DATASHEET

CRITICAL**START**® Security Services for SIEM

Reduce risk acceptance, resolve every alert, and maximize your SIEM investment.

KEY BENEFITS

- ✓ Proactive identification and resolution of SIEM coverage gaps
- ✓ Contractual Service Level Agreements (**SLAs**) of 10-minute notifications for Critical alerts and 60-minute or less Median Time to Resolution (**MTTR**) for ALL alerts, regardless of priority
- ✓ **24x7x365** real-time threat detection, response, and visibility via MOBILE**SOC**®
- ✓ **NIST CSF** maturity and **MITRE ATT&CK**® **Framework** coverage
- ✓ Provable metrics, peer benchmarking, and best practices for risk insights
- ✓ Reduce Total Cost of Ownership (**TCO**), increase Return on Investment (**ROI**), and improve team productivity
- ✓ Optimize SIEM configuration and management with **24x7x365** remote performance, availability, and capacity monitoring
- ✓ Health monitoring, Zero-Log Ingest Alerts, and Ingest Cost Analysis*

Eliminate SIEM complexity and reduce risk

Alert overload leads to missed threats, business disruption, and an inability to maximize Security Information and Event Management (**SIEM**) investments. Yet deploying and managing a SIEM creates significant complexity, resulting in more alerts than your team can handle and hindering threat detection and response if not correctly configured.

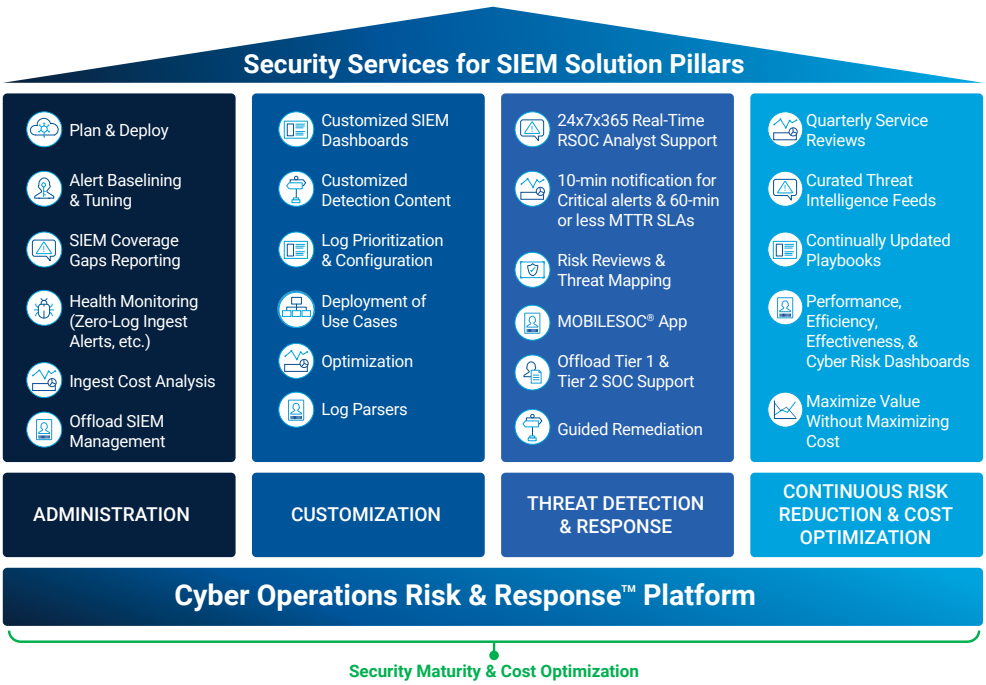
Critical Start Security Services for SIEM optimize environments for threat detection and accelerated response by simplifying operations, proactively identifying coverage gaps, and ensuring security-relevant logs are prioritized and properly ingested.

How it works

We provide Managed Detection and Response (**MDR**) for SIEM and Managed SIEM as one service for a comprehensive approach to SIEM administration and cybersecurity defense. Our experts fine-tune your SIEM environment by prioritizing relevant data sources, customizing detections, and streamlining response workflows. We proactively identify and resolve potential visibility gaps to maintain continuous coverage for threat detection.

Advanced analytics suppress false positives, enabling your team to focus on priority incidents. Our **24x7x365** Risk & Security Operations Center (**RSOC**) analysts accelerate response to validated threats by providing expert, on-the-go guidance via our MOBILE**SOC**® app and recommending **MITRE ATT&CK**®-based mitigations to prevent recurrence.

Customizable dashboards and transparent reporting provide visibility into activity trends, system health, team productivity, and compliance. By integrating leading SIEM platforms like **Microsoft® Sentinel, Splunk Cloud™, Splunk ES,** and **Sumo Logic®** with our purpose-built Trusted Behavior Registry® (**TBR®**), our proprietary **Cyber Operations Risk & Response™ platform**, and human-led expertise, Critical Start reduces complexity and risk while maximizing the value of your security resources. *(Fig 1)*



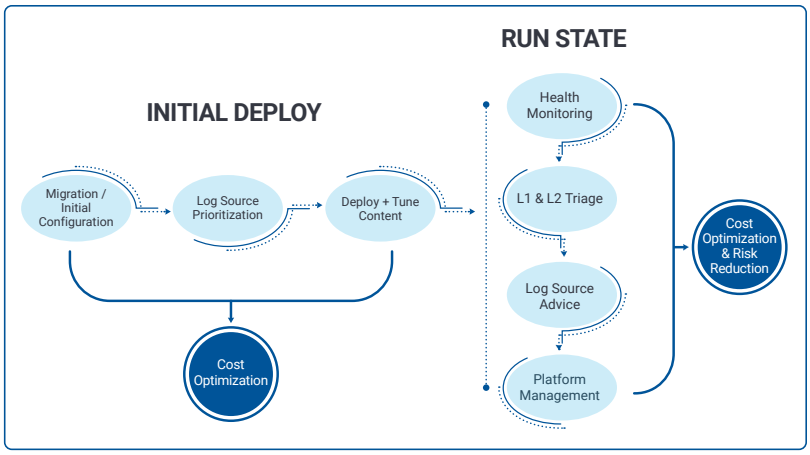
(Fig 1) The most cost-effective way to stop business disruption

Reduce complexity, increase visibility

The SIEM expertise needed to prioritize log sources for the best threat-centric outcomes is hard to come by. We augment your security team with seasoned experts available to adjust your SIEM as your needs change, ensuring you always have the most comprehensive compliance and threat detection coverage.

We prioritize data into three tiers based on **MITRE ATT&CK® Framework** coverage and what we have observed with other customers to protect you against the latest attacker Techniques, Tactics, and Procedures (**TTPs**). Then, we use **MITRE ATT&CK® Mitigations** Recommendations to prevent attacks that have already occurred from happening again.

We continue to help you minimize costs and maximize the value of your investment by relieving you of the burden of back-end maintenance (including version updates and application performance) and performing **Quarterly Service Reviews**, health checks, and resolution of visibility gaps to ensure your SIEM is always correctly configured and optimized. *(Fig 2)*



(Fig 2) Your entire SIEM program with Critical Start

(Fig 3) Custom dashboards for provable ROI

Eliminate false positives and stop business disruption

Gain insights into security gaps and see fewer false positives over time while still being able to add more log source feeds with threat detection content that turns your data into meaningful alerts. Confirm you're achieving better security and optimization outcomes with detailed dashboards and reports that provide the in-depth visibility and trend data you need to prove your ROI.

We manage Indicators of Compromise (**IOCs**) while our platform and TBR automate the investigation and triage of alerts to remove false positives, simplifying breach prevention and ensuring the most effective detection and response to cyberattacks per dollar invested.

Take advantage of direct collaboration with our skilled security analysts to help you make better response decisions and feel more secure with **24x7x365** monitoring, rapid investigation, continuous threat hunting, and two-person integrity on every action taken. *(Fig 3)*

Key Features of Critical Start Security Services for SIEM:

- Threat monitoring and investigation
- Guided response recommendations
- First- and third-party remediation actions
- Proactive identification and resolution of SIEM coverage gaps
- **Risk-Ranked Reduction Recommendations**
- **MITRE ATT&CK® Mitigations Recommendations**
- Optimization reviews (includes Ingest Cost Analysis*)
- Health monitoring (includes Zero-Log Ingest Alerts)
- Proprietary detections and IOCs
- Operationalized threat intelligence

*Sumo Logic and Microsoft Sentinel customers receive an ingest cost analysis to analyze billing vs. ingest for specific data sources based on security products and licenses.

Critical Start Security Services for SIEM

Critical Start Security Services for SIEM deliver cost-effective and comprehensive threat detection and response services and optimize the performance of leading SIEM platforms by reducing complexity and resolving every alert. Consider partnering with Critical Start to secure your business from the ever-evolving threat landscape by advancing, scaling, and maturing your cybersecurity capabilities over time.

Click here to contact us for more information about Critical Start Security Services for SIEM

CRITICALSTART®