

# Cisco Breach Protection Premier

Operate with confidence, future-proof your security and faster time to value

Cisco Breach Protection Suite unifies threat detection, investigation, mitigation and hunting solutions by integrating the Cisco security portfolio and select third-party tools across endpoint, email, network and cloud. But not every organisation has the capacity or expertise to deploy and manage this solution. A managed services engagement could be just what your organisation needs.

Cisco Breach Protection Premier 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 layers and solutions to the overall security strategy.

## Cisco Breach Protection Premier Tier

The Cisco Breach Protection Premier licence 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.

Cisco Managed Extended Detection and Response (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 Security technologies to monitor for and respond to potential security threats and breaches.

### MXDR service powered by Cisco XDR includes:

- Continuous security incident monitoring for events and alerts via Cisco's Security Operations Center (SOC) on a 24x7x365 basis.
- An MXDR SOC Analyst is responsible for analysing platform data, correlating, enriching, prioritising and reviewing all events through established playbooks.
- Escalation of potential security incidents, as needed.
- Guided response actions help you contain, mitigate, remediate or eradicate threats. Investigation and response actions will be conducted on your behalf, based on pre-approved response playbooks.

- Quarterly Threat Briefings provide updates on current threat patterns, detection volumes and trending events.
- Threat Advisories identify newly discovered threats, aiding in the proactive prevention incidents through the implementation of mitigating controls.

**CTSA** affords a suite of proactive services to assess your cyber-security preparedness and provide advice on the threats you face, the likelihood of those threats being realised and the impact to your operational resilience if they are. This includes, but is not limited to:

- Threat modelling/mitigation/simulation

- Penetration testing (Pen testing)
- Red/Blue/Purple teaming
- Security architecture assessments
- App/SOC/DevOps Assessments
- Build/configuration reviews

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

Talos IR and CTSA service hours are accrued in accordance with the number of Cisco Breach Premier licences 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
Organisation Digital Footprint Assessment	10
Security Design Thinking Workshop	20
Emergency Incident Response*	40
Penetration Testing	40
Threat Modelling	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

Operate with confidence, future-proof your security and realise faster time to value with a managed services engagement delivered by Cisco.

Learn more: [cisco.com/go/breach-protection](https://cisco.com/go/breach-protection)