LISTE

# Comment sécuriser l'OT ?

## La protection contre les menaces avancées nécessite l'automatisation et l'intégration de toutes les solutions de sécurité

Les conséquences d'une intrusion réussie dans l'OT sont graves. Dans les entreprises qui s'appuient sur des systèmes de production opérationnels et industriels, le Responsable de la sécurité des systèmes d'information (RSSI) doit s'assurer que les équipes de sécurité disposent de l'architecture et des solutions appropriées.

### 7 considérations pour le RSSI chargé de la sécurisation de l'OT

APIXIT et Fortinet aide les RSSI à réduire la complexité de la sécurité des réseaux et les coûts liés à l'ajout continu de produits plus isolés pour couvrir les nouvelles menaces ou expositions aux risques.

### ☑ Intégrer la sécurité informatique et celle de l'OT

La sécurisation des réseaux informatiques et de l'OT contre les menaces avancées exige du RSSI une approche multidimensionnelle. Cela ne signifie pas que les solutions de sécurité doivent fonctionner de manière indépendante. Au contraire, toutes les solutions protégeant les réseaux informatiques et l'OT doivent être étroitement intégrées et capables de partager les informations en temps réel. Cela permet de détecter une menace dans un domaine et de déclencher une réponse coordonnée dans toute l'infrastructure de sécurité de l'entreprise.

La Fortinet Security Fabric offre ce type d'infrastructure. Ensemble, les solutions étroitement intégrées de la Security Fabric fournissent une protection bien orchestrée qui atteint tous les aspects de l'OT et des réseaux informatiques des entreprises. Elles offrent également une large visibilité sur l'ensemble de la surface d'attaque numérique, tout en facilitant les flux de travail automatisés pour augmenter l'efficacité et la rapidité des opérations et des réponses.

### ☑ Contrôle efficace de l'accès aux ressources OT

Les entreprises ont de plus en plus recours à l'externalisation ou à d'autres changements de processus qui nécessitent une connectivité réseau pour les clients, les entrepreneurs et les fournisseurs. Dans de nombreux cas, des capacités d'accès sans fil et à distance sont nécessaires, tant pour les employés que pour les visiteurs qui ont besoin d'utiliser le réseau. De tels environnements exigent une attention particulière au contrôle d'accès, afin d'empêcher des connexions non autorisées aux ressources du réseau.

Les organisations peuvent s'appuyer sur la Fortinet Security Fabric pour offrir des solutions sophistiquées de gestion et de sensibilisation à l'identité des utilisateurs. Par exemple, FortiAuthenticator facilite les politiques d'accès basées sur les rôles et l'authentification multifactorielle pour tous les utilisateurs de systèmes informatiques et OT.

FortiAP et FortiSwitch fournissent respectivement un accès sans fil sécurisé et une commutation réseau. Ils sont tous deux conçus pour les environnements de production opérationnelle et industrielle; ils sont durcis, permettant un déploiement dans les conditions extrêmes des sites OT sur le terrain et des environnements de fabrication et d'entreposage.

### ☑ Utilisation de la segmentation de réseau pour contrôler les mouvements latéraux entre l'IT et l'OT

Placés entre les segments de réseau de l'OT et de l'IT, les pare-feux nouvelle génération (NGFW) peuvent contrôler les flux de trafic et recréer artificiellement le « fossé » qui permettait autrefois de séparer les ressources OT de nombreuses entreprises, des systèmes informatiques. Les pare-feux nouvelle génération FortiGate sont particulièrement performants dans cet environnement. Leur établissement de liste blanche adaptée aux applications OT peut être configuré pour n'autoriser que des protocoles spécifiques OT sur le réseau OT de l'entreprise et refuser tout autre trafic.

Le débit est une autre considération essentielle dans le choix des pare-feux de nouvelle génération FortiGate pour la segmentation du réseau ou la sécurité périphérique. Avec certains pare-feux, l'activation de fonctions de sécurité avancées réduit considérablement le débit du pare-feu. En revanche, les pare-feux nouvelle génération FortiGate sont spécifiquement conçus pour minimiser la latence, même lorsque le système de prévention des intrusions (IPS) et d'autres fonctionnalités avancées sont activés.

## ☑Veiller à l'intégration des renseignements sur les menaces

La protection contre les nouvelles souches de logiciels malveillants nécessite la diffusion en temps quasi réel des renseignements sur les menaces locales et mondiales sur le réseau. Les solutions de la Fortinet Security Fabric intègrent des flux de données basés sur l'intelligence artificielle (IA) provenant des services de renseignement sur les menaces de FortiGuard Labs. Avec l'une des plus grandes équipes d'experts en sécurité du secteur, FortiGuard Labs étudie en permanence le paysage des menaces pour identifier les menaces zero-day, non seulement pour les systèmes informatiques, mais aussi pour les protocoles OT les plus courants et les vulnérabilités des applications OT.

## ☑Recherche de technologies de Sandboxing et de tromperie compatibles avec l'OT

Aucun service de renseignement sur les menaces ne peut identifier toutes les menaces avant qu'elles n'atteignent le réseau de l'entreprise. Les organisations doivent également déployer des solutions conçues pour empêcher les menaces inconnues d'atteindre leurs systèmes OT. Dans la Fortinet Security Fabric, FortiSandbox reçoit les paquets suspects provenant d'autres composants de la Security Fabric et teste le code dans un environnement de quarantaine. Dans des environnements opérationnels, FortiSandbox peut émuler les plates-formes OT en ouvrant des fichiers qui sont uniques à des systèmes d'exploitation particuliers de l'OT.

Les technologies de tromperie sont également un élément important d'une infrastructure de sécurité globale. FortiDeceptor déploie des machines virtuelles (VM) ou des applications de leurre spécifiques à l'OT, dans le but d'inciter les attaquants à se dévoiler. Comme les menaces avancées sont en constante évolution, les RSSI doivent s'attaquer au problème des menaces zero-day en provenance de plusieurs directions simultanément.

## ☑Déploiement d'une protection contre les menaces d'initiés

Les attaques malveillantes et intentionnelles des initiés constituent une menace pour les environnements informatiques et l'OT. En outre, des initiés bien intentionnés peuvent involontairement offrir aux attaquants l'accès au réseau ou aux données. La solution d'analyse du comportement des utilisateurs et des entités (UEBA) de FortiInsight surveille en permanence les utilisateurs et les points d'extrémité. Elle exploite l'apprentissage automatique et l'analyse pour identifier automatiquement les comptes compromis lorsque les comportements sont suspects, non conformes ou autrement anormaux.

## ☑Priorité à une surveillance efficace des infrastructures de sécurité

Les équipes de sécurité doivent être capables de gérer de manière centralisée les politiques basées sur les normes de sécurité d'organisations telles que le National Institute of Standards and Technology (NIST) et le Center for Internet Security (CIS), et de les déployer efficacement dans l'ensemble des solutions de sécurité. Elles doivent également avoir accès à des rapports centralisés et automatisés sur les menaces détectées et sur la réponse des solutions de sécurité. Le Fortinet Security Fabric Management Center comprend une console unique de gestion, de reporting et d'analyse avec des flux de travail automatisés pour offrir une visibilité de bout en bout dans le paysage de la sécurité, ainsi que la collecte de données de sécurité OT nécessaire pour les audits de l'industrie et du gouvernement.

## Conclusion

Des brèches sur le réseau OT peuvent avoir des conséquences catastrophiques. Les RSSI des secteurs qui utilisent l'OT doivent déployer des solutions de sécurité qui intègrent les meilleures approches de détection avancée des menaces, et qui s'intègrent étroitement pour améliorer la visibilité et la réponse automatisée aux menaces.

La Fortinet Security Fabric répond à ces besoins, en facilitant une intégration étroite entre les solutions de Fortinet et celles de tiers. Soutenue par les recommandations des principaux organismes de test tels que NSS Labs, l'intégration de Security Fabric fait des meilleures solutions Fortinet le choix évident pour les organisations OT.

## A Propos d'APIXIT

Depuis plus de 30 ans, APIXIT éclaire la Cybersécurité, les Infrastructures et le Cloud des ETI et des Grands Comptes. En matière de protection du Système d'Information, notre proposition de valeur s'articule autour d'une démarche de Sécurité Opérationnelle alliant solutions technologiques d'éditeurs leaders du marché et offre de services à forte valeur ajoutée. APIXIT vous accompagne sur l'ensemble du cycle de vie de vos solutions au travers de prestations d'audit et conseil, d'intégration, de MCO et MCS ou encore de Services Managés et de services SOC. Grâce à leur sens de l'écoute et du service, nos équipes d'experts s'engagent à répondre avec agilité aux enjeux de transformation digitale de nos clients.

FORTINET®

www.fortinet.fr



janvier 5, 2023 5:23 PM

448524-0-1-FR