DATASHEET

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

Human-driven threat detection, proactive risk mitigation, & full protection for maximum security outcomes.

KEY BENEFITS

- ✓ **Eliminate security blind spots**
  Know every asset is accounted for and monitored, stop threats from exploiting hidden gaps, and trust that your SOC receives every critical signal
- ✓ **Reduce alert fatigue**
  Focus only on real threats through business-aware filtering, customize response strategies to your operations, and eliminate redundant alerts and false positives
- ✓ **Get expert support 24x7x365**
  Access U.S.-based security experts any time, contain threats instantly and anywhere with MOBILE**SOC**®, benefit from nuanced, human-led analysis
- ✓ **Achieve measurable risk reduction**
  Rely on 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
- ✓ **Maximize security ROI**
  Improve detection effectiveness with deep threat intelligence, detection engineering, and detections mapped to the **MITRE ATT&CK® Framework**

Validate defenses to mitigate breaches and minimize business disruption.

Most organizations find traditional Managed Detection and Response (**MDR**) falls short of expectations. Critical Start elevates MDR standards through a unique combination of **proactive** and **reactive** security measures, delivering complete signal coverage, flexible deployment options, and human-driven expertise. Our comprehensive approach ensures complete signal coverage across your environment, providing the high-quality MDR service you expect.

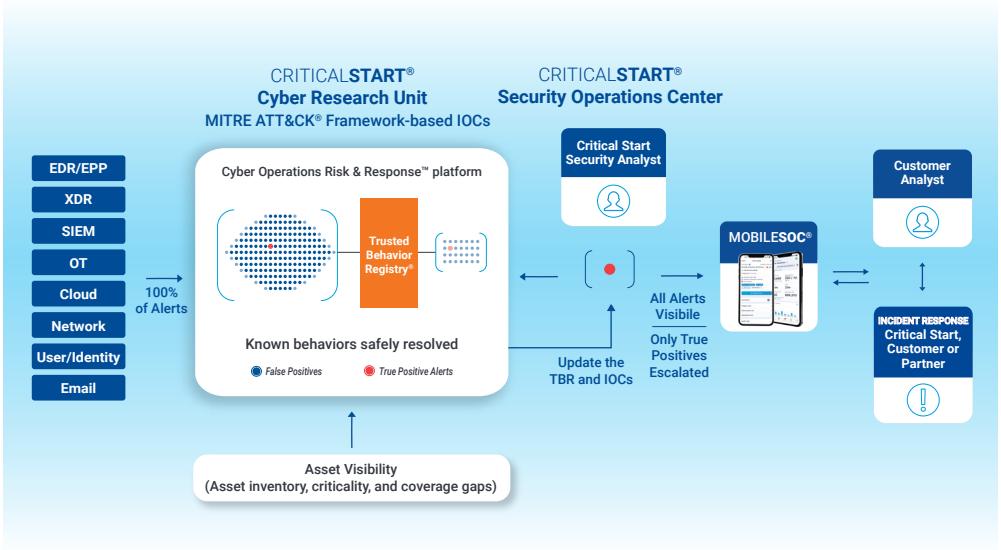
Our **Cyber Operations Risk & Response™ (CORR) platform** integrates 24x7x365 monitoring, investigation, and response with industry-leading tools and a comprehensive asset inventory so you can identify all hidden and unmonitored assets connected to your network and ensure your Security Operations Center (**SOC**) is receiving all expected threat signals.

We are the only MDR service that provides integrated asset visibility, including EDR, SIEM, and vulnerability scanner coverage gaps, SIEM log health, asset criticality ratings, and MITRE ATT&CK® Mitigations to help you significantly reduce the risk of a breach.

Human-driven MDR services.

Our human-driven MDR services are backed by our SOC, Cyber Research Unit, and Cyber Incident Response Team. You also have direct, 24x7 access to our security analyst through 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

Critical Start goes beyond traditional threat detection by delivering proactive, human-driven MDR. We help you identify solutions to your challenges and risks, empowering you to confidently mitigate breaches and effectively address both active threats and underlying vulnerabilities within your organization.

CHALLENGES	STANDARD WITH CRITICAL START MDR
Hidden and unmonitored infrastructure creating security blind spots	• **Proactive Security Gap Detection**: Identify and monitor Endpoint Detection and Response (**EDR**) and **vulnerability scanner** coverage gaps and overlooked **SIEM** log sources to reduce the risk of multi-vector threats slipping through the cracks • **SIEM Health Monitoring**
No signal assurance creates lack of confidence SOC is receiving all alerts	• **Comprehensive Signal Coverage**: Up-to-date asset inventories to ensure full signal coverage, ensuring the SOC receives all expected threat signals
One-size-fits-all MDR not aligned with organizational needs	• Visibility and threat detection across IT and Operational Technology (**OT**) systems • Integration with **100+ log sources** provides security coverage for a wide range of threat types, including **identity**, **email**, and **cloud** • Recommend and prioritize proactive controls with MITRE ATT&CK® Mitigations Recommendations built into the platform • Retain technical artifacts such as policy configurations and custom detections
Alert fatigue and lengthy investigations result in slower response times	• Trusted Behavior Registry® (**TBR®**) records and validates expected behaviors, eliminating redundant alerts and false positives • **Benign True Positive Verdict** identifies alerts resulting from expected actions, including security testing • Automatic, facilitated, and managed remediation options ensuring real-time protection of critical assets for maximum security operations effectiveness • **Response Authorizations** to customize Rules of Engagement (**ROE**) for streamlined notification and response actions based on alert and asset criteria • Threat intelligence operationalized with native detections increase the effectiveness of your investment in detecting attacks • **Asset Criticality Ratings** for prioritized protection • Contractual SLAs of 10-minute notification for Critical alerts and 60-minutes or less MTTR for ALL alerts, regardless of priority
Lack of human insight, security transparency, and SOC collaboration inhibit effective response	• Direct, **24x7x365** collaboration with Security Operations Center (**SOC**) analysts for rapid investigation and response • **Human-curated**, intelligence-driven threat detection and analysis, with two-person integrity review on every action to be taken • Threat Intelligence operationalized with native detections that increases the effectiveness of your investment in detecting attacks • Clear audit trail of all security decisions • 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 your existing security technologies to deliver complete signal coverage and trusted results. Ingested directly or through your Endpoint, SIEM, XDR, or OT security tools, we operationalize your security investments and work closely with you to detect, investigate, and respond to threats specific to your organization.

Microsoft Defender for Endpoint · Microsoft Defender XDR · Microsoft Sentinel

vmware Carbon Black · CROWDSTRIKE · BlackBerry CYLANCE · CORTEX BY PALO ALTO NETWORKS

splunk> · SentinelOne · sumo logic · DEVO

CRITICALSTART®