Service Description: Cisco Talos Incident Response Retainer Service

This document describes **Cisco Talos Incident Response Retainer Service.**

Related Documents: This document should be read in conjunction with the following documents also posted at www.cisco.com/go/servicedescriptions/: (1) Glossary of Terms; (2) List of Services Not Covered; and (3) Severity and Escalation Guidelines. All capitalized terms in this description have the meaning ascribed to them in the Glossary of Terms.

Direct Sale from Cisco. If you have purchased these Services directly from Cisco, this document is incorporated into your Master Services Agreement (MSA) with Cisco. In the event of a conflict between this Service Description and your MSA, this Service Description shall govern.

Sale via Cisco-Authorized Reseller. If you have purchased these Services through a Cisco-Authorized Reseller, this document is for description purposes only; is not a contract between you and Cisco. The contract, if any, governing the provision of this Service will be the one between you and your Cisco Authorized Reseller. Your Cisco Authorized Reseller should provide this document to you, or you can obtain a copy of this and other Cisco service descriptions at www.cisco.com/go/servicedescriptions/.

Cisco Talos Incident Response Retainer Service

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 review and evaluation of Customer's incident readiness program.

Cisco Responsibilities:

- Provide one or more of the following Security Incident Response Deliverables as part of the Retainer: –
  - Incident Readiness Assessment
  - Incident Response Strategy and Planning (e.g. incident response plans, playbook)
  - Tabletop Exercises
  - Proactive Threat Hunting
  - Compromise Assessment
- Emergency Incident Response, which can include triage, coordination, investigation (such as analysis and forensics), containment, and remediation.
- Provide a Cyber Range Training, specialized technical training workshop to help Customer's security staff build the skills and experience necessary to help combat modern cyberthreats.
- Provide emergency access to Incident Response Services for the duration of the subscription.
- 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 (based on Services purchased):

- Incident Readiness Assessment Report
- Incident Response Strategy and Plan Document & Playbook
- Tabletop Exercises Report
- Proactive Threat Hunting Report
- Compromise Assessment Report
- Cyber Range Workshop Certificate
- Emergency Incident Response Report

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 Security Incident Response Deliverables as part of the Retainer Enhanced:
  - Incident Readiness Assessment
  - Incident Response Strategy and Planning (e.g. incident response plans, playbook)
  - Tabletop Exercises
  - Proactive Threat Hunting
  - Compromise Assessment
- Emergency Incident Response which can include triage, coordination, investigation (such as analysis and forensics), containment, and remediation.
- Evaluate the Customer's attack prevention and detection capabilities through a Purple Team (i.e. operate as both attacker and defender) Assessment of a device and network segment.
- Provide a Cyber Range Training, specialized technical training workshop to help Customer's security staff build the skills and experience necessary to help combat modern cyberthreats.
- Provide emergency access to Incident Response Services for the duration of the subscription.
- 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.
- Provide monthly status update specific to the Customer's incident response status.

Deliverable

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

- Incident Readiness Assessment Report
- Incident Response Strategy and Plan Document & Playbook
- Tabletop Exercises Report
- Proactive Threat Hunting Report
- Compromise Assessment Report
- Purple Team Assessment Report
- Cyber Range Workshop Certificate
- Emergency Incident Response Report

Notes and Limitations

The following notes and limitations apply to both Cisco Talos Incident Response Retainer and Cisco Talos Incident Response Retainer - Enhanced Service:

- Given the variety of situations and issues that may be encountered, incidents may require a variety of Services 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.
- The hours identified for one (1) quantity of this deliverable is mentioned in the quote document. Security incident analysis activities sometimes might require additional hours in which case Customer's need to purchase additional quantities of this deliverable.

- Incident Response Services can provide insight into deficiencies of an Incident Response strategy and a plan for resolving an incident; however, executing the plan may require follow-on Services.
- Proactive Service needs 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 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.