Managed Detection and Response (MDR)

Overview

Companies today are experiencing a higher risk to 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.

Managed Detection and Response (MDR) combines an **elite team of researchers, investigators and responders** with a **purpose-built Cisco® MDR threat intelligence, automation and response platform**, and **defined investigations and response playbooks** supported by Cisco Talos® threat research. 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.

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.

Benefits

- A stronger security posture that protects against threats with an expert team of researchers, investigators, and responders
- Advanced security operations with a Cisco MDR Threat Intelligence and Automation Platform
- 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 mean-time-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** in a purpose-built security ecosystem that improves the mean time to detect and mean time to contain security threats. This gives you higher confidence in results using proven methodologies, unique intelligence and an experienced team.
- **Analysis** through automated enrichment from key Cisco security technologies and threat intelligence sources identifies attacker attributes and the potential impact and scope of an alert.
- **Investigation** of alerts by our team further identify indicators of compromise or attack. When malware, ransomware, bot-net, bad actors and other such bad behavior occurs, we make data-driven decisions to respond with relevant, meaningful, prioritized actions.
- **Response** utilizing proven security operations center case management and security orchestration, automation, and response to contain, mitigate, and eradicate threats using response playbooks and action plans.
- **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.

Next steps

Contact your Cisco sales representative, partner or visit cisco.com/go/cms.