ÉTUDE DE CAS

Un grand groupe industriel mondial comble ses failles de sécurité

FireEye Mandiant Cyber Defense Operations crée des cas d'usage personnalisés pour renforcer la couverture du framework MITRE ATT&CK

EN BREF

SECTEUR D'ACTIVITÉ

Industrie

SOLUTIONS

- FireEye Mandiant Cyber Defense Operations

AVANTAGES

- Création d'un profil de menaces spécifique à l'entreprise – par l'identification des attaquants et de leurs modes opératoires – pour renforcer les capacités de détection et de remédiation de l'entreprise
- Élaboration de 60 cas d'usage à intégrer au SIEM
- Protection renforcée face à plus de 40 techniques répertoriées par MITRE et optimisation de nombreux mécanismes existants pour gagner en efficacité

PROFIL CLIENT

L'entreprise est un grand groupe industriel d'envergure internationale, leader des nombreux marchés sur lesquels il opère. Elle figure au classement Fortune Global 500.

L'enjeu

Ce groupe représente une cible privilégiée pour des hackers à l'affût d'informations personnelles, financières et opérationnelles, mais aussi de données de propriété intellectuelle à revendre sur le marché noir.

Étant donné son statut et son exposition constante aux cyberattaques, l'entreprise s'attache à renforcer continuellement son niveau de sécurité afin d'assurer la protection permanente de ses ressources digitales et données critiques. Fort d'un investissement massif dans sa défense et d'une cybersécurité élevée au rang de priorité stratégique, ce groupe a su attirer les meilleurs talents et experts du secteur. Son équipe de sécurité a mis en place des mesures robustes et efficaces pour la protection de son écosystème face à toute la panoplie d'attaques courantes.

Pour valider son architecture de sécurité et structurer le développement de modèles de menaces et de méthodologies spécifiques, ce géant industriel s'appuie depuis longtemps sur le framework MITRE ATT&CK. Mais pour être sûr de ne rien laisser au hasard, il voulait encore identifier et écarter toute vulnérabilité potentiellement masquée et autres zones grises dans son système de défense.

La solution

Le groupe a fait appel à l'équipe FireEye Mandiant Cyber Defense Operations pour développer une série de cas d'usage très détaillés à intégrer à son SIEM. Objectif : renforcer ses capacités de détection et de réponse tout en durcissant ses défenses sur toute sa surface d'attaque internationale.

Phase 1

Pour commencer, l'équipe Mandiant s'est appuyée sur FireEye Threat Intelligence pour créer un profil de menaces spécifique à l'entreprise et à son secteur d'activité. Lors de cette première phase, les consultants Mandiant ont dressé une liste de tous les attaquants à l'échelle mondiale jugés les plus susceptibles de cibler les ressources digitales du groupe.

Ils ont ensuite procédé à une évaluation sur site de la topologie réseau du client, des cas d'usage existants et des niveaux de visibilité sur l'ensemble de l'infrastructure. Forte de sa longue expérience en réponse à incident, l'équipe Mandiant a analysé les résultats, puis les a recoupés avec la couverture existante du framework MITRE ATT&CK. Elle y a ensuite superposé les heat maps FireEye Threat Intelligence comportant les noms et modes opératoires des attaquants identifiés lors de la création du profil de menaces.

Phase 2

Une fois le problème posé, les consultants Mandiant Cyber Defense Operations ont travaillé en collaboration avec l'équipe FireEye Threat Intelligence pour élaborer des cas d'usage visant à pallier aux faiblesses détectées lors de la phase d'investigation. Chaque cas d'usage comportait des critères de détection soigneusement documentés pour faciliter et accélérer l'identification de chaque tentative de compromission nouvellement répertoriée.

Quelques exemples de cas d'usage :

- Variantes de malwares privilégiées par des attaquants identifiés par les experts Mandiant
- Techniques d'exploitation classées par MITRE ATT&CK et associées à des hackers identifiés
- Capacités de détection de techniques open-source employées par des assaillants à l'encontre d'entreprises du secteur concerné

Phase 3

Pour affiner chaque cas d'usage, l'équipe Mandiant a écrit ses logiques de détection en pseudo-code (dans un format compatible Sigma), avant d'intégrer le paquet final au SIEM de l'entreprise. Une fois assimilé au portefeuille SIEM, chaque cas d'usage a été testé, puis perfectionné pour assurer une efficacité optimale.

L'utilisation de modèles préconfigurés a permis d'homogénéiser la taxonomie et les méthodes de code de tous les cas d'usage, le tout étant aligné et coordonné de façon à lutter spécifiquement contre les auteurs préalablement identifiés et les menaces avancées les plus susceptibles de frapper.

Résultats

Chaque cas d'usage étant basé sur des éléments individuels du framework MITRE ATT&CK, l'intégration des logiques de détection au SIEM de l'entreprise lui permet de quantifier les améliorations de ses capacités de détection et de remédiation.

La mission de l'équipe Mandiant Cyber Defense Operations s'est déroulée sur une période de huit semaines et s'est soldée par la création de 60 nouveaux cas d'usage comprenant près de 800 objets de détection individuels. L'équipe a pu ajouter 40 techniques MITRE manquantes avant le lancement du projet, ce qui représente une progression à deux chiffres du nombre de techniques déployées au sein du groupe. En plus des nouveaux cas d'usage intégrés, les capacités de détection de plus d'une douzaine de techniques MITRE existantes ont été renforcées grâce à des informations générées directement au cours de la mission.

Au vu des résultats obtenus, le groupe a signé un accord annuel de collaboration exclusive avec Mandiant pour continuer à accélérer le développement des cas d'usage et renforcer continuellement son système de défense.

Pour en savoir plus, rendez-vous sur **www.fireeye.fr**

FireEye, France
Nextdoor Cœur Défense
110 Esplanade du Général de Gaulle
92931 Paris La Défense Cedex 92974
+33 1 70 61 27 26
france@FireEye.com | www.FireEye.fr
FireEye, Inc.
601 McCarthy Blvd.
Milpitas, CA 95035
+1 408 321 6300 | info@FireEye.com

À propos de FireEye, Inc.

FireEye est spécialisé dans la cybersécurité axée sur la Threat Intelligence. Prolongement naturel et évolutif des opérations de sécurité des clients, la plateforme unique de FireEye combine des technologies de sécurité innovantes, des services de CTI d'envergure internationale et les services réputés de Mandiant® Consulting. FireEye simplifie ainsi la cybersécurité et son administration, devenant un allié précieux des entreprises confrontées au casse-tête que représentent la prévention et la neutralisation des cyberattaques.

FIREEYE™