CRITICAL**START**® SIEM Security Services
Sumo Logic® Cloud SIEM

Achieve your full security and business potential

KEY BENEFITS

✔ **Maximize value**
Prioritize the data to be ingested and increase visibility across your security environment

✔ **Improve security posture & minimize risk**
Strategically add new data sources while continuously validating MITRE ATT&CK® Framework coverage

✔ **Reduce false positives**
Optimize threat-centric log source feeds

✔ **Increase efficiency**
Simplify architecture, deployment, and management of SIEM

✔ **Quarterly service reviews**
Constant assurance that the log sources coming in are accurate and optimal for detecting threats

Take control of your threat detection and response capabilities

Security and Information Event Management (**SIEM**) solutions are complex. They are also a core technology organizations use to address security operations, risk, and compliance monitoring use cases. However, deploying, tuning, and managing a SIEM can be a daunting challenge that further impacts the quality of threat detection and response use cases.

Together, **Critical Start** and **Sumo Logic** deliver a comprehensive solution that brings businesses the peace of mind, security, and expertise they need to optimize their SIEM and achieve their full security and business potential.
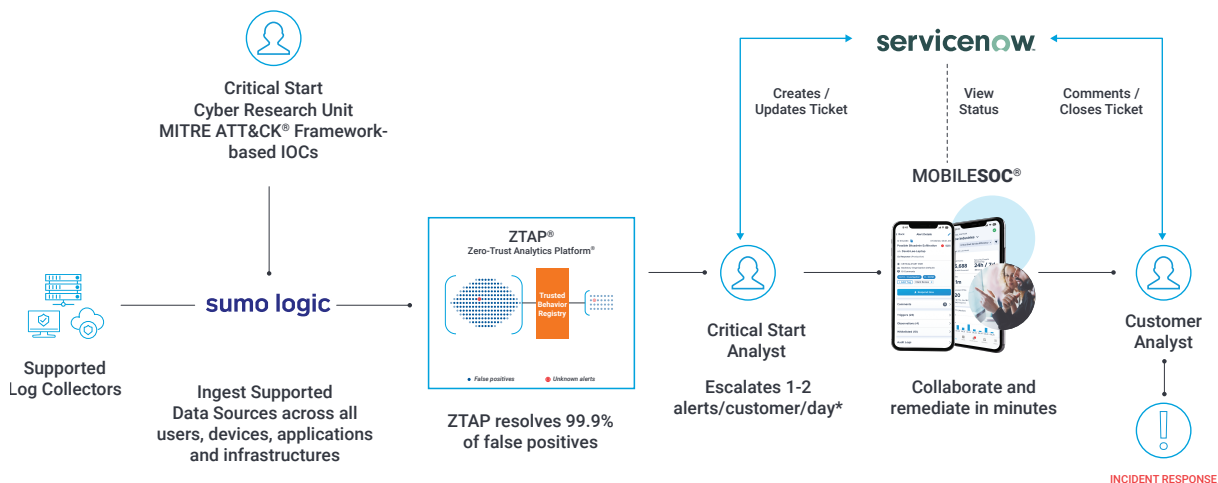
Solution

By supporting **Sumo Logic Cloud SIEM**, a security-first-focused SIEM solution, we are increasing our customers' choices for a cloud-based log management and analytics platform that will help them monitor, troubleshoot, and secure their applications and infrastructure in real time.

Critical Start SIEM Security Services is a single solution providing complete access to our Managed SIEM and Managed Detection and Response (**MDR**) for SIEM services, empowering Sumo Logic customers to achieve the full operating potential of their SIEM and maximize their security posture.

How it works

Critical Start's risk-based approach and context-driven insights help Sumo Logic's customers attain their business objectives by identifying and responding to security threats more quickly and effectively with **24x7x365** threat detection coverage. Our SIEM Security Services provides an adaptable and agile solution that minimizes the burden and cost of maintaining an in-house SIEM while effectively managing security incidents, improving overall security posture, and complying with relevant regulations and standards.

Critical Start Cyber Research Unit MITRE ATT&CK® Framework-based IOCs

Supported Log Collectors

sumo logic

Ingest Supported Data Sources across all users, devices, applications and infrastructures

ZTAP®
Zero-Trust Analytics Platform®

Trusted Behavior Registry

● False positives   ● Unknown alerts

ZTAP resolves 99.9% of false positives

Critical Start Analyst

Escalates 1-2 alerts/customer/day*

servicenow

Creates / Updates Ticket | View Status | Comments / Closes Ticket

MOBILESOC®

Collaborate and remediate in minutes

Customer Analyst

INCIDENT RESPONSE

*Based on an average of 15,000 alerts ingested into ZTAP per customer/per day

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

CRITICALSTART®