Service Description

Cisco Talos Incident Response Retainer Service

This Service Description is part of the Services Agreement (as defined in the Services Guide) and describes various Services that Cisco will provide to You. Capitalized terms, unless defined in this document, have the meaning in the Services Guide.

1. 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.

1.1 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
  - Intelligence on Demand
  - Purple Team Exercise
  - Red Team Exercise
- Use commercially reasonable efforts to (a) assign a resource remotely via telephone within four (4) hours of Cisco receiving notification by Customer of a security incident remotely via telephone, and (b) begin deployment of personnel to Customer location within twenty-four (24) hours of such notification.

1.2 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
- Purple Team Report
- Red Team Report

1.3 Notes and Limitations

The following notes and limitations apply to the Services:

- Once the number of hours in the retainer (as specified in the applicable quote or ordering documents) are used, Cisco may suspend work until additional hours are purchased or other written arrangements are made. Any unused hours expire at the end of a subscription term.
- The deidentified threat, indicator of compromise, vulnerability, attack, and techniques used (e.g., ATT&CK), and other related information that Cisco collects from Customer in relation to the Services is considered Systems Information, and we will treat it according to our security and privacy program referenced in the Services Guide.
- 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 may require additional hours to be purchased by Customer.
- A minimum of fifty (50) hours remaining under the purchased retainer is required to schedule proactive services. If hours are less than fifty (50) hours, emergency services or Intelligence On-Demand will be the only delivery options.
- 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.
- Work may occur after Standard Business Hours, as reasonably determined by Cisco.

- Travel will be determined at the reasonable discretion of Cisco. Cisco reserves the right to refuse travel to any location in Cisco's discretion.
- For Emergency Response services, and when reasonably required to deliver or complete the service in person, 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).