CYBERSECURITY

OT Asset Discovery & Analysis

Cartographiez aisément le fonctionnement de votre réseau industriel

Le numérique permet la mise en place de processus métier simplifiés. À cet effet, les systèmes industriels de production et de commande, qui restent aujourd'hui encore largement autonomes, sont de plus de plus interconnectés tout au long de la chaîne d'approvisionnement. Les systèmes bénéficient d'une intercommunication directe. Mais êtes-vous bien certain que seuls les systèmes autorisés se « parlent » ?

Fort de notre propre expérience terrain, Airbus CyberSecurity a constaté qu'une production efficace et un processus innovant ne peuvent prospérer que dans un contexte interconnecté et sécurisé.

Parvenir à une vision d'ensemble de tous les composants OT (y compris les systèmes ICS) et des risques corrélés constitue le fondement de la sécurisation de l'environnement des OT ou des ICS.

Notre service OT Asset Discovery & Analysis élabore pour vous cette vue globale, et vous livre ses recommandations en matière d'optimisation de la sécurité de vos systèmes OT.

Nous vous proposons :

- Analyse de l'environnement OT, avec inventaire des composants existants et représentation des flux de communication
- Identification et évaluation des failles de sécurité potentielles et des anomalies
- Recommandations pour l'optimisation de la sécurité

Contenu de la prestation :

- Capture de la communication interne des réseaux industriels, sur des points stratégiques
- Analyse par des experts, avec l'appui de logiciels spécialisés
- Rédaction d'un rapport incluant des recommandations d'actions

AIRBUS

OT Asset Discovery & Analysis : plus de détails

Lancement

- Définition exacte des éléments à l'étude
- Détermination des préalables organisationnels et techniques pour l'enregistrement sur le réseau
- Planification de la période de capture

Début de l'enregistrement

- Installation du système de capture, mis à disposition par Airbus CyberSecurity, sur un point stratégique du réseau

Capture

- Capture passif et automatisé de la communication interne du réseau sur la période définie (entre 24 heures et une semaine ouvrée)

Transmission des données

- Désinstallation du système de capture
- Récupération des données par Airbus CyberSecurity
- Clarification des premiers éléments à traiter et constat sur site

Évaluation et rapport final

- Analyse des données par les experts d'Airbus CyberSecurity
- Extraction des informations de version des systèmes et comparaison avec des bases de données sur les failles de sécurité
- Étude des protocoles réseaux et visualisation des circuits de communication
- Rédaction d'un rapport final incluant les informations suivantes, en complément des recommandations d'actions

Présentation des résultats

- Présentation et soutenance du rapport final auprès du donneur d'ordre

Vue d'ensemble de l'évaluation dans le cadre de l'Asset Discovery & Analysis

AIRBUS

Airbus CyberSecurity
Metapole 1, boulevard Jean Moulin / CS 40001 / 78996 Elancourt Cedex / France
Willy-Messerschmitt-Str. 1 / 82024 Taufkirchen / Germany
Quadrant House / Celtic Springs / Coedkernew / South Wales NP10 8FZ / United Kingdom
Etihad Towers T3 / Corniche Road, 19th floor / P.O.Box: 72186 / Abu Dhabi / United Arab Emirates
www.airbus-cyber-security.com / contact.cybersecurity@airbus.com