Service Description: Cisco Managed Service for Security

Technology Addendum to Cisco Managed Services for Enterprise Common Service Description

This document referred to as a Technology Addendum describes the Cisco Managed Service for Security Service Offering.

Related Documents: This document should be read in conjunction with the Cisco Managed Services for Enterprise Common Service Description posted at www.cisco.com/go/servicedescriptions.

Direct Sale from Cisco

If you have purchased these Services directly from Cisco, this document is incorporated into your Master Services Agreement (MSA), Advanced Services Agreement (ASA), or equivalent services agreement executed between you and Cisco. If not already covered in your MSA or equivalent services agreement, this document should be read in conjunction with the Related Documents identified above. In the event of a conflict between this Technical Addendum and your MSA or equivalent services agreement, this Technical Addendum shall govern.

Sale via Cisco Authorized Reseller

If you have purchased these Services through a Cisco Authorized Reseller, this document is for informational purposes only; it is not a contract between you and Cisco. The contract, if any, governing the provision of this Service is the one between you and your Cisco Authorized Reseller. Your Cisco Authorized Reseller should provide this document to you.

The Service

This Technology Addendum is designed to be read in conjunction with the Cisco Managed Services Common Service Description that provides a baseline understanding of and sets expectations about the Cisco Managed Services, hereinafter referred to as the Service, provided by Cisco. In addition to the activities and deliverables outlined in the Common Service Description, this Technology Addendum outlines the unique activities and deliverables for the Managed Service for Security devices and infrastructure that are being managed by Cisco. Both service descriptions should be read in combination to fully understand the scope of the services being purchased.

The Cisco Managed Service for Security offering described herein and other optional services are intended to supplement a current support agreement for Cisco products, and only available where all the Managed Components in a Customer's network and Cisco Unified Communications Solution are supported through a minimum of core services. Cisco shall provide the Service described below as selected and detailed on the Purchase Order for which Cisco has been paid the appropriate fee.

Cisco shall provide a Quote setting out the extent of the Service and the term for which Cisco will provide the Service. Cisco will receive a purchase order that references the Quote agreed between the parties and that, additionally, acknowledges and agrees to the terms contained therein. Cisco only provides support for Managed Components, unless specifically noted. For any device, component or solution element not specifically designated as a Managed Component, Cisco shall have no responsibilities whatsoever.

This Technology Addendum describes the services capabilities, supported devices, elective changes, and reports delivered.

Two managed service packages are available:

- Standard Managed Service level provides monitoring, correlation, and reporting of your security devices and infrastructure.
- Comprehensive Managed Service level provides additional services to the standard service: security event analysis, advanced security reporting, event classifications mitigations and remediation.

In addition to these two service packages, the Customer can also purchase Optional Services as needed to augment the selected package The table below outlines the Optional Services for the Service as well as specific activities and deliverables provided only under the Cisco Managed Service for Security offer.

Activities / Deliverables	Standard Services	Comprehensive Services	Optional Services
Management Readiness Assessment	X	X	
Incident Management	X	X	
Device Monitoring	X	X	
Incident Notification	X	X	
Advanced Security Event Correlation	X	X	
Web Accessible Portal	X	X	
Standard Reports	X	X	
Incident Priority and Classification		X	
Incident Investigation and Diagnosis		X	
Incident Resolution and Restoration		X	
Incident Escalations		X	
Incident Resolution		X	
Advanced Reports		X	
Root Cause Analysis Reports			X
Ticket Trending and Analysis			X
Review / Assess Cisco Field Notices			X
Custom Reporting			X
Operations Manager Level I and II			X
Customer Engineer Level I and II			X
Defined Changes			X
Custom Scoped Changes			X
Regulatory Compliance Management			X
Software Image Management (SWIM)			X

1 Management Readiness Assessment

Management Readiness Assessment is an assessment conducted by Cisco Managed Service for Security analysts that determines whether all Managed Components are in good working order prior to completion of Transition Management. Requires Managed Components are fully configured, deployed and functioning properly prior to the commencement of Incident and Problem Management services.

Software Image Management (SWIM)

Allows for creation, installation and substantiation of image updates to new or existing target devices by type, location, zone or other defined groups with alert in scheduled or ad hoc changed management

Device Software Image Maintenance Upgrade	Distributes and installs image updates to target devices. Activated for scheduled or on-demand changes. Allows automated provisioning of new devices deployed on a managed network.
Network Software Image Maintenance Upgrade	Distributes and installs image updates to groups of target devices across the network
Device Software Image Upload	Capture of the specific image that the device runs on with image optimization if the image already exists in the CMCS archives.
Device Software Image Archive	Retains the executable image from the device.
Device Software Image Reports	Extensive reporting capabilities on deployed images

2 Security Reporting

The Cloud and Managed Services Platform (CMSP) collects and gathers log and security event information from the Managed Security Components covered within the Service. This information is compiled and made available via reports available on the Portal. Device level reports available are listed below.

2.1 Standard Reports

Standard Reporting	Report Description
CPU and Memory Reporting	CPU utilization (%) memory pool utilization (%), memory pool free, memory pool largest free
Network Interface Reporting	Interface utilization (%) bandwidth usage, errors and discards
TCP/IP Port Monitoring	TCP/IP port availability reporting
IPSEC Statistics	Active tunnels, Total inbound authentication failures, total authentications, total packets received/dropped
Failover Status	Hardware information and status
Availability Reporting	System availability
Inspection Load	Indicates how much traffic inspection capacity the sensor is using
Missed Packet Percentage	Average of missed packet inspection
Partition Utilization	% of space allocated to each partition

2.2 Advanced Reports

Advanced Security Reports	Report Description
Intrusion Prevention Blocked Attack Report Summary A summary of suspected attacks in which the IPS sensor or enforcement point blocked a specific packet and/or connection, including signature fired, category, severity, and src/dst addresses.	
Top Blocked Attacks by Signature	A ranking of top fired signatures that resulted in a blocked attack
Top Blocked Attacks per Sensor	A ranking of top blocked attacks by IPS Sensor
Top Source Blocked Attacks	A ranking of the top Source IP address that was blocked
Top Destination Blocked Attacks	A ranking of the top destination IP address that was blocked
IPS Signature Categories	A ranking of the top fired signatures that resulted in a block by category
Intrusion Prevention Summary Reports	
Top Fired Signatures / Signature severity	A ranking of the signatures fired most often and the severities of those signatures by severity
Top Attacker Source	A ranking of the top Source IP address that resulted in a signature to alarm
Top Attacked Destinations	A ranking of the top destination IP address that resulted in a signature to alarm
Signature Severity Summary by Sensor	High, medium, and low severities per Intrusion Prevention Device A ranking by individual sensor of the top signatures triggered by severity
Top Fired Signatures Severity	Cumulative totals (high, medium, low) of IPS Signature severities triggered across the entire intrusion prevention environment
Firewall Summary Report A summary of the connections and traffic that have been denied or permitted as a result of the applied firewall policy or access control list.	
Total Denied Packets	A ranking by firewall of the total denied attempts
Top Denied Source Addresses	A ranking by top source IP address which resulted in a denied attempt by a firewall policy
Top Denied Destination Address	A ranking by top destination IP address which resulted in denied attempt by a firewall policy
Top Denied Protocols	A ranking by top protocols which resulted in a denied attempt by a firewall policy
Top Denies by Access Control Policy	A ranking by Access Control List of the most utilized polices which resulted in a denied attempt
Authentication Failure Summary Reports A summary of failed authentication attempts	
Top Source Address Failed Attempts	A ranking of the top source IP addresses which resulted in failed login attempt
Top Destination Address Failed Authentication Attempts	A ranking of the top destination IP addresses which resulted in a failed login attempt
Top Authentication Failures by Device	A ranking by device of the top failed login attempts
Top Username Failed Attempts	A ranking by Username of the top failed login attempts

Advanced Security Reports	Report Description
Bandwidth Summary Reports	
Top Applications	Presents the top applications across the environment in terms of bandwidth usage
Top Source / Destination	Presents Top bandwidth consumers by source address and destination address
Identity Services Engine (ISE) Advanced Reporting	
ISE Admin Nodes Monitored	Provides details on each of the ISE administrative nodes under management
ISE Policy Services Node Monitored	Provides details on each policy services node under management
Total ISE Devices Monitored	Provides details on each of the ISE infrastructure nodes under management
Total Authentication Last 24 Hours	Presents the total amount of authentications over a 24 hour period
Total Currently Authorized Users – All PSN	Provides the total active users authenticated to all of the policy service nodes
Total Current Authentication – Per PSN	Provides the total active users authenticated per each policy services node
Authorizations by Policy	A ranking of the top used authorizations by policy
Currently Authorized Users	A list of the current users authenticated to the network
Total ISE Failed Authentications	A list of the total failed authentications
Total Failed Authentications Last 24 Hours – Per PSN	A list of the total failed authentications by policy services node
Total Failed Authentications By User	A ranking of the total failed authentications by individual user
Passed Authentications – Last 24 Hours	A list of the total success authentications over the previous 24 hours
Top Locations for Auth Activity	A ranking of the authentication activity across the top active locations
Top Authentications by Device Type	A ranking of the top authentications by network device
Top Authentications by Device	A ranking of the top failed authentications by device
Top Failed Authentications by Device	A ranking of the top failed authentications by network device
Top Device Profiles	A ranking of the top device profile
ISE System Performance	System and services availability, performance management, disk, memory and CPU utilization
ISE Admin Node Application Status	Presents the availability of the ISE administration services and application
ISE PSN Node Application Status	Presents the availability of the ISE policy services node application

2.2.1 Security Event Rate Report

This report is also provided as part of the Advanced Reporting functionality.

The security event rate report provides detailed event classifications of each security incident from the Intrusion Prevention System (IPS). The classifications include the following:

- Exploits - Identifies alarms or traffic that contains an actual exploit to vulnerabilities.
- Successful Compromise – Identifies alarms or traffic that has successfully exploited a known vulnerability.
- Denial Of Service – Identifies alarms or traffic that is targeted at a specific set of devices or networks with the intent of causing the system or network to become unresponsive to legitimate requests.
- Malware/Virus/Trojan/Worm – Identifies alarms or traffic associated with malicious intent to compromise the integrity of a system or networks, obtain sensitive data or information and/or propagate malicious software with the intent of infecting other systems and networks.
- Authentication/Access/Authorization – Identifies alarms or traffic that attempt to improperly gain access or administrative privileges to a system or networks.
- Reconnaissance Attempts – Identifies alarms or traffic patterns which discover and gather network information, host identification, vulnerabilities and open ports.
- Misuse – identifies alarms that are in violation of corporate network policies; example, IRC, gaming, and torrent.
- Fault – Identifies alarms associated with device availability status including processes and connectivity.
- Suspicious Traffic - Identifies alarms considered suspicious either due to their unusual nature or due to the presence of only limited information.

2.3 Custom Reports

Provides for the ability to create or modify the types of reports based upon the available data. Each request for Custom Reporting must be evaluated and mutually agreed upon between Cisco and the Customer. Operations Manager Level 2 is a pre-requisite for Custom Reporting.

3 Customer Requested Change Management

Customers may purchase a block of support hours that can be leveraged across all Defined Changes Categories and Custom Scoped Elective Changes that a Customer has under their service contract. The Customer must have a sufficient balance of support hours on account to cover the requested change. Additional support hours may be purchased if required.

3.1 Defined Changes

Defined Changes are categorized into Small, Medium, and Large activities. A Defined Change is a requested change by the Customer. Defined Changes are not the result of Cisco Incident Management and Problem Management processes. The Customer identifies the needed type of change and submits a Defined Change Request on the Portal.

Customers purchase Support Hours that can be leveraged across all Defines and Customer Scoped Change Categories that a Customer has under their service contract. The Customer must have a

sufficient balance of Support Hours on account to cover the requested change. Additional Support Hours may be purchased if required.

Small Defined Changes (Type 1)

- Standard Access Control List (ACL) policy update
- Basic Network Address Translation (NAT) change or security device policy
- Single IPS signature basic tuning
- Adding of Access Control List (ACL) or policy

Medium Defined Changes (Type 4)

- Enabling and testing new feature or security functionality
- Multi-line firewall Access Control List (ACL) change and testing that spans multiple managed devices
- Detailed policy creation, Access Control List (ACL), or Network Address Translation (NAT)
- Advanced IPS tuning request
- Virtual Private Network (VPN) addition for remote device

Large Defined Changes (Type 8)

- Large scale changes that impact multiple devices
- Network address re-designs and network security policy changes
- Disaster recovery and failover testing for multiple sites and network security devices
- IPS rebuilds
- Creation of new virtual sensor
- Advanced security feature implementation, tuning and testing

3.2 Custom Scoped Changes

Custom Scoped Changes are Customer requested changes that fall outside Incident and Problem (Standard) changes for restoring service and requires custom scoping through an SOW. Custom Scoped changes will require a mutually agreed upon statement of work (SOW). See the Common Service Description for more details of Custom Scoped Change support. For example: Implementation and testing of new security features across multiple devices.