<< Cisco OT Asset Discovery Assessment Service >>
Service d'évaluation de la détection des ressources des TO de Cisco

Ce document doit être lu conjointement avec le document qui décrit comment Cisco fournit ses services (How Cisco Provides Services) et qui est intégré par renvoi au présent document.

Cisco Cyber Vision est un outil de cybersécurité utilisant la détection des ressources et des anomalies pour les environnements de systèmes de contrôle industriel (SCI). Il permet aux professionnels des technologies opérationnelles (TO) de consulter leurs réseaux industriels pour déterminer les vulnérabilités, surveiller l'intégrité des équipements et collaborer avec les TI pour combattre les attaques informatiques.

Le service (UGS : ASF-ESG-CCV-OTADA) décrit aux présentes utilise Cisco Cyber Vision pour effectuer une analyse passive des ressources (en déterminant les ressources et le schéma de trafic entre elles) au sein du réseau des SCI du Client.

Les données collectées à l'aide de la détection des ressources seront utilisées pour faire un récapitulatif des vulnérabilités et une cartographie des flux de communication entre toutes les ressources. Des capteurs pourront être placés jusqu'à un maximum de trois emplacements sur le réseau des TO du Client pour un même site. Les données d'un maximum de 300 points d'extrémité pourront être analysées. Pour des capteurs et des points d'extrémité supplémentaires, veuillez utiliser le service d'ajout de capteurs (UGS : ASF-ESG-CCV-SSR-M).

Cisco examinera l'architecture de sécurité des environnements de TO recommandée par les normes ISA/IEC 62443 ou NIST 800-82 et comparera les principales observations obtenues au site du Client à cette architecture de sécurité de référence. L'évaluation sera effectuée soit sur un banc d'essai des systèmes de contrôle, soit sur les systèmes de contrôle en production, selon ce qui sera convenu entre Cisco et le Client.

Livrables

Sommaire et recommandations

- À l'issue du service, Cisco organisera une réunion avec toutes les parties prenantes, selon les besoins, afin de partager les résultats et présentera les conclusions suivantes dans un rapport final :
    - Résultats de la mise en correspondance des ressources.
    - Cartographie des flux de communication.
    - Conclusions sur les vulnérabilités.
    - Recommandations pour les prochaines étapes en vue d'améliorer la sécurité des installations.

Responsabilités de Cisco

Procéder à une analyse qui comprendra une série de mesures destinées à déterminer les ressources des SCI, les flux de communication entre ces ressources et les vulnérabilités des SCI. Pour réaliser cette évaluation, Cisco appliquera les stratégies principales suivantes :

- Appel d'alignement et collecte de données
    - Communiquer par appel avec le responsable principal du Client.
    - Fournir le processus et le plan de projet global.
    - Planifier la réunion de lancement formelle et déterminer les participants attendus.
    - Fournir le plan et la liste des participants attendus.
    - Fournir la liste des documents requis (liste de contrôle).
    - Fournir une liste de questions initiales relativement à la collecte d'informations.
- Réunion de lancement
    - Organiser un appel pour la réunion de lancement.
    - Présenter le plan du projet.
    - Passer en revue les critères de réussite et les attentes.
    - Collaborer avec le gestionnaire de programme du Client pour déterminer les parties prenantes devant participer aux ateliers.
    - Déterminer les dates des ateliers sur les lieux.
- Analyse préliminaire
    - Effectuer la vérification avec le Client de ses ressources, du réseau, de l'architecture et des protocoles de TO.
    - Valider et confirmer la portée de l'évaluation.
    - Déterminer avec le Client le nombre de capteurs à utiliser et leur emplacement.
    - Déterminer si le service d'évaluation doit être fourni sur un banc d'essai des systèmes de contrôle ou sur les systèmes de contrôle en production.
- Séance sur les lieux :
    - Valider la compréhension de Cisco de l'environnement de TO du Client obtenue après examen des documents fournis par ce dernier.
    - Effectuer une séance de travail pour créer une carte globale du réseau des SCI.
    - Le cas échéant, installer des capteurs OU obtenir une capture de réseau statique (PCAP) de la part du Client.
    - Le cas échéant, installer et lancer le logiciel Cyber Cision Center.
    - Le cas échéant, utiliser le logiciel Cyber Vision Center pour analyser le réseau des TO inclus dans la portée, créer un inventaire des ressources connectées, regrouper les ressources par topologie logique du réseau des SCI en conformité avec les directives IEC 62443 et mettre en évidence les communications entre les ressources.
- Analyse hors site
    - Le cas échéant, examiner les données collectées par le logiciel Cyber Vision.
    - Évaluer la cartographie des ressources, les vulnérabilités et les schémas de trafic.

Responsabilités du Client

Fournir les renseignements, l'assistance et les ressources nécessaires pour permettre à Cisco de fournir le service à l'aide de la solution Cisco Cyber Vision.

- Réunion de lancement. Fournir à Cisco les documents suivants :
    - architecture du réseau industriel;
    - diagrammes de topologie physique et logique du réseau;
    - liste des équipements industriels pertinents;
    - protocoles industriels applicables;
    - sites et sections des installations à évaluer;
    - fichiers de capture du réseau (PCAP), le cas échéant;
    - validation de la portée de l'évaluation;
    - politique générale concernant les opérations de sécurité et la gestion des informations et des événements relatifs à la sécurité (SOC/SEIM), le cas échéant.
- Séances sur les lieux
    - Effectuer la configuration des commutateurs ou la configuration des ponts pour le déploiement de capteurs (si nécessaire).
    - Permettre la génération de trafic sur le réseau de contrôle en utilisant un poste de travail d'ingénierie pour accélérer la reconnaissance du réseau.
    - Le personnel de l'ingénierie de contrôle sera sollicité pour simuler des opérations (de maintenance, par exemple) afin de générer du trafic réseau dans différents modes opérationnels pour accélérer l'enrichissement de la représentation graphique du système de contrôle.
    - Fournir une capture de réseau statique (PCAP) (si nécessaire)

- La collecte de données pourrait nécessiter de configurer les commutateurs du réseau en mode « miroir de ports », si ce n'est déjà fait, ou de placer des capteurs Cisco Cyber Vision « en ligne » avec le trafic réseau si les commutateurs ne prennent pas en charge la mise en miroir de ports.
- Autoriser l'installation et l'utilisation des équipements et outils de Cisco dans l'environnement cible.
- Fournir tout le matériel, les logiciels et les accès à distance requis par Cisco pour le déploiement.
- Fournir des numéros de contrat valides et applicables, les numéros de série des composants ou tout autre renseignement d'admissibilité applicable tel que requis par Cisco ou le partenaire technologique de solution concernant les problèmes signalés à Cisco. Cisco peut également demander au Client de fournir des données supplémentaires, notamment le lieu d'utilisation des composants de la solution, des renseignements sur la ville, ainsi que le code postal.
- Pour les séances de connaissances spécialisées, le Client est responsable des coûts qu'il engage à l'occasion d'une séance donnée dans un bureau de Cisco. Si le Client demande qu'une séance à distance particulière soit donnée sur le site du Client, il est responsable des coûts que Cisco engagera pour ce faire.