

SOLUTION BRIEF

Optimize Your Security Tools' Detection & Operational Effectiveness

Managed Detection & Response Services

Are multiple security tools complicating threats detection?

Are you concerned about gaps in your threats coverage?

You're not alone: As technology and digital transformation has grown, attacks from threat actors are more complex than ever. **The security toolchain of a typical organization employs 76 tools to manage, and those with 10,000 employees or more have, on average, 96 tools¹.**

This results in:

- Complexities in configuring, deploying, and maintaining so many tools
- Threats evading security controls
- Heightened pressure to reduce Median Time to Detect (**MTTD**) and Median Time to Respond (**MTTR**) to threats

Increase Your Tools' Effectiveness with Managed Detection & Response

CRITICAL**START**® MDR services allow companies to reduce risk, maximize team efficiency and improve detection effectiveness. We integrate with all your tools and increase visibility across controls. By measuring all your security controls' effectiveness and coverage, you'll have greater confidence in your security program.

Our Approach

Our Managed Detection and Response (**MDR**) services optimize your security controls by providing complete coverage to respond and remediate threats faster.

By integrating with multiple vendors' technologies, we consolidate visibility across security tools, so you have a clear picture of performance and coverage gaps.

Our 24x7x365 security operations center (**SOC**) augments your team by continuously deploying new detections to your security tools based on the latest curated threat intelligence.

We struggled to maintain and deploy the large number of security tools we were using – especially since we had limited security personnel. We were also concerned that we didn't have complete coverage and threats could slip through.

*With Critical Start MDR services, we're confident that attacks are effectively detected, because we have greater visibility into our security tools' performance mapped to the **MITRE ATT&CK**® Framework. Critical Start also partners with us to add new detections.*

- CISO, FINANCIAL SERVICES



Figure 1: Critical Start MDR services provides a real-time, actionable view of attacks with step-by-step response guidance.

¹ 2023 Security Leaders Peer Report, Panaseer.

KEY SOLUTION BENEFITS

Optimize and operationalize security controls

Our Zero Trust Analytics Platform™ (ZTAP®) dashboards leverage the latest threat detection technologies that enable security teams to generate useful data for visibility across the security toolchain. The result is a comprehensive understanding of your risk profile and key operational metrics such as total number of events monitored, MTTD, MTTR and false positive alerts.

Our customer success and SOC teams' partner with you to provide personalized 24x7 coverage. We provide a seamless onboarding process, partnering with our security experts to build a customized program based on your use cases, controls and alerts. Our customer success teams provide ongoing guidance and help you protect critical assets as every single activity is monitored to prevent a breach.

Integration with your security tools

Disparate security tools increase risk and may result in threat actors slipping through your defenses. Our MDR services integrate with your existing security tools, so you'll have complete visibility and detection effectiveness. We use the MITRE ATT&CK® Framework to enforce, manage and maintain effective detection content. Our security experts partner with you to make risk-based decisions on attack coverage.

Minimize risks

We don't take a cookie-cutter approach to security. Our team goes beyond out-of-the-box detections by continuously adding new Indicators of Compromise (IOCs) to your security tools based on the latest curated threat intelligence and other sources. This improves your security tools' alert effectiveness to quickly pinpoint threats and hasten remediation.



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

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