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 Security Information and Event Management (**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 in a way sufficient 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.

KEY SOLUTION BENEFITS

Maximize the productivity of your team

Our security experts handle the heavy lifting around your SIEM implementation and management. We optimize your SIEM with dedicated operational services, including functional updates and version upgrades, so your team can focus on other business priorities.

Optimize financial stewardship & simplify resource management

We help manage your operating costs for SIEM by ensuring you are ingesting the right security data to get the most value from your threat-detection use cases. Critical Start helps you efficiently allocate resources—like understanding what type of log storage is best for your business—which decreases your in-house requirements and results in lower costs for your business.

Data when & where you need it

Configure and personalize your SIEM solution with customized SIEM dashboards, reports, and log sources to support your specific security, risk, compliance, and audit use cases. In addition, you can leverage “single pane of glass” datapoints to prove the value of your SIEM to your executive team.

Enhance your detection coverage & security posture

We map your threat detection content to the industry standard **MITRE ATT&CK® Framework** and provide the foundation to help you achieve optimal Managed Detection and Response (**MDR**) coverage and outcomes. We help you keep up with new threats and compliance requirements by ensuring your SIEM data is being properly ingested and the right detection content is being applied to your log sources. SIEM Coverage Gaps help avoid misconfigurations and we ensure your SIEM is running at optimal capacity with log source performance, Zero-Log Ingest Alerts, and availability and capacity monitoring to identify potential issues with log ingestion.

> “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 FEATURES

Microsoft Sentinel Workshop

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

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 AZ-500 Azure Security Engineer Associate, SC-200 Security Operations Analyst Associate, and SC-300 Identity and Access Administrator Associate 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, regardless of criticality, and only forwarding those that truly warrant additional investigation.

Triage on the go

Our industry-leading MOBILE**SOC**® iOS and Android application lets you manage risk and contain breaches right from your phone. Leverage access to 100% transparency on the go, showing a unified view that includes full alert and investigation details and a timeline of all actions taken.

Managed SIEM services for Microsoft Sentinel

Maximize the value of your Sentinel investment and stop struggling with 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.

Microsoft Intelligent Security Association

Microsoft Security

Microsoft Verified Managed XDR Solution

Microsoft Solutions Partner

Security

Specialist

Cloud Security

Threat Protection

CRITICALSTART®

For more information about Critical Start services and solutions for Microsoft Security, schedule a demo at:

www.criticalstart.com/contact/request-a-demo/

© 2024 CRITICAL**START**. All rights reserved.