

# CRITICALSTART® Security Services for Microsoft Sentinel

Reduce the cost of Microsoft Sentinel while improving security outcomes for your organization

## KEY BENEFITS

- ✓ **Right-size your Sentinel SIEM ingest** with ingest cost analysis, optimized, tailored onboarding, and future cost estimation.
- ✓ **Close coverage gaps** with proactive detection of log sources that are not being ingested or where ingestion has failed.
- ✓ **Trust your 24x7x365 security monitoring** to a team of highly trained Microsoft security experts.
- ✓ **Continually ensure SIEM log health** with asset-aware and data-aware monitoring.
- ✓ **Respond quickly to the alerts that matter** with contractual service level agreements (SLAs) for all alerts, regardless of priority.
- ✓ **Reduce the total cost of ownership (TCO)**, increase return on investment (ROI), and improve team productivity.

Microsoft Sentinel™ SIEM helps you uncover sophisticated threats in your environment. However, many organizations struggle with SIEM complexity. Knowing which log sources to integrate, fine-tuning alert thresholds, and monitoring log ingestion health all require dedicated, skilled team. And then there's alert triage, investigation, and threat mitigation, which requires an entirely separate skillset.

CRITICALSTART® helps you manage your SIEM from setup and tuning, through alert triage, threat detection, and response. Our security services empower you to reduce SIEM complexity and cost while accelerating threat detection and response.

### How it works

With a combination of Managed Detection and Response (MDR) and managed SIEM services, Critical Start offers a comprehensive solution for effective SIEM administration and cybersecurity defense. Our certified Microsoft experts conduct ingest cost analysis and help you prioritize relevant data sources. We also help you identify and prioritize unmonitored and those with failed log ingestion.

Once you are up and running, the Critical Start Trusted Behavior Registry® (TBR®) identifies and suppresses false positives and redundant alerts. All escalations pass through our human-driven analysis and two-person quality assurance to ensure your team focuses on priority incidents. Our 24x7x365 Security Operations Center (SOC) analysts accelerate response to validated threats by providing expert, on-the-go guidance via our MOBILESOC® app and recommending MITRE ATT&CK®-based mitigations to prevent recurrence.



Member of  
Microsoft Intelligent Security Association



### Right-size your Microsoft Sentinel deployment

Many organizations struggle to predict and manage the cost and complexity of Microsoft Sentinel. It takes specialized expertise to optimize and manage Sentinel, tune detections and alerts, and prioritize high security-value log sources. Critical Start helps you optimize your SIEM ingest and estimate future costs to accurately predict your security spend.

The Critical Start Cyber Operations Risk & Response™ (CORR) platform normalizes data across all connected sources. With this comprehensive asset inventory and customizable asset criticality ratings, you can quickly prioritize log sources in a way that further maximizes the value of your Sentinel deployment.

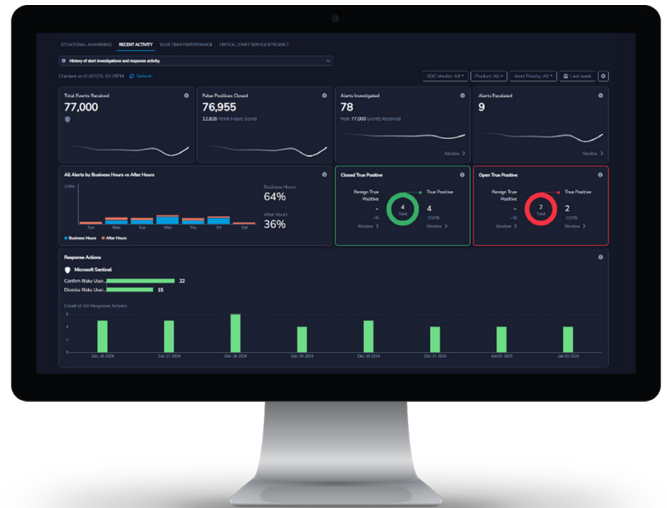
Once you are up and running, our team continuously works with you to tune detections, alerts, and log ingestion to lower your costs and improve security outcomes. Critical Start’s continuous health monitoring of your data sources means that you will know if a log ingestion fails, a connection drops, or expected log sources stop reporting in. You can be assured that the SOC is receiving all expected telemetry, so potential threats do not slip through the cracks.

Additionally, Critical Start provides regular service reviews and customized dashboards so you can continuously monitor and report on the efficiency and value of your security tools, including Sentinel. You will also have the data needed to continually improve your security posture, even as your environment changes and log sources grow.


### Eliminate false positives and stop business disruption


Critical Start couples automated technology, including the TBR and benign true positive detection, with human-powered analysis for fewer false positives at scale. That means you can add more log source feeds, and Critical Start will filter out the noise, so you only respond to true positives. With full SOC transparency, you can quickly confirm all alert verdicts, regardless of criticality, and see all context and rationale used to reach each conclusion.


When you do have an alert that requires your attention, Critical Start engages with your organizations per your instructions – either by auto-resolving issues, following prescriptive, auditable Response Authorizations, or escalating directly to your team based on the “Who’s on Call” screen. Contractual service level Agreements (SLAs) mean that you will have the information you need to stop business disruption quickly. You can then mitigate threats from wherever you are and communicate directly with our SOC analysts – not bots – either through the Critical Start Platform or the Critical Start MOBILESOC® app. You can also remediate from within your Microsoft tools.





### Key features of Critical Start security services for Microsoft Sentinel


- 


Sentinel log source analysis and prioritization
- 


Threat monitoring and investigation conducted by certified Microsoft experts
- 


Guided response recommendations and customizable Response Authorizations
- 


Regular optimization reviews (including ingest cost analysis)
- 

First- and third-party remediation actions
- 

Log and log-health monitoring (includes zero-log ingest alerts)
- 

Proactive identification and resolution of overlooked SIEM log sources
- 

Proprietary detections and Indicators of Compromise (IoCs) beyond those provided by Microsoft
- 

MITRE ATT&CK® Mitigations recommendations
- 

Operationalized threat intelligence

### Learn More

Book a demo to see how the Critical Start SOC can improve security outcomes for your organization.