Cisco Managed Detection and Response (MDR)

Overview

Today, companies are experiencing a higher risk of breach than ever before. They are unable to recruit and retain security expertise, keep pace with current threats, and a rapidly expanding attack surface. These challenges along with an overwhelming number of alerts create an increased risk to the business.

Cisco Managed Detection and Response (MDR) combines an elite team of researchers, investigators, and responders with threat intelligence, automation and response capabilities, and defined investigation and response playbooks supported by Cisco Talos® threat research. MDR can reduce the time to detect and respond from months to hours. The service leverages Cisco’s world-class integrated security architecture to advance security operations capabilities by delivering industry-leading, 24x7x365 threat detection and response to reduce mean time to detect and contain threats faster with relevant, meaningful, and prioritized response actions.

Benefits

- A stronger security posture that protects against threats with an expert team of researchers, investigators, and responders
- Advanced security operations with a Cisco threat intelligence and automation
- Management and prioritization of alert volume across cloud, network, and endpoints with defined investigation and response playbooks
- Powerful integrated security architecture providing greater visibility
- 24x7x365 analysis, investigation, and response to improve meantime-to-detect and mean-time to respond to security threats
Detection, Analysis, Investigation and Response with MDR

Elite researchers, investigators and responders in our global centers are alerted in near-real time to alerts occurring within your cloud, on-premises networks, and endpoints. We engage with you to advance your security operations capabilities by providing clarity on attacks and expert guidance on how to eliminate threats quickly and prevent breaches. MDR includes:

- **Detection**, uses an integrated cloud security ecosystem that improves mean time to detect and contain security threats. The service delivers relevant, high-confidence, and consistent results using proven methodologies, unique intelligence, and an experienced team.

- **Analysis**, through the enrichment of alerts, including Talos threat intelligence. MDR provides attacker attributes and tactics to analysts along with the critical context needed to prioritize the impact and urgency of a threat to an organization.

- **Investigation** of identified threats utilizing defined investigation playbooks, which provide added context. When malware, ransomware, botnet, bad actors, and other such bad behavior occurs, we make data-driven decisions that establish relevant, meaningful, and prioritized response actions.

- **Response** utilizes security orchestration and automated response (SOAR) and case management to execute defined response playbooks to provide detailed threat analysis, including recommended response actions.

- **Cisco Talos Intelligence Group**, the largest non-governmental threat intelligence research team in the world provides integrated threat intelligence that protects the Cisco MDR security technologies.

- Coordination with **Cisco Talos Incident Response** for breach and forensic investigations provides next-level capabilities when an alert becomes a breach. Our team of forensic investigators can leverage the MDR data repository and tools to respond to an emergency faster.

- A customer portal provides access to the supported Cisco security technologies and offers a robust dashboard, ticketing, reporting, and case management interface, providing both operations and executive visibility to all activities.
Cisco security technologies required for MDR

- **Stealthwatch® Cloud** proactively protects your cloud resources, internal network, and even encrypted traffic against new threats.

- **Advanced Malware Protection (AMP) for Endpoints** continually evolves your endpoint defenses with deep malware analysis, preventing malicious files from spreading.

- **Threat Grid** with advanced sandboxing analyzes the threat new malware poses to your specific environment and helps prioritize proactive defenses.

- **Cisco Umbrella™** enforces security at the DNS and IP layers and blocks threats before they reach the network or endpoints.

Next steps

Contact your Cisco sales representative, partner or visit [cisco.com/go/mdr](http://cisco.com/go/mdr)