SOLUTION QUICK CARD

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

Achieve your full security and business potential

KEY BENEFITS

- ✓ **Improve security posture** Identify and resolve SIEM coverage gaps, strategically add new data sources, and continuously validate **MITRE ATT&CK® Framework** coverage
- ✓ **Enhance visibility** Gain deeper insights into crucial data sets with out-of-the-box applications that provide an increased understanding of log sources and their context
- ✓ **Optimize SIEM performance** Reduce false positives and maximize value by optimizing threat-centric log source feeds and ensuring only security-relevant data is sent for correlation and response
- ✓ **Increase efficiency** Streamline SIEM architecture, deployment, and management to increase operational efficiency and minimize resource overhead
- ✓ **Proactively mitigate risk** Leverage continuous monitoring and data health checks to identify potential issues, minimize risk exposure, and maintain a strong security posture
- ✓ **Monitor MITRE ATT&CK® Framework coverage** Track the progress of **MITRE ATT&CK®** coverage within the Sumo Logic platform as Critical Start develops new detections tailored to your security needs

Unlock the full potential of your SIEM investment and reduce the risk of a breach

Security and Information Event Management (**SIEM**) solutions require expert technical resources. They are also a core technology organizations use to address security operations, risk, and compliance monitoring use cases. Now, you can offload the tuning, management, and maintenance of your **Sumo Logic** SIEM to maximize the value of your investment and realize an increase in the quality of your threat detection and response use cases.

Together, **Critical Start** and **Sumo Logic** deliver a comprehensive solution that starts with expert administration and customization to help you address core use cases like security operations, risk, and compliance monitoring and provides **24x7x365** threat detection and response. This continuous risk reduction and cost optimization enhances your security posture and frees up your time to focus on other core business initiatives.

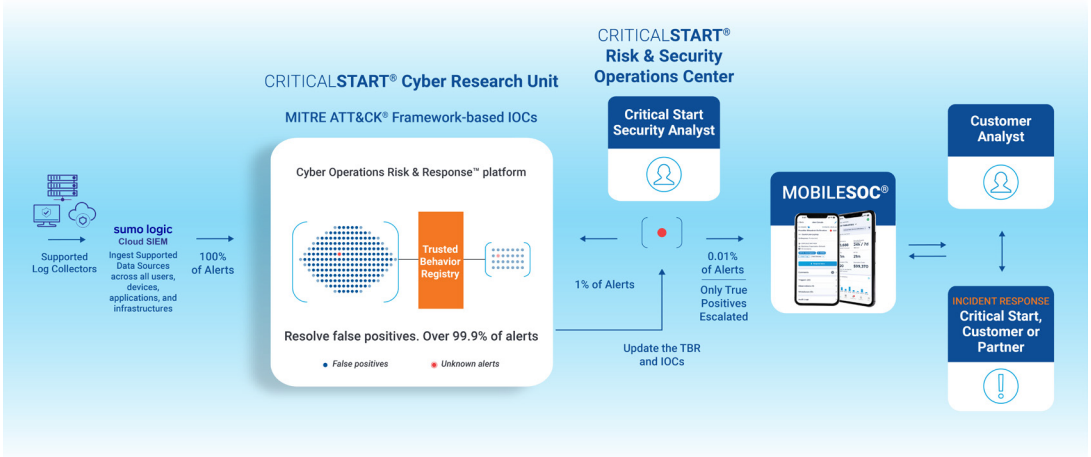
Our solution

By supporting **Sumo Logic Cloud SIEM**, we are increasing our customers' choices for a cloud-native, scalable log management and analytics platform that helps them monitor, troubleshoot, and secure their applications and infrastructure in real time.

Critical Start Security Services for SIEM empowers you with actionable insights, helping you identify coverage gaps and ensuring security-relevant logs are prioritized and properly ingested. This gives you more control over your security program by enabling you to rapidly respond to emerging threats, prevent breaches, and minimize risk.

How it works

Critical Start's risk-based approach and context-driven insights help Sumo Logic's customers attain their business objectives by uncovering and responding to security threats more quickly and effectively with **24x7x365** threat detection coverage and Risk & Security Operations Center (**RSOC**) analyst support. Our adaptable and agile solution minimizes the burden and cost of maintaining an in-house SIEM while effectively managing security incidents, improving risk resilience, and complying with relevant regulations and standards.



Contact us for more information about Critical Start Security Services for SIEM, or schedule a demo at: www.criticalstart.com/contact/request-a-demo/