securonix

SOLUTION BRIEF

Event Logging Maturity for Federal Agencies

Meeting the OMB Memo M-21-31 2023 Implementation Deadline

Problem Statement Title

The U.S. Office of Management and Budget (OMB) published a memorandum on August 27, 2021 outlining security event management requirements for federal agencies. The memo mandates a 24-month implementation deadline and expands upon Executive Order 14028, "Improving the Nation's Cybersecurity" that the White House released on May 12, 2021. The memo describes a maturity model with four tiers, EL0 to EL3, each tier incrementally expanding the scope of event collection and adding further required capabilities.

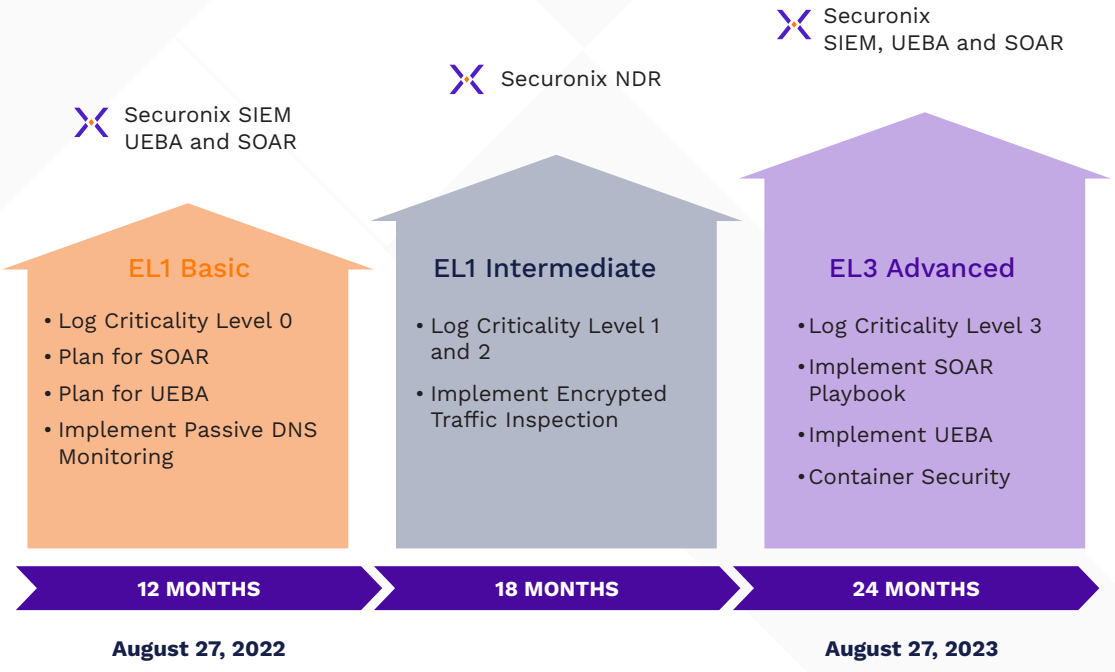
To achieve the ambitious timeframe, federal agencies cannot afford to experiment. Instead, they must adopt technologies that deliver a high level of out-of-the-box support for all requirements, integrate all required functions, and are proven to scale. Securonix is the only solution in the industry that fully meets those needs.

Cloud-Native SIEM With UEBA and SOAR

Built on big data, Securonix Next-Gen SIEM combines log management; user and entity behavior analytics (UEBA); and security orchestration, automation, and response (SOAR) into a complete, end-to-end security operations platform. It collects massive volumes of data in real time, uses patented machine learning algorithms to detect advanced threats and provides security incident response capabilities for fast remediation.

Our cloud-native SIEM assists federal agencies in progressing through all levels of the Event Logging Maturity Model (ELMM) to attain the EL3 Maturity Tier within the 24-month timeframe. The solution meets all critical criteria for User Behavior Analytics, SIEM, and SOAR in a single platform offered from a cloud-based certified FEDRAMP Moderate1, HIGH2, and DoD SRG IL–53 environment, including:

- Out-of-the-box support for minimum logging data, time standards, event forwarding, and protecting and validating data.
- Granular role-based access with 2FA for centralized access at an agency level.
- Combines SIEM and UEBA into a single unified platform.
- Network traffic analysis and SOAR add-ons seamlessly extend the platform.
- Rich set of usable content such as UEBA threat models and SOAR playbooks.
- Easily scales to years of data retention, including with Amazon AWS and Snowflake.



Securonix Next-Gen SIEM helps agencies achieve EL3 maturity within the 24-month timeframe

Benefits for Federal Agencies Implementing the ELMM

Covers Federal Compliance Mandates

Securonix covers FedRAMP Moderate[1], FedRAMP HIGH[2], and DoD SRG IL-5[3] certification.

Achieves EL0, EL1, EL2, and EL3

Meets all ELMM requirements within a single solution, including SOAR and UEBA.

Detect and Respond to Threats

Discover hidden threats using the ability to easily search on historical data as well as ability to act on real-time, streaming data.

Why Securonix?

Take a smarter approach to combating advanced threats with an analytics-based SIEM built for modernizing the government agency. Our cloud-native platform provides on-demand scaling as well as the architecture resiliency.

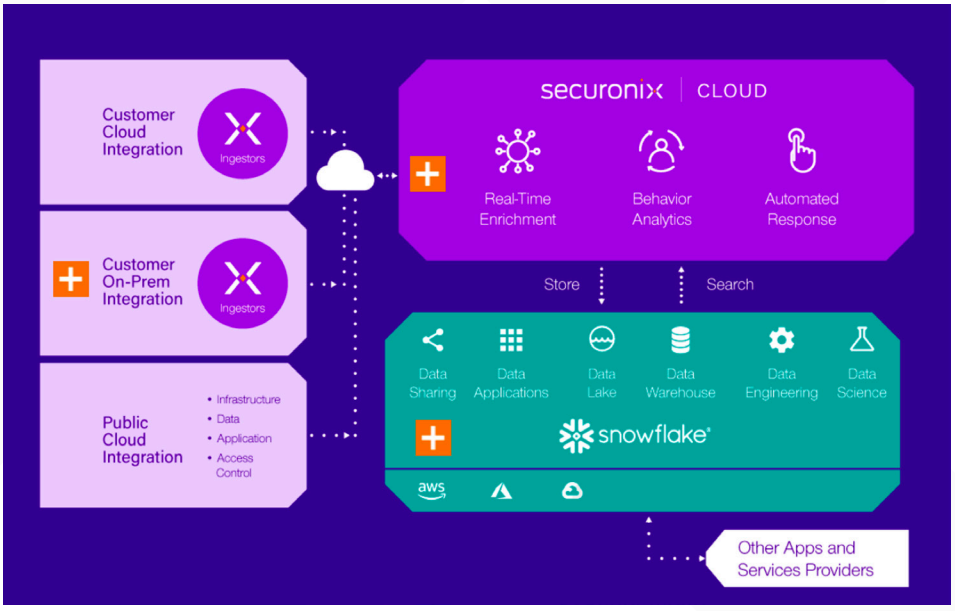
Securonix provides turnkey advanced analytics to detect and thwart complex threats.

Our approach to machine learning, context enrichment, and user risk scoring uncovers complex threats with minimal noise. Our UEBA has built-in proprietary machine learning to identify advanced and insider threats accurately. To automate incident response, Securonix SOAR provides fully configurable playbooks, letting you respond to threats at scale with less manual effort.

Securonix's world-class Threat Labs team provides substantial threat research and the latest use case content. We bring out-of-the-box (OOTB) threat material to your platform as an extension of your security operations center (SOC). Lastly, our SIEM is designed on an open and modular architecture, allowing you to select the deployment option that best suits your SOC operating model.

XDR and traditional SIEM solutions only retain data available for live search for short periods of time. They aren't effective in detecting threats with long dwell and hibernation times.

Our Security Data Lake is designed to meet long term data retention requirements. Furthermore, Snowflake users may also take advantage of the joint solution Securonix + Snowflake to save even more money on data storage.



Comprehensive Security Analytics and Operations Platform

[1]Fedramp Moderate: In-Process, With Ato Slated For 8/22

[2]Fedramp, High: Ato Slated For 12/22

[3]Dod Srg Il-5: Ato Slated For 12/22 Environments

About Securonix

Securonix is redefining SIEM for today's hybrid cloud, data-driven enterprise. Built on big data architecture, Securonix delivers SIEM, UEBA, XDR, SOAR, Security Data Lake, NDR and vertical-specific applications as a pure SaaS solution with unlimited scalability and no infrastructure cost. Securonix reduces noise and prioritizes high fidelity alerts with behavioral analytics technology that pioneered the UEBA category. For more information visit securonix.com

For more information about Securonix solutions for the federal market, contact fedsalesteam@securonix.com