SECURONIX™

SOLUTION BRIEF

Securonix Event Logging Maturity for Federal Agencies

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

The U.S. Office of Management and Budget (OMB) published a memorandum on August 27th 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 the 12th of May. The memo describes a maturity model with four tiers, Event Logging (EL) 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.

Securonix Cloud-Native SIEM With UEBA and SOAR

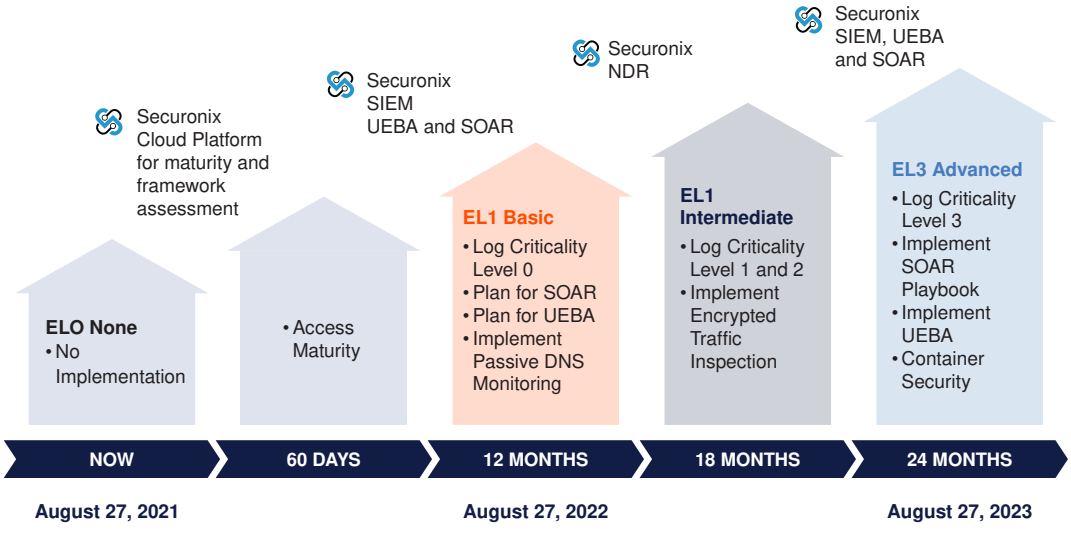
Built on big data, Securonix Next-Gen SIEM combines log management, user and entity behavior analytics (UEBA), and security orchestration, automation, and response (SOAR) into a complete, end-to-end security operations platform. It collects massive volumes of data in real time, uses patented machine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

Our cloud-native SIEM supports federal agencies in progressing through all Event Logging Maturity Model (ELMM) levels to ultimately achieve the EL3 Maturity Tier in the mandated 24-month timeframe. The solution meets all critical requirements for User Behavior Analytics, SIEM, and SOAR, all in a single platform delivered from a cloud-based certified FEDRAMP Moderate[1], HIGH[2], and DoD SRG IL–5[3] environment including:

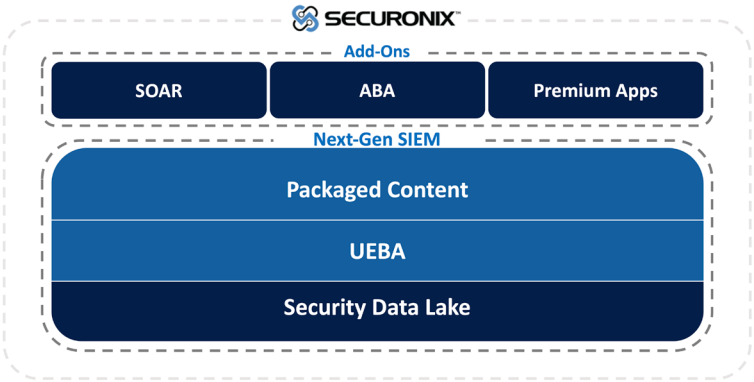
- Out-of-the-box support for minimum logging data, time standards, event forwarding, and protecting and validating data.
- Granular role-based access with 2FA for centralized access at an agency level.
- Combines SIEM and UEBA into a single unified platform.
- Network traffic analysis and SOAR add-ons 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.

Benefits for Federal Agencies Implementing the ELMM

- Scales with FEDRAMP Moderate[1], HIGH[2], and DoD SRG IL-5[3] certification.
- Meets all requirements with proven technology from a single provider, including SOAR and UEBA.
- Retains years' worth of data available for live search without limitations due to licensing or architecture.
- Beats the EL3 deadline for UEBA and SOAR with customizable out-of-the-box content like playbooks for diverse use cases and threat scenarios.



Product Features

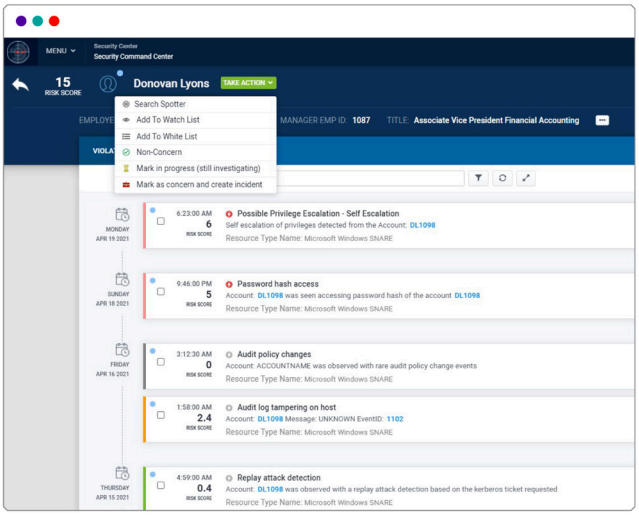


Comprehensive and Integrated Security Analytics and Operations Platform

Massively scalable open data platform that can ingest hundreds of terabytes per day.

Built-in UEBA with patented machine learning that accurately detects advanced and insider threats.

SOAR delivers fully customizable playbooks to automate incident response.

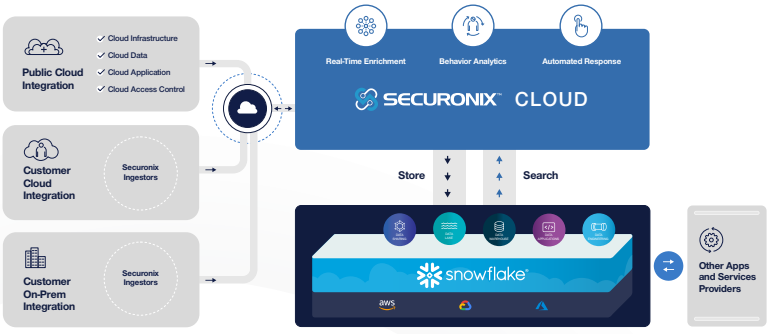


Incident Response and Threat Hunting

Blazing-fast threat hunting using natural language search and visual pivoting means you don't have to learn a new language to search and threat hunt.

An investigation workbench allows you to rapidly investigate incidents by pivoting on anomalous entities and tracing associated activities.

Response Bot gives you AI-based recommendations of remediation actions based on previous incidents.



Scalable Data Retention of Long-Term Historical Data for Live Search and Analysis

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 can benefit from our "Bring your own Snowflake" program to further save on cost of data storage.

For more information about Securonix, schedule a demo at www.securonix.com/request-a-demo.

About Securonix

Securonix transforms enterprise security with actionable intelligence. Using a purpose-built security analytics platform Securonix quickly and accurately detects high-risk threats to your organization. For more information visit www.securonix.com.

[1]FEDRAMP Moderate: In-process, with ATO slated for 2/22
[2]FEDRamp, HIGH: ATO slated for 4/22
[3]DoD SRG IL-5: ATO slated for 5/22 environments

SECURONIX

LEARN MORE
www.securonix.com

LET'S TALK
+1 (310) 641-1000
info@securonix.com