Service Description: Cisco Active Threat Analytics- Premier

This document describes the Cisco Active Threat Analytics security services ("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 (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/legal/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 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, 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.

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.

Cisco may collect data on Your use of the Services and threats or potential threats against your environment or network and the Services ("Telemetry Data") to maintain, improve, market or promote the Services. You acknowledge that Cisco may freely use the Telemetry Data as long as it is in a form that does not identify or imply Customer or any Customer end users. In any event, Cisco will comply at all times with applicable law related to Cisco's collection and use of all Telemetry Data and will use reasonable physical, technical, and procedural means to protect the Telemetry Data in accordance with Cisco's privacy policy found here:
http://www.cisco.com/c/en/us/about/trust-transparency-center/overview.html

Cisco ATA may include the following offerings as selected and detailed on the Purchase Order.

Cisco ATA core service offering may be purchased with any combination of ATA Add-On packages shown below.

Core Service Offerings: ATA Premier

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 (400,000 EPS peak) 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
- Threat Intelligence Analysis
- Metadata Extraction
- Advanced Analytics
- Up to 15 user licenses for Customer Portal access
- Investigations Manager
- Proactive Threat Hunting
- Incident Response Retainer
- Quarterly Business Review
- Monthly Technical Briefing

Add-On Packages to Core Service Offerings

The ATA Add-On Packages may only be purchased in addition to one of the Active Threat Analytics Core Service Offerings.

ATA Add-On: **Additional ATA Sensor Base**:

- Deploy an additional instance of ATA Sensor Base that supports up to 1gbps throughput.
- Each additional ATA Sensor Base requires connectivity to a DCAP deployment in order to capture and analyze data output from Sensor Base; 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.

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

- 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
- May only be added to an existing ATA Sensor Base deployment either purchased as part of an ATA Core Package or as an ATA Sensor Base Add-On

ATA Add-On: **Storage Expansion**:

- Expand DCAP or Sensor storage capacity allowing the capture of additional network forensic data—available in increments of 400 TB of raw Telemetry*.

ATA Add-On: **Development Requests**:

- Implement approved development requests with respect to the ATA solution, such as tailored reports or ingestion of additional device telemetry. These will be documented in the Quote or in a Change Request to this Service Description

ATA Add-On: **Additional User Licenses for Customer Portal Access:**

- Increase the number of user licenses for customer portal access beyond what is included with the Service.

Purchase of Add-On packages may require Cisco to ship additional Cisco-owned on-premise equipment to the Customer for installation at Customer's location.

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

1. Cisco Active Threat Analytics

Cisco Active Threat Analytics provides remote network security monitoring using network packet metadata and network behavior detection techniques 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 of the Services 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 and Service Delivery

1.1 Kickoff

1.1.1 Project Management

Cisco will assign a Project Manager (defined below) to act as a primary point of contact. Cisco will work with Customer to develop a comprehensive project plan, manage Cisco's people and processes to perform 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 Cisco point of contact ("CPOC") to whom all Cisco communications may be addressed and who has authority to act on all day to day aspects of the Services.
- Designate a backup, or secondary, contact if the primary contact is unavailable.
- 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 other scheduled implementation activities that may impact the Services 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 other 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).
- Perform any other tasks mutually agreed to in writing as a part of the project plan.

1.1.2 Kickoff

The Project Manager will contact the 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 ATA DCAP(s) and Base Sensor(s) ("on-premise equipment") included as part of the ATA service as indicated in the Purchase Order.

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
- Network diagrams and topology maps
- Enumeration of existing IP networks and IP schema
- Design review for physical and logical placement of ATA DCAP(s) and Base Sensor(s)
- 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 known 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 onsite equipment in order to comply with written and agreed to Customer requirements.

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 listing of contacts, including job descriptions, roles and responsibilities as required for Incident handling and escalation.
- 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(s) and Sensor(s), with installation by Customer at its site within eight (8) weeks of initial kickoff meeting; shipping details must be confirmed with the Customer prior to shipment.

The on-premise equipment 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 on-premise equipment shall remain with Cisco. Cisco expects that, at the time of removal, the on-premise equipment 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 any loss, damage, or theft of the on-premise equipment except to the extent caused by Cisco.

An asset tracking form will be provided to the Customer for sign off following shipment of on-premise equipment. 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.

The following may be provided as on-premise equipment

- VPN router
- Passive network tap/switch
- Information analysis engine(s)
- Data storage components

Cisco Responsibilities

- Ship all on-premise devices, servers, appliances and/or supporting applications.
- Assist the Customer with installation of on-premise equipment
- Confirm and assist with connectivity between DCAP(s) and Base Sensor(s)
- Establish connectivity between the Customer site and Cisco on-premise equipment
- Perform all required maintenance for hardware or software included with on-premise equipment.

Customer Responsibilities

- Installation of the on-premise equipment 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 on-premise equipment. 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 and/or Sensor:
    - 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.
    - Provision network requirements and conditions necessary to allow bidirectional communication between DCAP(s) and corresponding Sensor(s) as needed.
- Complete and return to Cisco the asset tracking form related to the on-premise equipment.
- Maintain the space, connectivity, and environmental conditions required for the on-premise equipment (e.g. power, cooling, etc.) and maintain the on-premise equipment in good working order. The Customer shall not, nor permit others to, rearrange, disconnect, remove, and attempt to repair, or otherwise tamper with the on-premise

equipment. 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 on-premise equipment.

- Return the on-premise equipment in working condition to Cisco immediately upon expiration or termination of the Term, reasonable wear and tear excepted.

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 (based on the size and complexity of the project) which may include the Internet, teleconference, email, video conference, and/or onsite.

Items covered in the Transition Out-brief may include:

- Discuss activation successes and challenges to Review incident escalation process
- Review ATA usage recommendations discovered during activation, if applicable

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. Monitoring will begin following Transition Out-brief; Telemetry Tuning (as described in section 1.4.3) may be provided at any point during Service Delivery.

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 1.4.3).

Upon automatic detection or manual submission of an Incident to the SOC, a case is created, which corresponds to the Incident. The ATA SOC is will help coordinate 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 in-scope Customer network infrastructure for Security Incidents as defined in the information gathering exercises of the activation phase.

Monitoring activities consist of monitoring and analyzing network based data and threat intelligence feeds in order to identify potential malicious Security Incidents.

Cisco Responsibilities:

- Create cases on the Customer Portal in response to a discovered or reported Security Incident.
- 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 significant data loss to the Customer
    - Medium: Adverse effect to Customer, potentially significant data loss, potential loss of service.
    - Low: Minimal adverse impact to Customer. No financial loss. Minimum or no data loss.
- 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.

1.4.2 Telemetry Tuning

The Customer may also send additional Telemetry, as mutually agreed by both Customer and Cisco, into the

DCAP to offer greater network visibility and context to active Security Incident investigations.

The amount of additional Telemetry is limited by the original DCAP telemetry thresholds as described in the Service offerings overview. As the amount of data ingested by the DCAP reaches the indicated storage thresholds, telemetry is rolled over with the oldest telemetry being purged to open storage for incoming telemetry. The Storage Add-On package, as described in Section 2.3, may be purchased if additional data retention is desired.

Telemetry from Customer specific specialized devices or applications may require the purchase of a Development Request Add-On prior to being ingested by DCAP.

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 recommendations to Customer on any changes required in order to enable the sending of Telemetry to the DCAP
- Validate receipt of approved 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

1.4.3 Customer Portal

The ATA Service includes a Customer Portal ("Portal") that will provide visibility into the delivery of the Service. During the initial setup phase, 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 via video, WebEx, or onsite as determined by Cisco.

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:

- 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. Instruction will be provided during the activation 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
- Manage and secure credential to access the Portal.

1.4.4 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 Security 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 Customer sites

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.

1.4.5 Proactive Threat Hunting

Cisco will perform activities involving seeking out malicious network 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 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 a Case if outcome of play displays evidence of a Security Incident as determined by Cisco.

Customer Responsibilities:

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

1.5 Incident Response Retainer

Cisco may provide any or all of the following Incident Response (IR) deliverables as part of the retainer: a) Readiness Assessment, b) IR Plan Development, c) Tabletop Exercises, d) Proactive Threat Hunting, and e) Emergency Incident Response—which may include Triage, Coordination, Investigation, Containment, and Remediation (See glossary for definitions of each listed deliverable) all up to a maximum of 160 hours of person hours.

Limitations: Given the variety of situations and issues that Cisco may encounter, incidents may require a variety of services to compliment this service. For example, incidents may require specialized tools to provide deeper visibility or access into the network. Any additional Services or tools that would require additional fees will be agreed to in writing via Change Order before Cisco proceeds.

Other limitations include:

- There is no guarantee that root-cause analysis will result in a root-cause being identified or confirmed for an incident
- Reasonable efforts will be made to provide conclusive findings and an issue resolution plan.
- IR services can provide insight into deficiencies of an IR strategy and a plan for resolving; however, executing the plan may require follow-on services that are not part of this Service.
- Work may occur after Standard Business Hours.
- Any hours not used during the term of the subscription retainer will be forfeited.

Each unit of Security IR Service includes:

- 160 hours—including two (2) trips with eight (8) hours of travel each

Cisco Responsibilities:

- Work with Customer to define how to leverage subscription hours.
- Provide emergency access to Incident Response services for the duration of the subscription.
- Provide an Incident Response resource within four (4) hours remotely via telephone.
- As requested, begin deployment of personnel to Customer location within 24 hours.
- Monthly status update specific to the Customer's environment.

Customer Responsibilities:

- Designate person(s) from within its organization to serve as a liaison to Cisco.
- Provide reasonable electronic and physical access to Customer's network and security devices to enable Cisco in providing support.
- Ensure access to Incident Response strategy information, to include processes and workflows, is made available to Cisco.
- Track and manage the retainer hours and the requested tasks to be performed.

1.6 Customer Reviews

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

1.6.1 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.

1.6.2 Monthly Technical Review- Delivery

Additional monthly technical review may be provided if requested by Customer. 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 Security 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 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 analytics capabilities supporting network segments with throughput of up to 1gbps.

Each Additional ATA Sensor Base deployment requires a DCAP deployed in order to capture and analyze data output from Sensor. The additional Sensor Base will include full packet capture capabilities and will support up to 20 TB of storage.

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 Section 1.2.2.
- Provide the following for Additional ATA Sensor Base deployment:
  - 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 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.

2.2 Add-On Package: ATA Sensor Expanded Throughput

For instances of each ATA Sensor Base (either included in core service offer or purchased as an Add-On as described in 2.1), the supported throughput of the monitored network segment may be increased in increments of 3gbps with purchase of the ATA Sensor Expanded Throughput Add-On ("Sensor Expansion"). The Sensor Expansion will also provide an additional 40 TB of storage to any Sensor.

Cisco Responsibilities:

- Procure and deliver Sensor Expansion components to increase throughput support of ATA Sensor Base.
- Assist in installation of Sensor Expansion components.
- Perform all required maintenance for hardware or software for Sensor Expansion.

Customer Responsibilities:

- See Customer Responsibilities in Section 1.2.2.
- Maintain the Sensor Expansion 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 Package: Storage Expansion

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

Cisco Responsibilities:

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

Customer Responsibilities:

- See Customer Responsibilities in Section 1.2.2
- Maintain the Additional Storage components in good working order and return the Sensor equipment in working condition to Cisco immediately upon expiration or termination of the Term.

2.4 Add-On Package: Development Requests

Customer may request one or more development efforts of the solution, such as custom reports or ingestion of additional, Customer specific device telemetry, which may be approved and delivered by Cisco. Cisco has categorized these Development Requests and their associated additional fees based on level of complexity required to implement the Request.

Category	Complexity	Items
Type 1	Low	• Onboarding of a single syslog telemetry feed from a Customer specific device • Single static automated report • Statistical anomaly detection for a single data source
Type 2	Medium	• Ingestion of Customer owned intelligence data (i.e. asset database) • Single enriched automated report
Type 3	High	• Statistical anomaly detection on correlated data (multiple data sources) • Advanced onboarding for a specialized device (i.e. requires a custom agent to extract data)

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:

- Provide requirements 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 Add-On Package: Additional Customer Portal User Licenses

The Customer may purchase additional Customer Portal user licenses above the fifteen that come included with the service.

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.

Advanced Analytics: Applying a variety of techniques proprietary and otherwise to capture window-based summaries of normal behavior through a variety of techniques, and alerting when behavior varies from those normal behaviors.

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 analytics 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.

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

Term- Duration of ATA Service purchased by Customer

Threat Intelligence Analysis: Cisco proprietary and third-party threat information used to provide situational and environment awareness of the latest threats. Cisco ATA leverages security knowledge from Cisco TALOS and Cisco Collective Security Intelligence to deliver global insights and context.

Incident Response (IR) Retainer Descriptions:

Readiness Assessment: Cisco evaluates a number of data points, including previous incidents, current roles and responsibilities, organizational design, patching operations, logging capabilities, and more to obtain a deep understanding of the environment.

IR Plan Development: Based on findings from the Readiness Assessment, work with customer to define runbooks for Incident Response.

Tabletop Exercises: Acting as an impartial 3rd party, to design, lead, and facilitate exercises to evaluate the effectiveness of the IR plan.

Proactive Threat Hunting: Work with customer to identify a use case (or set of cases) to test that may include finding evidence of compromise using lateral movement, web services compromise, embedded attacker, or privileged user access review approaches.

Emergency Incident Response:

Triage: Assessing the current situation to understand how best to initiate and design a response strategy.

Coordination: Tracking status, outstanding action items, and compiling updates as needed to ensure the incident is handled with care.

Investigation: Understanding the scope of the attack by deploying the necessary tools, reviewing log sources to analyze patterns and issues, performing needed forensics, and reverse engineering malware.

Containment: Quarantining and severing additional actions by the attacker.

Remediation: Removal of malware and other tools and artifacts left by the attackers