DATASHEET

CRITICAL**START**® Managed Detection & Response Services & Solutions

Critical Start delivers the most effective Managed Detection and Response (**MDR**) service per dollar invested. We help you address areas of risk exposure due to your lack of visibility, threat intelligence or detection and response abilities. We augment your security team to drive increased productivity and help you to move your security program forward, confidently.

HELP ME DO IT ▶ ▶ ▶ ▶ **DO** IT FOR ME ▶ ▶ ▶ ▶ **STAY** BY MY SIDE

Professional Services

Drive actional insights from your security controls, measure your current SecOps and bolster your defenses.

Proactive Services: Proactively find the gaps in your security and repair them before an incident occurs.

- Cyber Readiness Assessments
- Incident Response Plans & Playbooks
- Tabletop Exercises
- Threat Hunting
- Threat Hunting & Incident Readiness Training

Microsoft Professional Services help you optimize and improve your security postures with Microsoft security tools.

- Workshops
- Security Assessments
- Deployment Services
- Migration Services

Managed Detection and Response Services

Extend your team with complete 24x7x365 detection, investigation and response.

Stops business disruption from cybersecurity threats.

- 1-hour or less resolution Service Level Agreement (**SLA**) for every alert level
- Every alert actioned across multi-vendor EDR, XDR, SIEM & Identity security tools
- Deep threat intelligence
- Direct SOC analyst collaboration
- Complete visibility & actionability via MOBILE**SOC**®
- Rules of engagement tailored to your environment

Managed Security Information and Event Management (SIEM) Services

Manage costs and reduce threat coverage gaps.

Custom development for dashboards, reports and log sources.

- Quarterly service reviews to maximize total cost of ownership & increase security outcomes
- Health monitoring – log source performance, availability & capacity monitoring to identify potential issues with log ingestion
- Risk reduction reviews – analyze the potential impact of adding additional log sources & detection content under the **MITRE ATT&CK® Framework**

Incident Response Services

Minimize the impact of a breach and get peace of mind with IR experts.

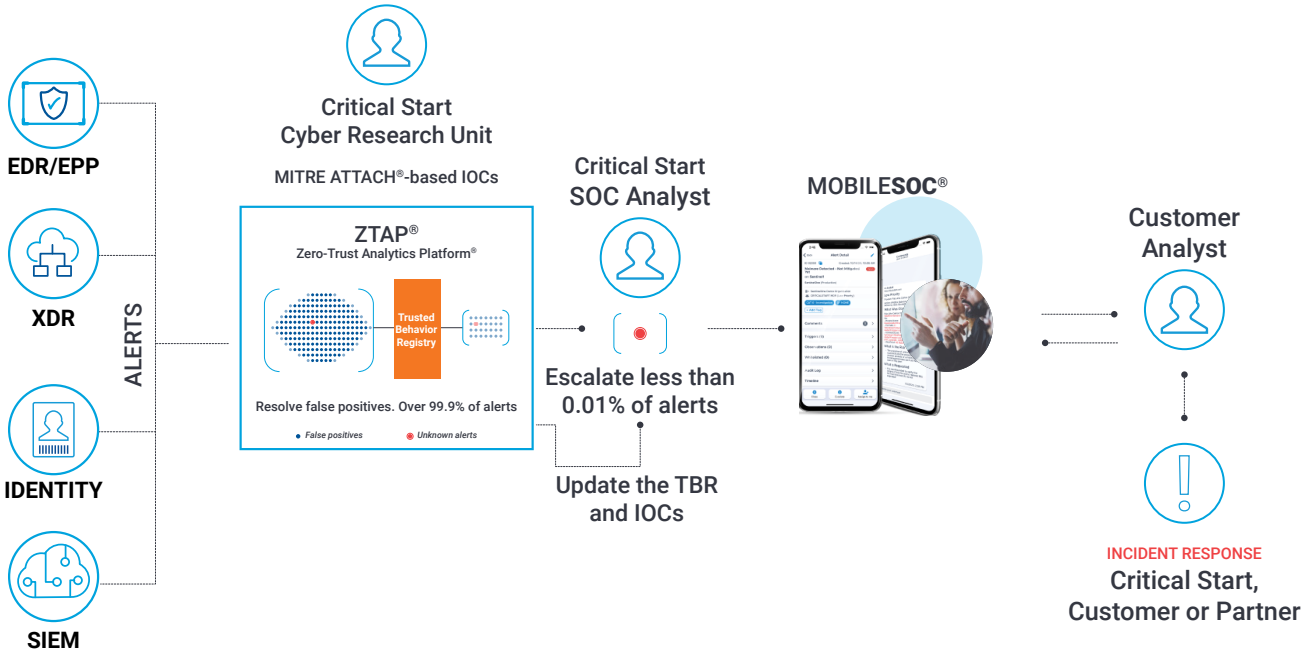
Reactive Services: An incident has occurred – we are just a phone call away 24x7x365.

- Incident Response
- Digital Forensics
- Compromise Assessment
- Incident Response Monitoring
- IR retainers are available with options for as-needed service hours

Our Cyber Research Unit works as an extension of your team to provide original and third-party threat intelligence research as well as develop and enrich new detections and IOCs.

CRITICALSTART®

Critical Start blends the potency of our security experts with the power of our Zero-Trust Analytics Platform® (ZTAP®) to stop business disruption by preventing breaches.



ZTAP

Within ZTAP, security teams can benchmark performance, track trends, understand how their security control coverage maps against the MITRE ATT&CK® Framework and prove ROI with visibility into how the MDR service is performing.

SOC

Our Security Operations Center (**SOC**) is staffed with experienced security analysts who extend the detection and response capabilities of your security operations 24x7x365 to keep your environment free from business disruption.

MobileSOC

Triage and contain alerts in minutes to protect your most valuable asset— your data, by taking immediate action based on information you receive directly from the ZTAP platform and our SOC analysts.

Integration Partners

Microsoft Defender for Endpoint
Microsoft Sentinel
Microsoft 365 Defender
CORTEX BY PALO ALTO NETWORKS
TREND MICRO
CROWDSTRIKE
SentinelOne
vmware
BlackBerry CYLANCE
splunk>
sumo logic

CRITICALSTART®