INSIGHTS | SOLUTION BRIEF

Goodbye SIEM: Achieve Next-Gen SOC Automation With WEI & Cortex XSIAM

An advocate of Cortex XSIAM since its 2022 inception, WEI can guide the migration of your SIEM environment to XSIAM to automate the capabilities of a modern SOC.

Palo Alto Networks has announced an agreement to acquire IBM's QRadar software-as-a-service (SaaS) assets, focusing on QRadar's customer base. After contractual obligations conclude, **IBM QRadar SaaS customers will either migrate to the Palo Alto Networks' Cortex eXtended Security Intelligence Automation Management (XSIAM) platform or find another SIEM vendor.**

As you oversee your current SIEM environment, we understand that you may be rethinking your approach to SecOps and wondering if Cortex XSIAM is the ideal solution. A believer in XSIAM since its debut in 2022, WEI has the proven expertise to guide your enterprise into this next-gen SOC platform.

SIEM No Longer Scales Effectively In The Modern SOC

Traditional SIEM platforms such as QRadar, Splunk, and Exabeam/LogRhythym face an uphill climb as they struggle in the era of next-gen SOC automation. Legacy SIEM is designed for analysts to intake and process human-readable alerts, which represent only a small fraction of the data. This approach limits detection, investigation, analytics, and automation capabilities to pre-processed, pre-filtered, and pre-prioritized alerts. This method is insufficient for comprehensive security coverage.

- **High Costs:** Implementing and maintaining a SIEM system is expensive and complex. This includes costs related to hardware, software licenses, and skilled personnel.
- **Scalability Issues:** As organizations grow, performance bottlenecks and frequent upgrades are required due to the increased volume of data that legacy SIEM systems handle.
- **Integration Challenges:** Legacy SIEM systems collect data from a wide variety of sources, leading to eventual compatibility issues with existing IT infrastructure.

Improved Outcomes With Cortex XSIAM

- Detection accuracy with native AI and ML models
- Extend SOC visibility and control
- Decrease time to detect and respond with automation playbooks
- MITRE ATT&CK framework alignment
- Comprehensive incident management designed to optimize SOC workflow

Substantial Cost Savings

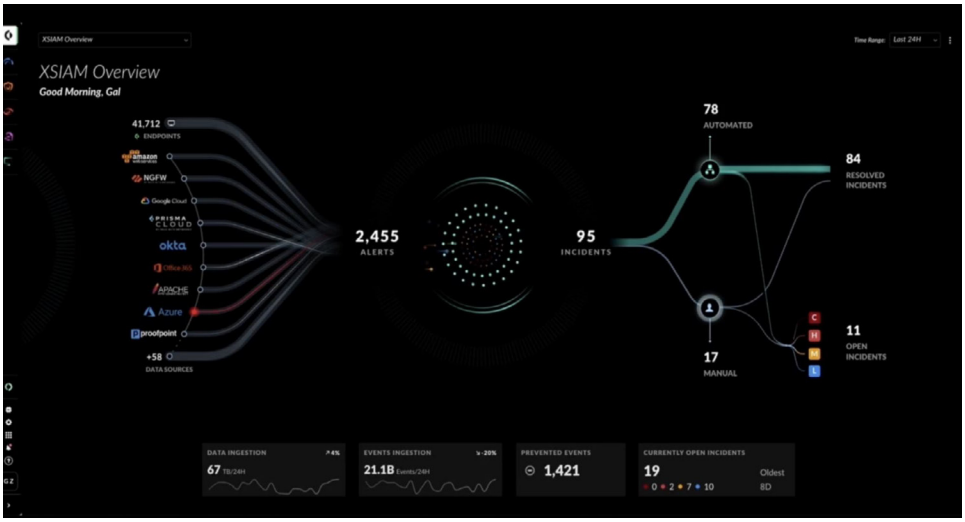
- Consolidate disparate SOC tools
- Leverage existing sensors
- Reduce SIEM storage, compute, and endpoint footprint
- Built-in analytics and automation

Achieve A Left of Bang Approach With WEI & Cortex XSIAM

As WEI's certified cyber experts have believed in XSIAM's next-gen capabilities since day one, the platform offers a unified, automated, and predictive approach to the modern SOC. This correlates with WEI's belief in the cyber posture of being "Left of Bang" – **a proactive cybersecurity approach designed to bolster incident detection and response by helping IT teams effectively identify and address threats.**

Cortex XSIAM simplifies architecture by integrating data and analytics across network, endpoint, cloud, and identity sources, leveraging existing sensors and providing a single interface with built-in automation and case management. This approach proactively addresses security gaps by utilizing AI and ML, enabling SOCs to handle massive data volumes efficiently and better positioning analysts to make critical decisions. XSIAM enhances traditional SOC operations by transforming detection, investigation, and response processes. **Its SOC stack capabilities include:**

- **SIEM:** Includes log management, correlation and alerting, compliance reporting,* and other common SIEM functions.
- **Extended Detection and Response (XDR)**: Integrates endpoint, cloud, network, and third-party telemetry for automated detection and response.
- **Endpoint Detection and Response (EDR):** Includes a complete endpoint agent and cloud analytics backend to provide endpoint threat prevention, automated response, and in-depth telemetry useful for any threat investigation.
- **User and Entity Behavior Analytics (UEBA):** Uses machine learning and behavioral analysis to profile users and entities and alert on behaviors that may indicate a compromised account or malicious insider.
- **Security Orchestration, Automation, and Response (SOAR):** Includes a robust SOAR module and marketplace to create and orchestrate playbooks for use with Cortex XSIAM.
- **Cloud Detection and Response (CDR):** The Cortex XSIAM analytics array includes specialty analytics designed to detect and alert on anomalies in cloud data, such as cloud service provider logs and cloud security product alerts.
- **Management, Reporting, and Compliance:** Centralized management functions simplify operations. Powerful graphical reporting capabilities support reporting for compliance, data ingestion, incident trends, SOC performance metrics, and more.



In Cortex XSIAM, monitor security operations with a new visualization of the entire SOC workflow.

Talk To WEI Today

Our certified experts help customers centralize, automate, and scale operations to better protect their organizations. We can test and benchmark your current solution against XSIAM's capabilities and offer consultation on Incident Response processes. We can also develop customized playbooks and content packs to help automate typically mundane analyst's activities and response processes.

Contact our security team today for a product demonstration. Discover how Cortex XSIAM can effectively pivot your enterprise toward an AI-driven architecture with business outcomes in mind.

REQUEST CONSULT

43 Northwestern Drive, Salem, NH 03079
(800) 296-7837
Visit wei.com