Cisco Talos Incident Response Retainer Service

This document must be read in conjunction with How Cisco Provides Services, which is incorporated into this document by reference. Cisco Talos Incident Response Retainer focuses on incident readiness and response to incidents through targeted activities that evaluate awareness and response process. Cisco Talos Incident Response Retainer is available in two (2) variants as described below. Customer will receive the version of the Services provided in a Quote.

Cisco Talos Incident Response Retainer

Cisco Talos Incident Response (IR) Retainer provides emergency support and proactive services to assess, strengthen, and evolve a Customer’s incident readiness program.

Cisco Responsibilities:

- Provide one or more of the following services as part of the IR Retainer:
  - Emergency Response to Cyber Incidents, which can include triage, coordination, investigation (such as analysis and forensics), containment, and guidance for remediation
  - Incident Response Readiness Assessment
  - Incident Response Plan review and/or development
  - Incident Response Playbook review and/or development
  - Tabletop Exercise creation and execution
  - Proactive Threat Hunting for adversaries within a target environment
  - Compromise Assessment of a target environment
  - Cyber Range Training of up to ten (10) students per three (3) day class, which is a specialized technical training workshop to help Customer’s security staff build the skills and experience necessary to help combat modern cyberthreats
  - Intelligence on Demand
  - Network Security Architecture Assessment

Use commercially reasonable efforts to (a) assign a resource within four (4) hours remotely via telephone, and (b) begin deployment of personnel to Customer location within twenty-four (24) hours.

Deliverables

The Deliverables for the Service may include one or more of the following:

- Emergency Incident Response Report
- Incident Readiness Assessment Report
- Incident Response Plan
- Incident Response Playbooks
- Tabletop Exercises Report
- Proactive Threat Hunting Report
- Compromise Assessment Report
- Cyber Range Training Certificates

Cisco Talos Incident Response Retainer - Enhanced

Cisco Talos Incident Response (IR) Retainer Enhanced focuses on incident readiness and response to incidents through targeted activities that evaluate prevention, detection, and response capabilities.
Cisco Responsibilities:

- Provide one or more of the following services as part of the Retainer Enhanced:
  - Emergency Response
  - Incident Response Readiness Assessment
  - Incident Response Plan review and/or development
  - Incident Response Playbook review and/or development
  - Tabletop Exercises creation and execution
  - Proactive Threat Hunting for adversaries within a target environment
  - Compromise Assessment of a target environment
  - Cyber Range Training of up to ten (10) students per three (3) day class, which is a specialized technical training workshop to help Customer’s security staff build the skills and experience necessary to help combat modern cyberthreats
  - Intelligence on Demand
  - Network Security Architecture Assessment
  - Purple Team exercises

- Use commercially reasonable efforts to (a) assign a resource within four (4) hours remotely via telephone, and (b) begin deployment of personnel to Customer location within twenty-four (24) hours.

Deliverable

The Deliverables for the Service may include one or more of the following:

- Incident Readiness Assessment Report
- Incident Response Plan and/or Playbook
- Tabletop Exercises Report
- Proactive Threat Hunting Report
- Compromise Assessment Report
- Purple Team Assessment Report
- Cyber Range Training Certificates
- Emergency Incident Response Report

Notes and Limitations

The following notes and limitations apply to the Services:

- Given the variety of situations and issues that may be encountered, incidents may require a variety of other services or capabilities to complement this Service. For example, incidents may require specialized tools to provide deeper visibility or access into the Network.
- There is no guarantee that root cause analysis will result in a root cause being identified or confirmed for an incident.
- Reasonable efforts will be made to provide conclusive findings and an issue resolution plan.
- Security incident analysis activities sometimes might require additional hours in which case Customer’s need to purchase additional quantities of this deliverable.
- A minimum of fifty (50) hours is required to schedule proactive services. If hours are less than fifty (50) hours, emergency services will be the only delivery option.
- Incident Response Services can provide insight into deficiencies of an Incident Response plan for resolving an incident; however, executing the plan may require the purchase of follow-on Services. Proactive Services need to be requested and scheduled at least ninety (90) days before the end date of the subscription contract.
- Work may occur after Standard Business Hours, as determined by Cisco.
- Cisco will use commercially reasonable efforts to have personnel start travel to Customer’s location within twenty-four (24) hours after receiving the written request if visas and/or other travel requirements are not needed. If visa and/or special travel requirements are needed, Cisco personnel will continue to work remotely while travel arrangements are being made (e.g. applying for visa).
- Cisco reserves the right to refuse travel to any location that is in Cisco’s reasonable opinion is unsafe, unlawful, or may require a forced intellectual property transfer by Cisco.