DATASHEET

CRITICAL**START**® Managed Detection and Response Services for Microsoft Security

Microsoft Security

KEY BENEFITS

- ✓ Comprehensive threat detection and response coverage
- ✓ Team expansion with Microsoft security expertise
- ✓ Every alert investigated and resolved
- ✓ Accelerate value from your Microsoft security tools
- ✓ Consolidated visibility in one portal
- ✓ Guarantee of a 10-minute notification for Critical alerts and 60-minute or less Median Time to Resolution (**MTTR**) for ALL alerts, regardless of priority
- ✓ Triage and contain alerts anytime, from anywhere with MOBILE**SOC**®

Reduce risk with expanded MDR capabilities.

Critical Start Managed Detection and Response (**MDR**) services, delivered through our deep integration with Microsoft security solutions, go beyond a reactive, threat-based approach to provide additional capabilities aligned to proactive security. These include closing Endpoint control and Security Information and Event Management (**SIEM**) coverage gaps and providing essential **MITRE ATT&CK® Mitigations** recommendations.This risk-based approach empowers our Microsoft-certified analysts to focus on threat detection and effective response. Through our **Cyber Operations Risk and Response™ platform** and **Trusted Behavior Registry®** (**TBR®**), we provide integrated operations that map alerts to the **MITRE ATT&CK® Framework** and prioritize operational response, reducing risk and delivering a contractual 10-minute notification for Critical alerts and a 60-minute or less Time to Detection (**TTD**) and Median Time to Resolution (**MTTR**) for ALL alerts, regardless of priority.

Seamless integration for faster ROI.

Our services seamlessly integrate with your existing Microsoft security solutions, making rapid implementation easy and resulting in an immediate Return on Investment (**ROI**) from the enterprise-wide detection and response your organization needs to protect against ever-evolving and advanced attacks.

Resolving alerts is good. Resolving all alerts is better.

We are the only service provider that addresses all alerts regardless of priority status. Our MDR services leverage our platform to collect, understand, enrich, and resolve every incident across your Microsoft environment. We combine automation with human-led investigation and response to eliminate false positives at scale. This results in a drastic reduction in the number of alerts escalated to your team, freeing them up to focus on other high-priority projects.

Elite Risk and Security Operations Center (RSOC) capabilities at your side, at your service.

Whether you are looking to expand your SOC's capacity, optimize your tools' efficiency or both, our Microsoft security experts stand ready to extend the detection and response capabilities of your cybersecurity operations **24x7x365** through real-time monitoring, rapid investigation, continuous threat hunting, and response.

Anytime, anywhere: Never miss a threat with MOBILE**SOC**®.

Take threat detection and response on the go with our MobileSOC application, an iOS and Android app that puts the power of our platform in your hands, giving you the ability to triage, escalate, and isolate attacks from your phone. With our full-parity MobileSOC, you can see complete alert data, communicate directly with senior RSOC security analysts, and take immediate action with the information gathered and in coordination with your MDR team.

CRITICALSTART® PARTNER

How We Do It

Critical Start MDR

- **24x7x365** threat monitoring, investigation, and guided remediation via the Cyber Operations Risk and Response™ platform and expert RSOC analysts
- Risk mitigation on the go through our full-parity MobileSOC app
- Unified visibility across Microsoft Defender XDR and Defender for Servers
- Contractual 10-minute notification for Critical alerts and 60-minute or less TTD and MTTR SLAs
- Auto-response to common threats with expert escalation and human-initiated response actions
- Risk assessments (**NIST CSF**, etc.) to measure current posture against industry peer benchmarks

SIEM Security Services for Microsoft Sentinel

- MDR services plus management and optimization for Microsoft Sentinel performance while enriching detections through advanced threat intelligence for all 3rd party data sources like firewalls, CEF, SysMon, etc.
- Includes:
  - ✓ Ongoing management (Cost ingest analysis, Quarterly Service Reviews, and updates)
  - ✓ Identifying and resolving SIEM coverage gaps (including Zero-log Ingest Alert analysis, health monitoring, and log prioritization)
  - ✓ Preventing the same attacks from reoccurring by ensuring the right mitigations are implemented with **MITRE ATT&CK® Mitigation** recommendations
  - ✓ Custom detection rules and log sources, guided response recommendations, and detailed reporting
  - ✓ Detection content and Indicators of Compromise (**IOCs**) mapped to the **MITRE ATT&CK® Framework**

MDR for Microsoft Defender XDR

- Cross-domain threat protection, including real-time detection, disruption of attacks, robust identity monitoring, and RSOC response actions for:
  - ✓ Microsoft Defender for Office 365 (**MDO**)
  - ✓ Microsoft Defender for Identity (**MDI**)
  - ✓ Microsoft Entra Identity Protection (**ME-ID**)
  - ✓ Microsoft Defender for Cloud Apps (**MDCA**)

MDR for Defender for Servers

- Threat detection and response for dynamic server workloads across hybrid and multi-cloud environments
- Automated provisioning and tailored policies by asset criticality

MDR for Defender for Endpoint

- Endpoint coverage gaps identification and remediation (assets missing Endpoint Protection (**EPP**)/Endpoint Detection and Response (**EDR**)) to ensure full coverage and protection
- Visibility into threats across Windows, Mac, and Linux
- Integrated management with Defender for Servers

Microsoft Professional Services

- Readiness assessments, deployment assistance, and optimization services for Microsoft Security solutions
- Jumpstart Services to accelerate MDR services readiness

Incident Response Services

- Breach preparedness training
- Customized exercises to practice response
- Expert incident response retainer for immediate support

CRITICALSTART® PARTNER