CRITICAL**START** Managed Detection and Response Services with Microsoft Azure Sentinel

Azure Sentinel

CRITICAL**START**™ Managed Detection and Response (MDR) Services with Microsoft Azure Sentinel provide a radical approach to threat detection and response built for your Microsoft business security challenges. Together, CRITICAL**START** MDR and Azure Sentinel focus on both containment and recovery actions for the Microsoft 365 Defender Security Suite —we don't stop at detection. We reduce risk acceptance and magnify security visibility by focusing on what makes Azure Sentinel different from other SIEMs.

MDR reinvented. SIEM reinvented. An integrated threat detection and response solution for the modern world that's more than good, *it's better.*

What sets us apart?

We do what others don't. CRITICAL**START** has built a MDR service that goes beyond just monitoring alerts to bring shared responsibility for cyber incident response and recovery using Microsoft Azure Sentinel. Azure Sentinel is raising the bar on what a SIEM should deliver in a security program –smarter investigation with context across security tools and faster threat response and recovery. It's not only good, but *better* to combine that with CRITICAL**START** MDR services built on the premise that *acceptable risk shouldn't be.*

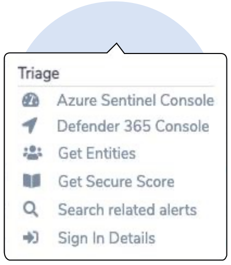
How we do it.

Unmatched investigations. Exceptional response. Leveraging Microsoft automated investigations and actionable incidents, our MDR service modulates and adapts for identity, checks for globally trusted behaviors, and escalates risky sign-ins, logons from unfamiliar IPs, and impossible travel violations for validation with enriched data. If a user is deemed not risky, CRITICAL**START** can dismiss the user's risk, allowing them access again. We can also confirm a user has been compromised following an investigation. As we learn about customer environments, tailored Trusted Behaviors in the Zero Trust Analytics Platform (ZTAP) allow CRITICAL**START** security analysts to focus future investigations, increasing alert effectiveness over time, not just during tuning or onboarding.

Integration, the better way.

Unlike other managed security services, CRITICAL**START** MDR services with Microsoft Azure Sentinel leverage:

- ✓ Microsoft User and Entity Behavior Analytics (UEBA) in every escalated alert, which increases the likelihood of detecting a true positive at multiple parts of the kill chain
- ✓ Azure Active Directory as an identity provider, single sign-on, and privileged access management for Security Operations Center (SOC) access
- ✓ Auto-Incident Response (IR) verdicts and conditional access policies to speed up response and recovery across the Microsoft 365 Defender Security Suite



Triage

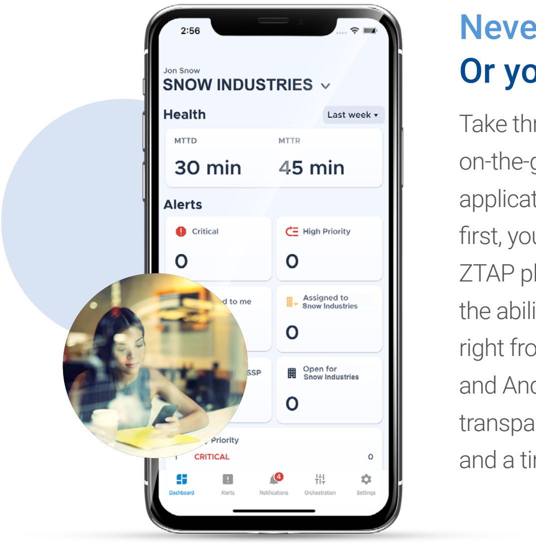
- Azure Sentinel Console
- Defender 365 Console
- Get Entities
- Get Secure Score
- Search related alerts
- Sign In Details

Not more resources. Better ones.

Our Security Information and Event Management (SIEM) engineering team has a collective 100+ years of experience and over 50PB of data management experience, including environments greater than 20PB in size. The team uses Microsoft Security Best Practices to deploy Azure Sentinel and Microsoft Defender 365 tools to optimize Microsoft content for both Scheduled Query Rules and Indicators of Compromise (IOCs).

So long, tedious IOC Management. Hello optimized rules.

A key feature of the MDR service with Azure Sentinel is IOC management. Microsoft is the fastest-moving security company today. IOCs are published and updated hourly across different locations. The process of publication and application of additional detections can be hard to manage and a full-time job, so we added this feature in the service for no additional cost.



2:56

Jon Snow
SNOW INDUSTRIES

Health — Last week

MTTD 30 min
MTTR 45 min

Alerts

Critical 0
High Priority 0
d to me
Assigned to Snow Industries 0
SSP
Open for Snow Industries 0

Priority
CRITICAL 0

Never miss a threat. Or your desk.

Take threat detection and response on-the-go with the MOBILE**SOC** application. An industry-leading first, you have the power of our ZTAP platform in your hands, with the ability to contain breaches right from your phone. Our iOS and Android app features 100% transparency, with full alert detail and a timeline of all actions taken.

KEY BENEFITS OF THE INTEGRATION

- ✓ Extend your team with threat detection and response expertise.
- ✓ Speed up investigation and response in one portal.
- ✓ Consolidate automation containment and recovery playbooks.
- ✓ Accelerate value from your Microsoft security investments .
- ✓ Trigger incident validation for compliance-related violations.
- ✓ Triage and contain alerts from anywhere with CRITICAL**START** MOBILE**SOC.**

DID YOU KNOW?

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

CRITICALSTART
They're good. We're better.

Capability Comparison

● COMPLETE OFFERING
◐ PARTIAL OFFERING
✕ NO OFFERING

	CRITICALSTART MDR + Microsoft Azure Sentinel	Other Managed SIEM/MDR Providers
Perform configuration, deployment, and health checks without requiring additional professional services	●	✕
Leverage Microsoft user-based detections	●	●
Keep Microsoft template rules up-to-date	●	✕
Investigate every user	●	✕
Audit all user access to customer environments	●	✕
Use cross-Microsoft correlations in investigations	●	●
Perform cross- and multi-tenant management without requiring Azure Lighthouse	●	✕
Enable one-click enterprise enrollment consent	●	✕
Auto-Incident Response (IR) aware investigations	●	✕
Close and comment on all false positive investigations in Azure Sentinel	●	✕
Complete recovery response actions	●	✕
Manage and maintain cross-ecosystem IOCs	●	✕
Leverage multiple Microsoft security tools for response	●	✕

Member of
Microsoft Intelligent Security Association
Microsoft

Gold
Microsoft Partner
Microsoft

Goodbye, alert fatigue. Hello, CRITICALSTART.

Contact Us

Request a Free Assessment

CRITICALSTART
They're good. We're better.