Industrial Security avec Palo Alto Networks

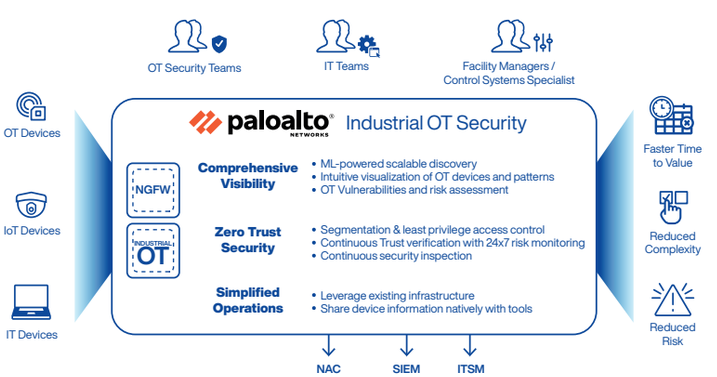
L'utilisation de technologies réseau avancées s'étend progressivement à de nombreux domaines de l'entreprise. Les systèmes industriels et de production qui étaient auparavant isolés ou déconnectés ont de plus en plus besoin d'une connectivité interne et/ou externe au réseau de l'entreprise et à Internet pour surveiller et contrôler les processus critiques et les optimiser en permanence à l'aide de l'intelligence artificielle.

Conformité des exigences air gap

Pour pouvoir se conformer aux réglementations sectorielles et aux meilleures pratiques, il faut des solutions qui prennent en charge la séparation «logique» des réseaux OT et permettent une communication sécurisée avec les services externes. Les données en temps réel pour la surveillance et le contrôle dans les réseaux OT nécessitent un streaming en temps réel des données télémétriques (de sécurité). Palo Alto Networks propose une architecture de streaming de données de télémétrie sécurisée, composée de pare-feux de segmentation (pare-feu de couche 7), d'une passerelle de télémétrie et d'un stockage de données dans le cloud (data lake) disponible en Suisse.

Une visibilité complète

La détection et l'évaluation continues de tous les systèmes cyberphysiques connectés assurent une visibilité complète. Pour ce faire, Industrial OT Security combine le machine learning (ML) avec la technologie App ID et Device ID ainsi que des données de télémétrie crowdsourcées pour établir rapidement un profil de tous les appareils et équipements OT, IT et IoT. Sont notamment concernés les appareils OT sensibles, tels que les systèmes de contrôle distribués (DCS), les systèmes de contrôle industriels (ICS), les interfaces homme-machine (HMI), les contrôleurs logiques programmables (PLC), les unités de terminaux distants (RTU), les systèmes de contrôle et d'acquisition de données (SCADA), les historians et jump server. Les appareils IoT courants tels que les caméras de sécurité, les imprimantes et les systèmes HVAC sont également reconnus et protégés. La technologie basée sur l'IA/ML reconnaît les appareils de manière passive (non intrusive) et les classe en fonction de plus de 80 attributs uniques (type, fabricant, modèle, système d'exploitation, version d'exploitation, niveau de patch, adresse MAC, protocole OT, etc.)



Segmentation et contrôle d'accès avec le moins de droits possible

Industrial OT Security permet de séparer les réseaux OT de l'informatique de l'entreprise et d'Internet et de sécuriser les installations OT grâce à des politiques de zonage et de segmentation fines basées sur les installations OT, les protocoles et le contexte de risque. Ces fonctions empêchent les systèmes infectés ou infiltrés de s'étendre à d'autres zones de l'installation, respectivement de les perturber (lateral movement, selon les normes de segmentation CEI-62443).

Pour ce faire, la solution fournit des recommandations automatisées pour les politiques d'accès avec le principe de moindre privilège (least privilege access), basées sur des informations contextuelles et des profils de comportement. En outre, les politiques de sécurité automatisées éliminent la création manuelle de politiques sujette à des erreurs et chronophage, et peuvent être facilement appliquées à des installations ayant le même profil. Avec les pare-feux de couche 7 (physiques ou virtuels) de Palo Alto Networks, ces politiques peuvent être facilement appliquées à l'aide de Device ID. Sinon, elles peuvent être appliquées en les intégrant dans une solution basée sur le contrôle d'accès réseau (NAC).

Contrôle de sécurité continu

Industrial OT Security empêche les attaques zero-day grâce à l'apprentissage en profondeur en ligne, à la détection d'anomalies dans le comportement des installations et à l'évaluation continue des processus ICS afin de garantir l'intégrité des processus et la sécurité des systèmes cyberphysiques. Complétées par une prévention avancée des menaces (advanced threat Prevention [ATP]), les attaques connues et inconnues peuvent être détectées et contrées avec succès dans les installations et les processus OT critiques.

Industrial OT Security de Palo Alto Networks: les points forts

- Visibilité des ressources OT, aperçu des risques et des comportements
- Détection et défense avancées contre les menaces sur les réseaux OT déconnectés (air gap environment)
- Recommandations et mise en œuvre de politiques basées sur l'ID des appareils et des applications pour la microsegmentation des réseaux OT avec le moins de privilèges (least privilege microsegmentation).
- Passerelles de télémétrie renforcées pour la sécurisation des flux de données des réseaux OT
- Transmission sécurisée et cryptée des données de télémétrie des réseaux OT vers le cloud via une connexion sortante mTLS (authentification mutuelle basée sur un certificat X.509)
- Environnements cloud certifiés et centres de données physiques utilisés par Industrial OT Security pour le traitement et le stockage de la télémétrie réseau (SOC 2 Type II Plus, ISO 27001/27701, BSI C5)

BOLL
IT Security Distribution

BOLL Engineering SA

En Budron H15 | 1052 Le Mont-sur-Lausanne
Tél. 021 533 01 60
vente@boll.ch | www.boll.ch