Service Description: Cisco Active Threat Analytics – Premier

This service description ("Service Description") describes the Cisco Active Threat Analytics security services ("Services").

Related Documents: This Service Description should be read in conjunction with the following documents also posted at www.cisco.com/go/servicedescriptions/:

(1) List of Services Not Covered;
(2) Severity and Escalation Guidelines;
(3) Service Activation Process: Cisco Active Threat Analytics
(4) Threat Detection Catalog (;
(5) Telemetry Support List

All capitalized terms in this Service Description shall have the meaning ascribed to them in the Glossary of Terms at the end of this document.

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 (the "Agreement"). If you do not have an Agreement in place with Cisco, the following terms will be deemed the Agreement: http://www.cisco.com/c/dam/en_us/about/doing_ business/le gal/docs/Advanced_Services_Click-to- Accept_Agreement_sample.pdf
If not already covered in your Agreement, this document should be read in conjunction with the 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 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, service order, SOW, or similar document ("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. Any additional Purchase Order terms are deemed rejected.

1.0 Summary

This Service Description summarizes the activities, deliverables and service delivery processes that Cisco uses to deliver the Services. Cisco will only provide support for the Active Threat Analytics service offerings that have been selected on the Purchase Order. Cisco ATA may include the following offerings as selected and detailed on the Purchase Order. Customer may purchase optional Add-On packages shown below as a part of the core Services.

1.1 Core Service: ATA Premier Summary

Cisco Active Threat Analytics provides remote network security monitoring using network packet metadata and detection techniques (defined in Telemetry Support List and the Threat Detection Catalog) over the to help detect and respond to Security Incidents and events.

ATA Premier:

- One (1) Instance of on premise Data Collection and Analysis Pod (DCAP) to support up to 250,000 Events per Second (EPS) sustained and rolling

storage of up to 400 TB of raw Telemetry
- One (1) Instance of on premise ATA Sensor Base with Full Packet Capture
- One (1) ATA Sensor Expanded Throughput Add- On to offer total Sensor support of up to 4gbps throughput and 60 TB storage
- Metadata Extraction
- Up to 15 user licenses for Customer Portal access
- Monitoring and Incident Records
- Investigations Manager
- Engagement Manager
- Incident Response Retainer
- Quarterly Business Review
- Monthly Technical Briefing

The term of the Services begins at the start of Monitoring and Service Delivery (referenced below), or eight (8) weeks following the start of the Kickoff, whichever comes first.

Delivery of the Services consists of four (4) phases. The four (4) phases are:

1. Kickoff
2. Activation
3. Transition
4.Monitoring and Service Delivery (described in this document)

Kickoff Activation and Transition are described in the document named Service On-boarding Process Description: Cisco Active Threat Analytics.

1.2 Monitoring and Service Delivery

The Cisco ATA Security Operations Center ("SOC" or "ATA SOC") will proactively monitor for threats or Security Incidents identified in the Threat Detection Catalog within the Customer's in-scope network infrastructure. Monitoring will begin following the Transition Out-brief;

In the case of undetected Security Incidents, the Customer may report a Security Incident by contacting the ATA SOC, communicating via telephone any high priority Incidents (e.g. system down, significantly degraded performance, etc.) as a result of a Security Incident. Low priority incidents should be reported to the SOC via the Customer Portal (described below). Cisco will work with the Customer to verify any Security Incidents

Upon automatic detection or manual submission of a Security Incident to the SOC, a Case is created, which corresponds to the Security Incident. Cisco will investigate and then recommended remediation actions for any verified Security Incidents. The SOC is also available to answer questions related to the Security Incident and provide additional information, dependent upon data sources available to the SOC and available information about the Security Incident.

1.2.1 Monitoring and Incident Records

Cisco will monitor the Customer's in-scope environment as described in the Telemetry Support List for Security Incidents as described in the Threat Detection Catalog. These documents may be updated by Cisco in their discretion. The latest version Updated versions of these documents are available upon written request.

Monitoring activities consist of monitoring and analyzing network and telemetry-based data (including Metadata) in order to identify potential threats or Security Incidents.

Cisco Responsibilities:
• Monitor Customer's in-scope environment for Security Incidents.
• Create Cases in response to a discovered or reported Security Incident.
• Electronically notify designated Customer contacts for new incidents via Customer Portal
• Provide mitigation recommendations as available for associated Security Incident

Customer Responsibilities:
• Review Cases on the Portal and provide details for Case closure.
• Implement recommended mitigation techniques, if available.

1.2.2 Telemetry Tuning

Telemetry tuning is the adjustment of the amount and type of Telemetry data sent from a security device to provide the most usable data while minimizing limited or no value data (for purposes of the Services). The amount of Telemetry processed is limited by the original DCAP telemetry thresholds as described in the

Service Offerings overview (Section 1.1). As the amount of data ingested by the DCAP reaches the indicated storage thresholds. The Storage Add-On package, as described in Section 2.3, may be purchased if additional data retention is desired. Otherwise, the oldest Telemetry will be overwritten as new Telemetry is created. Telemetry Tuning may be provided at any point during Service Delivery or at the request of either party.

Cisco may collect data on Your use of the Services, threats or potential threats against your environment and Telemetry to maintain, improve, market or promote the Services. Customer acknowledges that Cisco may freely use this data as long as it does not identify or imply Customer or contain any personal or confidential information of Customer (or it's personnel).

Cisco Responsibilities:

- Work with Customer on network device discovery to understand network device roles and functions
- Prioritize Telemetry-based on value to Security Incident monitoring
- Provide instruction to Customer on any changes required in order to allow the sending of updated Telemetry values to the DCAP
- Validate receipt of Telemetry into the DCAP

Customer Responsibilities:

- Provide information required for network device discovery
- Work with Cisco to prioritize sources of telemetry
- Implement recommended changes to applicable network applications or devices in order to enable the sending of Telemetry into the DCAP
- Work with Cisco to ensure Telemetry is received by DCAP

1.2.3 Customer Portal

The ATA Service includes a Customer Portal ("Portal") that will provide visibility into the delivery of the Service. Customers will receive up to 15 user accounts for authorized employees to access the Portal. Instructions to access and navigate the Portal will be provided as a part of the activation phase. Customer is responsible for information and requests submitted to the Portal by its users.

Information available from the Portal may include:

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

Cisco Responsibilities:

- Establish and maintain Customer Portal
- Provide up to 15 users' access to Customer to dedicated Customer Portal (more if Customer purchases additional user access).
- Provide accounts for authorized Customer personnel to access the Portal.
- Provide instructions to access and navigate the Portal to end users.

Customer Responsibilities:

- Determine and maintain list of authorized users with privilege to use Customer Portal.
- Review information presented in the Portal
- Manage and secure credential to access the Portal.

1.2.4 Designated Investigations Manager

A designated Investigations Manager with Security Incident analysis and investigation skills will be assigned to Customer.

This Investigations Manager will be responsible for:

- Working with SOC in responding to Customer inquiries and assisting with Security Incident resolution as needed by Customer
- Working with Customer in staying current with Customer environment and relay any changes or updates to SOC
- Research and observe trends on in-scope Customer environment

- Responding to Customer requests for new/additional threat detections or telemetry sources.

Cisco Responsibilities:

- Assign a qualified Investigations Manager to assist Customer throughout Services 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.

1.2.5 Designated Engagement Manager

A designated Engagement Manager will be assigned.

This Engagement Manager will be responsible for:

- Single point of contact for Customer/Account within Cisco ATA services
- Leads Quarterly Business Review ("QBR") meetings with the Customer
- Responding to general Customer inquiries and assisting with resolution as needed by Customer
- Staying current with Customer environment and relay any changes or updates to SOC

Cisco Responsibilities:

- Assign a qualified Engagement Manager to assist Customer throughout service delivery.

Customer Responsibilities:

- Provide the Engagement Manager with necessary information, documentation, and/or status as it relates to changes to the Customer.

1.3 Customer Reviews

Quarterly and monthly reviews will take place to review the performance of the Services, identify issues, discuss changes in the Customer environment or requirements and similar matters.

1.3.1 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 the Services.

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
- Summarize overall performance of the Services

2. Optional ATA Add-On Services

The optional ATA Add-On Services may only be purchased as a part of the Active Threat Analytics Core Service Offerings and not on a stand-alone basis.

Note, the purchase of Add-On packages may require Cisco to ship additional Cisco-owned Data Collection Tools to the Customer for installation at Customer's location.

2.1 Add-On Service: Additional ATA Sensor Base

The Additional ATA Sensor Base Add-On provides visibility to an additional segment of the Customer network. The Additional ATA Sensor Base will provide base level network data analysis capabilities supporting network segments with throughput of up to 1gbps.

ATA Add-On: Additional ATA Sensor Base:

- Deploy an additional instance of ATA Sensor Base that supports up to an additional 1gbps throughput.
- Each additional ATA Sensor Base requires connectivity to a DCAP device in order to capture and analyze data output from Sensor Base; it cannot not be purchased as a standalone add-on.
- ATA Sensor Base includes full packet capture capabilities and supports up to 20 TB of storage.

Sensor Base Deployment Requirements

- A publicly 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 Additional ATA Sensor Base in good working order and return the Sensor equipment in working condition to Cisco immediately upon expiration or termination of the Term.

Cisco Responsibilities:

- Procure and deliver additional ATA Sensor Base components and ship to Customer.
- Remotely assist the Customer with installation of components and validate accessibility to the Additional ATA Sensor Base from Cisco.
- Perform all required maintenance for hardware or software for the Additional ATA Sensor Base.

Customer Responsibilities:

- See Customer Responsibilities in Service On-boarding Process Description: Cisco Active Threat Analytics document.
- Provide the following for Additional ATA Sensor

2.2 Add-On Service: ATA Sensor Expanded Throughput

ATA Add-On Services: ATA Sensor Base Expanded Throughput:

For instances of each ATA Sensor Base (either included in core service offer or purchased as an Add-On)

- Increase throughput for an existing, single instance of ATA Sensor Base—available in increments of 3gbps of additional throughput up to 16 gbps total for the complete Sensor Base.
- Each ATA Sensor Base Expanded Throughput Add-On also provides an additional 40 TB of storage to the ATA Sensor Base deployment
- This may only be added to an existing ATA Sensor Base deployment either purchased as part of an ATA Core Service or as an ATA Sensor Base Add-On

Cisco Responsibilities:

- Procure and deliver Sensor Expansion Throughput components to increase throughput support of ATA Sensor Base.
- Remotely assist in installation of Sensor Expansion components.
- Perform all required maintenance for hardware or software for Sensor Expansion.
- Customer Responsibilities:
- See Customer Responsibilities in Service On-boarding Process Description: Cisco Active Threat Analytics document.
- Maintain the Sensor Expansion Throughput components in good working order and return the Sensor equipment in working condition to Cisco immediately upon expiration or termination of the Term.

2.3 Add-On Service: Storage Expansion

The Customer may purchase DCAP Storage Expansion (“Additional Storage”) to increase the DCAP storage capacity of Telemetry data, in increments of 400 TB.

Cisco Responsibilities:

- Procure and deliver additional equipment to provide Additional Storage.
- Assist in installation of Additional Storage components.
- Perform all required maintenance for hardware or software for Additional Storage.

Customer Responsibilities:

- See Customer Responsibilities in Service On-boarding Process Description: Cisco Active Threat Analytics document.
- Maintain the Additional Storage components in good working order and return the Additional Storage equipment in working condition to Cisco immediately upon expiration or termination of the Term.

2.4 Optional Add-On Service: Development Requests

Customer may request (in writing) development such as custom reports or ingestion of unsupported Customer specific telemetry (see Telemetry Support List). Note, the acceptance and implementation of custom requests are solely at the discretion of ATA Product Management. Approved requests will be documented in a change request or separate statement of work.

Cisco Responsibilities:

- Confirm and approve ability to deliver on Development Requests received from Customer.
- Collect and document requirements from Customer for each Development Request
- Implement and deliver requests as requested according to Development Request requirements document
- Provide a quote or proposed Change Request to document the fees for the Development Request.

Customer Responsibilities:

- Submit Development Requests, if desired
- Provide requirements, logs and data samples of the telemetry of Development Request to Cisco.
- Review and validate requirements documentation from Cisco prior to implementation of custom request.
- If requested or required, provide PO to Cisco for Development Request.

2.5 Optional Add-On Service: Additional Customer Portal User Licenses

The Customer may purchase additional Customer Portal user licenses above the number that come included with the service (standard offer is 15).

Cisco Responsibilities:

- Validate and set-up additional users for access to the Customer Portal.

Customer Responsibilities:

- Purchase the appropriate number of user licenses
- Provide user credentials to include to active user list

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 Cases and reports.

Customer Premises- The physical Customer location where the DCAP resides.

Data Collection and Analysis Pod or DCAP- The set of Cisco owned security networking and monitoring equipment that will reside on the Customer physical premise that is responsible for collecting, aggregating, and analyzing telemetry from the Sensor(s) and/or Customer applications and security devices.

Full Packet Capture: The process of extracting raw packet (header and payload) from a network and persisting all of that packet data to a disk for later retrieval. The Cisco ATA solution performs full packet capture using our ATA Sensor component, and our Investigators are trained to gather that packet data as evidence when processing cases generated by one or more of our detection toolsets.
Investigations Manager- A security engineer designated to Customer with deep incident and investigation skills responsible for responding to Customer inquiries and staying current with the Customer environment.

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

ISO-International Standards Organization

Metadata Extraction: Also known as “deep packet inspection”, inspecting network traffic (header and payload) to pull out summaries of layer 7, protocol-level traffic. A form of metadata extraction may include an extract URL accessed, URL parameters, and the response code from the website (HTTP 200, 302, etc.). This differs from netflow and other such technologies in that it sees the payload data and summarizes that in addition to the simple IP / port combinations used in the exchange.

NCE– Network Consulting Engineer

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 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).

Sensor Base- the set of Cisco owned security equipment that will reside on the Customer physical premise that is responsible for network data analysis by passively monitoring a defined segment of the Customer network. The Sensor Base will include full packet capture capabilities.

Sensor Expansion- ATA Add-On: ATA Sensor Expanded Throughput

SOC- Security Operations Center

Telemetry- Information and/or data that provides awareness and visibility into what is occurring on the network at any given time from networking devices, appliances, applications or servers in which the core function of the device is not to generate security alerts designed to detect unwanted or malicious activity from computer networks.

Raw Telemetry- Uncompressed Telemetry that consists of approximately 90% text data.

Term- Duration of ATA Service purchased by Customer