PRÉSENTATION DE LA SOLUTION

FortiSOAR permet aux équipes chargées des opérations de sécurité d'accélérer la réponse aux incidents

Résumé

Les surfaces d'attaque des réseaux continuent de s'étendre en raison de l'évolution des menaces et des nouvelles innovations numériques. Pour essayer de suivre le rythme, de nombreuses entreprises ajoutent des solutions individuelles. Cette complexité accrue en matière de sécurité contribue à un certain nombre de problèmes : trop de fournisseurs à gérer, trop d'alertes à examiner, des processus manuels qui augmentent les temps de réponse et un manque de personnel formé pour gérer la charge de travail croissante chaque jour.

L'ajout de fonctionnalités d'orchestration, d'automatisation et de réponse en matière de sécurité (SOAR) à l'architecture de sécurité peut atténuer ces pressions. FortiSOAR permet aux équipes chargées des opérations de sécurité de créer une infrastructure automatisée et personnalisée qui rassemble tous les outils de sécurité de l'entreprise, tout en éliminant la désensibilisation aux alertes et en réduisant le changement de contexte. Les équipes chargées des opérations de sécurité peuvent ainsi non seulement adapter mais aussi optimiser leurs processus de sécurité.

Une sécurité désagrégée crée une désensibilisation aux alertes pour le personnel et engendre des risques

Les analystes de la sécurité sont actuellement submergés par le nombre d'alertes de sécurité auxquelles ils sont confrontés chaque jour. Les infrastructures de sécurité de plus en plus complexes et fragmentées (trop de produits individuels de différents fournisseurs) sont la principale raison de ce problème. Pour faire face aux menaces émergentes et aux nouveaux risques, l'entreprise moyenne déploie aujourd'hui 47 solutions et technologies de sécurité différentes.[1]

Bien que le volume d'alertes constitue une grande partie du problème, le suivi, l'analyse et la correction des alertes provenant de nombreuses sources différentes nécessitent un effort manuel important de la part du personnel du centre des opérations de sécurité (SOC). Ces flux de travail inefficaces ralentissent le processus de réponse aux incidents, la moyenne actuelle étant de 279 jours pour identifier et contenir une seule violation.[2]

Dans le même temps, les entreprises ont tendance à manquer de personnel lorsqu'il s'agit d'opérations de sécurité. Près des deux tiers (65%) des entreprises manquent actuellement de personnel qualifié nécessaire pour maintenir des opérations de sécurité efficaces.[3] Ces facteurs qui se recoupent augmentent encore les chances qu'une violation ne soit pas détectée.

L'année dernière, les violations ayant un cycle de vie inférieur à 200 jours ont été, en moyenne, 1,22 millions de dollars moins coûteuses que celles ayant un cycle de vie supérieur à 200 jours (3,34 millions de dollars contre 4,56 millions de dollars, respectivement), soit une différence de 37%.[4]

Le marché SOAR devrait croître pour atteindre près de 1,8 milliard de dollars avec un taux de croissance annuel composé (TCAC) de 15,6% entre 2019 et 2024.[5]

Une solution SOAR peut aider la sécurité à intégrer des outils de sécurité, permettant ainsi à des composants individuels de communiquer et de fonctionner ensemble dans une coordination défensive. Elle offre non seulement une meilleure visibilité du réseau, mais aussi des alertes plus stratégiques et réduites en matière de cybersécurité.[6] Plus précisément, la solution SOAR permet aux équipes chargées des opérations de sécurité d'automatiser les éléments fastidieux et répétitifs des flux de travail qui ne nécessitent pas de surveillance humaine. Les meilleures solutions SOAR enrichissent et contextualisent les menaces afin d'aider les analystes à trier rapidement les cas en fonction de la gravité des risques, de la sensibilité ou de la criticité des fonctions d'entreprise menacées.[7]

FortiSOAR intègre la sécurité et automatise les réponses

FortiSOAR offre la possibilité de regrouper et d'enrichir les alertes d'une large gamme de produits de sécurité. Cette solution simplifie l'orchestration et la gestion en adoptant des stratégies bien définies. De plus, elle élimine les opérations manuelles fastidieuses grâce à des réponses automatisées.

En tant que partie intégrante de l'architecture de Fortinet Security Fabric, FortiSOAR unifie les outils de sécurité en une seule solution fédérée. FortiSOAR peut ainsi automatiser de nombreux processus d'alerte de niveau inférieur, permettant aux analystes SOC de se concentrer sur des tâches plus essentielles. Les quatre principaux cas d'usage suivants démontrent la valeur immédiate que FortiSOAR offre aux équipes SOC en difficulté :

Cas d'usage 1 : Une plateforme SOC unifiée

FortiSOAR réduit la complexité du centre des opérations de sécurité (SOC) en intégrant des solutions de sécurité individuelles disparates dans un système d'orchestration centralisé qui peut être déployé dans pratiquement n'importe quel environnement. Cette solution comprend plus de 280 connecteurs prêts à l'emploi. Ceux-ci permettent aux équipes SOC d'utiliser FortiSOAR en toute transparence avec les solutions de sécurité existantes d'autres fournisseurs, et d'ingérer des informations d'alerte tout en fournissant un point de visibilité et de contrôle centralisé dans l'ensemble de l'entreprise Cette intégration élimine la fragmentation de l'écosystème, simplifie les processus des opérations de sécurité et prolonge la durée de vie utile des outils existants afin de maximiser le retour sur investissement (RSI) de ces achats.

Cas d'usage 2 : Le tri automatique des alertes

FortiSOAR regroupe les alertes en un seul endroit tout en les enrichissant d'un contexte supplémentaire pour réduire le temps de résolution. Cette solution permet également de réduire le nombre d'alertes « faussement positives » et offre des fonctions avancées de gestion de cas qui aident à définir, guider et accélérer les analyses. FortiSOAR rationalise les tâches simples du centre des opérations de sécurité (SOC), telles que l'ingestion des alertes, la hiérarchisation en fonction des niveaux de gravité et l'attribution des tâches. Il automatise également les tâches plus complexes d'échange à échange (E2E) telles que le tri, l'enrichissement, l'analyse et la correction. Ces fonctionnalités d'intégration et d'automatisation sophistiquées contribuent à éliminer bon nombre des charges courantes qui sont à l'origine de la désensibilisation aux alertes. Les analystes SOC peuvent ainsi se concentrer sur la chasse aux menaces et la réduction des fenêtres d'exposition à la menace d'une violation active.

Cas d'usage 3 : L'accélération des réponses aux incidents

Les opérations manuelles ralentissent l'analyse et la résolution des alertes, tout en introduisant des possibilités d'omissions et d'erreurs humaines. FortiSOAR étend les fonctionnalités d'automatisation offertes par FortiAnalyzer et FortiSIEM (solution de gestion des informations et des événements de sécurité) avec une orchestration et une automatisation solides de tous les processus SOC. Les équipes de sécurité peuvent accroître l'efficacité en automatisant chaque tâche, modification ou mise à jour en fonction des besoins spécifiques de l'entreprise. Au lieu de se contenter d'automatiser une seule entité, FortiSOAR peut couvrir l'ensemble du centre des opérations de sécurité et améliorer la sécurité globale.

En outre, FortiSOAR offre la possibilité unique d'automatiser toute réponse. Si une certaine criticité a été atteinte, les équipes de sécurité peuvent décider de mettre immédiatement une identité hors ligne et d'exploiter les stratégies et les connecteurs du produit.

Cas d'usage 4 : L'allègement de la charge sur les ressources limitées de l'équipe SOC

L'élimination des tâches manuelles soulage les équipes SOC surchargées en termes de temps et de coûts de main-d'œuvre, augmentant ainsi également le coût total de possession (TCO) en matière de sécurité. FortiSOAR rationalise intelligemment les opérations et les processus de sécurité grâce à des flux de travail automatisés. Les équipes SOC peuvent personnaliser les protocoles et les réponses de sécurité automatisées pour répondre aux exigences spécifiques du centre des opérations de sécurité (SOC).

En termes de facilité d'intégration, FortiSOAR offre la possibilité de créer des stratégies prêtes à l'emploi, par glisser-déposer, pour une configuration instantanée et un retour rapide à la valeur initiale. FortiSOAR permet également aux équipes SOC de conserver des connaissances tribales. Ici, si un employé quitte l'entreprise, son expérience et ses connaissances en matière de flux de travail restent documentées dans le système.

La gestion des risques, des ressources et des résultats

Les équipes chargées des opérations de sécurité continueront à être confrontées à la double pression d'une surface d'attaque en expansion et d'un manque de ressources, et devront donc lutter pour faire face à l'exposition croissante aux risques. Une solution SOAR efficace et complète peut aider les équipes SOC à surmonter ces difficultés, tout en améliorant, optimisant et renforçant les processus de sécurité de leur entreprise.

FortiSOAR constitue une solution flexible et personnalisable qui permet aux équipes chargées des opérations de sécurité de répondre à un paysage de menaces en constante évolution. Les fonctionnalités d'automatisation et d'orchestration de FortiSOAR aident les entreprises à simplifier l'écosystème de sécurité, ainsi que réduire la désensibilisation aux alertes, les temps de réponse et la charge sur les ressources limitées des équipes SOC.

Par ailleurs, FortiSOAR simplifie la gestion des licences grâce à un modèle de licence prévisible et basé sur l'utilisateur. Son architecture intrinsèquement évolutive offre une haute disponibilité pour les entreprises en pleine croissance, lui permettant de s'étendre à des entreprises en pleine expansion et/ou décentralisées sans affecter sérieusement les ressources nécessaires au déploiement et à la gestion à grande échelle.

[1] « 53% des entreprises ne savent pas si leurs solutions de sécurité fonctionnent correctement », Help Net Security, 31 juillet 2019.

[2] « Rapport sur les coûts 2019 liés aux Failles de Sécurité », Ponemon Institute et IBM Security, 2019.

[3] « Les stratégies pour construire et renforcer vos équipes en charge de la CyberSécurité : (ISC)² Cybersecurity Workforce Study, 2019 », (ISC)², 2019.

[4] « 2019 Cost of a Data Breach Report », Ponemon Institute et IBM Security, 2019.

[5] « Security Orchestration Automation & Response (SOAR) World Markets, Outlook to 2024: The High Number of False Security Alerts Presents Lucrative Market Opportunities », Research and Markets, 15 novembre 2019.

[6] Muhammad Omar Khan, « Why SOAR is a Good Bet For Fighting Mega Cyber Security Breaches », Entrepreneur, 23 mai 2019.

[7] Cian Walker, « SOAR: The Second Arm of Security Operations », Security Intelligence, 9 avril 2019.

FORTINET

www.fortinet.fr

21 avril, 2020 1:59 PM

587297-0-1-FR

sb-FA-fortisoar-empowers-security-operations-to-accelerate-incident-response-A4_FR