CRITICALSTART

Managed SIEM services with Microsoft Azure Sentinel

A simple yet comprehensive approach to magnify security visibility and stop breaches for Microsoft security customers.

CRITICAL**START™ managed SIEM services with Microsoft Azure Sentinel compound the security value provided by Microsoft security tools by leveraging our considerable multi-platform SIEM expertise, comprehensive Microsoft integration, and our trust-oriented approach to MDR which eliminates false positives at scale.**

The Key Benefits of the Integration

With experience across multiple verticals/industries, CRITICAL**START** provides expert guidance around how to deploy Azure Sentinel in your Microsoft environment and optimize your log data sources for effective threat detection.

For customers already using Microsoft security tools, CRITICAL**START** Managed SIEM services for Azure Sentinel allow you to accelerate return on your Microsoft security investments, gain full visibility of your Microsoft environment, and tighten your security strategy to protect assets.

SIEM Expertise

The SIEM engineering team at CRITICAL**START** has a collective 100+ years of experience managing over 50PB of data including environments greater than 20PB in size.

Trust-Oriented MDR Approach

The Trusted Behavior Registry (TBR) automatically resolves what is known-good and can be safely addressed first – shifting focus to unknown alerts for triage and quick resolution. With 24x7x365 monitoring, our highly skilled analysts work in a SOC 2 Type 2 certified Security Operations Center (SOC) to investigate, escalate, contain, and respond to threats – helping to significantly reduce attacker dwell time. CRITICAL**START** allows limitless detections in Azure Sentinel – our service sees through the noise.

Comprehensive Integration

Unlike other managed security services, our Azure Sentinel MDR service uses the Microsoft ecosystem of tools and user behavior analytics to provide a unique solution for effective threat detection and response. Integration with Microsoft security tools is focused on Azure principals of least privilege and investigations that take advantage of user- based detections in Azure Sentinel. This all-in on security approach is applied at every security layer – least privilege, rule creation and integration points.

CRITICAL**START** is a Microsoft MSSP Pilot Program Partner, and a member of the Microsoft Intelligent Security Association (MISA).

MOBILE**SOC**

CRITICAL**START** offers native iOS and Android apps to give analysts full access to their MDR toolset on the go. Within the fully featured app, analysts can investigate alerts, communicate with CRITICAL**START** Security Experts, and respond, all without needing a computer.

CRITICALSTART