CRITICAL**START**

Microsoft

100%
Total Security Events
Generated Monthly

99.9%
Events Resolved by
Trusted Behavior Registry

.1%
Investigated

.01%

Escalated

Managed Detection and Response (MDR) services from CRITICAL**START**™ powered by Microsoft Threat Protection.

An **MDR Platform** Built to Resolve Every Alert

Using the power of Microsoft Threat Protection, CRITICAL**START** enables customers to centralize, ingest and correlate 100% of their logs to ensure their environment is secure. CRITICAL**START**'s MDR utilizes a Trusted Behavior Registry to investigate every alert generated until they are classified as known good and can be safely resolved. Customers see every action our CYBER**SOC** analysts take since our platform provides 100% transparency across the entire process.

Microsoft Threat Protection
Components and Benefits

Endpoints with Microsoft Defender ATP – A unified endpoint platform for preventative protection, post-breach detection, automated investigation, and response.

Email and collaboration with Office 365 ATP - Safeguards your organization against malicious threats posed by email messages, links and collaboration tools. Built-in Advanced email protection against phishing attempts, and unknown threats leveraging on 400B emails analyzed every month.

Identities with Azure ATP and Azure AD Identity Protection – Utilizing Active Directory signals to identify, detect, and investigate advanced threats, compromised identities, and malicious insider actions directed at your organization.

Applications with Microsoft Cloud App security - A comprehensive cross-SaaS solution bringing deep visibility, strong data controls, and enhanced threat protection to your cloud apps.

Enterprise with Azure Sentinel - A scalable, cloud-native, SIEM and SOAR solution that delivers intelligent security analytics and threat intelligence across the enterprise from on-premises and cloud signals, providing a single solution for alert detection, threat visibility, proactive hunting, and threat response.

Combined Together - Provides seamless integration across services and attack vectors to stop advanced threats and quickly detect anomalous behavior. Integrated detection across Endpoints, Identities and Office 365 helps to reduce false positives by contextually aggregating alerts together to identify attacks and create unique insights from trillions of signals.

CRITICALSTART

RESOLVE EVERY ALERT
Our cloud-based SOAR platform built to resolve 99.9% of security events

100% TRANSPARENCY
Nothing to hide – Customers view the same data as CRITICALSTART's SOC analysts

INDUSTRY'S FIRST MOBILESOC™
Direct communication with SOC analysts on the go with native iOS and Android app

24x7x365 MDR
Provided by highly experienced analysts and incident responders

SOCREVIEW
Two-person integrity review process designed to eliminate human error

ADAPTABILITY
Extends the one-size-fits-all approach to fit the unique processes of each customer

THE CRITICALSTART DIFFERENCE:
REDUCES DWELL TIME

TALK TO AN MDR SPECIALIST
To see how we can help, contact us at criticalstart.com