DATASHEET

CRITICALSTART® Managed Detection & Response (MDR) Services

Comprehensive. Simplified. Flexible.

KEY BENEFITS

- ✓ **Optimize security investments**
  80% reduction in false positives on the first day of production monitoring and escalation of less than 0.1% of alerts
- ✓ **Reduce risk exposure**
  resolution of more than 99% of alerts
- ✓ **Decrease complexity**
  Over 40% of our customers rely on us to bring together conceptual insights across multiple security tools.

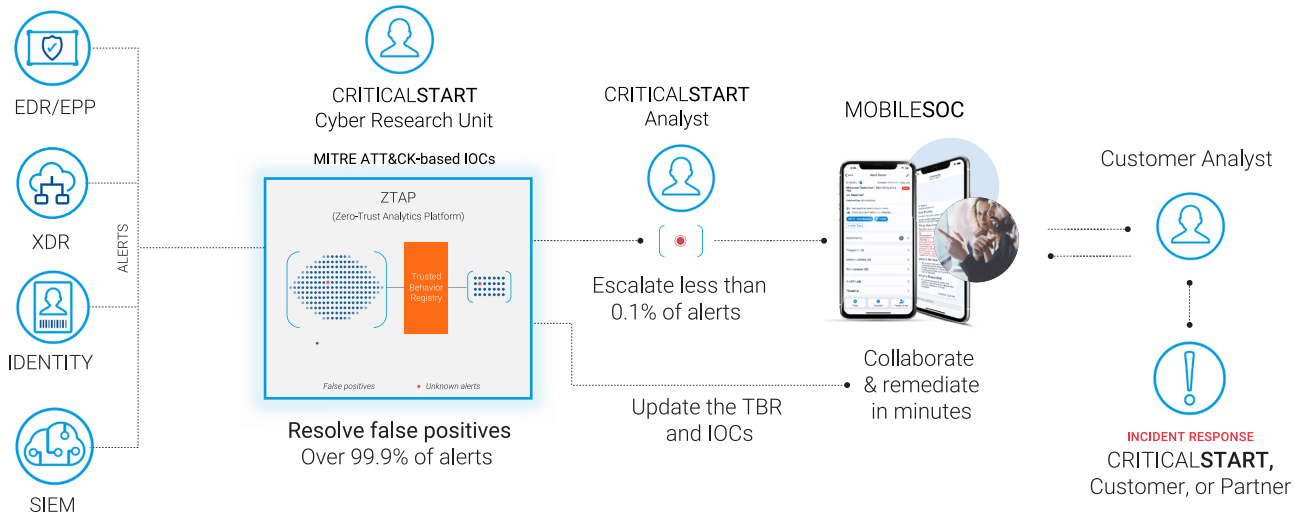
CRITICALSTART is the only MDR provider on the market today who dared to approach simplifying the cybersecurity problem by first embracing the complex. While others are focused on finding bad, we focus on finding good. While others prioritize or suppress alerts, we resolve all alerts.

We bring you a team of skilled security experts who will deeply understand your environment to adapt and scale with your organization's needs and partner with you to detect, investigate and respond to threats specific to your organization.

We also deliver something priceless – the peace of mind that comes from:

- ✓ Available on-site and remote incident response and digital forensics capabilities, for situations requiring trained incident responders
- ✓ 100% visibility to every action and every data point our team has examined, what our detection engineers see, and a view of the detection coverage delivered by your security tools and MDR service
- ✓ Service Level Agreements for Time-to-Detect (TTD) and Median-Time-to-Resolution (MTTR) for all alerts, regardless of severity level – guaranteed in one hour or less – with no fine print

We purpose-built the industry's only Trusted Behavior Registry™ (TBR) within our Zero-Trust Analytics Platform™ (ZTAP™) to resolve all alerts. We integrate with multiple security tools, including endpoint, SIEM, XDR, and identity, to reduce the volume of alerts by more than 99%, escalate less than 0.1% of alerts, and never send you the same alert twice.



© 2022 CRITICALSTART. All rights reserved.

CRITICALSTART

How We Do It

Detect the right threats.

- ✓ We manage, maintain and curating out-of-the-box detections and IOCs released by the security tool manufacturer.
- ✓ We curate original and third-party threat intelligence, combined with real-time threat analysis, to create a high-fidelity, actionable view of existing and emerging threats.
- ✓ We continuously develop and enrich new threat detections and Indicators of Compromise (IOCs) based on the evolving security landscape.
- ✓ We map threat detection content to the MITRE ATT&CK® Framework to ensure you are protected against the latest attacker Techniques, Tactics, and Procedures (TTPs).

Respond with the right actions.

- ✓ We provide expert Security Operations Center (SOC) Analysts, to quickly investigate and respond to all escalated alerts through 24x7x365 monitoring, rapid investigation, and continuous threat hunting.
- ✓ Our MOBILE**SOC**® application allows you to communicate with the SOC and perform response actions on the go.

Provide agility and adaptability.

- ✓ A dedicated project manager and implementation team dig in deep from the start to understand your environment, unique needs and business objectives.
- ✓ Our Customer Success Team is your advocate and there with you on the journey, providing recommendations and support as your needs change.

We only work with **the best.**

CRITICAL**START** MDR services integrate with leading security technologies to detect every alert, resolve every alert and respond to breaches.

Microsoft Defender for Endpoint

Microsoft 365 Defender

Microsoft Sentinel

CORTEX BY PALO ALTO NETWORKS

splunk>

DEVO

vmware Carbon Black

BlackBerry CYLANCE

SentinelOne

CROWDSTRIKE

Contact Us **Request a Free Assessment**

CRITICALSTART®

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