Cisco Talos Incident Response (CTIR)

Emergency Contact:
1-844-831-7715
+44 808 234 6353

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

Cisco Talos Incident Response (CTIR) provides a full suite of proactive and emergency services to help you prepare, respond and recover from a breach. CTIR enables 24-hour emergency response capabilities and direct access to Cisco Talos, the world's largest threat intelligence and research group.

Benefits:

Greater visibility: Access to the largest combined set of telemetry, threat traps and partner intel data available anywhere.

Actionable threat intelligence: Enhanced services based on the latest malware campaigns and actionable notifications on emerging threats.

Faster response: Combination of world-class incident response & threat intelligence capability accelerates resolution of incidents.

Threat Intelligence: Access to the full breadth of Talos, backed by the most-trusted responder and analysts, via Insights on Demand.

CTIR Services:

Emergency Services: In case of a breach, Talos is available within hours to Triage, Coordinate, Investigate, Contain and Remediate the threat.

Incident Response Readiness Assessment (IRRA): Evaluate a number of data points, including previous incidents, current roles and responsibilities, organizational design, patching operations, logging capabilities, and more to customize recommendations for your environment.

Incident Response Plan: Develop a tailored process to support coordinated response and communications during cybersecurity events or review your organization's existing plan.

Incident Response Playbooks: Develop customized playbooks based on the threats most relevant to your organization.

Tabletop Exercises: Discover gaps in policy, procedure, and process and understand important communications activities in this interactive exercise.

Threat Hunting: Proactive data review to search for attack signs which may have evaded the previous detection. We focus on finding evidence of the post-exploitation phase in the kill chain.

Compromise Assessment: An assessment that searches for indicators of compromise (IOCs) or threat actors present in the customer's environment.

Cyber Range Training: Specialized technical training workshop to help your staff build the skills and experience necessary to combat modern cyber threats.

Intel on Demand: Request the latest threat intelligence and net-new custom research from Talos.

FAQs:

Q: What does CTIR offer?
A: Cisco Talos Incident Response offers several ways to help the customer's organization through reactive or proactive services that prepare them for potential intrusions and recover from attacks already in progress.

Q: May unused retainer hours be rolled over to a new contract?
A: No. All subscription hours must be used by end date of contract, but the hours can be used for proactive services, so they don't go unused.

Q: What if the customer has competitor devices in their network?
A: The CTIR team is vendor-agnostic and will work with just about any vendor the customer has and provides necessary intel to analysts. Talos also offers free trial licenses to many Cisco products, as needed during an engagement.

Q: What if the customer does not have devices that can provide intel?
A: If needed, CTIR will install Cisco technologies such as *Secure Endpoint*, *Umbrella*, *Secure Analytics* and *Duo* with temporary licenses.

Q: Can Cisco Talos Incident Response be "white-labeled" or partner-branded?
A: No. CTIR cannot be white- or partner-labeled. Partners may position complimentary services they deliver alongside CTIR services.

CTIR Retainers & Packages:

- 24x7x365 access worldwide for Emergencies
- Dedicated Talos IR Consultants
- Service Level Objective (SLO): 4 hours by phone for all services listed below

Small (SVS-CTIR-S)
- Hours: 40
- Travel: n/a

Medium (SVS-CTIR-M)
- Hours: 80
- Travel: 1-trip, 3-days
- 1 Consultant

Large (SVS-CTIR-L)
- Hours: 120
- Travel: 2-trips, 3-days ea.
- Up to 2 Consultants

Resources:

SalesResources	At-a-Glance	Talos Tube
CTIR BDM Deck	Readiness & Retainer	IRSalesSupport@cisco.com
Ordering Guide	CTIR Retainer Service	TalosIntelligence.com/IR

Example SKU: ***CTIR-SUB***