

CRITICALSTART Managed Detection and Response Services for Microsoft Azure Sentinel

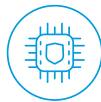


KEY BENEFITS

- ✓ Reduce risk acceptance
- ✓ Increase SOC efficiency & productivity
- ✓ Take advantage of limitless amounts of detection content
- ✓ Accelerate value from Azure Sentinel
- ✓ Triage and contain alerts from anywhere with MOBILESOC™

MDR reinvented. SIEM reinvented. An integrated threat detection and response solution for the modern world that's more than good, *it's better.*

We do what others don't. Most Security Information Event Management (SIEM) solutions are leveraged for compliance, but only partially optimized for threat detection. CRITICALSTART™ Managed Detection and Response (MDR) services integrate with Microsoft Azure Sentinel to detect every event, resolve every alert, and escalate only the alerts that matter to you. We provide you full operating potential for threat detection and response, while providing your security operations team increased efficiency and productivity gains.



Why CRITICALSTART

Resolving alerts is good. Resolving all alerts is better.

- ✓ Our trust-oriented approach leverages the power of the Zero Trust Analytics Platform (ZTAP) and Trusted Behavior Registry (TBR) to address all alerts
- ✓ We auto-resolve more than 99% of alerts
- ✓ We escalate less than 0.01% of alerts – the alerts that really require the attention of your security team

Unmatched SIEM detection engineering expertise.

- ✓ Dedicated Cyber Research Unit team has a collective 100+ years of experience across multiple verticals/industries curating content to ensure detections are working
- ✓ Leveraging the CRITICALSTART™ Threat Navigator, we manage, maintain, and curate Azure Sentinel out-of-box detections and Indicators of Compromise (IOCs)
- ✓ Detection content is mapped to the industry approved MITRE ATT&CK® Framework
- ✓ Our services include CRITICALSTART proprietary detections and IOCs
- ✓ We provide expert guidance around how to deploy Azure Sentinel in your environment and optimize your log data sources for effective threat detection with the Microsoft Defender security suite or with other third-party security tools in your environment

Not more resources. Better ones.

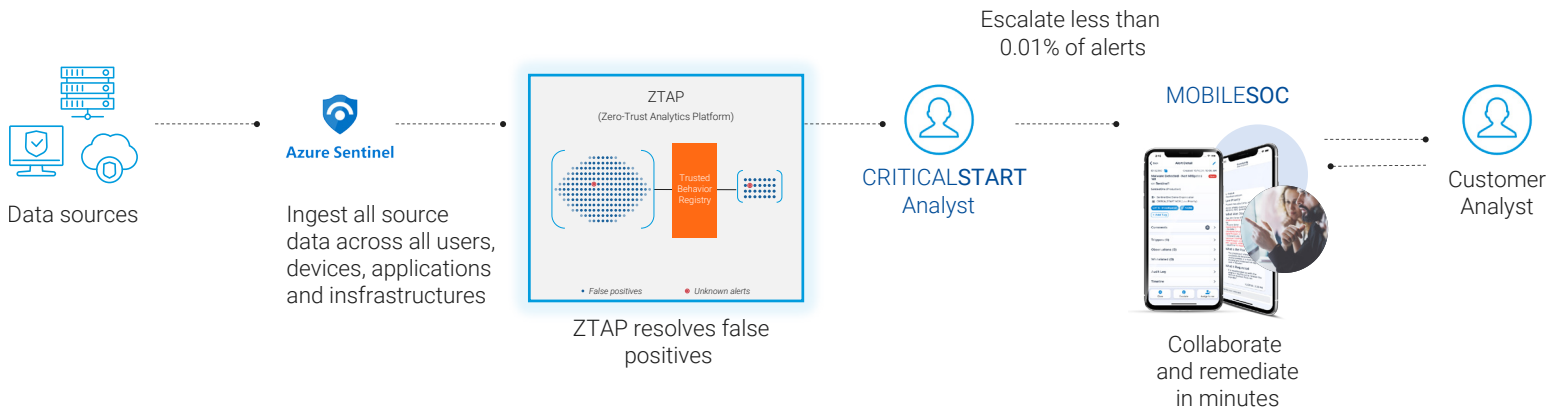
- ✓ Security analysts have MS-500: Microsoft 365 Security Administration, SC200 and AZ-500: Microsoft Azure Security Technologies certifications
- ✓ We use [Microsoft Security Best Practices](#) to deploy Azure Sentinel and Microsoft 365 Defender tools to optimize Microsoft content for both Scheduled Query Rules and Indicators of Compromise (IOCs)
- ✓ Our team provides 24x7x365 end-to-end monitoring, investigation, and response by highly skilled analysts





How we do it

We take every alert from Microsoft Azure Sentinel into ZTAP and match it against known good patterns in the TBR. If there is a match, the alert is automatically resolved and incorporated into the TBR. If there is no match, the CRITICALSTART Security Operations Center (SOC) investigates and collaborates with you to remediate the alert.



Never miss a threat. Or your desk.

Take threat detection and response on-the-go with our MOBILESOC application. An industry-leading first, MOBILESOC puts the power of our ZTAP platform in your hands, allowing you to contain breaches right from your phone. Our iOS and Android app features 100% transparency, with full alert detail and a timeline of all actions taken.



Capability Comparison

- COMPLETE OFFERING
- ◐ PARTIAL OFFERING
- ✗ NO OFFERING

	CRITICALSTART MDR + Microsoft Azure Sentinel	Other MDR/ Managed SIEM providers
24x7x365 monitoring, investigation, and guided response by security analysts	●	◐
Contractually guaranteed Service Level Agreement for Time to Detect and Median Time to Resolution for all alerts, regardless of priority level	●	✗
Native iOS and Android applications for alert investigation, collaboration, and response	●	✗
Customer and vendor work from the same platform and see the same information	●	◐
Custom Indicator of Attack (IOA) Monitoring	●	✗
Two-person integrity review process that provides quality control of SOC orchestration for every customer	●	✗
Manage, curate, and maintain Azure Sentinel out-of-box detections and IOCs	●	✗
Detection content mapped to the MITRE ATT&CK framework	●	◐
Continuous threat hunting	●	◐
Perform configuration, deployment, and health checks without requiring additional professional services	●	◐
Close and comment on all false positive investigations in Azure Sentinel	●	✗
Alert notifications that include both security event data and expert analysis	●	●
Custom CRITICALSTART detections and IOCs included	●	✗
Combine data-rich insights across endpoint, network, and identity for investigation and response	●	◐
Automatically enable new Microsoft rules	●	✗
Manage and report on all alerts from Azure Sentinel and non-Microsoft security tools in one platform	●	✗

Member of
**Microsoft Intelligent
Security Association**



Gold
Microsoft Partner



Goodbye, alert fatigue. Hello, CRITICALSTART.

[Contact Us](#)

[Request a Free Assessment](#)