DATASHEET

CRITICAL**START**® SIEM Security Suite
Reduce risk acceptance, resolve every alert and maximize your SIEM investment

KEY BENEFITS

- ✓ **1-hour** Time to Detection (**TTD**) and Median Time to Resolution (**MTTR**) **SLA** for every alert
- ✓ **24/7/365** 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
- ✓ Reduced Total Cost of Ownership (**TCO**) and improved team productivity
- ✓ Streamlined SIEM management with **24/7/365** remote performance, availability and capacity monitoring

*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.

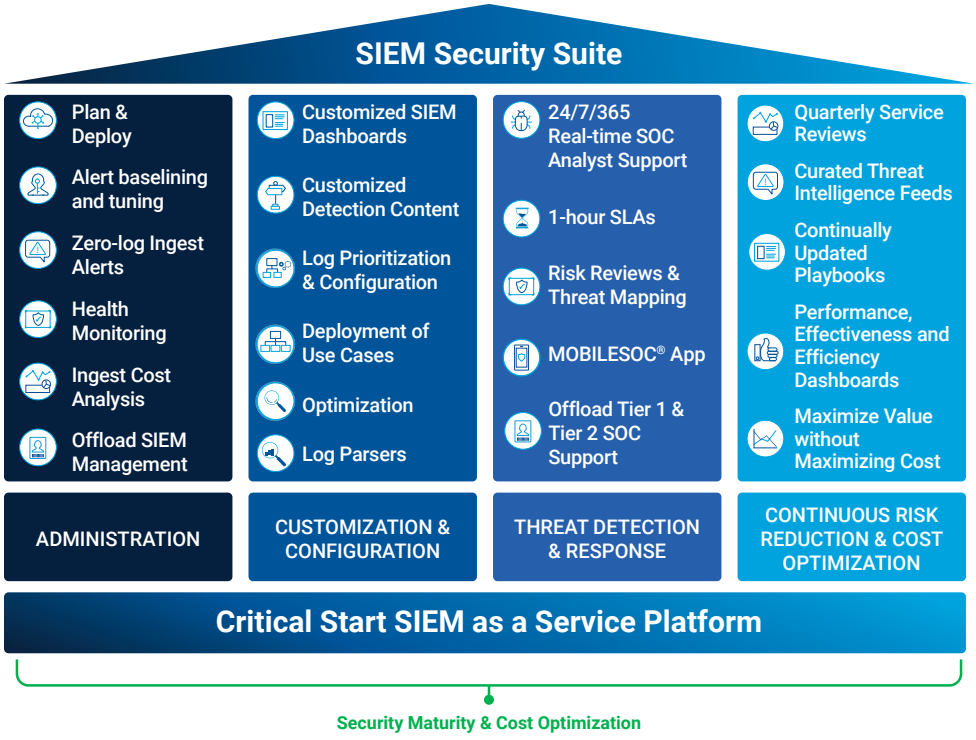
Fully optimize the operating potential of your Security Information and Event Management (**SIEM**) system and maximize your security posture with the **Critical Start SIEM Security Suite**: a single solution giving you complete access to our **Managed SIEM and Managed Detection and Response (MDR) for SIEM** services.

How it works

Critical Start SIEM Security Suite brings together pro-active SIEM management with the industry's only purpose-built **Trusted Behavior Registry®** (**TBR**) and our proprietary **Zero-Trust Analytics Platform®** (**ZTAP®**) to reduce complexity and resolve all alerts.

We help our customers achieve the full operating potential of their SIEM investments for increased cost optimization and better threat detection. Then we use our trust-oriented approach to MDR to investigate and respond to threats specific to your organization, regardless of criticality.

Our **SIEM Security Suite** integrates with leading SIEM platforms, including **Microsoft® Sentinel, Splunk Cloud™** and **Sumo Logic®**, to bring you continued risk reduction and the most effective threat detection and response solution per dollar invested. *(Fig 1)*



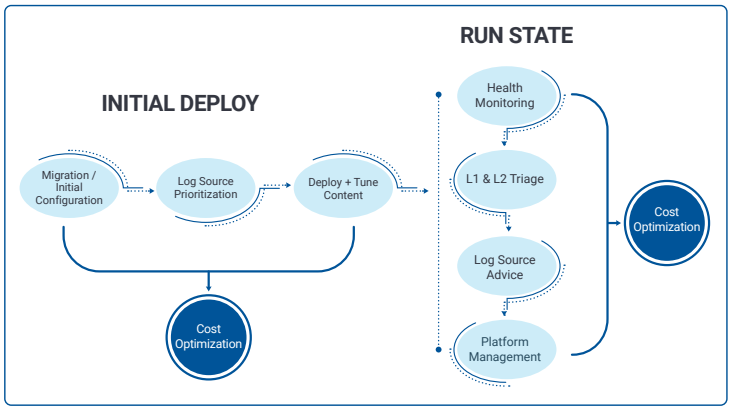
(Fig 1) The most cost-effective way to stop business disruption

Reduce complexity, increase visibility

Customers don't always have the SIEM expertise to prioritize log sources for the best threat-centric outcomes and make adjustments as their needs change, compromising their compliance and threat detection coverage.

We simplify this process by prioritizing data 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 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** 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 insight into security gaps and achieve better outcomes with threat detection content that turns your data into meaningful alerts. Leverage detailed dashboards and reports to provide the in-depth visibility and trend data you need to prove your ROI.

The Critical Start **Threat Navigator** manages Indicators of Compromise (**IOCs**) while our ZTAP 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.

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 SIEM Security Suite:

- Log prioritization
- Custom content and configuration
- Operational monitoring
- Platform management
- Optimization review (includes Ingest Cost Analysis*)
- Threat monitoring and investigation
- Guided response recommendations
- First- and third-party remediation actions
- Operationalized threat intelligence
- Proprietary detections and IOCs

*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 SIEM Security Suite

The **Critical Start SIEM Security Suite** optimizes the performance of leading SIEM platforms, delivering cost-effective and comprehensive threat detection and response services 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 SIEM Security Suite