CRITICAL**START**.

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 bring them together to increase efficiency and security effectiveness across your entire organization.

Our Approach

We help you get past the complexity with 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, it's essential to learn how to secure your organization and mitigate and protect against threats moving forward. 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 Zero Trust Analytics Platform™ (ZTAP™), 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 the leader in MDR, you have access to integrated threat protection that speeds up investigation and response beyond the endpoint. Indicators of Compromise (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.

CRITICALSTART®

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 how to upgrade 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 have MS-500: Microsoft 365 Security Administration, SC200 and AZ-500: Microsoft Azure Security Technologies certifications.

Direct-action responses

Minutes count. While other MDR providers may only give recommended actions for the user to take, Critical Start has natively integrated our web interface and MOBILE**SOC**® mobile application with Microsoft 365 Defender APIs to create a single interface to perform manual and automated response actions. False positives are automatically resolved with our Zero Trust Analytics Platform™(ZTAP™). True positives are escalated to our security analysts for further investigation and response.

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.

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.