SOLUTION BRIEF

Fortinet Security Operations : accélérer la détection et la neutralisation des attaques, assurer les investigations et la remédiation post-incident

Synthèse

Il n'est guère surprenant que les cybercriminels disposent souvent de temps après s'être introduits au sein d'une entreprise et avant de se faire détecter, pour atteindre leurs objectifs. Selon une étude, il faut en moyenne entre 16 et 204 jours à une équipe de sécurité pour détecter un incident de sécurité en cours.[1] D'autre part, 75 % des professionnels de la sécurité affirment que l'univers actuel des menaces est le plus complexe qu'ils aient connu au cours des cinq dernières années.[2]

La solution Fortinet Security Operations capitalise sur l'IA et un traitement analytique avancé pour surveiller l'activité des utilisateurs, des dispositifs, des réseaux, de l'email, des applications, des fichiers et des logs, afin d'identifier toute activité suspecte ou malveillante que l'œil humain pourrait facilement négliger. De plus, les intégrations natives entre les composantes de la Fortinet Security Fabric permettent de partager des informations de veille pour une prise en charge automatisée des menaces et une capacité à anticiper et maîtriser les risques. Les équipes de sécurité disposent ainsi de plus de temps pour mener leurs investigations et restaurer chaque incident de manière automatisée et orchestrée, dans un objectif d'efficacité renforcée et de cohérence.

La moitié des entreprises déclarent investir dans l'IA et le ML pour détecter plus rapidement les menaces, et 44 % déclarent tirer parti des offres SIEM et SOAR pour accélérer leur temps de réponse aux incidents.[4]

En moyenne, les clients de la solution Fortinet Security Operations ont accéléré leur capacité à détecter et maîtriser les attaques de 180 heures à moins d'une heure (quelques minutes, dans la plupart des cas). Quant aux investigations et aux remédiations, elles s'effectuent en 10 à 15 minutes.[3]

L'évolution des menaces et l'expansion de la surface d'attaque donnent lieu à des incidents plus complexes et coûteux

Entre des menaces en constante évolution, une surface d'attaque qui ne cesse de s'étendre et une pénurie de professionnels qualifiés, les équipes de sécurité font face à de nombreux défis au quotidien. Ainsi, même les équipes importantes de professionnels chevronnés peinent à protéger efficacement les réseaux de leur entreprise. L'équipe FortiGuard en charge de la réponse aux incidents est fréquemment appelée à enquêter sur les cyberattaques. Les assaillants restent non détectés sur les réseaux d'entreprise pendant 36 jours en moyenne.[5] Ce chiffre est évalué à 204 jours dans un récent rapport d'IBM.[6] Dans les deux cas, il est clair que les assaillants disposent généralement de beaucoup de temps pour atteindre leurs objectifs malveillants.

En outre, il est de plus en plus coûteux de garder la main sur les effets des incidents de sécurité. Selon une enquête récente, 84 % des entreprises ont subi un ou plusieurs incidents au cours des 12 derniers mois. 48 % ont été victimes d'incidents de cybersécurité dont la facture s'élève à 1 million de dollars ou plus. [7]

Fortinet Security Operations : accélérer la détection et la réponse aux incidents

En conséquence, les entreprises déclarent donner la priorité à des investissements dans des technologies avancées comme l'IA et le ML pour détecter plus rapidement les signaux d'intrusion, dans des technologies centralisées comme le SIEM et le SOAR pour accélérer la réponse aux incidents de sécurité, ainsi que dans des produits de sécurité capables de s'intégrer entre eux pour fonctionner de manière simple.[8]

Ainsi, la solution Fortinet Security Operations s'impose auprès des entreprises, compte tenu de ses multiples avantages :

- Un vaste panel de capteurs comportementaux, déployés sur un domaine spécifique ou dans plusieurs domaines, pour une détection précoce des cyber-intrusions et leur prévention.
- Une automatisation centralisée de la sécurité pour agréger, enrichir et analyser les informations de sécurité provenant de ces capteurs et d'autres, ainsi que pour visualiser, orchestrer et automatiser les investigations et la réponse aux incidents

- Un panel de services SOC complémentaires pour évaluer et améliorer l'état de préparation des équipes et des technologies internes, étoffer ces équipes de manière ad hoc ou permanente, et apporter une assistance en cas d'incident ou de crise.
- Une fonctionnalité d'IA générative pour informer et accélérer les tâches des analystes en matière d'investigation sur les menaces, de stratégie de réponse et autres activités clés.

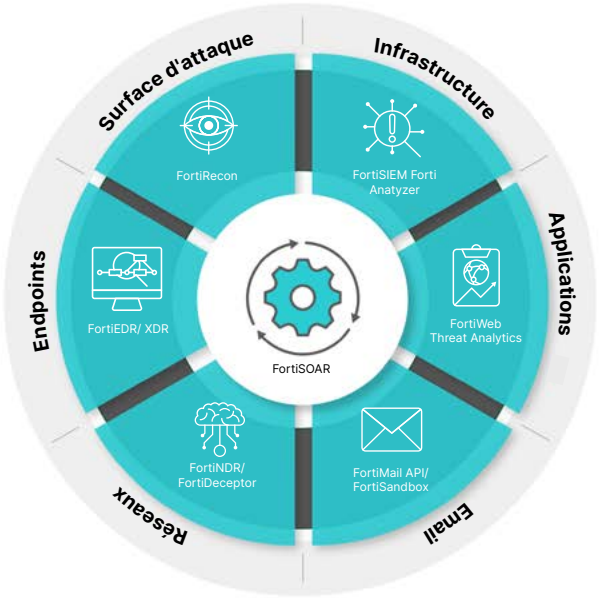

Schéma 1 : Solution Fortinet Security Operations

Intégration & automatisation

L'offre Fortinet Security Operations intègre différentes composantes. Chacune d'entre elles assure efficacement des tâches de détection des menaces en toute autonomie. Mais elles partagent également des informations de veille qui permettent à l'entreprise de migrer vers un modèle proactif de cyber-défense. Voici quelques exemples qui illustrent comment la solution Fortinet Security Operations s'intègre avec d'autres produits Fortinet au service d'une sécurité renforcée.

- **FortiEDR :** Cette solution effectue une détection de type comportementale des activités suspectes ou malveillantes sur un terminal. En cas de menace identifiée, elle prévient toute action à risque telle que le chiffrement de données ou l'établissement d'une connexion réseau. L'intégration native entre FortiEDR et les pare-feu NGFW FortiGate permet un partage bidirectionnel en peer-to-peer d'informations de veille sur les menaces.
- **FortiNDR :** Suite à une détection d'une activité réseau suspecte ou malveillante provenant d'un dispositif, FortiNDR peut intégrer des informations sur ce dispositif provenant de FortiEDR et déclencher, si nécessaire, une mise en quarantaine.
- **FortiRecon :** Après évaluation des ressources visibles depuis l'extérieur, l'intégration native avec FortiRecon permet à la solution Security Operations de recevoir des ressources supplémentaires depuis les pare-feu NGFW FortiGate afin de les inclure dans ses fonctions d'inventaire et d'analyse.
- **FortiDeceptor :** Lorsqu'un assaillant est détecté, l'intégration native permet à FortiDeceptor de signaler aux pare-feu NGFW FortiGate de neutraliser tout accès aux autres dispositifs, tout en relayant les réponses de l'assaillant pour continuer à le surveiller à son insu.
- **FortiSandbox :** Après évaluation d'un risque sur la base du comportement, FortiSandbox peut partager le score d'évaluation avec de nombreux équipements Fortinet, y compris les NGFW FortiGate et FortiMail, pour une neutralisation en temps réel d'un malware, avant toute infection.
- **FortiAnalyzer :** Une intégration native avec l'ensemble des solutions Fortinet permet aux entreprises de définir des déclencheurs d'événements et des réponses automatisées.
- **FortiSIEM :** Les incidents détectés suite à un traitement analytique de données de sécurité, assuré notamment par Machine Learning, font l'objet d'actions correctives rendues possibles grâce à plus de 300 intégrations technologiques. Ces incidents peuvent également être traités par FortiSOAR qui assure les tâches d'orchestration et d'automatisation.
- **FortiSOAR :** Lorsque FortiSOAR reçoit des alertes sur des activités suspectes, des actions automatisées par playbook peuvent être exécutées, comme déployer des outils de leurre qui permettent de piéger les assaillants.

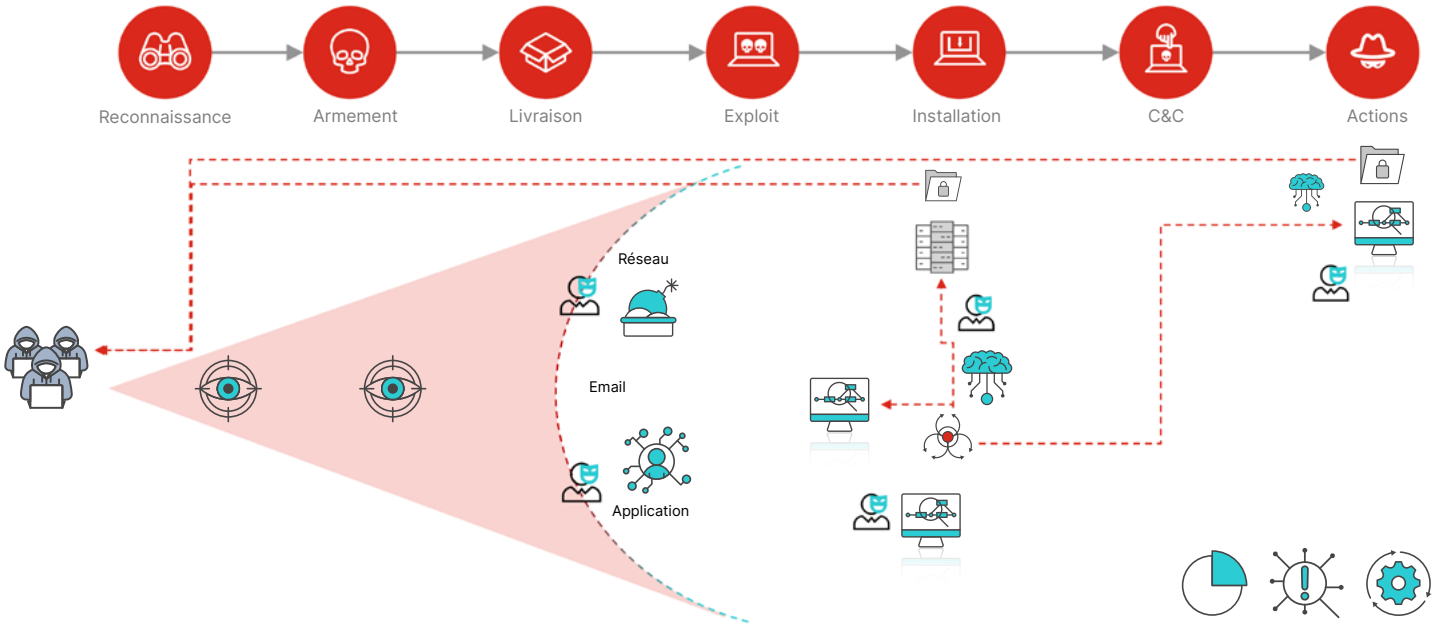

Schéma 2 : Composantes de la solution Fortinet Security Operations appliquée à l'ensemble de la chaîne de frappe d'une attaque

Les clients de la solution Fortinet Security Operations bénéficient d'un retour sur investissement de 597 %[9]

Investir dans les composants de la solution Fortinet Security Operations Solution permet de réduire considérablement le délai de présence d'un assaillant sur le réseau, les risques cyber et les efforts de sécurité opérationnelle. Plus précisément :

- Avant d'investir dans des capteurs de détection et de prévention, les clients de Fortinet indiquent qu'il fallait en moyenne 21 jours à leurs équipes pour détecter les intrusions et un jour et demi de plus pour les maîtriser.[10] Après avoir déployé des produits tels que FortiEDR, FortiNDR ou FortiDeceptor, les clients déclarent être capables de détecter et maîtriser en moins d'une heure (quelques minutes pour la plupart) l'activité des assaillants.[11]
- Avant de déployer la solution Fortinet Security Operations, les entreprises indiquent que les investigations suite aux alertes et la remédiation prenaient deux à trois jours.[12] En déployant des composantes comme FortiAnalyzer, FortiSIEM ou FortiSOAR, les investigations sont désormais réalisées en 10 à 15 minutes.[13]
- De plus, les clients indiquent qu'une équipe de 6 (voire 3 dans un cas) peut assurer la charge de travail de 12 personnes, pointant ainsi une nette amélioration de la productivité opérationnelle.[14]

Schéma 3 : Avantages quantifiés du déploiement des composantes de Fortinet Security Operations

ESG Research a quantifié la valeur de ces améliorations en termes de maîtrise des risques et d'avantages financiers escomptés. L'étude montre qu'une entreprise type a près de 30 % de chances de subir un incident de sécurité au cours d'une année donnée, ce qui se traduit par un coût annuel estimé à 1,4 million de dollars.[15] De plus, en prenant en compte les délais accélérés pour détecter et maîtriser les menaces, mener des investigations et assurer les restaurations, ESG Research a calculé une économie annuelle de 1,39 million de dollars résultant d'une réduction des coûts potentiels liés aux incidents, ceci grâce au déploiement des composantes de la solution Fortinet Security Operations.[16]

En outre, en raison de la productivité renforcée qui résulte de l'adoption de la solution, les équipes de sécurité devraient économiser en moyenne 1,9 million de dollars sur les charges de personnel.[17] En fin de compte, ESG Research table sur un retour sur investissement de 597 % pour les entreprises qui investissent dans la solution Fortinet Security Operations, avec une période de payback de deux mois.[18]

Conclusion

La solution Fortinet Security Operations octroie aux entreprises des capacités puissantes de détection basées sur l'IA, sur l'ensemble de leur périmètre digital. La solution s'intègre aux contrôles de sécurité existants afin de comprimer le délai nécessaire pour perturber les cyberattaques tout au long de leur chaîne de frappe. La solution permet également aux équipes de sécurité d'orchestrer, d'automatiser et de renforcer leurs efforts d'investigation et de remédiation aux incidents, pour une réponse plus rapide et plus cohérente. Enfin, des services experts sont disponibles pour évaluer l'état de préparation des opérations de sécurité et contribuer à la réponse aux incidents de sécurité. Les possibilités d'intégration de la solution Fortinet Security Operations invitent les équipes de sécurité à passer d'une approche classique et chronophage de type "détection et réponse aux menaces" à une approche plus performante et complète qui consiste à détecter et perturber les menaces, puis enquêter et assurer la remédiation.

1 Cost of a Data Breach Report 2023, IBM, 24 juillet 2023.

2 How the Economy, Skills Gap, and Artificial Intelligence are Challenging the Global Cybersecurity Workforce, ISC2, 31 octobre 2023.

3 ESG Economic Validation: The Quantified Benefits of Fortinet Security Operations Solutions, Enterprise Strategy Group, 1er août 2023.

4 2023 Global Ransomware Report, Fortinet, 20 avril 2023.

5 FortiGuard Labs, consulté le 21 novembre 2023.

6 Cost of a Data Breach Report 2023, IBM, 24 juillet 2023.

7 2023 Global Cybersecurity Skills Gap Report, Fortinet, 21 mars 2023.

8 2023 Global Ransomware Report, Fortinet, 20 avril 2023.

9 ESG Economic Validation: The Quantified Benefits of Fortinet Security Operations Solutions, Enterprise Strategy Group, 1er août 2023.

10 Ibid.

11 Ibid.

12 Ibid.

13 Ibid.

14 Ibid.

15 Ibid.

16 Ibid.

17 Ibid.

18 Ibid.

février 13, 2024 1:44 PM

2431037-0-0-FR