SOPHOS

XIGENT
Result Driven IT

Managed Threat Response (MTR)

Expert-Led Threat Response

Sophos Managed Threat Response (MTR) provides 24/7 threat hunting, detection, and response capabilities delivered by an expert team as a fully-managed service.

Highlights

- Advanced threat hunting, detection, and response capabilities delivered as a fully- managed service
- Collaborate with a 24/7 response team that takes action to remotely contain and neutralize threats
- You decide and control what actions the MTR team takes and how incidents are managed
- Combines top-rated machine learning technology with a highly-trained team of experts
- Two tiers of service (Standard and Advanced) provide a comprehensive set of capabilities for organizations of all maturity levels

Threat Notification Isn't the Solution – It's a Starting Point

Few organizations have the right tools, people, and processes in-house to effectively manage their security program around-the-clock while proactively defending against new and emerging threats. Going beyond simply notifying you of attacks or suspicious behaviors, the Sophos MTR team takes targeted actions on your behalf to neutralize even the most sophisticated and complex threats.

With Sophos MTR, your organization is armed with a 24/7 team of threat hunters and response experts who will:

- Proactively hunt for and validate potential threats and incidents
- Use all available information to determine the scope and severity of threats
- Apply the appropriate business context for valid threats
- Initiate actions to remotely disrupt, contain, and neutralize threats
- Provide actional advice for addressing the root cause of recurring incidents

Machine-Accelerated Human Response

Built on our Intercept X Advanced with EDR technology, Sophos MTR fuses machine learning technology and expert analysis for improved threat hunting and detection, deeper investigation of alerts, and targeted actions to eliminate threats with speed and precision. This fusion of Sophos' consistently top-rated endpoint protection and intelligent EDR, with a world-class team of security experts results in what we call "machine-accelerated human response."

Complete Transparency and Control

With Sophos MTR, you own the decisions and control how and when potential incidents are escalated, what response actions (if any) you want us to take, and who should be included in communications. Sophos MTR features three response modes so you can choose the best way for our MTR team to work alongside you during incidents:

Notify: We notify you about the detection and provide detail to help you in prioritization and response.

Collaborate: We work with your internal team or external point(s) of contact to respond to the detection.

Authorize: We handle containment and neutralization actions and will inform you of the action(s) taken.

Sophos MTR Service Tiers

Sophos MTR features two service tiers (Standard and Advanced) to provide a comprehensive set of capabilities for organizations of all sizes and maturity levels. Regardless of the service tier selected, organizations can take advantage of any of the three response modes (notify, collaborate, or authorize) to fit their unique needs.

Sophos MTR: Standard

24/7 Lead-Driven Threat Hunting

Confirmed malicious artifacts or activity (strong signals) are automatically blocked or terminated, freeing up threat hunters to conduct lead-driven threat hunts. This type of threat hunt involves the aggregation and investigation of causal and adjacent events (weak signals) to discover new Indicators of Attack (IoA) and Indicators of Compromise (IoC) that previously could not be detected.

Security Health Check

Keep your Sophos Central products--beginning with Intercept X Advanced with EDR--operating at peak performance with proactive examinations of your operating conditions and recommended configuration improvements.

Activity Reporting

Summaries of case activities enable prioritization and communication so your team knows what threats were detected and what response actions were taken within each reporting period.

Adversarial Detections

Most successful attacks rely on the execution of a process that can appear legitimate to monitoring tools. Using proprietary investigation techniques, our team determines the difference between legitimate behavior and the tactics, techniques, and procedures (TTPs) used by attackers.

Sophos MTR: Advanced *Includes all Standard features, plus the following:*

24/7 Leadless Threat Hunting

Applying data science, threat intelligence, and the intuition of veteran threat hunters, we combine your company profile, high-value assets, and high-risk users to anticipate attacker behavior and identify new Indicators of Attack (IoA).

Enhanced Telemetry

Threat investigations are supplemented with telemetry from other Sophos Central products extending beyond the endpoint to provide a full picture of adversary activities.

Proactive Posture Improvement

Proactively improve your security posture and harden your defenses with prescriptive guidance for addressing configuration and architecture weaknesses that diminish your overall security capabilities.

Dedicated Threat Response Lead

When an incident is confirmed, a dedicated threat response lead is provided to directly collaborate with your on-premises resources (internal team or external partner) until the active threat is neutralized.

Direct Call-In Support

Your team has direct call-in access to our security operations center (SOC). Our MTR Operations Team is available around-the-clock and backed by support teams spanning 26 locations worldwide.

Asset Discovery

From asset information covering OS versions, applications, and vulnerabilities to identifying managed and unmanaged assets, we provide valuable insights during impact assessments, threat hunts, and as part of proactive posture improvement recommendations.

Xigent
Tel: 800-298-9543
Web: www.xigentsolutions.com

North American Sales
Toll Free: 1-866-866-2802
Email: nasales@sophos.com

2019-09-17 DS (GH)

XIGENT Result Driven IT

SOPHOS