White Paper

# How Corelight's uniform network visibility helps agencies comply with OMB M-21-31

The Office of Management and Budget (OMB) recently issued M-21-31,[1] a landmark cybersecurity memo that creates a maturity model for event log management and sets agency implementation requirements with specific compliance timelines. In the months ahead federal agencies must demonstrate continued advancement along this maturity curve and reach the ultimate "advanced" tier stage within two years. Corelight stands ready and willing to help shepherd organizations through each step of this data-driven journey with the delivery of uniform and uncompromising network logs and insights.

| Tier | Rating | Compliance | Description |
|---|---|---|---|
| EL0 | Not Effective | 60 days to assess | Logging requirements of highest criticality either not met or only partially met |
| EL1 | Basic | 1 year | Only logging requirements of highest criticality are met |
| EL2 | Intermediate | 18 months | Logging requirements of highest and intermediate criticality are met |
| EL3 | Advanced | 2 year | Logging requirements at all criticality levels are met |

The OMB memo rightly observes that "information from logs on Federal information systems is invaluable in the detection, investigation, and remediation of cyber threats." While endpoint logs offer a critical source of information, organizations who single thread their operational awareness on endpoints do so at their peril. Endpoints offer excellent depth of information, but that depth does not reach where endpoint agents cannot go, such as BYOD or cloud, and that depth is rendered meaningless when adversaries succeed in compromising the endpoints themselves.

Comprehensive network monitoring can address the security gaps left by endpoint technology and help organizations achieve log management compliance with OMB M-21-31 at all stages of the maturity model. No matter the environment, nearly all cyberattacks must communicate over networks and organizations that can silently capture, analyze, and store those communications gain an immutable record of malicious activity. Unlike endpoints, the network cannot lie.

The attacks on SolarWinds cited on the first page of the OMB memo provide strong evidence for these claims. Consider that the SolarWinds attack specifically looked for the presence of EDR agents in the target environment to inform evasive maneuvers. What the attack couldn't avoid, however, was communicating over the network. While it took pains to obfuscate and disguise the nature of its communications, it ultimately left indelible evidence of its activity for organizations with comprehensive network logging capabilities in place. The Mandiant research team that discovered these attacks was able to do so in part because they had these network monitoring capabilities on hand, a fact publicly acknowledged by one of the researchers involved in the investigation who credited[2] the open source technology on which Corelight runs.

**How Corelight helps**

The OMB memo addresses a fundamental event logging problem in the security space: the systems generating logs have traditionally operated in isolation from one another with little or no regard for standardization. Rather than conversing easily in a lingua franca, security teams must instead confront disparate logs and formats in their attempt to form an operational picture of their environment. It's no wonder federal agencies have struggled to share information amongst themselves, much less deduce the ground truth in their own environments. The very root of the problem is one of holistic information design.

From the beginning Corelight focused on building a unified security platform to address these issues by adhering to key principles of information design for security teams. At Corelight, we believe data produced should be:

- **Uniform in format**—security analysts, automation tools, and machine learning algorithms need clean, consistent data formats to make quick judgment calls, convict and remediate threats with confidence, and train detection models.

- **Purpose-built for security**— the data should be designed for security use cases to avoid the pitfalls of common telemetry sources intended for IT and compliance. Their data collection biases leave gaping security visibility holes behind.

- **Resistant to compromise**— — adversaries will attempt to muddle the "operational picture" by compromising upstream telemetry, up to and including generating false information from hijacked sources.

- **Designed for interoperability**— information collected should interoperate with tools and complementary data sources to facilitate fast correlations for analysis and investigation tasks.

Corelight can help agencies advance through each stage of the log management journey outlined in the OMB memo and reach the highest levels of EL maturity through our Open Network Detection and Response (NDR) platform. Corelight's platform delivers comprehensive network logging across dozens of protocols with pre-built SIEM integrations, targeted packet capture capabilities, and actionable security insights and threat detections across both on premise networks and cloud environments. The following

tables document requirements of the maturity model and demonstrate where Corelight can equip agencies with the logging and insight capabilities to advance to the next stage of compliance:

| Maturity | Requirement | Corelight's Mapping |
|---|---|---|
| EL0 | Criticality 0 Log | Network Device Infrastructure [All Devices: DHCP]<br>Network Device Infrastructure [DNS]<br>Network Device Infrastructure [Passive DNS]<br>Network Device Infrastructure (General Logging) [IDS; NDR; Network flow; DNS query/response; PCAP]<br>Network Device Infrastructure [Load Balancer/Reverse Proxy]<br>Network Device Infrastructure [Proxies and Web Content Filters]<br>Cloud Environments (General Logging) [IDS; NDR; Flow; DNS query/response]<br>Cloud AWS [AWS Cloudtrail; Amazon VPC Flow logs] |

To move beyond an Event Logging 0 (EL0) maturity, agencies need a comprehensive network monitoring solution to capture network flows for event correlation. Corelight's Open NDR platform allows organizations to meet the requirements and avoid being locked into a proprietary data format since Corelight's open source data format is widely accepted by major security tools. In one federal organization Corelight replaced nine different network data sources that took over three years to on-board in a SIEM. By comparison, getting Corelight logs into the SIEM took fewer than three months.

| Maturity | Requirement | Corelight's Mapping |
|---|---|---|
| EL1 | Minimum logging data | With its comprehensive logging fields, JSON key-value pair format, and published log standards, Corelight ensures that agencies meet the logging minimums for network data. Going beyond the minimum, though, Corelight's Community ID allows its data to integrate across disparate datasets and supporting tools with a unique event identifier. |
| | Time standard | Corelight supports centralized timing to ensure that all network data logs collected have a unifying, correlated timestamp with microsecond accuracy. |
| | Event forwarding | Send filtered Corelight log data to SIEMs and send an unfiltered copy to long term storage sources (e.g. S3, data lake, SAN, etc.). |
| | Passive DNS | Network-based, passive DNS monitoring paired with DNS logs provide unparalleled visibility into DNS requests. Alerts to highlight direct IP connections without preceding DNS lookups that a DNS system would be blind to. |
| | Logging orchestration, automation, and response planning | Automation gives defenders a scalable, iterative way to build and sustain the strategic advantage. With SOAR playbooks[3] powered by Corelight network data, you can finally manage your workload, empower your team, and focus on high-priority work. |
| | User behavior monitoring - planning | Splunk CDM (Common Data Model) and Elastic ECS (Elastic Common Schema) mappings for day 0 utility of Corelight data to feed UEBA processes. |

As agencies advance to the EL1 maturity model, the utility of the network logs that Corelight produces increases. The journey through EL1 emphasizes the requirement to centrally store network data and to follow common SIEM data standards. Corelight has a data-first strategy and believes customer data should not be stuck in a closed-source, proprietary system. Corelight supports common data schemas for the leading SIEMs including the Splunk Common Information Model (CIM)[4] and Elastic Common Schema (ECS). Moreover, this normalized network data set is well suited for UEBA modeling. Whether an agency has an existing SIEM or is looking to transition to one as part of their EL maturity plan, Corelight Sensors can concurrently feed multiple data stores or cloud endpoints. This allows agencies that may need to transition SIEMs to meet the OMB memo without operational impact, or enable agencies to meet the centralized logging mandate while allowing for a two-tier logging design.

| Maturity | Requirement | Corelight's Mapping |
|---|---|---|
| EL2 | Criticality 1 and 2 logs | Application Level [Web Applications: PCAP plaintext HTTP]<br>Network Traffic [Full Packet Capture: decrypted plaintext and cleartext] |
| | Standardized log structure | All Corelight logs are based on a published standard and agencies can extend the logs to suit their needs. |
| | Inspection of encrypted data | Corelight supports encrypted traffic capture as well as unencrypted traffic. Corelight's Encrypted Traffic Collection allows for deep insights into encrypted traffic when proxying or break/inspect solutions are not in place. |

For those agencies that have used network data to build and sustain a strategic advantage, leveraging Corelight's Encrypted Traffic Collection (ETC)[5] and Smart PCAP capability[6] easily allow agencies to advance to EL2 maturity. Corelight's ETC is a series of detections and data enrichments created by the Corelight research team, Corelight Labs, to maximize network knowledge, even when the traffic is encrypted. With Smart PCAP, agencies can surgically decide which traffic profiles need to be enhanced with packet captures. For example, when matching traffic is seen—based on deep packet inspection—not only are the rich Zeek data logs created, but a correlated packet capture is made, linked to the logged traffic, allowing for easy one-click pivoting in a SIEM. This ensures analysts can have what they need without having to sift through expansive, packet archives and allows for longer targeted PCAP retention times, rather than paying to cast wide PCAP nets with limited utility. These features, in combination, will enable agencies to capture cleartext and plaintext traffic across their data flows, regardless of the communication port, and provide the maximum amount of knowledge on flows that are encrypted.

| Maturity | Requirement | Corelight's Mapping |
|---|---|---|
| EL3 | Criticality 3 logs | Virtual infrastructure monitoring |
| | Logging orchestration, automation, and response - finalizing implementation | Leveraging an open source data format allows defenders to more easily share playbooks and gain the upperhand on adversaries by leveraging a widely-known, documented, and used data format. |
| | User behavior monitoring - finalizing implementation | Corelight's insight capabilities include detection of issues such asprivileged-user compromise (e.g., Corelight's RDP brute forcing detection) and lateral movement of threat actors (e.g., the MITRE BZAR script). |

For agencies that have capitalized on Corelight's capabilities to attain EL2 maturity and are heading towards EL3, Corelight's Software Sensor[7] expands logging to include not only physical networks, but also virtual infrastructure and, most importantly, container-based networks. This ensures agencies have a unified logging source across their physical networks, virtual networks, microservice networks, and beyond. If your agency is looking to reach EL3 maturity in the shortest time horizon, Corelight is ready to assist.

[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] https://twitter.com/srunnels/status/1338329916304199680

[3] https://corelight.com/integrations/soar-playbooks/

[4] https://corelight.com/blog/maximize-your-splunk-es-investment-with-corelight

[5] https://corelight.com/products/collections/encrypted-traffic

[6] https://corelight.com/products/smart-pcap

[7] https://corelight.com/products/software-sensor/