MXDR

Managed eXtended Detection & Response

Extend your security operations with a 24×7 managed SOC helping across the security lifecycle

Today's threat landscape is increasingly complex and treacherous. Sophisticated attacks, such as supply chain, ransomware, and fileless malware, occur regularly. Typical managed detection & response (MDR) services take a lowest common denominator approach that doesn't adapt to the unique attributes and needs of different businesses. Logs flow into a black hole, leaving you guessing if you have effective detection coverage to identify threats across the business.

Our MXDR leverages an interactive, risk-focused methodology across the entire security lifecycle—from prevention to detection to response—keeping you one step ahead of the latest threats. During a goal-focused onboarding, our team learns where your data resides, what systems you use, and how you operate to develop a personalized plan of action to rapidly strengthen security postures.

Our team utilizes the advanced security features built into our security platform to help enhance your prevention and detection. When an incident occurs, our team is with you every step of the way, utilizing an array of rapid response options such as host isolation, LAN ZeroTrust, firewall updates, and more to shut down attacks in their tracks.

Benefits

Unmatched Threat Detection
With complete visibility across your environments, our 24×7 SOC detects threats others miss across endpoint, user, networks, cloud, and more

Expert Response
Our 24×7 SOC consists of former NSA analysts, Air Force cybersecurity specialists, and leaders at enterprise incident response companies with deep experience responding to large scale incidents

Continuously Stronger Security
We work with you on an ongoing basis to strengthen your security, providing countermeasure and prevention control recommendations, security strategies, and more

Highlights

24×7 Security Operations Center
Our team of experts works around the clock, vigilantly monitoring your environments for earlier detection, faster investigation, and rapid response.

Complete Visibility
Leveraging our Managed Cloud SIEM, the MXDR team helps prioritize integrations across user, network, endpoint, cloud, hardware firewalls, SaaS apps, and other tools for holistic coverage.

Visibility Analysis and Custom Detection Rules
We help eliminate blind spots by increasing visibility across your security and technology stack while creating custom detection rules to ensure effective detection coverage.

Continuous Threat Hunting
The MXDR team's highly trained security experts leverage global threat insights, intelligence sources, and sophisticated technology to conduct proactive threat hunting.

Our MXDR Experience

Onboarding

Understand Your Environments
Learn about your applications, systems, networks, and data

Develop Plan of Action
Synthesize inputs to identify gaps in detections, visibility, prevention controls, compliance requirements, and security posture

Ongoing Enhancement

Incident and Security Posture Review
Recap of prior month and provide recommendations to improve your security posture

Prevention Control Review & Recommendations
Review recently implemented controls and provide an overview of what's next

Visibility, Custom Detections, and Reporting
Assess progress on your visibility coverage based on current ingestion, custom detection rules, and identification of new reporting or visibility needs

Threat Hunting Recap & Countermeasure Recommendations
Recap of threat hunts conducted during the month and countermeasure recommendations to defend against findings

24x7 Threat Detection & Response

Triage and Investigate
Analyze and investigate incidents around the clock to determine the impact, scope, severity, and risk

Expert Response
Containment support, remediation guidance, and post-incident assessments to help eliminate threats faster

Proactive Threat Hunting
Ongoing threat hunting for the latest TTPs to find persistent threats

Contact us today at 210-761-3332 to learn how our 24×7 managed SOC and MXDR team can help you stay one step ahead of the latest threats.