Service Description: Cisco Active Threat Analytics

This document describes the Cisco Active Threat Analytics security services.

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.

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 Service Description and your MSA or equivalent services 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/.

Cisco shall provide the Cisco Active Threat Analytics (ATA) security services described below as selected and detailed on the Purchase Order for which Cisco has been paid the appropriate fee. Cisco shall provide a Quote for Services ("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.

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 ATA. This service description is also designed to properly set the Customer's expectations regarding these services.
Cisco ATA may include the following offerings as selected and detailed on the Purchase Order.

Cisco ATA core service offering is comprised of various service tiers. Each tier may be purchased alone, or with any combination of ATA Add-On packages shown below.

Active Threat Analytics Core Service Offerings Overview:

ATA: **Enhanced:**

- One (1) Base Instance of on-premise Data Collection and Analysis Pod (DCAP) to cover:
  - One (1) Internet points of presence
  - One (1) data center (multiple connections)
  - Supports data ingest of throughput up to 5 gigabits per second (gbps)
- 24/7 monitoring & management of the following devices:
  - One (1) Cisco AMP for Networks
  - One (1) Cisco NGIPS
- Threat Intelligence & Correlation
- Metadata Extraction and Netflow Generation
- Advanced Analytics: Rule and Statistical Based
- ThreatGrid Analysis
- Active Customer Portal Access
- Investigations Manager
- Quarterly Business Review
- Total Telemetry Feeds from Non-Security Alerting Devices up to 50 GB per day

ATA: **Premier:**

Includes everything in Enhanced above, as well as:

- Full packet capture
- Advanced Analytics: Rule, Statistical, and Big Data Hadoop-Based Analytics
- Proactive Threat Hunting
- Monthly Technical Briefing
- Total Telemetry Feeds from Non-Security Alerting Devices up to 100 GB per day

Active Threat Analytics Add-On Packages:

The Active Threat Analytics Add-On packages may only be purchased with an existing or planned purchase of one of the above Active Threat Analytics Services.

ATA Add-On: **Additional Threat Telemetry**:

- Monitoring of additional telemetry feeds from Non-Security Alerting Devices beyond the included limits for each ATA Core Package, outlined above

Cisco will only provide support for the Active Threat Analytics service offerings that have been selected on the Purchase Order.

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

1. Cisco Active Threat Analytics

Cisco Active Threat Analytics provides remote network security monitoring using 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 at the start of Monitoring and Service Delivery (Section 1.4), or eight (8) weeks following the start of the Kickoff (Section 1.1), whichever comes first.
Delivery for ATA services will include four (4) phases as described in this document:

1. Kickoff
2. Activation
3. Transition
4. Monitoring (Service Delivery)

Also includes:

- Customer Reviews:
  - Quarterly Business Review
  - Monthly Technical Review (for Premier Tier only)

1.1 Kickoff

1.1.1 Project Management

Cisco will assign a Project Manager to act as a primary point of contact. Cisco will work with Customer to develop a comprehensive project plan, manage the people and processes required for the Services, and monitor that the services are provided according to the plan.

Cisco Responsibilities

- Provide a single point of contact ("Project Manager" or “PM”) for all issues relating to the ATA Services delivered within the scope of this Service. Such person shall be identified and shall be available during Standard Business Hours.
- Designate a backup contact when the Project Manager is not available.
- Define the communication flow with the Customer’s project sponsor and key stakeholders.
- Participate in regularly scheduled meetings with the Customer to discuss the status of the service, identify and document dependencies, risks and issues associated with the successful delivery of the service.
- Act as the focal point for change management procedures.

Customer Responsibilities

- Designate a single point of contact to whom all Cisco communications may be addressed and who has authority to act on all aspects of the ATA services.
- Designate a backup, or secondary, contact that has the authority to act on all aspects of the Services in the absence of the primary contact.
- Participate in regularly scheduled project review meetings or conference calls.
- Review the project schedule, objectives, services, and roles and responsibilities with Cisco.
- Identify a project sponsor and key stakeholders and define their roles in supporting this project.
- Work with the Cisco PM to ensure the Customer’s project sponsor, key stakeholders and all project team members receive project communications and are included in regularly scheduled communications sessions.
- Work with Cisco to schedule the kick-off meeting, and communicate the meeting schedule to the Customer-identified stakeholders.
- Provide information and documentation required by Cisco within a timely manner in order to maintain project schedules.
- Notify Cisco of any Hardware and/or Software upgrades that relate to the delivery of the Services or any other changes within Customer’s current network that relate to the delivery of the Services at least ten (10) business days prior to such upgrade.
- Notify Cisco of any scheduled implementation activities within ten (10) business days of the scheduled activity.
- Notify Cisco of any installation scheduling change at least seventy-two (72) hours prior to the originally scheduled installation date.
- Notify Cisco of any scheduling changes related to this Term at least ten (10) business days of the scheduled activity.
- Schedule the necessary facilities and access for on-site meetings (such as: badge or visitor access, conference rooms, projectors and conference bridges).

1.1.2 Kickoff

The Project Manager will contact the Customer’s point of contact (CPOC) 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.

Cisco Responsibilities

- Conduct remote (Cisco WebEx) kickoff workshop(s) to review the activation activities, and services purchased as indicated on the Purchase Order.

Customer Responsibilities

- Identify key contacts and authorized personnel required for the kickoff meeting and coordinate with the Project Manager to facilitate and organize kickoff meeting.
- Provide necessary inputs necessary for scheduling activation activities.

1.2 Activation

Activation is primarily an information-gathering phase that will provide the foundation for delivery of the ATA service. It will also include delivery and installation of the Data Collection and Analysis Pod ("on-premise") equipment included as part of the ATA service.

1.2.1 Information Gathering

To effectively manage a security incident lifecycle, Cisco needs to fully understand the Customer environment and security workflows. Information gathering during the activation phase will be primarily performed remotely via a series of WebEx meetings with key customer personnel and stakeholders.
Information gathered during this phase may include:

- Organizational structure and introductions
- Solution goals, as well as business, technical, and operational requirements
- Current security policy, current security incident management environment, and incident handling procedures, including Customer's response stance to potential incidents
- Network diagrams and topology maps
- Enumeration of existing IP networks and IP schema
- Asset Classification and Prioritization Documents
- Existing information and/or policies referencing normal and permissible network traffic required to properly tune on-premise equipment
- Quarterly vulnerability scan reports that provide details such as listening ports, version of services, and point-in-time baselines of vulnerabilities associated with critical assets such as servers or software applications.
- Future technology plans

Cisco Responsibilities

- Schedule and coordinate remote information gathering meetings with Customer to collect relevant information as required.
- Review information as provided by the Customer, identifying any gaps in the information provided and noting any corrective actions requiring action by the Customer.
- Review situations and locations in the network where full-packet capture may not be permissible. Properly tune DCAP equipment in order to comply with Customer requirements.
- Follow Customer Response Stance as defined by Customer.

Customer Responsibilities

- Ensure that Customer's subject matter experts attend information gathering workshop(s) and provide required information, as required
- Provide to Cisco appropriate documentation and resources to review requested information prior to or during workshops, as requested.
- Provide enumeration of existing IP networks and IP schema. If none exists, Customer is responsible for working with Cisco to create a topology map using discovery and scanning tools.
- Provide a full listing of contacts, including job descriptions, roles and responsibilities as required for incident handling and escalation.
- Ensure policies are in place that outline and describe the organization's Response Stance. The Customer will be responsible for defining and directing the Response Stance and communicating this to Cisco.
- Provide quarterly service and vulnerability scan reports of relevant devices to Cisco, if available.
- Work with Cisco to review documents and information collected, and assist the Cisco NCEs in the process of documenting the identification, classification and prioritization of critical systems and data.
- Define situations and locations in the network where full packet capture may not be permissible and provide this information to Cisco.
- Provide any additional information as requested by Cisco. Work with Cisco to develop detailed design and configuration templates by providing information and feedback

1.2.2 On-Premise Equipment Installation

Cisco will ship the DCAP to be used as on-premise equipment, with installation by Customer at its site within four (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 ATA service.

The DCAP must be installed at a mutually agreed upon physical/logical location and will reside at the Customer's premises for the duration of the ATA service purchased.

Title to the DCAP shall remain with Cisco. Cisco expects that, at the time of removal, the DCAP shall be in the same condition as when installed, with the expectation of normal wear and tear. Customer shall reimburse Cisco for the costs of DCAP that is deemed beyond normal wear and tear.

An asset tracking form will be provided to the Customer for sign off following shipment of DCAP. This form will include the following details regarding Cisco equipment placed at Customer premise: 1) Itemized descriptions and product numbers, including serial numbers; 2) Physical address where equipment will be located; 3) Purchase Order number of corresponding service purchased by Customer.

As scheduled between Cisco and Project Manager, a Cisco Network Consulting Engineer (NCE) may travel onsite to provide assistance with on-premise equipment installation and testing.

For the **ATA Enhanced** package, the following may be provided.

- Network intrusion detection systems
- Malware analysis engines
- Sandboxing technologies
- VPN router
- Passive network tap/switch
- Application flow collection engine
- Metadata extraction engine
- Additional data storage components

The **ATA Premier** package may include all components in the Enhanced package, and may add:

- Full packet capture storage and file extraction engine
- Big data master and cluster nodes

Cisco Responsibilities

- Shipping all devices, servers, and/or appliances supporting applications on the DCAP.
- Assist the Customer with installation of DCAP
- Establish connectivity between the Customer site and Cisco DCAP
- Perform all required maintenance for hardware or software within the DCAP.
- Schedule and provide e-mail notification to Customer regarding routine maintenance or upgrade to DCAP. Cisco will use reasonable efforts to provide 1-week notice prior to the implementation of an update. Customer-specific considerations stemming from upgrade will also be communicated to Customer and addressed as part of maintenance.

Customer Responsibilities

- Installation of the DCAP per Cisco-supplied guidelines
- Work with Cisco to provide onsite support in order to implement required maintenance at agreed upon physical/logical location, such as racking, connection to network, and power.
- Allow Cisco, or its subcontractors, access to the Customer Premises to the extent reasonably determined by Cisco for the inspection or emergency maintenance of the DCAP. Failure to allow timely access may invalidate service delivery and delay restoration and performance of services.
- Provide onsite access and/or assistance to Cisco for required hardware maintenance
- 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 Cisco.
  - Physical space, physical security, power availability, cooling, and suitable environmental conditions required for computer operations of on-premise equipment.
- Maintain the DCAP in good working order. The Customer shall not, nor permit others to, rearrange, disconnect, remove, and attempt to repair, or otherwise tamper with the DCAP. Should this occur without first receiving written consent from Cisco, the Customer will be responsible for reimbursing Cisco for the cost to repair, or replace, any damaged equipment. Under no circumstances will Cisco be held liable to the Customer or any other parties for the interruption of service, or for any other loss, cost, or damage that is a result from the improper use or maintenance of the DCAP.
- Return the DCAP in working condition to Cisco immediately upon expiration or termination of the Term.

1.3 Transition

Cisco will deliver a Transition out-brief to the Customer upon completion of the Activation 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.

Items covered in the Transition out-brief may include:

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

Once the Transition Out-brief has been completed, monitoring and incident management will be transferred to the ATA SOC as described in section 1.4. Furthermore, billing and invoicing for the ATA Service will also commence following the Transition out-brief event.

Cisco Responsibilities

- Deliver a Transition out-brief session to the Customer upon completion of the Activation phase.

Customer Responsibilities

- Designate at least two (2) security representatives to participate in the Transition Out-brief.

1.4 Monitoring and Service Delivery

The Cisco ATA Security Operations Center (SOC or ATA SOC) will proactively monitor for key Security Incidents and thresholds in the Customer's network infrastructure. In the case of undetected Security Incidents, the Customer may declare a Security Incident by contacting the ATA SOC, communicating via telephone any high priority Incidents (system down, degraded performance, etc.). Low priority incidents should be

reported to the SOC via the Customer Portal (described in Section 1.4.2).

Upon automatic detection or manual submission of an Incident to the SOC, an Incident Ticket is created. The ATA 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

1.4.1 Monitoring and Incident Records

Cisco is responsible for monitoring the Customer environment, systems and data as defined in the asset classification and prioritization exercises of the activation phase.

Activities primarily include monitoring and analyzing network based data and correlating threat intelligence feeds in order to identify potential malicious Security Incidents.

Cisco Responsibilities:

- Collect and correlate related security events into Security Incidents
- Create Incident Tickets on the Customer Portal.
- Classify each Security Incident into security category. Categories are based on a modified version of the US-CERT incident categories: http://www.us-cert.gov/government-users/reporting-requirements
- Prioritize all Incidents into High, Medium, and Low priority based on several criteria such as the type of infection, confirmation of the incident, or the number assets associated with the Incident. Priorities are defined as:
  - High: Critical business impact or data loss to the Customer
  - Medium: Adverse effect to Customer, potential data loss, potential loss of service.
  - Low: No adverse impact to Customer. No financial loss. No data loss.
- Electronically notify designated Customer contacts for new incidents via email and/or Portal
- Provide mitigation recommendations as available for associated Security Incident

Customer Responsibilities:

- Review Incident Tickets on the Customer Portal and provide details for ticket closure.
- Implement recommended mitigation techniques, if available.

1.4.2 Customer Portal

The ATA Service includes a Customer Portal (“Portal”) that will provide visibility into the delivery of the service, including Incident Tickets and reports.

During the initial setup phase, Customers will receive accounts for authorized employees 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.

Information available from the Portal may include:

- Incident Ticket identification number – The tracking number assigned by the ATA 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.

Cisco Responsibilities:

- Provide access to Customer to dedicated Customer Portal.
- Provide accounts for authorized Customer personnel to access the Portal.
- Provide instructions to access and navigate the Portal. Instruction will be provided during the on-boarding phase via video, WebEx, or onsite as determined by Cisco.

Customer Responsibilities

- Determine and maintain list of authorized users with privilege to view Customer Portal.
- Review information presented in the Portal

1.4.3 Designated Investigations Manager

A designated Investigations Manager with deep Incident analysis and investigation skills will be assigned.

This Investigations Manager will be responsible for:

- Responding to Customer inquiries and assisting with Incident resolution as needed by Customer
- Staying current with Customer environment and relay any changes or updates to ATA SOC
- Research and observe trends at client sites in order to provide reports and presentations to clients representing trends and incidents at Quarterly Business Reviews or Monthly Technical Reviews

Cisco Responsibilities:

- Assign an Investigations Manager to assist Customer throughout service delivery

Customer Responsibilities:

- Provide the Investigations Manager with necessary information, documentation, and/or status as it relates to changes to the customer network environment monitored by Cisco

1.4.4 Proactive Threat Hunting (Premier)

For Customers who have purchased the Premier package: Cisco will perform activities involving seeking out malicious activity not identified by traditional alerting mechanisms.

Cisco Responsibilities:

- Actively search for attacks by applying ongoing working knowledge of current threats and intelligence attributed to these threats.
- Document and update a living playbook that provides 'plays' for hunting threats specific to the Customer's environment
- Run plays according to frequency outlined by Cisco for each specific play. Create and prioritize an Incident Ticket if outcome of play displays evidence of a Security Incident as determined by Cisco.

Customer Responsibilities:

- Review Incident Tickets created by Cisco as a result of a proactive play.
- Implement mitigation and/or remediation recommendations, if available.

1.5 Customer Reviews

Quarterly or monthly reviews will take place to recap the joint collaboration and work accomplished to date for ATA.

1.5.1 Quarterly Business Review

Cisco and Customer will conduct quarterly business review(s) (QBR). The QBR is targeted for Customer business and security leaders in order to provide a high level view of the outcomes and value provided by ATA service.

Activities and items covered in the QBR include:

- Review of reported Incidents
- Discuss potential mitigation and/or remediation plans
- Review of planned or completed major Customer network changes

Cisco Responsibilities:

- Deliver Quarterly Business Review: may be up to four (4) hours in length with no labs and no printed materials.
- 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 Responsibilities:

- Ensure that Customer's appropriate executive staff is available to attend the Quarterly Business Review.
- Designate at least two (2) technical security representatives and one (1) executive sponsor or appropriate proxy to participate in the Quarterly Business Review.
- Review and provide feedback during the Quarterly Business Review meeting.

1.5.2 Monthly Technical Review Delivery (Premier)

For Premier Customers, an optional monthly technical review may be provided. This technical review may be held every month to provide mutual feedback and program recommendations.

Activities and items covered in the Monthly Technical Review include:

- Review of reported Incidents
- Discuss potential mitigation and/or remediation plans
- Review of planned or completed major Customer network changes

Cisco Responsibilities:

- Deliver the Monthly Technical Review, which will be up to one (1) hour in length, with no labs and no printed materials.
- Method of delivery for the Monthly Technical Review will be remote over Webex or teleconference.

Customer Responsibilities:

- If desired, ensure that Customer's appropriate technical staff is available to attend the Monthly Technical Review
- Designate one (1) technical security representatives to participate in the Monthly Technical Review.
- Review and provide feedback during the Monthly Technical Review meeting

2. ATA Add-On Packages

2.1 Add-On Package: Additional Threat Telemetry

The Customer will have the option to purchase an Add-On Package for Additional Threat Telemetry for capturing and analyzing additional network forensic telemetry and data from Non-Security Alerting Devices beyond the included limits for each package. Purchase of this Add-On package may require Cisco to ship additional DCAP components to the Customer for installation at Customer's location to support the additional daily data index requirements.

Additional telemetry from Security Alerting Devices (such as sensors or endpoint security applications) is permitted and will be included in the Quote provided by Cisco, based on the requirements needed for security monitoring of each additional device.

Additional telemetry from Non-Security Alerting Devices (such as from firewalls, proxies, DNS, DHCP, Directory Services, or other unclassified devices) may be added to existing cap limits outlined in Active Threat Analytics Core Service Offerings Overview section of this document and purchased in

increments up to 200GB/day and included in the Quote provided by Cisco.

The ATA SOC is responsible for adding tracking telemetry collected and notifying the Customer if limits are close to being reached. Cisco will work with the Customer to properly scope additional telemetry add-on based on Customer requirements.

If the daily telemetry limitation for Non-Security Alerting Devices is reached during delivery of any of the ATA Core Packages and the Additional Threat Telemetry Add-on Package is not purchased, then the SOC will work with the Customer to filter telemetry captured in order to stay under telemetry limits.

Cisco Responsibilities:

- Provide guidance to Customer as needed for additional telemetry collection based on Customer requirements
- Determine with Customer what additional DCAP components are needed to support Customer requirements.
- Procure and deliver additional DCAP components and ship to Customer, if necessary.
- Track telemetry collected and notify the Customer if limits are close to being reached. If limits are reached, work with the Customer to identify telemetry that may be filtered in order to stay within telemetry limits.
- Assist in installation of additional DCAP components as necessary for service.

Customer Responsibilities:

- Provide information requested from Cisco in order to properly scope and define requirements for additional telemetry collection.
- Install additional DCAP components as prescribed by Cisco.
- Work with Cisco to identify telemetry that may be filtered if telemetry limits are reached.

APPENDIX: 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.

ATA- Active Threat Analytics

Customer- The entity purchasing Services for its own internal use

Customer Portal- Web application provided by Cisco to Customer that details visibility into ATA service, including incident tickets and reports

Customer Premises- The physical Customer location where the DCAP resides

DCAP- Data Collection and Analysis Pod

Investigations Manager- A security engineer designated to Customer with deep incident and investigation skills responsible for responding to Customer inquires and staying current with the Customer environment

Incident Tickets- An enumerated report that provides details about a Security Incident detected by the SOC and requires attention from the Customer.

ISO-International Standards Organization

NCE– Network Consulting Engineer

NetFlow- A network protocol used by networking devices to characterize network operation and monitor IP traffic

Non-Security Alerting Device – A networking device, appliance, application or server in which the core function of the device is not to generate security alerts designed to detect unwanted or malicious activity from computer networks. Examples include firewalls, proxy services, directory services, DNS/DHCP servers, or business application servers.

Response Stance- A documented policy that describes how the Customer's 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

Security Alerting Device – A security device, appliance, or application in which the core function is to generate security alerts designed to detect unwanted or malicious activity from computer networks. Examples include security sensors or endpoint security detection applications.

Security Event - An 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)

Security Incident or **Incident**- 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)

SOC- Security Operations Center

Term- Duration of ATA Service purchased by Customer