PRÉSENTATION DE LA SOLUTION

Transparence totale et contrôle centralisé dans les environnements OT

Synthèse

La convergence entre les technologies de l'information (IT) et les technologies d'exploitation (OT) étend la surface d'attaque OT, plaçant ainsi les analystes SOC sous une pression énorme pour garantir la sécurité, la disponibilité et la sûreté. Les technologies d'exploitation nécessitent désormais une infrastructure de sécurité intégrée pour assurer la visibilité, le contrôle et la connaissance du contexte des appareils, ainsi que de leur exposition à un éventail toujours plus large de menaces provenant d'Internet. Fortinet Security Fabric fournit une architecture de sécurité de bout en bout pour les environnements OT. Cette solution offre une protection intégrée et automatisée grâce à la segmentation, au contrôle d'accès réseau (NAC) et à la gestion des informations et des événements de sécurité (SIEM).

Près des trois quarts des entreprises OT ont subi une intrusion de logiciels malveillants au cours des 12 derniers mois, avec des impacts sur la productivité, les revenus, la confiance dans la marque, la propriété intellectuelle et la sécurité physique.[1]

Selon un rapport, 78% des entreprises OT n'ont qu'une visibilité centralisée partielle des solutions de cybersécurité déployées dans leurs environnements.[4]

Nécessité d'une plus grande visibilité, d'un contrôle accru et d'une meilleure connaissance du contexte

La surface d'attaque OT s'étend rapidement. Les systèmes sensibles des infrastructures critiques et des environnements industriels sont confrontés à de nouveaux risques en raison des changements infrastructurels, tels que le remplacement des connexions OT en série par des connexions numériques et la croissance rapide du nombre de systèmes et d'appareils connectés à Internet.

Malgré tous ces défis, les analystes SOC doivent garantir la disponibilité et la sécurité opérationnelles à tout moment. Mais les environnements OT ont été historiquement négligés en matière de cybersécurité. En effet, jusqu'à récemment, un « air gap » (séparation complète du réseau informatique) maintenait ces systèmes à l'écart des menaces. Aujourd'hui, cependant, les logiciels malveillants peuvent attaquer les systèmes OT par le biais de connexions informatiques, comme les campagnes de phishing par e-mail.[2,3]

La priorité accordée à la sécurité des technologies d'exploitation a fait l'objet d'une grande attention récemment. Mais la transposition des stratégies de sécurité informatique traditionnelles aux technologies d'exploitation n'est pas appropriée pour les systèmes sensibles, souvent hérités, de ces environnements. Pour garantir des opérations sûres et fonctionnelles, les entreprises ont besoin de trois fonctionnalités de cybersécurité essentielles :

La visibilité

La sécurisation des environnements OT modernes commence par l'établissement d'une visibilité continue de chaque actif connecté au réseau, qu'il soit câblé ou sans fil. La sécurité doit assurer le suivi de tous les appareils connectés dans l'ensemble de l'entreprise lorsqu'ils rejoignent et quittent le réseau ou se déplacent d'un site à un autre.

Le contrôle

Les entreprises doivent être en mesure d'appliquer et de faire respecter des politiques d'accès basées sur les personnes et les objets connectés afin de sécuriser les opérations OT contre les menaces informatiques potentielles. Des contrôles dynamiques, basés sur les rôles, peuvent regrouper les applications, relier les données et limiter l'accès à des groupes spécifiques afin de renforcer les défenses des technologies d'exploitation. Ce type de segmentation basée sur l'intention fournit un contrôle précis qui ajuste l'accès en fonction de l'évaluation continue de la confiance des appareils et des utilisateurs.

La connaissance de la situation

Lorsqu'un appareil individuel dans un environnement OT est attaqué, les entreprises ont besoin d'alertes instantanées et d'informations contextuelles sur les menaces afin de comprendre rapidement quelles mesures prendre et où chercher. La sécurité des technologies d'exploitation nécessite une corrélation des événements et une gestion des risques unifiées pour faciliter l'analyse, automatiser les réponses et accélérer les mesures correctives, surtout compte tenu du manque sérieux de ressources en personnel dans la plupart des entreprises.

Plus de la moitié (53%) des entreprises ne disposent pas d'une segmentation interne du réseau pour limiter la propagation des menaces au sein des réseaux OT.[5]

La pénurie mondiale de professionnels de la cybersécurité a atteint près de 3 millions de postes non pourvus.[6]

Une architecture de sécurité intégrée pour les technologies d'exploitation

La **Fortinet Security Fabric** connecte différentes solutions de sécurité déployées dans un environnement OT en un écosystème de sécurité coordonné. Ce type d'architecture de sécurité intégrée coordonne les cyberdéfenses dans l'ensemble de l'entreprise pour permettre une visibilité, un contrôle et une connaissance de la situation de bout en bout afin de protéger les environnements OT d'aujourd'hui. Si un appareil connecté présente un comportement suspect, la Security Fabric dispose à la fois de la couverture et des fonctionnalités nécessaires pour détecter et résoudre rapidement le problème.

Dans les environnements OT, la Security Fabric inclut des solutions Fortinet, telles que les pare-feux de nouvelle génération (NGFW) **FortiGate** renforcés, les commutateurs **FortiSwitch** sécurisés (câblés), les points d'accès **FortiAP** (sans fil), **FortiClient** garantissant la protection des terminaux et **FortiManager** offrant une visibilité transparente et une gestion centralisée de tous les appareils déployés dans l'entreprise.

La Fortinet Security Fabric permet également de contrôler l'accès aux systèmes critiques sans en perturber le fonctionnement. Traditionnellement, les contrôles d'accès supposaient des valeurs de confiance immuables pour les utilisateurs, les appareils et les applications. Mais en réalité, la confiance des utilisateurs et des appareils peut fluctuer en raison de changements normaux dans les opérations de l'entreprise ou à la suite de nouvelles menaces. La **segmentation basée sur l'intention** associe le contrôle d'accès à des niveaux de confiance continuellement mis à jour en fonction d'informations acquises de sources internes et externes.

Plus précisément, la segmentation basée sur l'intention de Fortinet assure un contrôle d'accès dynamique et granulaire qui surveille continuellement le niveau de confiance de l'utilisateur et adapte les politiques de sécurité en conséquence. Les actifs informatiques critiques sont isolés pour assurer une détection et une prévention rapides des menaces grâce à l'analyse et à l'automatisation. S'appuyant sur les **pare-feux NGFW FortiGate** physiques et virtuels, la segmentation basée sur l'intention permet un contrôle de bout en bout du réseau OT pour le trafic est-ouest et nord-sud.

Mais la sécurité ne sert à rien dans les environnements OT si elle interrompt le fonctionnement des systèmes critiques de quelque manière que ce soit. Au cours de son histoire, Fortinet a prouvé son expertise en matière de technologies d'exploitation en investissant dans une architecture de sécurité dédiée aux technologies d'exploitation. Les solutions Fortinet sont développées par des experts techniques qui comprennent les besoins particuliers de ces environnements uniques en matière de sécurité et d'exploitation. La Security Fabric offre une solution architecturale complète pour garantir une protection de bout en bout, par rapport à l'approche à la carte d'autres fournisseurs dont les produits et les services individuels ne peuvent s'attaquer qu'à un seul vecteur d'attaque à la fois.

Des solutions garantissant une transparence totale dans les environnements OT

Les solutions de protection des terminaux améliorent la visibilité et le contrôle des appareils dans les environnements OT. Trois composants de Fortinet Security Fabric jouent un rôle essentiel dans la protection des terminaux :

FortiSIEM

Une sécurité efficace des technologies d'exploitation requiert à la fois transparence et contexte pour aider les analystes SOC à trier rapidement les alertes, à suivre les appareils et à résoudre les problèmes. FortiSIEM offre une solution SIEM multi-fournisseurs permettant une visibilité complète, une corrélation unifiée, des réponses automatisées et des mesures correctives pour aider à réduire les ressources en personnel, tout en améliorant la détection des violations.

FortiClient

FortiClient garantit la sécurité dans les environnements OT pour les postes de travail et les appareils BYOD connectés. Cette suite permet une protection des terminaux critiques, via un antivirus, un anti-logiciel malveillant, un anti-exploitation, une solution WAF (Web Application Firewall) et un filtrage Web. Elle comprend également un Fabric Agent pour la télémétrie des points terminaux, qui connecte FortiClient au pare-feu NGFW FortiGate.

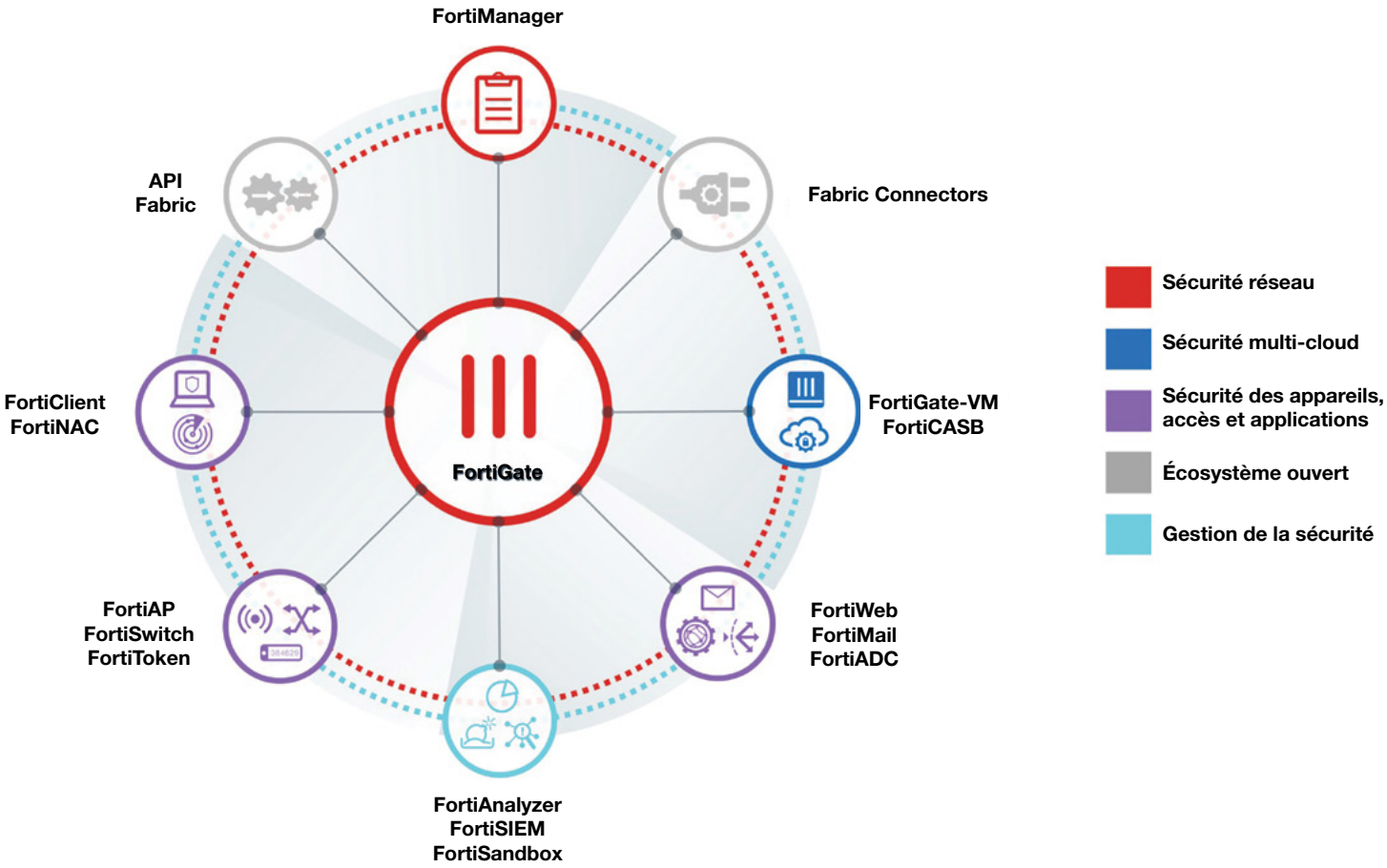
FortiNAC

FortiNAC aide à protéger les appareils et les systèmes dans les environnements OT qui ne disposent pas d'une sécurité intégrée suffisante, notamment les appareils IoT (Internet of Things – Internet des objets) et IIoT (Industrial Internet of Things – Internet industriel des objets), les automates programmables industriels (API), ainsi que les systèmes de contrôle industriel (ICS) et les systèmes de contrôle de supervision et d'acquisition de données (SCADA). En coordination avec d'autres solutions Security Fabric, FortiNAC aide à sécuriser les réseaux OT distribués contre les menaces en détectant les terminaux présentant des vulnérabilités non corrigées.

Par ailleurs, cette solution peut retirer instantanément et automatiquement les terminaux non critiques du réseau jusqu'à ce qu'ils soient suffisamment corrigés. Elle peut également réintégrer automatiquement ces terminaux dans le réseau à partir d'un tableau de bord central. En cas d'attaque multivectorielle à grande échelle (comme les botnets) ou dans toute autre situation d'urgence où l'accès doit être strictement limité pour des raisons de sécurité, FortiNAC a la possibilité de verrouiller le réseau et de ne pas permettre à de nouveaux appareils de le rejoindre sans autorisation manuelle.

Le choix d'une sécurité conçue pour les technologies d'exploitation

En raison de la convergence entre les technologies de l'information et les technologies d'exploitation, les analystes SOC doivent désormais protéger leurs systèmes OT sensibles contre une vague croissante de menaces provenant d'Internet. Pour accompagner cette évolution, Fortinet Security Fabric offre une visibilité transparente, un contrôle basé sur les politiques et une connaissance immédiate de la situation, dédiés aux environnements OT.



La Fortinet Security Fabric offre une architecture de sécurité unifiée et intégrée qui permet de débloquer l'automatisation.

La Security Fabric intègre des technologies spécialement conçues (segmentation, SIEM, NAC, protection des terminaux, commutation et sans fil) pour sécuriser les environnements OT contre les menaces informatiques omniprésentes. Les analystes SOC doivent évaluer la sécurité actuelle de leurs technologies d'exploitation en se posant quelques questions de base :

La sécurité de mes technologies d'exploitation...

- ...exploite-telle une architecture de sécurité intégrée qui connecte tous les composants de l'infrastructure de sécurité en un écosystème collectif et cohésif ?
- ...fournit-elle une plus grande visibilité pour la découverte de réseau OT afin de comprendre la posture de sécurité actuelle ?
- ...détecte-t-elle et classe-t-elle les appareils IoT et IIoT en fonction des facteurs de risque associés, tels que les vulnérabilités, les cotes de sécurité et même l'utilisation ?
- ...applique-t-elle la segmentation basée sur l'intention pour accroître la résilience des réseaux OT ?
- ...intègre-t-elle des solutions SIEM et NAC pour détecter les utilisateurs et les appareils suspects ?
- ...opérationnalise-t-elle les renseignements pour permettre une connaissance de la situation en temps réel sans perturber les opérations essentielles ?
- ...permet-elle une gestion simplifiée de la sécurité via une interface unique ?

[1] « State of Operational Technology and Cybersecurity Report », Fortinet, mars 2019.

[2] « DHS Alert ICS-ALERT-14-176-02A », CISA (Cybersecurity and Infrastructure Security Agency), 22 août 2018.

[3] Catalin Cimpanu, « Visant le secteur de l'Energie aux USALes astuces de phishing les plus sophisitiqués utilisées par les Hackers », BleepingComputer,10 juillet 2017.

[4] « Rapport sur l'état de l'OT (Operational Technology) et de la Cybersécurité », Fortinet, mars 2019.

[5] Ibid.

[6] « La pénurie en compétences en Cybersécurité s'envole, approchant les 3 millions », (ISC)², 18 octobre 2018.

FORTINET

www.fortinet.fr

13 mai, 2020 3:31 PM

360483-0-1-FR

sb-network-operations-analyst_FR