DATASHEET

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

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

KEY BENEFITS

- ✓ **Ensure security controls coverage** for endpoint and SIEM
- ✓ **Protect against threats** with contractual Service Level Agreements (**SLAs**) of 10-minute notifications for Critical alerts and 60-minute 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 share** 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 Assessments

It's Time for a Risk-Based Approach to MDR

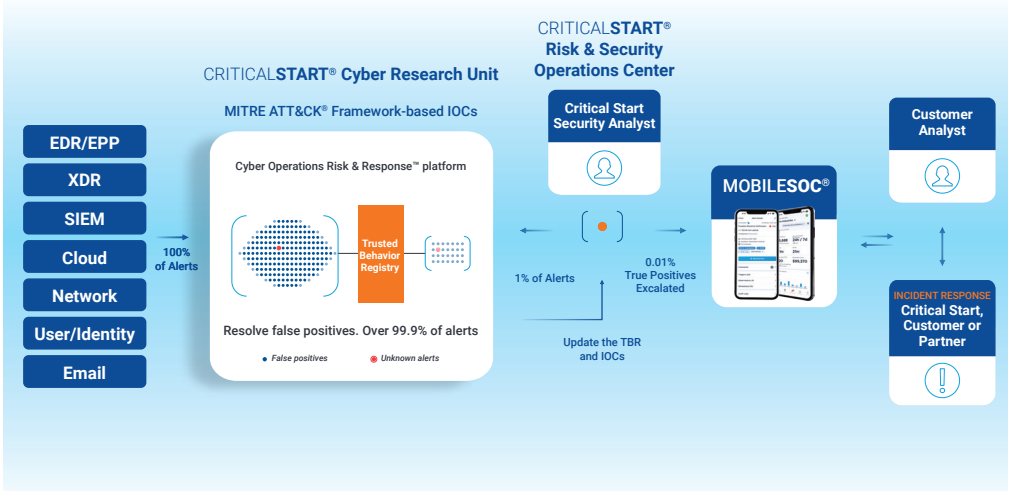
The traditional, threat-based approach of Managed Detection and Response (**MDR**) services is no longer enough to effectively manage cyber risk and build risk resilience. Critical Start MDR, a foundational component of our Managed Cyber Risk Reduction (**MCRR**) solution, takes a risk-based approach to Detection and Response and now also provides additional capabilities aligned to proactive security. These expanded capabilities are a standard requirement to uncover vulnerabilities and ensure optimal threat identification and containment, allowing you to bolster your cybersecurity posture and validate defenses to mitigate breaches and stop business disruption.

Making MDR Different

Our enhanced MDR service takes a holistic approach to risk mitigation by closing Endpoint and Security Information and Event Management (**SIEM**) coverage gaps and providing essential **MITRE ATT&CK® Mitigations** recommendations. This helps ensure that security signals are accurately reported and received by the Risk and Security Operations Center (**RSOC**) and that the right mitigations are implemented to prevent the same attack from happening again and again.

Our MDR services are backed by 24x7x365 skilled security experts, a purpose-built Trusted Behavior Registry® (**TBR**®) integrated into our platform to evaluate every alert and remove the noise, and a MOBILE**SOC**® application for swift triage and incident containment on-the-go. Our risk-based approach to MDR gives you the actionable insights needed to respond rapidly to emerging threats, prevent breaches, and minimize risk.

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
Incomplete controls coverage creates blind spots for MDR and openings for attackers	• Identify assets missing Endpoint Protection (**EPP**)/Endpoint Detection and Response (**EDR**) to ensure full coverage and protection
Preventing attacks with security posture improvements that last	• Recommend and prioritize proactive controls with **MITRE ATT&CK® Mitigation** 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 • Quarterly Service reviews and 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 notifications 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 Risk and Security Operations Center (**RSOC**) 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 365 Defender · Microsoft Sentinel · TREND MICRO · CROWDSTRIKE · BlackBerry CYLANCE · vmware Carbon Black · splunk> · SentinelOne · sumo logic · DEVO · CORTEX BY PALO ALTO NETWORKS

CRITICALSTART®