DATASHEET

CRITICAL**START**® Managed SIEM Services
Achieve the full operating potential of your SIEM investment

KEY BENEFITS

- ✓ Reduce total cost of ownership (**TCO**)
- ✓ Streamline SIEM management with 24/7/365 remote performance, availability and capacity monitoring
- ✓ Optimize SIEM for complete coverage of threat detection use cases
- ✓ Strengthen security posture with improved data-driven threat detection
- ✓ Maximize team productivity with better allocation of in-house responsibilities
- ✓ Proactively detect potential data ingestion issues*
- ✓ Simplify architecture and deployment of SIEM

Better threat detection and prevention

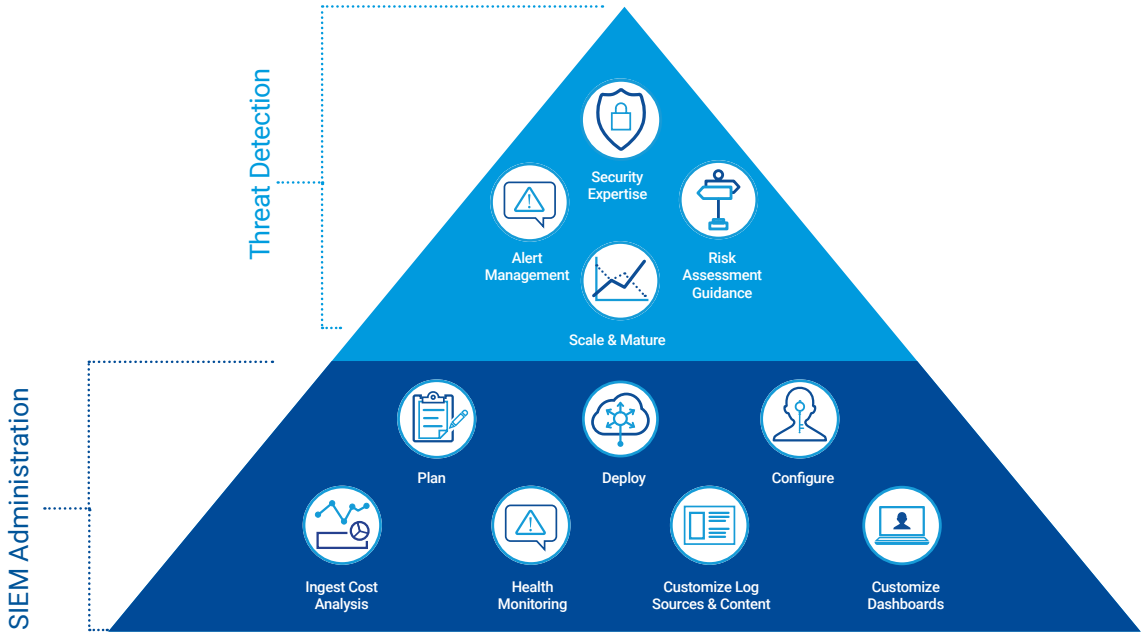
Revitalize your Security Information and Event Management (**SIEM**) system and go from a cost center delivering suboptimal outcomes to a value-added solution that provides better threat detection and prevention across your organization.

Integrating with Microsoft® Sentinel, Splunk Cloud™ and Sumo Logic®, Critical Start Managed SIEM maximizes your ROI and holistically improves your security and compliance posture by closing security-awareness gaps, increasing breach resiliency and expanding the reach of your team.

How it works

Critical Start helps you minimize costs and maximize the value of your investment by taking responsibility for the back-end components of your SIEM solution and relieving you of the burden of maintaining your application. *(Fig 1)*

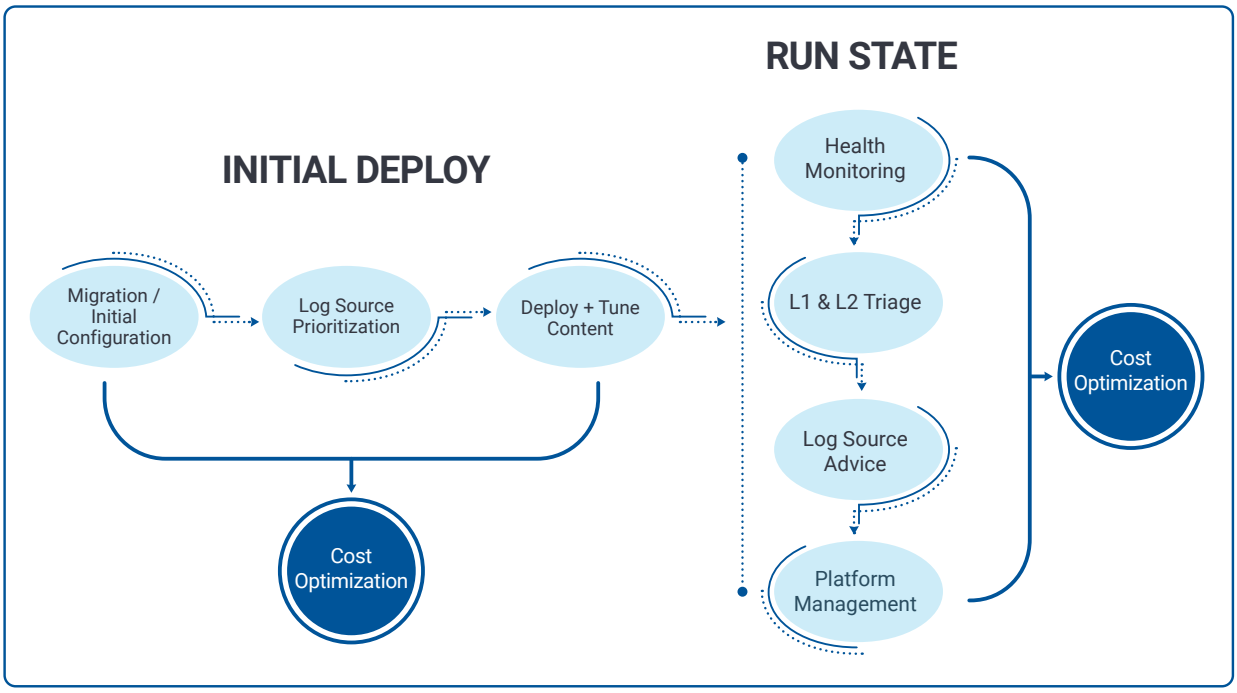
We enhance your detection coverage and compliance posture by ensuring you are ingesting the right security data and getting the most value from your threat-detection use cases. Finally, we partner with you to advance, scale and mature your cybersecurity capabilities over time, at a pace that matches your business needs. *(Fig 2)*



(Fig 1) Simplifying breach prevention

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

CRITICALSTART®



(Fig 2) Your entire SIEM program with Critical Start

Mature your security program

We map your threat detection content to the industry standard **MITRE ATT&CK® Framework** to measure the security effectiveness of your data sources, to help you make risk-based decisions on attack coverage and provide the foundation to empower you achieve optimal MDR coverage and outcomes.

A SIEM is not a "set it and forget it" solution

The lack of dedicated resources to tune, configure and test the right log files is preventing you from getting the greatest security value out of your SIEM. It's also leading to an increase in false positives and alert saturation that clouds decision-making and hides genuine threats.

With Critical Start Managed SIEM, you can rely on our dedicated team of security experts to help you gain complete visibility and control of your data. Let us identify and manage the back-end components and maintenance of your SIEM application and help you keep your business secure by partnering with you to navigate the ever-evolving threat landscape.

Critical Start Managed SIEM services addresses your core challenges by focusing on six specific areas:

- Migration and implementation
- Configuration
- Content
- Operational monitoring
- Tech management
- Threat monitoring and investigation

Contact us for more information about Critical Start Managed SIEM and our other SIEM solutions, or schedule a demo at: www.criticalstart.com/contact/request-a-demo/

CRITICALSTART®