CRITICALSTART

Managed SIEM services for Splunk

Gain data-rich visibility and comprehensive insight into your security environment.

CRITICAL**START™ managed SIEM services for Splunk** leave nothing to chance, with data-rich visibility and seamless orchestrated detection and response beyond the endpoint. We quickly and effectively accomplish true managed detection and response for SIEM; we help you build it effectively, deploy it quickly and use it actively to detect threats.

The Key Benefits of the Integration

CRITICAL**START** Managed SIEM services for Splunk offer you comprehensive insight into your security environment while reducing alerts. You will be able to accelerate return on your Splunk SIEM investment, tighten your security strategy with deeper insights, and stop breaches.

Deepen Your Available SIEM Expertise

The SIEM engineering team at CRITICAL**START** has a collective 100+ years of experience managing over 50PB of data including environments greater than 20PB in size. Team members have deployed SIEM in 50+ Fortune 500 companies and have experience across multiple industries and verticals.

Increase Your Security Efficacy Through a Trust-Oriented MDR Approach

Ingest all Splunk data - on-premise and cloud data across all users, devices, applications, and infrastructures for automatic resolution of known good through the Trusted Behavior Registry (TBR). This shifts focus to unknown alerts for triage and quick resolution. With 24x7x365 monitoring, our highly skilled analysts work in a SOC 2 Type 2 certified Security Operations Center (SOC) to investigate, escalate, contain, and respond to threats – helping to significantly reduce attacker dwell time. CRITICAL**START** allows limitless amounts of detection content in Splunk – no matter how much noise is generated.

MOBILE**SOC**

CRITICAL**START** offers native iOS and Android apps to give analysts full access to their MDR toolset on the go. Within the fully featured app, analysts can investigate alerts, communicate with CRITICAL**START** Security Experts, and respond, all without needing a computer.

CRITICALSTART

Capability Comparison

	CRITICAL**START** MDR + Splunk	Arctic Wolf	eSentire	Secureworks
Cloud-Native SIEM offering	●	●	○	○
Custom Use Cases	●	✕	✕	●
MDR Platform with Trusted Behavior Registry that resolves 100% of alerts	●	✕	✕	✕
Native iOS and Android applications for alert investigation, collaboration and response	●	✕	✕	✕
Multi-Tenant so client can have multiple organizations with N-level hierarchy	●	●	●	✕
Manage and report on all alerts from SIEM and EDR in one platform	●	○	✕	●
Review process available to customers, providing transparent quality control for analyst investigations	●	✕	✕	✕
Contractually guaranteed Service Level Agreement for Analyst Time to Detect and Respond to Alert (as compared to SLO)	●	✕	✕	○
Alert Notifications that include both security event data and expert analysis	●	●	●	●
Customer and vendor work from same platform and see the same information for security event analysis (Transparent view to all rules, comments, audit logs, and metrics)	●	✕	✕	✕
Custom Indications of Attack (IOA) Monitoring	●	✕	✕	●
24x7 monitoring by Cybersecurity Analysts (Security Alert Investigation and Notification performed by Security Analysts)	●	●	●	●
Advanced Threat Detection and Hunting	●	●	●	●
Analyst will proactively respond to stop attacks (isolate, block, whitelist, etc.)	●	○	○	○
Managed policy tuning and updating of agents	●	●	●	●
Optional Incident Response	●	●	●	●
Privacy Shield Certified	●	✕	✕	✕
SSAE 18 SOC 2 (TYPE 2) Certified	●	●	●	●

● Complete Offering ○ Partial Offering ✕ No offering

CRITICALSTART