Cisco Active Threat Analytics Essential Security Addendum to the Service Description for Cisco Managed Services

This Security Addendum (the "Addendum") to the Service Description for Cisco Managed Services (the "Service Description") describes the Service elements, features, and components of Cisco's Active Threat Analytics Essential. This Addendum supplements the terms and conditions set forth in the Service Description.

General

Related Documents. This document should be read in conjunction with the Service Description, its related Glossary of Terms, applicable Ordering Documents, and the applicable Agreement (as defined in the Service Description). The Ordering Documents shall detail the quantity, pricing, tier and type of Services Customer has purchased, and additional details on the Services to be provided.

Order of Preference. If there is a conflict between this Addendum, an Ordering Document, the applicable Agreement, the Service Description, or any other Addendum to the Service Description, the following priority will apply (from highest to lowest): (a) any Ordering Document, as applicable; (b) any Addendum(s); (c) the Service Description; and (d) the applicable Agreement.

Defined Terms

Unless otherwise defined in the body of this Addendum, the Service Description, an Ordering Document, or the Agreement, capitalized terms used in this Addendum are defined in the Glossary of Terms (available at http://www.cisco.com/c/dam/en_us/about/doing_business/legal/service_descriptions/docs/glossary-of-terms-for-cms.pdf) and the Service Description for Advanced Threat Analytics (ATA) Premier.

Summary Table
The following tables summarize the Service elements that Cisco provides for each tier of the Cisco Managed Service for Security.

Service Elements	Foundation	Standard	Comprehensive
10 GB/Day Indexed Event Data	✓	✓	✓
Security Event Analysis			✓
Security Incident Notification			✓
Security Operations Manager			✓

Optional Service Element*	Foundation	Standard	Comprehensive
Customer Security Engineer			✓

*subject to additional charges and separate purchase

Reporting
Cisco will provide, or make available via the Portal, the reports listed in Reporting Appendix for Cisco Managed Services, which will be provided by Cisco, based on the tier of Service purchased by Customer.

Foundation and Standard Tiers

Service Elements Included with Foundation and Standard Tiers
The Foundation and Standard tiers include all Service elements and reports specified for the Foundation and Standard tiers described in the Service Description, as applicable, and the following:

10 GB/Day Indexed Event Data
Cisco will collect and retain up to 10 GB per day of Indexed Event Data from Managed Components. Cisco will use the Indexed Event Data to support performance and welfare monitoring and reporting for Managed Components. Indexed Event Data will be retained by Cisco based solely on available disk space and indexed data will be overwritten on a first in, first out basis once disk capacity is reached. Additional capacity may be purchased separately, as specified in an Ordering Document.

Cisco Responsibilities
- Collect and analyze Indexed Event Data from Managed Components
- Provide hardware, software, and applicable licenses to support 10 GB/day indexing rate (as part of Data Collection Tools)

Customer Responsibilities

- Assist Cisco with initial analysis of daily volume of Indexed Event Data by Managed Components to ensure accuracy of daily indexing capacity
- If capacity exceeds the 10 GB/day allocation, follow Change Management procedures to either reduce the Indexed Event Data (which may impact the quality of the Services) or procure additional capacity to support Managed Components

Comprehensive Tier

Service Elements Included with Comprehensive Tier

The Comprehensive tier includes all Service elements and reports for the Standard tier described in this Addendum, all service elements included in the Comprehensive tier described in the Service Description, and the following:

Security Event Analysis

Cisco will monitor for Security Events received from supported Managed Components. Security Event types are periodically updated and available upon written request.

Cisco Responsibilities

- Create and implement automated Security Event analysis rules (aka. Plays)
- Detect Security Events
- Review Security Event data, as warranted, to determine if the Security Event warrants escalation to Incident
- Provide telemetry tuning guidance for existing analysis rules

Customer Responsibilities

- Provide Cisco with any access and configuration changes to the Managed Components
- Provide feedback to analysts in Cisco's Active Threat Analytics Security Operations Centers (SOC) regarding validity of Security Events to assist with tuning of analysis rules
- Procure sufficient Indexed Event Data capacity to support collection of Security Event data

Security Incident Notification

Cisco will escalate identified Security Events to Incidents and use the Incident Management process and responsibilities, as described in the Cisco Managed Services Service Description.

Cisco Responsibilities

- Respond to requests for additional information and provide mitigation guidance (if available) while Customer is responding to security Incidents

Customer Responsibilities

- Provide appropriate resources and personnel to carry out Customer security Incident response plans

Customer Security Operations Manager

Cisco will make available a security operations manager to the Customer to act as a SPOC to respond to Customer's inquiries regarding security Incidents and to act as a liaison to Customer's security team to gather additional information or provide additional guidance in supporting Customer's efforts to resolve an Incident.

Cisco Responsibilities

- Make available Security Operations Manager to Customer
- Review security Incident tickets with Customer and provide guidance, as needed
- With respect to security Incidents, coordinate resources, as appropriate, to gather additional available and relevant information from Managed Components and/or security intelligence sources to respond to customer inquiries

Customer Responsibilities

- Provide a Single Point of Contact (SPOC) to work with the Cisco specialist
- Provide copies of relevant security policies and processes to Cisco