Accélérer l'efficacité des opérations de sécurité dans l'ensemble de la Security Fabric grâce à une réaction rapide

Table des matières

Synthèse

Rien qu'en 2019, plus de 124 milliards de dollars ont été dépensés pour la cybersécurité[1], mais les équipes de sécurité de nombreuses organisations ont du mal à suivre. Les défis à relever sont notamment le nombre trop élevé de consoles, la surcharge d'alertes, le recours à des processus manuels et la pénurie de personnel de cybersécurité.

Le modèle de maturité du Centre des opérations de sécurité (Security Operations Center – SOC) est conçu pour aider les équipes de sécurité à identifier les capacités dans la Fortinet Security Fabric et en fonction de leur investissement actuel dans les personnes et les processus de leurs équipes du SOC, guidant ainsi les entreprises à l'aide des solutions nécessaires pour résoudre les défis rencontrés par les organisations à chaque niveau de maturité.

Les solutions Fortinet, telles que FortiAnalyzer (analyse et automatisation de la Security Fabric), FortiSIEM (gestion des informations et des événements de sécurité) et FortiSOAR (orchestration, automatisation et réponse de sécurité) tirent parti de l'automatisation de la sécurité pour relever les principaux défis auxquels sont confrontés les architectes de sécurité et faire progresser leur automatisation du SOC. La Security Fabric relie toutes ces solutions entre elles, ce qui permet aux équipes de sécurité d'optimiser leur capacité à protéger l'entreprise.

Introduire l'automatisation de la sécurité dans la Security Fabric

La complexité opérationnelle est un défi pour les équipes de sécurité de toute taille. Le modèle d'automatisation du SOC aide l'équipe de sécurité d'une organisation à identifier son niveau de maturité actuel et à choisir les solutions de sécurité Fortinet qui sont les plus appropriées à son environnement.

Le modèle d'automatisation du SOC est divisé en trois domaines clés : les personnes, le processus et le produit. Dans chaque domaine, une organisation peut être classée à un niveau de maturité de 1 à 3 en fonction de sa posture de sécurité dans ce domaine. Par exemple, une organisation de niveau 1 dans toutes les catégories dispose d'une petite équipe informatique sans personnel de sécurité (personnes), sans manuels de réponse aux incidents (processus) et sans solutions de sécurité dédiées (produit). À l'autre extrême, une organisation peut avoir une grande équipe de sécurité avec des analystes SOC expérimentés, des manuels bien définis, et avoir non seulement déployé, mais aussi mesuré l'efficacité de ses solutions SIEM et SOAR.

Avec un manque de compétences en matière de cybersécurité de plus de 4 millions et en constante augmentation[2], il peut être impossible d'améliorer la composante humaine de l'automatisation du SOC d'une organisation. Cependant, si l'on met en œuvre les processus appropriés et que l'on sélectionne les bons produits, une organisation peut compenser un manque de personnel au sein de son équipe de sécurité.

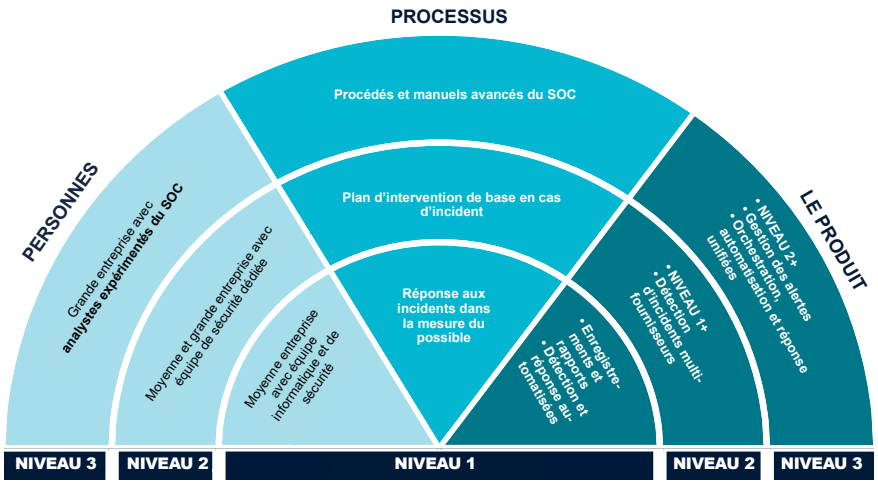


Schéma 1 : Le modèle d'automatisation du SOC.

Niveau 1 : Atteindre la visibilité en tirant parti de l'analyse de la Security Fabric

Au niveau 1 du modèle d'automatisation du SOC, une équipe de sécurité ne dispose pas de personnel de sécurité dédié ni de processus pour traiter les incidents potentiels. De plus, une entreprise moyenne reçoit plus de 10000 alertes par jour[3], ce qui signifie que les analystes du SOC sont débordés et ont peu de temps pour identifier et remédier aux véritables menaces qui pèsent sur le réseau.

Sans solutions dédiées, l'équipe de sécurité d'une organisation manque de visibilité sur les menaces éventuelles qui pèsent sur son réseau. Toutes les données des journaux doivent être collectées et corrélées manuellement avant de pouvoir être analysées. De nombreux SOC de niveau 1 n'ont pas les connaissances ou les ressources nécessaires pour identifier les véritables menaces, ce qui laisse l'organisation en danger.

FortiAnalyzer est une solution facile à déployer pour centraliser la visibilité et la détection des menaces dans l'ensemble de la Fortinet Security Fabric d'une organisation, y compris les déploiements in situ et dans le cloud. FortiAnalyzer met en corrélation les données des journaux de plusieurs dispositifs Fortinet, fournissant ainsi un contexte précieux aux analystes de la sécurité. En analysant ces données à l'aide de l'apprentissage machine (ML) et des indicateurs de compromis (IoC) fournis via un flux global de renseignements sur les menaces, FortiAnalyzer peut aider même la plus petite équipe de sécurité à identifier et à répondre rapidement aux menaces au sein de leur réseau.

Niveau 2 : Améliorer la visibilité des fournisseurs multiples avec les solutions SIEM (gestion des événements et informations de sécurité)

L'entreprise moyenne dispose de 75 solutions de sécurité ponctuelles différentes déployées sur son réseau.[4] Bien que chacune de ces solutions fournisse des renseignements précieux sur les menaces éventuelles pesant sur le réseau de l'entreprise, elles ne disposent souvent pas du contexte nécessaire pour faire la différence entre une menace réelle et un faux positif. En outre, un ensemble de solutions de sécurité autonomes rend difficiles l'application de politiques de sécurité cohérentes et le maintien de la conformité avec les nouvelles réglementations strictes en matière de protection des données, telles que le règlement général sur la protection des données (RGPD) de l'Union européenne ou la loi californienne sur la protection de la vie privée des consommateurs (CCPA).

Un système SIEM est la solution logique à la complexité de la sécurité causée par un environnement multi-fournisseurs. Une solution SIEM ingère des données collectées à partir de produits créés par plusieurs fournisseurs différents et effectue une corrélation et une analyse automatisées afin de fournir une image plus claire de l'état général de l'environnement protégé.

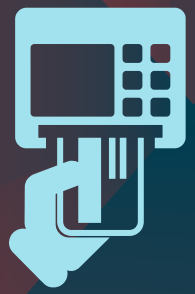
FortiSIEM permet aux équipes de sécurité d'adapter leurs opérations aux meilleures pratiques de l'industrie et aux normes de sécurité, telles que celles publiées par le National Institute of Standards and Technology (NIST) et le Center for Internet Security (CIS). De cette façon, FortiSIEM élargit la visibilité que FortiAnalyzer apporte à la Fortinet Security Fabric.

Niveau 3 : Intégrer la réponse automatisée au SOAR (orchestration, automatisation et réponse en matière de sécurité)

Le paysage de la cybermenace s'accélère, les cybercriminels s'appuyant de plus en plus sur l'automatisation pour accélérer leurs attaques. Alors que la visibilité d'un écran unique accélère la vitesse à laquelle une équipe de sécurité peut identifier une menace potentielle, le recours à des processus manuels de réponse aux incidents signifie que les défenseurs seront toujours un pas derrière les attaquants.

Les solutions de SOAR permettent à l'équipe de sécurité d'une organisation de tirer parti de l'automatisation pour accélérer la réponse aux incidents. En créant un cadre automatisé pour relier l'architecture de sécurité complète d'une organisation, des actions défensives peuvent être prises par plusieurs systèmes différents de concert. Cela permet de réduire au minimum les changements de contexte nécessaires au personnel de sécurité, de diminuer la fatigue des alertes et d'accélérer la réponse aux incidents.

FortiSOAR permet également à une organisation d'optimiser ses processus de sécurité en s'appuyant sur des référentiels de sécurité bien définis. En automatisant les tâches répétitives et les réponses aux menaces communes, FortiSOAR permet à une équipe de sécurité de concentrer ses efforts et ses ressources limitées sur des tâches de plus haut niveau.



L’automatisation peut réduire les temps de réponse à quelques minutes plutôt qu’à quelques jours.

Exploiter le modèle d'automatisation du SOC pour traiter intelligemment la complexité du SOC

Le paysage des menaces à la cybersécurité s'accélère, mais de nombreuses organisations souffrent d'un manque de ressources adéquates et de personnel qualifié. Pour se défendre contre les cyber-menaces croissantes, il faut des solutions de sécurité qui permettent de soulager la charge de travail des équipes SOC surchargées et en sous-effectif.

Le modèle d'automatisation du SOC aide les architectes de la sécurité à identifier leur niveau de maturité actuel et les étapes qu'ils doivent franchir pour atteindre le niveau suivant. Les solutions Fortinet, telles que FortiAnalyzer, FortiSIEM et FortiSOAR, sont conçues pour aider à réaliser cette transition.

En exploitant l'automatisation de la sécurité intelligente, ces outils réduisent le temps moyen de détection (MTTD) et le temps moyen de réponse (MTTR), diminuant ainsi l'exposition d'une organisation aux cybermenaces.

En un an, dans 65 pays[5]

- **2216 violations de données signalées**
- **53000 incidents de cybersécurité signalés**

[1] Lawrence Pingree, et coll., « Forecast: Information Security and Risk Management, Worldwide, 2017-2023, 3Q19 Update (Prévisions : sécurité de l'information et gestion des risques dans le monde entier, 2017–2023, mise à jour au T3 2019) » Gartner, 3 octobre 2019.

[2] « (ISC)² Finds the Cybersecurity Workforce Needs to Grow 145% to Close Skills Gap and Better Defend Organizations Worldwide ((ISC)² constate que la main-d'œuvre dans le domaine de la cybersécurité doit augmenter de 145 % pour combler le déficit de compétences et mieux défendre les organisations dans le monde) », (ISC)², 6 novembre 2019.

[3] « How Many Daily Cybersecurity Alerts does the SOC Really Receive? (Combien d'alertes de cybersécurité le SOC reçoit-il réellement par jour ?) » Bricata, 2 octobre 2019.

[4] Kacy Zurkus, « Defense in depth: Stop spending, start consolidating (La défense en profondeur : arrêter les dépenses, commencer à consolider) », CSO, 14 mars 2016.

[5] Gil Press, « 60 Cybersecurity Predictions For 2019 (60 prévisions en matière de cybersécurité pour 2019) », Forbes, 3 décembre 2018.

www.fortinet.fr

616492-0-0-FR

septembre 24, 2020 2:09 PM

ebook-FA-accelerate-efficiency-of-security-operations-across