Service Activation Process
Cisco Active Threat Analytics- Premier

This document describes the Cisco Active Threat Analytics security services ("Services") Activation process ("Activation").

1. Cisco Active Threat Analytics Activation Process

Cisco Active Threat Analytics provides remote network security monitoring using network packet metadata and network detection techniques over the Term in order to 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 (covered in Service Description)

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 project plan, manage Cisco's people and processes to perform the Services, and monitor that the services are provided according to the plan and the Service Description.

Cisco Responsibilities

- Provide a single point of contact ("Project Manager" or "PM") for all issues relating to the Activation Services. 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 Services, 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.

1.2.1 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 personnel assigned to the Customer account typically facilitates the kickoff phase.

Cisco Responsibilities

- Conduct remote (e.g. 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.

2.1 **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) ("individually or collectively, Data Collection Tools") included as part of the ATA service as indicated in the Purchase Order.

2.1.1 Information Gathering

To provide the Services effectively, Cisco needs to fully understand the Customer environment and security workflows. Information gathering during the activation phase will be 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
- Business or technical 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 the Data Collection Tools
- 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 known corrective actions requiring action by the Customer.
- Review situations and locations in the network where full- packet capture may not be permissible.

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 Network Configuration Engineers 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 reasonably requested by Cisco.
- Work with Cisco to develop detailed design and configuration templates by providing information and feedback.

2.1.2 On-Premise Equipment Installation

Cisco will ship the DCAP(s) and Sensor(s), to Customer within eight (8) weeks of initial kickoff meeting; shipping details must be confirmed with the Customer prior to shipment. Customer will be responsible for installation of the Data Collection Tools, with assistance from Cisco

The Data Collection Tools 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. Customer will use reasonable security and care to protect the Data Collection Tools from theft, loss or damage. Customer shall reimburse Cisco for the costs of any loss, damage, theft of, or failure to return the Data Collection Tools, except to the extent caused by Cisco.

An asset tracking form will be provided to the Customer for sign off following shipment of Data Collection Tools. 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.

If included in the Order, a Cisco Network Consulting Engineer (NCE) may travel onsite to provide assistance with installation and testing of the Data Collection Tools. If ordered, the parties will mutually agree to a scheduled time for this assistance.

The following may be provided as Data Collection Tools

- 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.
- Provide Customer with technical requirements for Data Collection Tools (e.g. Power, rack-space, HVAC)
- Confirm and assist with connectivity between DCAP(s) and Base Sensor(s)
- Establish connectivity between the Customer site and Data Collection Tools
- Perform all required maintenance for hardware or software included with on-premise equipment.

Customer Responsibilities

- Installation of the Data Collection Tools 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, installation of software updates, 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 delay or prevent Services 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 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.
    - 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 Data Collection Tools. 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 Services, reasonable wear and tear excluded.

3.1 Transition

Cisco will deliver a transition out-briefing 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 activation challenges and 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 ATA Premiere Service Description document. 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 one (2) security representatives to participate in the transition out-briefing.