CRITICALSTART®

SOLUTION BRIEF

Achieve full Microsoft Sentinel™ operating potential

Managed Detection & Response Services
Managed SIEM Services
Microsoft Security Consulting Services

Optimize Sentinel for threat detection use cases

As security becomes more strategic, fully cloud native SIEM solutions with robust security analytics and cross-domain threat intelligence, like Microsoft Sentinel, become an integral part of an effective security program.

However, most SIEM solutions are not configured and deployed sufficiently for threat detection use cases. Organizations need a solution that can help them optimize Microsoft Sentinel for true security outcomes.

Our Approach

Our Microsoft security experts help you sort out the highest-fidelity telemetry, which you can use to take actions and leverage for specific detections or enrichment purposes. We then provide 24x7x365 monitoring and investigation of Microsoft Sentinel and manage the hundreds of out-of-the-box Indicators of Compromise (IOCs) published by Microsoft.

> Monthly, we look at 10 to 12 million alerts. Of that, about 250-300 are escalated to our team. Because Critical Start takes care of the Tier 1 and Tier 2 triage for us, only true positives are escalated to us for investigation. On a weekly basis, this saves us close to 50 to 60 hours.
>
> **-SR. MANAGER, SECURITY ENGINEERING FINANCIAL SERVICES**

KEY SOLUTION BENEFITS

Accelerate ROI and gain visibility

Not all log sources are created equal. We work with you to define a deployment roadmap aligned to your goals and prioritize the data to be ingested across your environment.

Reduce the noise

SIEMs are noisy. Leveraging our seamless integration with Microsoft Sentinel, our Zero Trust Analytics Platform™ (ZTAP™) automates the investigation and triage of alerts and incidents across all users, devices, applications and infrastructure. ZTAP removes the false positives and escalates true positives to the Critical Start Security Operations Center (SOC) for enrichment and investigation.

Improve security posture

Your environment and objectives will evolve. We give you the flexibility to strategically add new data sources while continuously validating against the industry-leading MITRE ATT&CK® Framework for coverage against the latest techniques, tactics and procedures (TTPs).

Increase productivity

We do the heavy lifting for you as our team investigates escalated alerts and incidents and curates out-of-the box detections and IOCs. A named Customer Success Manager (CSM) ensures you are receiving the tools and support for continuous security improvement.

CRITICALSTART®

KEY SOLUTION FEATURES

Microsoft Sentinel Workshop

Learn more about the features and benefits of Microsoft Sentinel and how to integrate it into your existing security program.

Microsoft experts at your service

Our Microsoft-certified security staff has deep experience with Microsoft tools and uses Microsoft Security Best Practices. Team members have MS-500: Microsoft 365 Security Administration, SC200 and AZ-500: Microsoft Azure Security Technologies certifications.

Detection engineering expertise

Our detection engineering team has 100+ years of collective experience curating content to ensure detections are working across multiple threat vectors and industries.

Resolution of all alerts

We take a different approach than most MDR providers by resolving every alert and only forwarding those that truly warrant additional investigation.

Triage on the go

An industry-leading first, MOBILE**SOC®,** an iOS and Android application, let's you contain breaches right from your phone. It features 100% transparency, with full alert detail and a timeline of all actions taken.

Managed SIEM services for Microsoft Sentinel

Maximize the value of your Sentinel investment and stop struggling with the deployment, maintenance and staffing. We take responsibility for the back-end components of your Sentinel solution and relieve you of the burden of maintaining your application, including managing version updates and application performance.

For more information about Critical Start services and solutions for Microsoft Security, schedule a demo at:
www.criticalstart.com/contact/request-a-demo/

About Critical Start

Today's enterprise faces radical, ever-growing, and ever-sophisticated multi-vector cyber-attacks. Facing this situation is hard, but it doesn't have to be. Critical Start simplifies breach prevention by delivering the most effective managed detection and incident response services powered by the Zero Trust Analytics Platform™ (ZTAP™) with the industry's only Trusted Behavior Registry™ (TBR) and MOBILE**SOC®**. With 24x7x365 expert security analysts, and Cyber Research Unit (CRU), we monitor, investigate, and remediate alerts swiftly and effectively, via contractual Service Level Agreements (SLAs) for Time to Detection (TTD) and Median Time to Resolution (MTTR), and 100% transparency into our service. For more information, visit criticalstart.com. Follow Critical Start on LinkedIn, @CRITICALSTART, or on Twitter, @CRITICALSTART.

Member of
Microsoft Intelligent Security Association

Microsoft

Gold
Microsoft Partner

Microsoft

CRITICALSTART®