todyl

MXDR
Managed eXtended Detection & Response

Extend your security operations with a 24×7 managed SOC and dedicated account manager 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.

Todyl's 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, Detection & Response Account Managers (DRAMs) learn where your data resides, what systems you use, and how you operate to develop a personalized plan of action to rapidly strengthen security postures.

DRAMs utilize the advanced security features built into the Todyl Security Platform to help enhance your prevention and detection. When an incident occurs, the MXDR 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, Todyl's 24×7 SOC detects threats others miss across endpoint, user, networks, cloud, and more

Expert Response
Todyl's MXDR team 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
Todyl works with you on an ongoing basis to strengthen your security, providing countermeasure and prevention control recommendations, security strategies, and more

Highlights

True Extension of your Team
You get a named Detection & Response Account Manager (DRAM) assigned to your account who meets with you monthly for full transparency and ongoing optimization.

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

Direct Lines of Communication
Direct access to Todyl's team of experts via Slack or Microsoft Teams.

Visibility Analysis and Custom Detection Rules
DRAMs 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 Todyl's global threat insights, intelligence sources, and sophisticated technology to conduct proactive threat hunting.

Todyl's MXDR Difference

Onboarding

Understand Your Environments

Learn about your applications, systems, networks, and data

Deep Dive on Your Customers

Understand your risk profile, compliance requirements, their industry's threat landscape, and what keeps you up at night

Develop Plan of Action

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

Monthly Touchpoints

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

Use Case of the Month

Explanation of new attacker tactics, techniques, and procedures (TTPs)

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

Slack and Microsoft Teams Integration

Ongoing intelligence updates, countermeasure recommendations, and access to our team of experts