DATASHEET

CRITICAL**START**®
Managed Detection and Response (**MDR**) Services

Bolster cybersecurity posture and validate defenses to mitigate breaches and stop business disruption.

KEY BENEFITS

- ✓ **Identify security coverage gaps** and reduce the risk of multi-vector threats slipping through the cracks
- ✓ **Protect against threats** with contractual Service Level Agreements (**SLAs**) of 10-min notification for Critical alerts and 60-min or less Median Time to Resolution (**MTTR**) for ALL alerts, regardless of priority
- ✓ **Improve team efficiency** with 24x7x365 Tier 1 and Tier 2 coverage and access to our MOBILE**SOC**®
- ✓ **Improve detection effectiveness** with deep threat intelligence, detection engineering, and detections mapped to the **MITRE ATT&CK® Framework**
- ✓ **Confidently measure** team performance benchmarks and align cybersecurity spend to business outcomes with provable security operations metrics
- ✓ **Understand your current** security posture with a **Quick Start Risk Assessment**

Validate defenses to mitigate breaches and minimize business disruption.

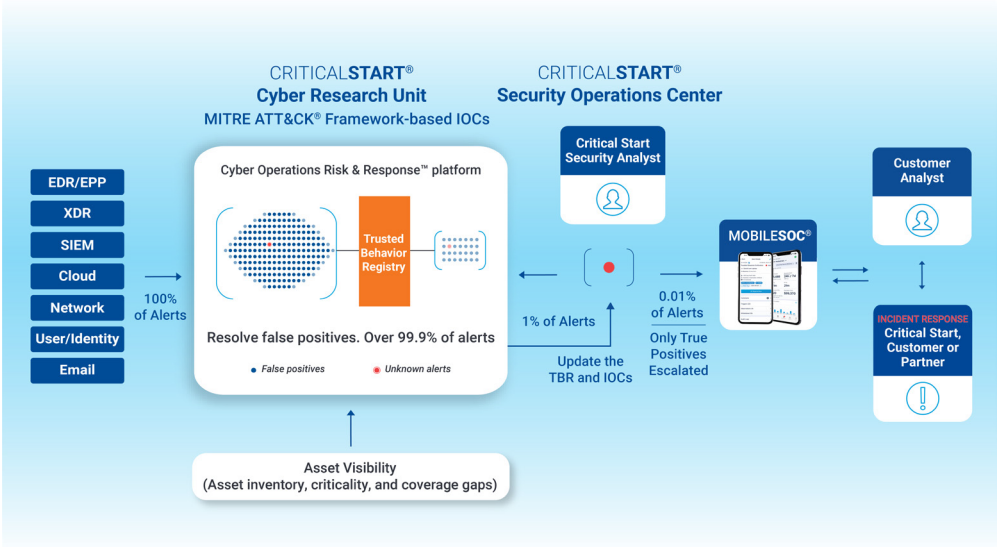
Critical Start Managed Detection and Response (**MDR**) is built on a foundation of asset visibility and offers 24x7x365 monitoring, investigation, and response. By seeing all the assets connected to your network, you can ensure your Security Operations Center (**SOC**) is receiving all expected threat signals, empowering you to manage cyber risk and build risk resilience effectively.

Utilizing our **Cyber Operations Risk & Response™ (CORR) platform**, we integrate industry-leading tools and proactive cybersecurity intelligence into our SOC, including comprehensive asset inventories, EDR coverage gaps, asset criticality, and **MITRE ATT&CK® Mitigations**.

Human-driven MDR services.

Our human-driven MDR services are backed by our SOC, Cyber Research Unit, and Cyber Incident Response Team, plus our MOBILE**SOC**®, which provides remote threat containment capabilities. This unmatched approach enhances your security operation's productivity, reducing risk exposure and ultimately strengthening your organization's security posture in response to emerging threats and changing business needs.

Our Platform and Process



CRITICALSTART®

Confidently Reduce Risk, Mitigate Breaches, and Stop Business Disruption

Businesses looking to bolster their security posture and validate their defenses may need help knowing where to begin. Critical Start helps you identify solutions to your challenges and risks, empowering you to confidently mitigate breaches and stop business disruption.

CHALLENGES AND RISKS	STANDARD WITH CRITICAL START MDR
Create measurable improvements in security posture	• Provable metrics, shared customer learnings, and best practices • Threats and attacks are mapped in a definitive manner using the **MITRE ATT&CK® Matrix** for effective response
Lack of a centralized asset inventory and incomplete controls coverage creates blind spots for MDR and openings for attackers	• Identify security coverage gaps by finding hosts in your network that do not have an agent or SIEM coverage and reduce the risk of multi-vector threats slipping through the cracks • Ensure your SOC is receiving all expected signals
Preventing attacks with security posture improvements that last	• Recommend and prioritize proactive controls with **MITRE ATT&CK® Mitigations Recommendations** built into the platform • **Quick Start Risk Assessment** to uncover security gaps, identify remediation, and gather data to support budget requests • Retain technical artifacts such as policy configurations and custom detections
Ineffective detections fail to identify malicious behavior	• Threat Intelligence operationalized with native detections that increase the effectiveness of your investment in detecting attacks
Knowing whether the right Security Information and Event Management (**SIEM**) log sources are being ingested	• Log source prioritization and management • SIEM health monitoring
Alert fatigue and lengthy investigations increase vulnerability to attackers and lead to slower response times	• Threat Intelligence operationalized with native detections that increase the effectiveness of your investment in detecting attacks
Lack of confidence in vendor response actions	• Contractual SLAs of 10-minute notification for Critical alerts and 60-minutes or less MTTR for ALL alerts, regardless of priority • Two-person integrity review on every action to be taken
Ensuring response engagement is aligned to organizational needs	• Automatic, facilitated, and managed remediation options • Custom rules of engagement for notification and response actions
Extended dwell time during after-hours attacks	• Direct, 24x7x365 collaboration with Security Operations Center (**SOC**) analysts for rapid investigation and response • Analyst response actions or incident containment on-the-go (e.g., host isolation, disabling user accounts, email removal) from your phone via a native MOBILE**SOC**® app

Security Technology Integrations

We integrate with hundreds of leading security technologies, ingested directly or through your Endpoint or SIEM solution, to operationalize your security investment and work closely with you to detect, investigate, and respond to threats specific to your organization, ensuring you receive the greatest cyber risk reduction per dollar invested.

Microsoft Defender for Endpoint · Microsoft Defender XDR · Microsoft Sentinel · TREND MICRO · CROWDSTRIKE · BlackBerry CYLANCE · vmware Carbon Black · splunk> · SentinelOne · sumo logic · DEVO · CORTEX

CRITICALSTART®