Service Description: Cisco Security Service for Managed Threat Defense [CON-AS-SMTD]

This document describes the **Cisco Security Service for Managed Threat Defense**

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. Related Documents: The following documents will be provided with your Cisco Security Service for Managed Threat Defense Quote for Services ("Quote"), as described below, and should be read in conjunction with this Service Description and are incorporated into this Service Description by this reference:

Cisco MTD Service Level Agreement

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

Cisco shall provide the Cisco Security Service for Managed Threat Defense (Cisco MTD) 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 Services and duration that Cisco shall provide such Services. Cisco shall receive a Purchase Order that references the Quote agreed between the parties and that, additionally, acknowledges and agrees to the terms contained therein.

Cisco MTD Service Summary

This service description is designed to provide the Customer with a baseline understanding of the activities, deliverables and service delivery processes that Cisco uses to deliver Cisco MTD. This service description is also designed to properly set the Customer's expectations regarding these services.

Cisco MTD may include the following work items as selected and detailed on the purchase order:

Managed Threat Defense Core Offering:

The Managed Threat Defense Core Offering may be purchased alone or with the Managed Threat Defense Add-On Packages shown below.

WORK ITEM	MTD CORE OFFERING	DESCRIPTION
[OPT-SO-TDMAN]	Managed Threat Defense Core Service (MTD)	• Two (2) Internet points of presence (5Gb/sec cap) • Two (2) data centers (multiple connections) • Active Customer Portal Access • Quarterly business review • 24 / 7 management • 2000 incidents / year

Managed Threat Defense Add-On Packages:

The Managed Threat Defense Add-On packages may only be purchased with an existing or planned purchase of the Managed Threat Defense Core Service.

WORK ITEM	MTD ADD-ON PACKAGE	DESCRIPTION
[OPT-SO-TDAIS]	Managed Threat Defense Incident Add-On Package	• Additional 500 incidents / year
[OTP-SO-ITDMAN]	Managed Threat Defense Incremental Coverage Add-On Package	• Additional Internet point of presence • Additional data center • Additional 1000 incidents / year

Managed Threat Defense Proof of Concept Offering:

The Managed Threat Defense Proof of Concept offering is offered as a standalone service. It is not to be combined or purchased with any other MTD work items.

WORK ITEM	MTD PROOF OF CONCEPT OFFERING	DESCRIPTION
[OPT-SO-TDPOC]	Managed Threat Defense Proof of Concept	• • One (1) Internet points of presence (5Gb/sec cap) • • One (1) data center (multiple connections) • • Active Customer Portal Access • • Executive Outbrief • • 24 / 7 management

		• 500 incidents • No SLA •

Cisco Security Service for Managed Threat Defense is designed to provide Customers with an extended security support staff with a core competency in advanced security threats and computer security incident response. This service enables the Customer to out-task core security operation/incident response administration by utilizing Cisco's security personnel and Cisco's process-driven security event lifecycle management methodology. Other benefits of these services include:

- Enabling the Customer to re-capture IT support team capacity by utilizing the Cisco Security Operations Center (SOC) as an extension of their IT security staff
- Reducing security risk by improving the Customer's awareness of and visibility into advanced persistent network security threats and vulnerabilities
- Providing the Customer with engineering recommendations from Cisco SOC security engineers that will help a Customer decide which tactical operational steps they should take to mitigate threats, address vulnerabilities and, over time, improve their overall network security posture

Cisco will only provide support for the Managed Threat Defense Service work items that have been selected on the Purchase Order.

Please read this document carefully as it contains important information regarding the Managed Threat Defense Service that you have purchased from Cisco.

1 Cisco Managed Threat Defense Service (Cisco MTD)

Cisco Managed Threat Defense provides remote network security monitoring utilizing network packet metadata, advanced malware and network behavior anomaly detection techniques, sandboxing capabilities, as well as leveraging a wide set of security intelligence feeds over the Term in order to rapidly detect and respond to security incidents and events. The Term begins on the date that a Cisco Network Consulting Engineer (NCE) is onsite as part of the on-boarding phase, as described in 1.1.2.

1.1 Transition Management

Transition Management is a phased process approach in which Cisco works with the Customer to prepare the Customer infrastructure, gather information, and establish the proper workflow. The Customer must place a Purchase Order with Cisco to initiate the Transition Management process.

1.1.1 Kickoff Meeting

Cisco will assign a Project Manager to act as a primary point of contact during the Transition Management phase. The Project Manager will contact the Customer to schedule the kickoff meeting within forty-five (45) days from receipt of a valid Purchase Order. The kickoff meeting is typically accomplished via a conference call with the executed contract detail and may include a Cisco partner. The Project Manager in collaboration with Cisco Engineers assigned to the Customer account typically facilitates the kickoff phase, as well as all remaining phases within Transition Management.

The Customer will identify the resources required for the kickoff meeting and coordinate with the Project Manager to facilitate and organize the kickoff meeting.

Items discussed during the kick off meeting may cover:

- Overview of MTD service delivery
- On-boarding timeline
- Determination of date, location, and logistics for Cisco NCE onsite visit to begin on-boarding phase

1.1.2 On-Boarding

On-Boarding is the information gathering phase that will provide the foundation for delivery of the MTD service.

A Cisco NCE will be onsite to initiate the on-boarding phase and begin meetings with Customer to collect relevant information. This onsite visit will indicate the initiation of the Term for the MTD service. Cisco will provide an MTD Requirements Document that captures information gathered during on-boarding.

The Customer is responsible for providing information as required, reviewing completed MTD Requirements Document, and acknowledging receipt of MTD Requirements Document by signing the document.

Information gathered during this phase may include:

- Organizational introductions
- Solution goals, as well as business, technical, and operational requirements
- Current security policy and incident handling procedures
- Network diagrams
- Future technology plans

1.1.2.1 Plan and Prepare

In order to effectively manage the lifecycle of a security incident, it is critical that the Cisco analysts fully understand the Customer environment and security workflow.

The Customer will provide appropriate resources and contacts to assist Cisco in assessing the organization's strategies and methodologies of incident response.

Cisco will define and document the incident response process used by the Cisco Analyst and Incident Investigators.

The strategies and methodologies created provide the framework needed to rapidly determine the answers to the following questions in a streamlined manner:

- What has happened?
- What location of the network is affected (e.g. IP address, subnet, VPN, wireless, data-center)?
- What assets (anything of value to the organization – e.g. servers, data, network) were affected?
- Has the compromised system/s been modified?
- Who should be contacted?
- What steps should be taken to mitigate the incident?
- What steps should be taken to remediate the issues?

1.1.2.2 Network Layout

Every organization has a unique IP address schema designed that aligns with business needs. The address space may be private (RFC 1918), public, or a combination of both. Cisco will be responsible for assigning NCEs to work with the Customer in enumerating the existing IP networks. The Customer is responsible for providing IP address schema and an up-to-date network diagram. In rare cases where the Customer does not have up-to-date diagrams of the network, Cisco will create a topology map as part of the MTD service using scanning tools. The Cisco analysts will use this information during the detection and response phases.

1.1.2.3 Asset Classification and Prioritization

Not all systems and data are created equally. There are certain systems within an organization that store critical data and/or serve critical applications. These are the types of systems that if unavailable, unreliable, or compromised could potentially negatively impact the Customer's productivity, competitive advantage, or reputation. Cisco NCEs will be responsible for assessing any existing Customer asset classification and prioritization documents.

The Customer will be responsible for providing appropriate resources to review the asset classification and prioritizations documents or assist the Cisco NCEs in the process of documenting the identification, classification and prioritization of critical systems and data. This information will be used to properly identify the areas of the network that will need full network security visibility.

1.1.2.4 System Readiness

Once the assets have been classified and prioritized they must be assessed to establish a baseline. Cisco is responsible for performing a baseline assessment of the environment. The assessment is focused on three items: logging, services, and vulnerabilities.

- **Logging**: Specified network devices (e.g. routers, switches) should have NetFlow enabled. A copy of the flows should be sent to the Data Capture and Analysis Pod (DCAP).
- **Services**: Each asset that has been identified, classified, and prioritized in the previous stage will be actively scanned from the DCAP to determine open/listening network services (ports). The active scanning will also attempt to enumerate the version of the services that are listening. The results of the scans will be compiled, documented and reviewed with the Customer. The services may be rescanned on a quarterly basis and the results will be compared to the previous scan and any discrepancies will be noted and reviewed with the Customer. An exception may be made if the Customers performs comparable quarterly scans using their own tools and shares the reports of these scans with Cisco.
- **Vulnerability**: Each asset that has been identified, classified, and prioritized in the previous stage will be scanned for network-based vulnerabilities from the DCAP. The vulnerability scan provides a point-in-time baseline of the vulnerability status of the environment, which can then be proactively used to mitigate or remediate any issues. The scan will be initiated from the internal Customer network to simulate an internal attack. Where applicable a scan may also be performed from the Internet simulating the type of access that any Internet user would have. The results of the scans will be compiled, documented and reviewed with the Customer. The services may be rescanned on a quarterly basis and the results will be compared to the previous scan. Any discrepancies will be noted and reviewed with the Customer. An exception may be made if the Customers performs comparable quarterly vulnerability scans using their own tools and shares the reports of these scans with Cisco.

1.1.2.5 Security Policies and Considerations

It is a standard procedure for Customer organizations to document or describe the types of activities that are permitted in their environment. Many times the permitted activities are documented in detail in a formal policy or procedure. Other times the policy or procedure may only describe permissible network use at a very high level. In rare cases there may not be a formal document that describes permissible use.

Cisco will be responsible for reviewing Customer requirements and interviewing appropriate Customer resources to better understand normal and permissible network traffic in order to properly tune the DCAP.

The Customer is responsible for providing the appropriate resources and data points associated with permitted traffic flows.

The Customer is responsible for having policies in place that outline and describe the organization's response stance. A response stance is a documented policy that describes how the organization will react and respond to incidents. The response stance should align with local/state/national law and any regulations that the organization is required to follow.

The Customer is responsible for defining response stance. For example, an organization's website is hacked and the pages are altered to display pornographic material. The Customer must define the preferred response (example: best action is to take the system offline, remediate the issue and then bring it back online without performing forensics to identify how the incident took place or where the attack originated, OR the Customer may decide that the asset is too valuable to rush through the process of remediation and instead accept the downtime and associated loss and perform a thorough forensic investigation.) The Customer will be responsible for defining and directing the response stance and communicating this to the Cisco SOC. The Cisco NCEs will be responsible for documenting the requested response.

The MTD service is capturing full packet level data at key points of the network for forensic purposes. During an investigation it is possible that full sessions may need to be re-assembled or systems may need to be monitored closely which could reveal sensitive information (e.g. emails, chat transcripts). Due to legal or compliance regulations there may be situations or specific areas of the network where full packet capture may not be allowed. The Customer is responsible for defining the situations and locations in the network where full packet capture may not be permissible and providing this information to Cisco. Cisco will document these agreed areas of the network in the MTD Requirements Document. In some cases the Customer may authorize Cisco to perform a trap and trace. A trap and trace is a situation where a specific network location is identified and packet capturing is permitted for a qualified amount of time.

1.1.2.6 Contact List

The Customer is responsible for providing a full listing of contacts including job descriptions and roles and responsibilities required for the MTD service. This list is a critical component for a successful service. Cisco will review and identify any potential gaps within the Customer's organizational structure and may require the Customer to define resources with the ability to address the required roles and responsibilities.

The contact list should identify the proper resources for notification and escalation that have the authority to make decisions within the organization. The identified resources should be able to triage events and identify additional Customer resources as required to address security incidents.

1.1.2.7 Tabletop Exercises

Tabletop exercises are very important during the plan and prepare phase of an engagement. The goal of these exercises is to walk through a few types of incidents that are commonly seen by organizations in order to test the workflow established previously in this phase of the engagement. The Customer must provide resources with the ability to define and approve incident response processes and procedures during a strategic simulation. The exercise is highly dependent on Customer interaction and may last one or more days.

1.1.2.8 Transition Outbrief

Cisco will deliver a Transition Outbrief to the customer upon completion of the On-boarding phase. Cisco will determine an appropriate format and delivery method that may include but shall not be limited to using a shared medium via the Internet, teleconference, and/or onsite.

Customer is responsible for designating at least two (2) security representatives to participate in the Transition Outbrief.

Items covered in the Transition Outbrief may include:

- Review of data collected during on-boarding
- Discuss on-boarding successes and challenges
- Review incident escalation process
- Review MTD recommendations discovered during on-boarding

Once the Transition Outbrief has been completed, monitoring and incident response management will be transferred to the MTD SOC as described in section 1.4 and the Commencement Date for the Service Level Agreement (SLA) will begin. Furthermore, billing and invoicing for the MTD Service will also commence following the Transition Outbrief event.

1.2 Customer Portal

The MTD Service includes a Customer Portal that will provide visibility into the delivery of the service, including incident tickets and reports.

Customers receive end-user accounts to access the Portal. Instructions to access and navigate the Portal will be provided as a part of the on-boarding phase via video, Webex, or onsite as determined by Cisco. During the initial setup phase, Customers will receive accounts for authorized employees to access the Portal. Information available from the Portal may include:

- Incident Ticket identification number – The tracking number assigned by the Cisco SOC to each ticket.
- Incident Ticket opened date and time – The date the ticket was opened.
- Incident Ticket description – A brief description of the incident(s) detailed in the ticket.
- Incident Ticket status – The current status of the ticket as determined by the most recent note entered in to the ticket.

1.2.1 Reports

The MTD Service provides reports that are generated on the Customer Portal and available in HTML format.

Reports on the Customer Portal may include:

- Security Incident Rate of Occurrence – shows the number of security incidents categorized into each malicious security categories handled by the Cisco SOC during the given time period.
- Daily Threat Exposure – shows a normalized aggregate total impact of all detected malicious security incidents handled by the Cisco SOC during a particular day.
- Monthly Threat Exposure – shows a normalized aggregate total impact of all detected malicious security incidents handled by the Cisco SOC during a particular month.
- Top 10 Sources of Attack – shows the most frequent sources of attack for detected security incidents handled by the Cisco SOC during the given time period.

1.3 Customer Premise Devices

Cisco will ship a set of security networking equipment (the Cisco MTD Data Collection and Analysis Pod (DCAP)) for installation at each Customer site within 4 weeks of initial kickoff meeting; shipping details must be confirmed with the Customer prior to shipment. The DCAP contains the network security equipment necessary to execute the MTD service. Up to 2 DCAPs will be provided for the MTD core service. The following is a list of some of the components that may be included:

- NetFlow collection/analysis
- Malware detection/analysis (e.g. sandboxing)
- Network data forensics collection/analysis
- Protocol metadata forensics
- Protocol anomaly detection
- Web malware analysis
- Email malware analysis
- Network intrusion detection
- VPN router

- Passive network tap/switch

The DCAP is capable of a maximum sustained throughput of 5Gb/s on the monitored connection(s).

The DCAP (specifically the passive network tap and network monitoring switch) must be installed in the Customer and Cisco agreed upon physical/logical location as documented in the MTD Requirements document and will reside at the Customer Premises for the Term of the MTD service agreement.

The Customer must also provide the following for each DCAP:

- A publically routed non-NAT IP address and network access with at least 10Mbs bandwidth to the Internet for the VPN router in order to establish a secure connection to the Cisco SOC.
- At least 13kW of power
- 42 Rack Units (RU) of physical space

Title to all DCAP components shall remain with Cisco. Upon expiration or termination of the Term, Cisco will remotely destroy the data on all hard drives and device configurations provided within the DCAP. Customer must return the DCAP in working condition to Cisco immediately upon expiration or termination of the Term.

Cisco, or its subcontractors, shall be allowed access to the Customer Premises (location occupied by Customer) to the extent reasonably determined by Cisco for the inspection or emergency maintenance of the DCAP. Failure to allow timely access may invalidate Cisco SLAs, if any, and delay restoration and performance of Services.

All hardware or software maintenance of the DCAP equipment will be implemented by Cisco. The Customer is responsible for working with Cisco and providing onsite support in order to implement required maintenance.

In addition to the above, the Customer is responsible for the physical security, physical location, power availability, and cooling of the DCAP.

1.4 Managed Threat Defense (MTD) - Service Delivery

Cisco MTD provides a hosted security service to rapidly detect and respond to organizations' security incidents by analyzing network traffic, evaluating security telemetry and leveraging intelligence feeds.

The Cisco MTD SOC will proactively monitor for key incidents and thresholds in the Customer's network infrastructure. In the case of undetected incidents, the Customer may declare an Incident by contacting the MTD SOC, communicating via telephone any high priority Incidents (system down, degraded performance, etc.). Low priority incidents should be reported to the MTD SOC via the Cisco MTD Customer Web Portal.

Upon automatic detection or manual submission of an Incident to the MTD SOC, an Incident Ticket is created. The MTD SOC is ultimately responsible for coordinating the management of the Incident, which includes communicating with the Customer throughout the Incident management process. This communication also includes notification to the Customer that the Incident has been resolved or remediated.

Coverage for up to 2,000 incidents is provided as part of the MTD service. More can purchased as part of the Managed Threat Defense Incident Add-On package, as described in Section 2.1. In the event that 2,000 incidents is reached prior to the end of the Term and the Customer chooses not to purchase the Add-On package, service delivery will be deemed complete and the service contract will terminate along with any associated SLA.

1.4.1 Incident Lifecycle

The MTD Service provides a managed service of the organization's network security incident lifecycle. The network security incident lifecycle comprises four (4) phases including: detection, investigation, mitigation, and remediation recommendation.

1.4.1.1 Detection

Cisco is responsible for monitoring the Customer environment, systems and data as defined in the asset classification and prioritization exercises of the on-boarding phase. The DCAP detects items such as: anomalous traffic, traffic behavior patterns,

malicious and security events. A security event is defined as a identified occurrence of a system, service or network state indicating a possible breach of information security policy or failure of controls, or a previously unknown situation that may be security relevant (ISO 27035).

Activities may include:

- Monitoring and analyzing network based data and security analytics in order to identify potential malicious security events and incidents utilizing many different types of security telemetry (e.g. NetFlow, DNS, syslog, identity) as inputs per the Cisco Service Level Agreement.
- MTD will utilize Cisco security products, as well as third-party security products and threat intelligence feeds/tools for security event and incident detection and correlation.

1.4.1.2 Incident Record

Cisco is responsible for the Cisco MTD ticketing system that captures incident details, either through automated or manual means. A security incident is defined as a single or series of unwanted or unexpected information security events that have a significant probability of compromising business operations and threatening information security (ISO 27035). If an incident is discovered and reported to the Customer, and then the same incident is discovered again 24 hours or more after the initial incident, this will be considered two separate incidents. If two separate incidents (i.e. different types of malware) are discovered on the same host regardless of timeframe, this will also be considered two separate incidents.

As a part of the MTD service, time is allocated for handling up to 2000 incidents per year. The MTD SOC is responsible for updating the MTD Customer Portal with a current listing of the number of incidents handled to date.

Activities may include:

- Collection of security events triggered from the DCAP.
- Correlation of related security events into a security incident.

Deliverable(s):

- Create Incident Ticket on the Customer Portal.
- Update Customer Portal with total number of incidents addressed.

1.4.1.3 Incident Communication (E-notification)

Cisco will electronically notify (E-notify) designated Customer contacts for new Incidents or milestones achieved during the incident lifecycle. E-notifications are sent to any email address or email-capable mobile device and will include the Incident Ticket number. The Customer can always view Incident status and detailed information via the Customer Portal.

Automated electronic notification (E-notification) to specific Customer contact(s) based on Customer's notification requirements as agreed on during the Service Activation process.

Activities may include:

- Matching Customer's notification profile with Incident Ticket milestones.

Deliverable(s):

- Perform E-notification of Incident Tickets per Customer's notification profile.
- Log E-notification records in the Incident Ticket

1.4.1.4 Categorization and Priority

Incidents will be managed according to the CAT level as determined by a modified version of the US-CERT Reference: http://www.us-cert.gov/government-users/reporting-requirements. Incident CAT level depends on a variety of factors including pre-defined Incident Ticketing attributes such as business impact, urgency and asset value (if applicable and entered into context repository during the On-boarding phase) as well as the categories listed in the table below. Incident CAT level will determine the Incident Priority level set by the MTD SOC on a per-incident basis.

Category	Name	Description
CAT 0	Exercise/Network Defense Testing	This category will be utilized when the Cisco MTD DCAP or Customer is conducting an internal approved penetration test
CAT 1	Unauthorized Access	In this category an individual gains logical or physical access without permission to a client network, system, application, data, or other resource
CAT 2	Denial of Service (DoS)	An attack that successfully prevents or impairs the normal authorized functionality of networks, systems or applications by exhausting resources.
CAT 3	Malicious Code	Successful installation of malicious software (e.g., virus, worm, Trojan horse, or other code-based malicious entity) that infects an operating system or application.
CAT 4	Scans/Probes/Attempted Access	This category includes any activity that seeks to access or identify a client computer, open ports, protocols, service, or any combination for later exploit.
CAT 5	Investigation	Unconfirmed incidents that are potentially malicious or anomalous activity deemed by the reporting entity to warrant further review
CAT 6	Threat Outreach	This category will be utilized for distribution of intelligence briefings to MTD customers.

Activities:

- Evaluate Incident CAT and prioritize all Incidents into High (Priority 1), Medium (Priority 2) and Low (Priority 3) Incident categories.

Deliverable(s):

- Properly prioritized Incidents based on Incident Ticketing attributes.
- Report prioritized Incident as defined in the Service Level Agreement (SLA).

1.4.1.5 Incident Investigation and Diagnosis

Cisco SOC engineers utilize Incident Remediation procedures to collect any additional data required to fully diagnose and match the Incident to a known event type in the Cisco MTD Knowledge Base (KB). Cisco SOC engineers will work to quickly isolate the root cause of the Incident. Once root cause isolation has occurred, Cisco SOC engineers will update the Incident Ticket with information related to root cause isolation and then proceed to the Incident resolution and restoration phase.

Activities:

- Collect additional data to properly diagnose root cause of the incident.
- Attempt to match Incident to a known event type in the Cisco MTD Knowledge Base (KB).

Deliverable(s):

- Update Incident Ticket with root cause security event information for security incidents.
- Perform E-notification for this Incident Ticket event milestone (if requested by the Customer).

1.4.1.6 Incident Mitigation and Remediation Recommendations

Cisco SOC engineers will work with the Customer to restore affected services. The Customer is responsible for implementing all recommended mitigation techniques.

The goal of mitigation is to put measures in place that stop or minimize the impact of the incident. Some examples of mitigation measures that might be used are:

- Access control lists
- Web proxy filters

- DNS redirects
- Modifications to existing processes or procedures

After the Incident has been isolated down to its root cause, Cisco SOC engineers will provide recommendations to the Customer to remediate the Incident. Remediation is complete when full functionality is restored to the affected devices. Cisco SOC security engineers may provide recommendations for remediation of an infected host (if detected). The Customer is responsible for all remediation activities.

Activities:

- Assist in developing strategies for mitigating and remediating security incidents on the Customer's network infrastructure.
- Update Incident Ticket to include notes detailing incident resolution or recommendations for remediating security incidents.
- Perform E-notification for these Incident Ticket milestones, if requested by the Customer.

Deliverable(s):

- Updated Incident Ticket with recommendations detailing how to remediate a malicious security incident.
- Updated Incident Ticket with justification for classifying benign security incidents.

1.4.1.7 Incident Escalations

The Cisco SOC will refer incidents to the Customer as needed and escalate the incident with the Customer within the Customer's escalation guidelines until the incident is mitigated. A Customer may request escalation of an incident ticket at any time via the Customer Portal or telephone call to the Cisco SOC.

Activities:

- Ensure appropriate Cisco SOC engineering resources handle incidents.
- Escalate incident as appropriate in the Cisco SOC or with the Customer per the established escalation procedures.

Deliverable(s):

- Updated incident ticket to include escalation notes.
- Perform E-notification for this incident ticket event milestone, if requested by the Customer.

1.4.1.8 Incident Closure

Once the Cisco SOC declares an incident resolved and verified the incident will be closed. In the event that the incident reoccurs, a new incident ticket will be created to accurately reflect the recurring nature of the incident and aid in the identification of problems.

Any authorized Customer agent may also proactively request incident ticket closure via the Customer Portal or Telephone. The Cisco SOC will review the request and close the incident ticket or follow up with the Customer for more information as needed.

Activities:

- Confirm incident is resolved.

Deliverable(s):

- Update incident ticket to include closing notes.
- Close the incident ticket.

1.4.2 Quarterly Business Review (QBR)

A quarterly business review will take place once every three months to recap the joint collaboration and work accomplished to date for MTD.

1.4.2.1 QBR Delivery

Cisco is responsible for delivering the Quarterly Business Review remotely for up to four (4) hours in length, with no labs and no printed materials. Cisco will determine an appropriate format and delivery method that may include but shall not be limited to using a shared medium via the Internet, teleconference, and/or onsite.

Customer is responsible for designating at least two (2) technical security representatives and one (1) executive sponsor or appropriate proxy to participate in the Quarterly Business Review.

Activities:

- Review of reported incidents
- Discuss potential mitigation and/or remediation plans
- Determine service status per the terms of the Service Level Agreement
- Review of planned or completed major customer network changes

Deliverable(s):

- SLA Report, as indicated in the Service Level Agreement

2 MTD Add-On Packages

2.1 Managed Threat Defense Incident Add-On Package

The Incident Add-On package provides Customers with an additional amount of time that can be used for investigating up to an additional 500 incidents in the Customer environment. The Cisco SOC is responsible for tracking and updating the Customer Portal with a current listing of the number of incidents handled to date.

It is the Customer's responsibility to purchase this add-on package as needed.

Activities:

- Validate purchase of extra incidents.
- Update Customer Portal with total number of incidents addressed.

Deliverable(s):

- Apply an additional 500 incidents to Customer's contract.

2.2 Managed Threat Defense Incremental Coverage Add-On Package

Cisco will ship an additional DCAP for installation at the Customer site. The DCAP contains the network security equipment necessary for the MTD service. The following is a list of some of the components:

- NetFlow collection/analysis
- Malware detection/analysis (e.g. sandboxing)
- Network data forensics collection/analysis
- Protocol metadata forensics
- Protocol anomaly detection
- Web malware analysis
- Email malware analysis
- Network intrusion detection
- VPN router
- Passive network tap/switch

The DCAP (specifically the passive network tap and network monitoring switch) must be installed in the Customer and Cisco agreed upon physical/logical location as documented in the MTD Requirements document and will reside at the Customer Premises.

The Customer must also provide the following for each DCAP:

- A publically routed non-NAT IP address and network access with at least 10Mbs bandwidth to the Internet for the VPN router in order to establish a secure connection to the Cisco SOC.
- At least 13kW of power
- 42 Rack Units (RU) of physical space

Title to all DCAP components shall remain with Cisco. Upon expiration or termination of the Term, Cisco will remotely destroy the data on all hard drives provided within the DCAP. Customer must return the DCAP and associated network security equipment to Cisco immediately upon expiration or termination of the Term.

Cisco, or its subcontractors, shall be allowed access to the Customer Premises (location occupied by Customer) to the extent reasonably determined by Cisco for the inspection or emergency maintenance of the DCAP. Failure to allow timely access may invalidate Cisco SLAs, if any, and delay restoration and performance of Services.

Customer must return the DCAP in working condition to Cisco immediately upon expiration or termination of the MTD service agreement.

All hardware or software maintenance of the DCAP equipment will be implemented by Cisco. The Customer is responsible for working with Cisco and providing onsite support in order to implement required maintenance.

In addition to the above, the Customer is responsible for the physical security of the DCAP.

Activities:

- Work with Customer to identify DCAP installation location.
- Deliver additional DCAP to identified Customer location.
- Install additional DCAP into Customer environment.

Deliverable(s):

- Apply an additional time to cover up to 1000 additional incidents to the MTD service agreement.

3 Managed Threat Defense Proof of Concept

The Cisco Managed Threat Defense Proof of Concept package provides an opportunity to review MTD prior for a 3-month trial period. Similar to the MTD Core service, it provides remote network security monitoring utilizing network packet metadata, advanced malware and network behavior anomaly detection techniques, sandboxing capabilities, while leveraging a wide set of security intelligence feeds.

The MTD Proof of Concept service is provided with a 3-month service period in order to rapidly detect and respond to security incidents and events in one data center location. The 3-month service period begins on the date that a Cisco Network Consulting Engineer (NCE) is onsite as part of the on-boarding phase. This Proof of Concept service is provided without an SLA.

3.1 Customer Premise Devices

Cisco will ship a set of security networking equipment (the Cisco MTD Data Collection and Analysis Pod (DCAP)) for installation at the Customer site within 4 weeks of initial kickoff meeting for the MTD Proof of Concept; shipping details must be confirmed with the Customer prior to shipment. The DCAP contains the network security equipment necessary to execute the MTD service. One (1) DCAP will be provided for the MTD Proof of Concept. The following is a list of some of the components that may be included:

- NetFlow collection/analysis
- Malware detection/analysis (e.g. sandboxing)
- Network data forensics collection/analysis
- Protocol metadata forensics
- Protocol anomaly detection
- Web malware analysis
- Email malware analysis
- Network intrusion detection
- VPN router
- Passive network tap/switch

The DCAP is capable of a maximum sustained throughput of 5Gb/s on the monitored connection(s).

The DCAP (specifically the passive network tap and network monitoring switch) must be installed in the Customer and Cisco agreed upon physical/logical location as documented in the MTD Requirements document and will reside at the Customer Premises for the trial period.

The Customer must also provide the following for the DCAP:

- A publically routed non-NAT IP address and network access with at least 10Mbs bandwidth to the Internet for the VPN router in order to establish a secure connection to the Cisco SOC.
- At least 13kW of power
- 42 Rack Units (RU) of physical space

Title to all DCAP components shall remain with Cisco. Upon completion of the MTD Proof of Concept, the Customer has the option to move forward with MTD Core. If the Customer chooses not to move forward with MTD Core, Cisco will remotely destroy the data on all hard drives provided within the DCAP. Customer must return the DCAP in working condition to Cisco immediately upon completion of the MTD Proof of Concept.

Cisco, or its subcontractors, shall be allowed access to the Customer Premises (location occupied by Customer) to the extent reasonably determined by Cisco for the inspection or emergency maintenance of the DCAP.

All hardware or software maintenance of the DCAP equipment will be implemented by Cisco. The Customer is responsible for working with Cisco and providing onsite support in order to implement required maintenance.

In addition to the above, the Customer is responsible for the physical security, physical location, power availability, and cooling of the DCAP.

3.2 MTD Proof of Concept Executive Outbrief

At the end of the Proof of Concept, an Executive Outbrief review will take place to recap the joint collaboration and work accomplished.

3.2.1 Executive Outbrief Delivery

Cisco is responsible for delivering the Executive Outbrief remotely for up to four (4) hours in length, with no labs and no printed materials. Cisco will determine an appropriate format and delivery method that may include but shall not be limited to using a shared medium via the Internet, teleconference, and/or onsite.

Customer is responsible for designating at least two (2) technical security representatives and one (1) executive sponsor or appropriate proxy to participate in the Executive Outbrief Review.

Activities:

- Review of reported incidents
- Discuss potential mitigation and/or remediation plans

Deliverable(s):

- Outbrief Presentation

APPENDIX A: Glossary of Terms

Glossary of Terms should be read in conjunction with this Service Description. Capitalized terms not otherwise defined above have the meanings assigned to them in the Glossary of Terms.

ASA – Advanced Services Agreement.
CPE – Customer Premise Equipment.
Customer - The entity purchasing Services for its own internal use.
Customer Premises - The physical Customer location where the DCAP resides
DCAP - Data Collection and Analysis Pod.
ISO - International Standards Organization.
MHSA - Master Hosted Services Agreement
MTD – Managed Threat Defense.
MTDA - Managed Threat Defense Assessment.
MSA – Master Services Agreement.
NCE – Network Consulting Engineer.
NetFlow – A network protocol used by networking devices to characterize network operation and monitor IP traffic.
SLA – Service Level Agreement.
SOC – Security Operations Center.
Term – Duration of MTD Service purchased by Customer