Cisco OT Anomaly Detection Assessment and POV Service

This document must be read in conjunction with the How Cisco Provides Services document, which is incorporated into this document by reference.

Cisco Cyber Vision is a cyber security tool with asset discovery and anomaly detection solution for the industrial control systems (ICS) environment. It gives operational technology (OT) professionals visibility into their industrial networks to help identify vulnerabilities, equipment integrity, and collaborate with IT to fight cyber-attacks.

The Service (SKU: ASF-ESG-CCV-OTANDA) described here utilizes Cisco Cyber Vision to perform a passive asset discovery (identifying assets and traffic pattern between them) within the Customer's ICS network. In addition, Cisco Cyber Vision will be used to demonstrate anomaly detection on the Customer ICS network through simulated threats.

Data collected with the asset discovery will be used to generate a vulnerability summary and a communication flow map between all assets. Sensors will be placed at a maximum of three locations in Customer's OT network at one site. Data will be analyzed for a maximum of 300 endpoints. For additional sensors and endpoints, please use the Sensor Add-On Service (SKU:ASF-ESG-CCV-SSR-M).

Cisco will review security architecture for OT environment recommended by ISA/IEC 62443 or NIST 800-82 standards and compare the key findings from Customer's site to this reference security architecture. The assessment will be run on either a control system test bench or on a control system in production as agreed upon between Cisco and the Customer.

Deliverables

Recommendation and executive summary.

- Upon completion of the assessment service Cisco will conduct a feedback meeting with all stakeholders as applicable and present the following as a finding it the final report:
    - Asset mapping findings.
    - Communications flow map.
    - Vulnerabilities findings.
    - Proof of real-time threat detection using Cisco Cyber Vision Anomaly detection features.
    - Next step recommendations to improve plant security.

Cisco Responsibilities

Conduct an analysis that includes a range of techniques intended to identify ICS assets, communication flows between ICS assets, and ICS vulnerabilities. Cisco will apply the following core strategies in performing the assessment:

- Alignment call and Data Gathering
    - Call with the primary sponsor from the Customer.

- Share the process and overall project plan.
- Plan for the formal Kick-off Meeting and share the expected participants for the Kick-off.
- Share outline and expected participants.
- Provide the list of documents required (checklist).
- Provide initial information gathering questions.

- Kickoff
  - Conduct remote kick-off call.
  - Review project plan.
  - Review expectations and success criteria.
  - Work with client PM to define stakeholders to participate in workshop.
  - Decide the dates for the onsite workshop.
- Initial Analysis
  - Verification with the Customer of their assets, OT network, architecture and protocols.
  - Acknowledgment and validation of the assessment perimeter.
  - Agree upon the number of sensors to be used and the sensor placement location.
  - Determine whether the assessment service will be run on a control system test bench or a control system in production.
- Onsite Session
  - Validate Cisco's understanding of OT environment.
  - Working session to create high-level ICS network map.
  - If applicable, install sensors OR receive a static network capture (PCAP) from Customer.
  - If applicable, install and start Cyber Vision Center software.
  - As applicable, use Cyber Vision Center to discover the OT network in scope, create an inventory of connected assets, group assets per logical topology of the ICS network in alignment with IEC 62443 guidelines, and highlight communications between the assets.
  - Demonstrate anomaly detection by simulating ICS threat.
- Offsite Analysis
  - If applicable, review data collected by Cyber Vision software.
  - Evaluate asset maps, vulnerabilities, traffic patterns.

Customer Responsibilities

- Provide input, support and resources to successfully let Cisco complete the Service using Cisco Cyber Vision solution:
- Kickoff: Provide Cisco with the following documents
  - Industrial network architecture.
  - Physical and logical network topology diagrams.
  - Relevant industrial equipment list.
  - Applicable Industrial protocols.
  - Site and section of the plant to be assessed.
  - PCAP files if applicable.
  - Validation of the assessment perimeter.
  - General SEIM/SOC strategy if applicable.
- Onsite Sessions

  - Perform switch configuration or bridge configuration for sensors deployment (as needed).
  - Enable traffic generation on the control network using engineering workstation to accelerate the network recognition.
  - The control engineering staff will be required to simulate operations (maintenance, for example) to generate network traffic at different operating modes to accelerate the enrichment of the graphical representation of the control system.
  - Provide a static network capture (PCAP) (as needed)
- Data gathering could require configuring the network switches in “Port Mirroring" mode, if not already so configured, or to place the Cisco Cyber Vision sensor “in line” with network traffic if the switches do not support port mirroring.
- Review and approve simulated threat scenario for testing.
- Allow Cisco equipment and tools to be placed on and used against the target environment.
- Provide any hardware, software or remote access required for Cisco to do the deployment.
- Provide valid and applicable contract numbers, component level serial numbers or other applicable entitlement information as requested by Cisco or the applicable Solution Technology Partner for problems and issues reported to Cisco. Cisco may also require Customer provide additional information in the form of location of solution components, city location details and Postal code information.
- For specialized knowledge sessions, the Customer is responsible for its own costs incurred for a session delivered at a Cisco office. If the customer requests a designated, remotely delivered session to be delivered onsite at a customer site, the customer is responsible for Cisco’s costs to deliver the session onsite.