forensics and lateral threat detection are based on an immutable raw packet source. This assures the security, compliance, and integrity of data-in-motion and powers existing tools with context metadata, enabling them to detect and remediate issues with greater precision and speed. With the growing threat of supply chain cyberattacks, the immutable data provided by GigaVUE can help identify these types of attacks and validate trust across hybrid cloud infrastructure.

Simplicity

GigaVUE-FM, a fabric manager, provides a single pane of glass from which to manage all platforms, network feeds into tools, and workflows across hybrid cloud infrastructure, simplifying the complexity inherent in hybrid models. This helps lower the operation and maintenance (O&M) costs of security tools and frees up teams to focus on challenges and risk mitigation.

Application-level visibility

In-depth application visibility enables NetOps and SecOps teams to capture known and unknown events to detect and speed the analysis of security and performance bottlenecks, enabling consistent, high-quality customer experiences. Supporting close to 6,000 protocols, applications, and user behaviors, Application Metadata Intelligence allows detailed investigation and threat hunting, both strategically and tactically. It is the network Swiss Army knife in the incident responder's tool bag.

Secure by Design

Traditional networks are built not for security but to maximize bandwidth and minimize latency. SecOps teams need to be able to see any traffic, on any network, at any speed, and in any environment (on-premises, tactical, virtual, public cloud, deployed). Gigamon adds this capability securely and in a solution designed to meet government requirements, certified and with authority to operate.

Better alignment between teams

Enabling all tools and teams to work from the same set of high-fidelity network data and metadata reduces finger-pointing and lets teams focus on solving the real problems impacting the network and applications.

Gigamon Security Certificates:

- FIPS 140-2
- Department of Defense (DoDIN APL)
- IPv6 compliant
- NIAP Common Criteria
- Trade Agreement Act (TAA) compliant
- Conforms with OMB M-22-18 on secure software supply chain and secure software development.

Gigamon Authority to Operate in Networks:

- Federal Civilian Agencies
- Department of Defense
- Intelligence Community

Contracting Information:

- General Service Administration (GSA) Schedule 70
- NASA's Solutions for Enterprise-Wide Procurement (SWEP)
- CAGE: 4XKN9
- DUNS: 362737251

About Gigamon

Gigamon offers a deep observability pipeline that harnesses actionable network-derived intelligence to amplify the power of observability tools. This powerful combination helps IT organizations to assure security and compliance governance, speed root-cause analysis of performance bottlenecks, and lower operational overhead associated with managing hybrid and multi-cloud IT infrastructures. The result: Modern enterprises realize the full transformational promise of the cloud. Gigamon serves more than 4,000 customers worldwide, including over 80 percent of Fortune 100 enterprises, 9 of the 10 largest mobile network providers, and hundreds of governments and educational organizations worldwide. To learn more, please visit gigamon.com.

Gigamon®

Worldwide Headquarters
3300 Olcott Street, Santa Clara, CA 95054 USA
+1 (408) 831-4000 | gigamon.com

07.24_03