Managed Detection & Response (MDR)

Cisco Partner
https://cs.co/1page

Cisco **Managed Detection and Response** (MDR) combines an elite team of researchers, investigators and responders with integrated threat intelligence to detect and contain threats faster while delivering relevant and prioritized response actions. The service leverages defined investigations and response playbooks supported by Cisco Talos threat research.

Benefits:

- A stronger security posture that protects against threats with an expert team of researchers, investigators, and responders.
- Advanced security operations with threat intelligence and automation.
- Single portal experience for all incidents and response actions
- 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.

Target Customers:

- Company Size: Employees: 1,000 – 10,000 and Endpoints: 25,000+
- High-risk vertical industries including Financial, Manufacturing and Healthcare.
- Has/open to implementing: Secure Endpoint, Secure Malware Analytics & Umbrella.
- Struggling with security operations staffing, overwhelmed with growing volume of alerts, and unable to keep pace with current threats.
- Seeking advanced SOC capabilities with expert resources that understand the expanding attack surface.

MDR Elements:

- **Detection**, using an integrated cloud security ecosystem that improves mean time to detect and contain security threats.
- **Analysis** through enrichment of alerts, including Talos threat intelligence. MDR provides attacker attributes and to prioritize the impact and urgency of a threat to a business.
- **Investigation** of identified threats utilizing defined investigation playbooks, which provide added context. When malware, ransomware, and other such bad behavior occurs, we make data-driven decisions that establish meaningful response actions.
- **Response**, which utilizes Security Orchestration and Automated Response (SOAR) and case management to execute defined response playbooks and provide detailed threat analysis, including recommended response actions.

Conversation Starters:

- How confident are you of your ability to detect and respond to all the critical security incidents occurring within your environment?
- What are you doing to increase your speed to respond to threats?
- How do you handle 24x7 security threat detection and response?
- What are you using to gain visibility across the attack surface of your entire organization - network, cloud and endpoints?
- How well do your security products integrate to present consistent information about threats in context of one another?
- How are you keeping pace with current and emerging threats?
- How do you prioritize alerts to quickly investigate the ones that matter?

Supported Tools:

Secure Endpoint: (Advantage or Premier required)
- Map the entire attacker infrastructure
- Leverage predictive intelligence to uncover future threats
- Analyze relationships between domains, IPs, and files

Secure Malware Analytics: (Required – included w/Secure Endpoint)
- Correlate against samples of malware artifacts
- Apply dynamic analysis and sandboxing to detect malicious files
- Automate submission of suspicious files

Umbrella (optional)
- Detect threats across all operating systems
- Monitor process and system behavior
- Prioritize malware response

XDR Analytics (optional)
- Detect threats on premises and across multi-cloud environments
- Classify devices and model normal behavior
- Detect threats in encrypted traffic without decryption

Resources:

Services Partner Program	Proposal Template	Questions
MDR Solution Overview	Security Services	Service Description
	Talos Incident Response	Public page

Example SKU: ***CX-SEC-MDR***