



Service Description: Advanced Services – Fixed Price

Cisco Talos Incident Response Service (ASF-CORE-IN-RESP)

This document describes the fixed price Cisco Talos Incident Response 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. 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 for your own internal use, this document is incorporated into your Master Services Agreement, Advanced Services Agreement, or other services agreement covering the purchase of Advanced Services-based services with Cisco ("Master Agreement"). If no such Master Agreement exists, then this Service Description will be governed by the terms and conditions set forth in the Terms & Conditions Agreement posted at www.cisco.com/go/legalterms. If you have purchased these Services directly from Cisco for resale purposes, this document is incorporated into your System Integrator Agreement or other services agreement covering the resale of Advanced Services ("Master Resale Agreement"). If the Master Resale Agreement does not contain the terms for the Purchase and Resale of Cisco Advanced Services or equivalent terms and conditions, then this Service Description will be governed by the terms and conditions of the Master Resale Agreement and those terms and conditions set forth in the SOW Resale Terms & Conditions Agreement posted at www.cisco.com/go/legalterms. For purposes of the SOW Resale Terms and Conditions this Service Description shall be deemed as a Statement of Work ("SOW"). In the event of a conflict between this Service Description and the Master Agreement or equivalent services exhibit or agreement, 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/.

Service Summary

The Cisco Talos Incident Response Service provides Customer with support for Incident Response services upto a maximum of 120 hrs along with an additional 12 hrs of Project Management.

Cisco will provide Talos Incident Response Service for one (1) of the following service options (described below) and its associated deliverable(s):

- Emergency Incident Response & Emergency Incident Response report
- Threat Hunting & Threat Hunting Report.
- Compromise Assessment & Compromise Assessment Report

Each option Includes two (2) trips for an on-site engineer for up to three (3) days each

Location of Services

Services are delivered both remotely and onsite to Customer.

Pre-Analysis

Cisco Responsibilities

The Responsibilities of the parties are dependent on the service option the Customer selects from above and are as follows:

- Conduct remote Kick-off call and identify key stakeholders from Cisco and Customer and their role in the delivery of the Services.
- Cisco will provide Project Management to monitor the timeline & schedule of Cisco's delivery of the Services.

Emergency Incident Response

- Work with Customer to define a custom plan to perform any needed data collection, forensics, tool installation, and as required to respond to a security Incident.

Threat Hunting

- Work with the Customer to define a custom hunting plan and execute the hunt. At the conclusion of the engagement, provide a Threat Hunting report.

Compromise Assessment

- Work with the Customer to define a Compromise Assessment plan and execute the same. At the conclusion of the engagement, provide a Compromise Assessment report.

Analysis

Cisco Responsibilities

Emergency Incident Response

- Provide an Incident Response resource to perform remote troubleshooting support (via telephone)
- Begin deployment of personnel to Customer's location within 24 hours of receipt of written request
- Utilize the following techniques:

Triage - Assessing the current situation to understand how best to initiate and design a response strategy.

Coordination – Tracking status, outstanding action items, and compiling updates as needed to ensure the incident is handled with care.

Investigation – Understanding the scope of the attack by deploying and using the necessary tools, reviewing log sources to analyze patterns and issues, performing needed forensics, and reverse engineering malware.

Containment – Quarantining and severing additional actions by the attacker

Monitoring – Development of signatures and continuous monitoring of the environment during the engagement to ensure the ongoing health of the network is maintained. As required to help Customer respond and recover from the incident.

Use of additional Cisco tools such as AMP, Stealthwatch, Umbrella, or third party tools may require additional fees and will be agreed to by the parties before Cisco provisions them.

Threat Hunting

- Work with the Customer to gather requirements by reviewing past attacks, intrusions and breaches, as well as existing concerns around specific actors, events, observations or high value assets or targets
- Confirm understanding of adversaries and associated tactics, techniques and procedures.
- Develop context around visibility into Customer's network by evaluating available tools and Customer tools and logs in the environment
- Define threat hunting use cases
- Identify required logs and accesses
- Execute the Threat Hunt by following the defined use cases

Compromise Assessment

- Work with the Customer to gather requirements by reviewing past attacks, intrusions and breaches, as well as existing concerns around specific actors, events, observations or high value assets or targets
- Confirm understanding of adversaries and associated tactics, techniques and procedures.
- Review the data, logs and existing telemetry of the Customer environment

- Perform the high-level review of the Customer organization to determine the indicators of compromise or threat actors present in the environment.

Reporting

Cisco Responsibilities

Emergency Incident Response

- Provide the Customer with Incident Response Report at the end of the engagement

Threat Hunting

- Provide the Customer with the Threat Hunting Report at the end of the engagement

Compromise Assessment

- Provide the Customer with the Compromise Assessment Report at the end of the engagement

Customer Responsibilities

- Participate in Kick-Off call and provide Cisco with:
 - Contact information for key stakeholders
- Review with Cisco, and approve, the agreed upon report.

General Customer Responsibilities

- All information (such as but not limited to: designs, topologies, requirements) provided by Customer is assumed to be up-to-date and valid for the Customer's current environment. Cisco Services are based upon information provided to Cisco by Customer at the time of the Services.
- Customer acknowledges that the completion of Services is dependent upon Customer meeting its responsibilities as indicated herein.
- Customer will identify Customer's personnel and define their roles in the participation of the Services. Such personnel may include but is not limited to: architecture design and planning engineers, and network engineers.
- Customer will ensure Customer's personnel are available to participate during the course of the Services to provide information and to participate in scheduled information gathering sessions, interviews, meetings and conference calls.
- Customer expressly understands and agrees that support services provided by Cisco comprise technical advice, assistance and guidance only.
- Customer expressly understands and agrees that the Services shall take place and complete within ninety (90) calendar days from issuing a Purchase Order to Cisco for the Services herein and any unused hours will expire and be forfeited. Customer is responsible for determining if the receipt and use of the Services complies with any internal requirements, complies with any third-party agreements, and complies with any applicable laws or regulations.

Invoicing and Completion

Invoicing

Services will be invoiced upon completion of the Services.

Completion of Services

Cisco will provide written notification upon completion of the Services to Customer. The Customer shall within five (5) Business Days of receipt of such notification provide written acknowledgement of Cisco's completion of the Services. Customer's failure to acknowledge completion of the Services or to provide reasons for rejection of the Services within the five (5) Business Day period signifies Customer's acceptance of completion of the Services in accordance with this Service Description.