Talos INCIDENT RESPONSE

In today's uncertain threat environment, you need a strong incident response and threat intelligence partner– that's us. At Cisco, our job is your defense.

Partner with Cisco Talos Incident Response

Cisco Talos® Incident Response (Talos IR) Retainer Service provides emergency response services to support you through active incidents, plus proactive services to assess, strengthen and evolve your incident response readiness program. With this flexible service, you benefit from:

- Incident response expertise: Our global team of seasoned incident responders is available during active incidents and to help strengthen your overall defenses.
- Swift action: One of our incident responders can be remotely dispatched within four hours of reporting an active incident, which minimizes downtime and accelerates incident resolution.
- Intelligence-enriched analysis: Driven by an evergreen library of threat intelligence and backed by proven incident response processes.
- Vendor-agnostic approach: You can leverage your existing security investments or benefit from supplemental visibility with temporary licenses for Cisco Secure products to minimize costs.

With the Cisco Talos IR Retainer Service, our global intelligence, research, and response teams are available when it matters most to you – whether preparing for or addressing an active incident.

Talos IR in action: A customer success story

Health care company resumes business as usual after a ransomware attack

Challenges:

- Pressure to reduce operational downtime and fully resume normal business operations.
- In-house security team with limited experience with ransomware attacks.
- Limited logging collection with no available threat detection and response solution to correlate activity across the organization.

Talos IR solution:

- Readily available, seasoned incident responders to guide the forensic investigation.
- Analysis of their current available data and greater visibility from deploying Cisco Secure products.
- Incident command activities and communication to convey forensic analysis findings and recommended expert remediation.

Outcomes:

- Quickly resumed normal business operations and could mitigate follow-on encryption events.
- Gained valuable experience alongside Talos IR to better respond to future security incidents.
- Fortified additional security controls by implementing expert remediation guidance such as deploying a multi-factor authentication (MFA) solution.

Talos IR Retainer Service overview

With a Talos IR Retainer, you have access to several service options, wherever you are on your security journey. From emergency incident response to proactive services, we have you covered.

Services offered

Use your retainer hours for one or several service options to best meet your current needs:

- **Emergency Incident Response:** Gain access to 24x7x365 incident coordination and command, investigative analysis and forensics, and expert remediation guidance to any security incident – enhanced by our intelligence with comprehensive after-action reporting.
- **Intel On-Demand:** Unlock direct access to Talos intelligence research by requesting information on emerging and relevant threats to your organization.
- **Incident Response Plan and Playbooks:** Develop tailored IR processes, procedures and communication guidance based on best practices and expertise from our seasoned incident responders.
- **Incident Response Readiness Assessment:** Evaluate and get recommendations related to your organization's current IR readiness to detect, response and recover from an incident.
- **Tabletop Exercise:** Increase organizational familiarity with the IR lifecycle and individual roles and responsibilities by collaborating with your cross-functional teams to respond to a custom-designed incident scenario.
- **Cyber Range Training:** Increase your team's IR capabilities with immersive, hands-on digital forensic and incident response training based on practical, real-world incidents.
- **Compromise Assessment:** Identify signs of active or historical adversary activity with a holistic review of your organization's environment with threat intelligence enrichment.
- **Threat Hunting:** Identify signs of a specific set of threats through a targeted review of your organization's environment based on a threat intelligence-driven hypothesis.
- **Purple Team Exercise:** Enhance your prevention, detection, and response capabilities by engaging with responders to collaboratively identify simulated adversarial tactics, techniques, and procedures.

Next steps

For more information on Cisco Talos Incident Response Retainer Service:

Cisco Talos Incident Response

Cisco Talos Intelligence

Cisco Talos Incident Response Retainer Service Description

Contact us: IncidentResponse@cisco.com

Contact your dedicated Cisco sales representative.