Realize the power of Cisco XDR, faster

Cisco Managed Extended Detection and Response for Cisco XDR

Cisco XDR can change the way security teams look at detection and response. But not every organization has the capacity or expertise to plan, deploy, and operate this game-changing solution. A managed services engagement could be just what your organization needs to get you started on the extended detection and response (XDR) journey.

The Cisco XDR Premier license tier meets you and your team where you are now, working with the tools and telemetry sources currently in place, applying our unmatched expertise and guidance, and growing with you as you expand and add more security layers and solutions to the overall XDR strategy.

Cisco XDR Premier Tier

The Cisco XDR Premier license tier provides a managed extended detection and response (MXDR) powered by Cisco, provided by an elite team of Cisco security experts. This includes integration support for Cisco security solutions and Cisco-curated integrations with select third-party security tools, Cisco Software Support Services (SWSS) Enhanced support, security assessment, validation, and enhancement through Cisco Technical Security Assessment (CTSA) and select Cisco Talos Incident Response (Talos IR) services.

The Cisco MXDR service uses a combination of Cisco's elite team of researchers, investigators, and responders, the Cisco XDR solution, integrated tool sets and additional Cisco Secure technologies to monitor for and respond to potential security threats and breaches.

MXDR service powered by Cisco XDR includes:

- 24x7x365 Security incident and alert monitoring
- 24X7 Monitoring through Cisco's Security Operations Centers (SOC) using "a follow the sun" model.
- Cisco's team of researchers, investigators and responders leveraging both Talos Threat Intelligence and defined investigation and response playbooks to help detect, investigate, and respond to threats and alerts. Cisco's responses may include information, recommendations, or changes based on the type of threat or indication of compromise.

- Quarterly Threat Briefing: Talos IR hosts remote review meetings on a quarterly basis open to all MXDR customers. This quarterly briefing will provide updates on current threat patterns, detection volumes, and trending events.
- Investigation and response playbooks.
- Guided response actions: Cisco recommends responses to help contain, mitigate, remediate, or eradicate the threat.
- Threat advisories: Cisco issues threat advisories for new threats discovered helping Customers to proactively prevent incidents, or compromises through the implementation of mitigating controls.

Talos IR provides a full suite of proactive and emergency services to help you prepare, respond, and recover from a cybersecurity incident.

CTSA affords a suite of proactive services to assess a customer's cyber security preparedness and provide advice on the threats they face, the likelihood of those threats being realized, and the impact to their operational resilience if they are. This includes, but is not limited to:

- Threat modelling
- Penetration testing (Pen testing)
- Red Team Threat Simulation
- Security architecture assessments
- Application security assessments
- Security Operations Assessments
- DevOps Assessments
- Build / Configuration Reviews

Talos IR and CTSA service hours are accrued in accordance with the number of Cisco XDR Premier licenses purchased for Covered Users (CUs). Additional hours can be purchased with a-la-carte offerings from Talos IR and CTSA.

Service	Min. Hours
Intel on demand	5
Breach Susceptibility Workshop	5
Organization Digital Footprint Assessment	10
Security Design Thinking Workshop	20
Emergency Incident Response*	40
Penetration Testing	40
Threat Modeling	40
Device Configuration and Build Review	40
IR Plan	50
IR Playbooks	50
Tabletop Exercise	50
Security Architecture Assessment	80
IR Readiness Assessment	80
Compromise Assessment	80
Cyber Range	80
Proactive Threat Hunting	100
Red Team Threat Simulation	160
Purple Teaming	160
Security Operations Assessment	160

*Customers with 20 to 39 hours are eligible to benefit from limited emergency incident response services

Start your journey to XDR today with a managed services engagement delivered by Cisco.