

DATASHEET

CRITICALSTART® Managed Detection and Response Services for Microsoft Defender for Endpoint

KEY BENEFITS

- ✓ **Team expansion** with Microsoft Security expertise
- ✓ **Every endpoint** alert investigated
- ✓ **Guaranteed 60-minute or less** SLAs for Time to Detect (TTD) and Median Time to Resolution (MTTR)
- ✓ **Personalized playbooks** for the unique needs of your organization
- ✓ **100% visibility** consolidated in one portal
- ✓ **Containment of** infected devices
- ✓ **Tool configuration** and tuning
- ✓ **Triage and contain** alerts anytime, from anywhere with MOBILESOC®

At Critical Start, our Managed Detection and Response (MDR) service is all about simplifying your security. We built our MDR service for Microsoft Defender for Endpoint to go beyond monitoring alerts to help customers see attacks across hybrid device types and operating systems to reduce risk exposure, eliminate alert fatigue, and optimize Security Operations Center (SOC) efficiency.

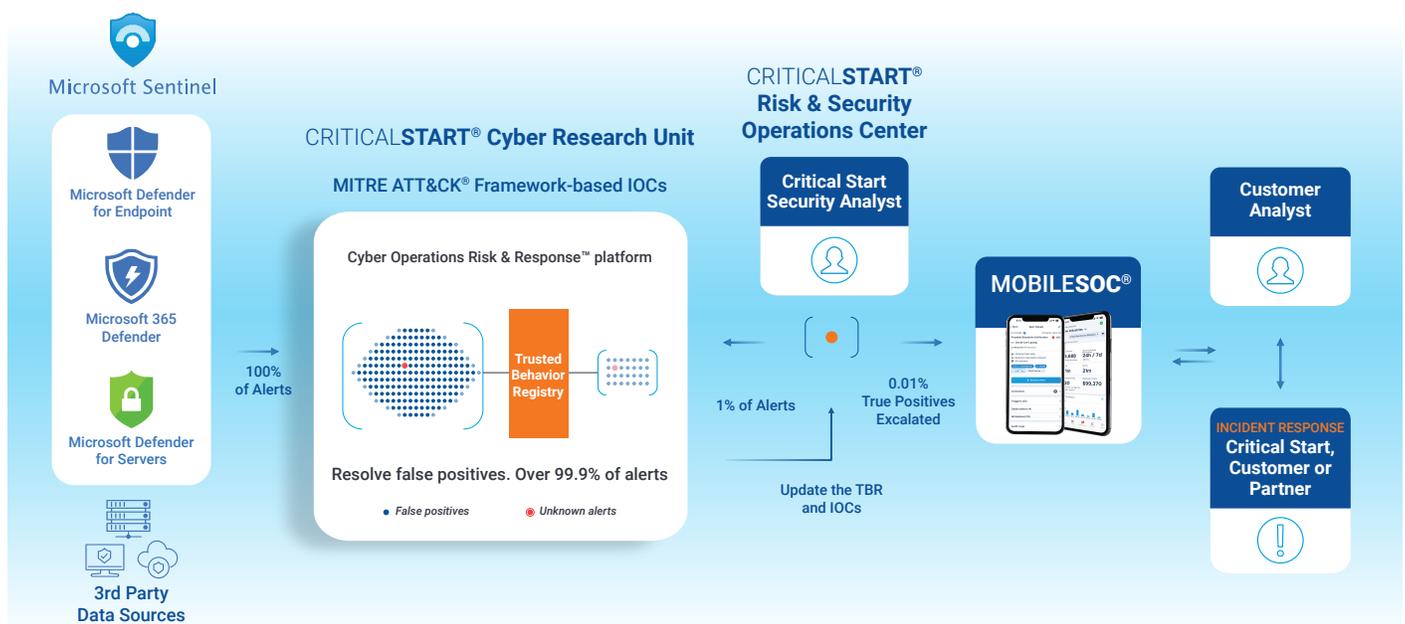
We detect the right threats and respond with the right actions

Critical Start does this by ingesting every alert from Microsoft Defender for Endpoint (MDE) into our **Cyber Operations Risk & Response™ platform**, the backbone of our MDR service. We compare alerts against known good behaviors in our purpose-built **Trusted Behavior Registry® (TBR®)**, where playbooks auto-resolve known good alerts. Alerts not identified by the TBR are escalated for investigation to the Critical Start Risk & Security Operations Center (RSOC), where our human-led service helps you make more accurate decisions on which response action to take.

How we do it

Resolving alerts is good. Resolving all alerts is better.

- ✓ Risk-based approach leverages the power of our platform and TBR to address all alerts
- ✓ We resolve more than 99.9% of alerts across Microsoft Security resources
- ✓ We escalate less than 0.01% of alerts—the alerts that really require the attention of your security team





Critical Start MDR services for Microsoft Defender for Endpoint leverage:

- ✓ Cross-operating system (Windows, Mac, Linux) Indicators of Compromise (IOCs)
- ✓ Microsoft Entra ID (formerly AAD) as an identity provider, single sign-on, and user provisioning management
- ✓ Microsoft automated alerts and actionable incidents
- ✓ Cross-signal context in device timeline investigations
- ✓ Ability to pivot directly to the device timeline from any generated IOC



Elite RSOC capabilities, at your side, at your service.

Whether you are looking to expand the capacity of your SOC, optimize the efficiency of your tools, or both, our highly proficient team of Microsoft security experts stand ready to extend the detection and response capabilities of your cyber security operations **24x7x365** through real-time monitoring, rapid investigation, and proactive response to endpoint alerts, with full-scale, complete alert resolution.

Our security experts:

- ✓ Are Microsoft Certified Security Operations Analyst Associates
- ✓ Use Microsoft Security Best Practices to deploy Microsoft Defender for Endpoint



So long, tedious IOC Management. Hello, optimized rules.

A key feature of the MDR service for MDE is IOC management. Microsoft is the fastest-moving security company today. IOCs are published and updated hourly across various locations. Leveraging the Critical Start manages, maintains, and curates MDE out-of-box detections and IOCs. Threat detection content is also mapped to the industry-leading **MITRE ATT&CK® Framework**.



Never miss a threat. Or your desk with MOBILESOC.

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 MobileSOC, you're able to see the full alert data, can communicate directly with senior RSOC security analysts, and can take immediate action with information gathered by tools and in coordination with your MDR team.