SOLUTION BRIEF

Protection beyond the endpoint: SIEM + XDR

Managed Detection & Response Services
Microsoft Security Consulting Services

Strengthen SIEM + XDR defenses to stay ahead of advanced attacks

Security Information and Event Management (**SIEM**) solutions ingest event logs and offer a single view of this data with additional insights. Extended Detection and Response (**XDR**) solutions break down traditional security silos to deliver detection and response across all data sources, including endpoint, network, and cloud data, while applying analytics and automation to address increasingly sophisticated threats.

Organizations need a solution that helps them navigate each technology's limitations and challenges and brings them together to increase efficiency and security effectiveness across the entire organization.

Our Approach

We help you get past the complexity of SIEM and XDR by diving in deep to understand your existing security controls. Our Microsoft Consulting Services team offers workshops focused on helping you achieve your broader security objectives with SIEM + XDR.

Managed Detection and Response (**MDR**) services provide **24x7x365** cross-domain threat protection with capabilities that go beyond the endpoint to detect, investigate, and respond to alerts and incidents across your Microsoft ecosystem.

KEY SOLUTION BENEFITS

Enhance protection for advanced use cases

Given the volume and complexities of identities, data, applications, and infrastructure, learning how to secure your organization and mitigate and protect against threats moving forward is essential. The Microsoft experts at Critical Start work with you to develop a strategic plan customized to your organization's priorities. MDR services, powered by the industry's only **Cyber Operations Risk & Response™ platform**, provide comprehensive coverage against advanced threats targeting endpoints, identity, email, and cloud.

Extend your capabilities to detect and respond

When minutes count, our team can become an extension of your team and provide remediation and response actions to the threat as soon as it's detected. You get 24x7x365 MDR, management of out-of-the-box indicators of compromise (**IOCs**), freedom from intelligence overload, and visibility across your Microsoft ecosystem—all in one portal.

Strengthen your security posture

Your goal is to stay ahead of advanced threats. Our Microsoft experts help you understand your environment and map a deployment strategy. With Microsoft Security and Critical Start MDR, you have access to integrated threat protection that speeds up investigation and response beyond the endpoint. IOCs are mapped to the **MITRE ATT&CK® Framework** for visibility into detection coverage from your security controls and current adversarial activity in your environment.

Increase productivity

We do the heavy lifting for you, so your team can focus on what matters. Our team investigates escalated alerts and incidents and curates out-of-the-box Microsoft detections and IOCs. Our team can respond on your behalf and work with your team until remediation is complete. A named Customer Success Manager (**CSM**) ensures you are receiving the tools and support for continuous security improvement.

KEY SOLUTION FEATURES

Microsoft Workshops
Learn more about the features and benefits of Microsoft Sentinel and the Microsoft Defender security suite. Through available workshops, our team helps you gain visibility into immediate threats across email, identity, and data, plus clarity and support on upgrading your security posture for the long term.

Microsoft experts at your service
Our Microsoft-certified security staff has deep experience with Microsoft tools and uses Microsoft Security Best Practices. Team members are Microsoft Certified as Security Operations Analyst Associates (Threat Protection Designation) and in Exam AZ-500: Microsoft Azure Security Technologies (Cloud Security Specialization).

Direct-action responses
Minutes count. While other MDR providers may only give the user recommended actions, Critical Start has natively integrated our web interface and MOBILE**SOC**® mobile application with Microsoft Defender XDR APIs to create a single interface to perform manual and automated response actions. False positives are automatically resolved with our platform. True positives are escalated to our security analysts for further investigation and response.

Triage on the go
An industry-leading first, MobileSoc, an iOS and Android application, lets you contain breaches right from your phone. It features 100% transparency, with full alert detail and a timeline of all actions taken.

What Critical Start has done with its MDR service for Microsoft 365 Defender is a game changer for my team. It's turned a 2am problem into a 9am problem. Our analysts now have the capability to disrupt and contain an attack with the click of a button as soon as the attack occurs. They then can go back to assess the scope and restore later.

- SECURITY OPERATIONS MANAGER, FINANCIAL SERVICES, MICROSOFT SENTINEL, MICROSOFT DEFENDER FOR ENDPOINT, MICROSOFT DEFENDER XDR USER

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/