DATASHEET

CRITICALSTART® Managed Detection and Response Services for Microsoft Sentinel

KEY BENEFITS

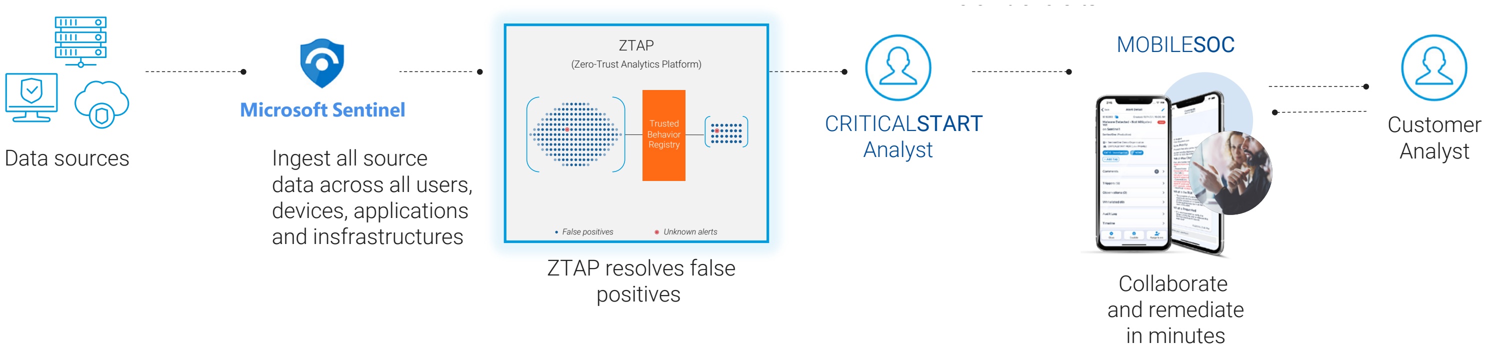
- ✓ Reduce risk acceptance
- ✓ Increase SOC efficiency & productivity
- ✓ Take advantage of limitless amounts of detection content
- ✓ Accelerate value from Microsoft Sentinel
- ✓ Triage and contain alerts from anywhere with MOBILESOC®

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 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.

How we do it

We take every alert from Microsoft Sentinel into the Zero Trust Analytics Platform™ (ZTAP™) and match it against known good patterns in the Trusted Behavior Registry™ (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.



Ingest all source data across all users, devices, applications and insfrastructures

ZTAP resolves false positives

Collaborate and remediate in minutes

© 2022 CRITICALSTART. All rights reserved.

Why CRITICAL**START**

Resolving alerts is good. Resolving all alerts is better.

✓ Our trust-oriented approach leverages the power of ZTAP and 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 CRITICAL**START**® Threat Navigator, we manage, maintain, and curate Microsoft 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 CRITICAL**START** proprietary detections and IOCs

✓ We provide expert guidance around how to deploy Microsoft 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 Security Technologies certifications

✓ We use Microsoft Security Best Practices to deploy Microsoft 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

Never miss a threat. Or your desk.

✓ Take threat detection and response on-the-go with our MOBILE**SOC** application. An industry-leading first, MOBILE**SOC** 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.

Contact Us **Request a Free Assessment**

CRITICAL**START**®

© 2022 CRITICAL**START**. All rights reserved.