proofpoint

TÉMOIGNAGE CLIENT

Une banque élimine presque entièrement les vulnérabilités de sécurité liées aux identités grâce à Proofpoint

Le défi

- Identifier les failles potentiellement exploitables entre les contrôles de sécurité multicouches
- Accélérer la correction, le cas échéant
- Devancer les cybercriminels

La solution

Plate-forme Proofpoint Identity Threat Defense

- Proofpoint Spotlight
- Proofpoint Shadow

Les résultats

- Réduction des privilèges administrateur de domaine de 350 à zéro
- Identification et suppression des voies d'accès à haut risque aux ressources stratégiques
- Renforcement de la confiance des dirigeants et membres du conseil d'administration à l'égard des contrôles organisationnels

L'entreprise

Cette banque nationale, qui appartient à une entreprise multinationale de services financiers, dispose de succursales sur l'ensemble du territoire américain. Elle propose une vaste gamme de services bancaires, de carte de crédit, de prêt et de gestion de patrimoine. Responsable de la gestion de plusieurs milliards de dollars, la banque s'attache à maintenir le nombre de vulnérabilités de cybersécurité aussi proche de zéro que possible.

Le défi

L'équipe de cybersécurité de la banque est responsable de plus de 10 000 endpoints utilisateur, ainsi que de la sécurisation des processus d'ingénierie, d'exploitation et d'accès. Elle avait déployé plusieurs couches de sécurité, notamment des solutions de sensibilisation aux menaces et de gestion des cyberrisques, dans l'ensemble de son infrastructure. Cependant, un grand nombre des couches de sécurité étaient isolées les unes des autres. Seule la solution SIEM de la banque fonctionnait en tant que couche « horizontale », procédant à la collecte et l'analyse des événements au niveau de tous les contrôles. Pourtant, malgré des défenses sophistiquées, l'équipe de cybersécurité continuait d'observer des signes d'attaques incessantes, tout en sachant qu'aucune entreprise n'est à l'abri d'une compromission potentielle.

« Je savais qu'il y avait un certain degré de vulnérabilité que nous devions accepter », explique le RSSI. « Certaines ressources sont très difficiles à corriger sans interrompre les activités, et la perfection n'existe pas en matière de bonnes pratiques de cybersécurité. Nous voulions disposer d'une visibilité et d'une protection sur l'ensemble de notre réseau et de nos endpoints afin d'identifier les failles, là où nos autres contrôles n'étaient peut-être pas aussi efficaces. »

La solution

Le RSSI a découvert Proofpoint Identity Threat Defense grâce à des homologues du secteur. Il savait que plusieurs grandes banques avaient adopté la plate-forme, mais il ne l'avait pas encore vue à l'œuvre.

« Lorsque j'ai vu la plate-forme Proofpoint, la logique qui la sous-tendait m'a semblé très intéressante », précise le RSSI. « Elle nous permettait de voir le réseau tel qu'un cybercriminel le voit. »

Proofpoint Shadow est une solution sans agent et pilotée par la threat intelligence, capable de créer sans effort un réseau dense de leurres à l'échelle de l'infrastructure. Il accélère la détection des menaces de manière déterministe en identifiant les menaces en fonction des interactions des cybercriminels avec les leurres, sans avoir recours à des analyses probabilistes basées sur des signatures ou des comportements. Contrairement à d'autres technologies de leurre qui déploient des agents ou des honeypots susceptibles d'attirer l'attention du cybercriminel ou d'être exploités par celui-ci, son architecture sans agent l'empêche d'être découverte par le cyberpirate. Le RSSI et son équipe ont réalisé une validation de concept (PoC) de 60 jours avec Proofpoint afin de mettre la solution à l'épreuve. Ils ont également chargé des spécialistes en tests d'intrusion d'essayer de contourner la solution, et ceux-ci ont échoué à chaque fois.

« Grâce à Proofpoint Identity Threat Defense, nous avons beaucoup plus confiance dans nos contrôles de sécurité. Nous avons constaté une amélioration quantifiable de la qualité globale de la protection. »

RSSI

Proofpoint Spotlight a également permis à l'équipe de découvrir les voies d'accès à haut risque susceptibles d'être utilisées par un cybercriminel pour se déplacer plus rapidement à travers le réseau afin d'accéder aux ressources stratégiques. Il identifie en permanence les privilèges d'accès non utilisés ou superflus, ainsi que les identifiants de connexion stockés de façon inappropriée pouvant être compromis par les cybercriminels et utilisés à leur profit.

« Proofpoint Spotlight a rapidement identifié nos failles les plus exploitables sur la base de modèles de cyberattaques réels », explique le RSSI. « Il nous a fourni les preuves et le contexte dont nous avions besoin pour hiérarchiser les mesures correctives et optimiser les autres contrôles de sécurité, si nécessaire. »

Pour maximiser l'efficacité de la solution, seuls quelques membres de l'équipe de sécurité de la banque savent qu'elle est déployée. Les alertes de Proofpoint Identity Threat Defense sont traitées comme des violations des règles et envoyées à la solution SIEM. La banque dispose d'un analyste exclusivement chargé d'examiner les « violations des règles » signalées par la plate-forme. Les membres de l'équipe de sécurité qui ont déployé la solution n'ont eu aucun problème de faux positifs : chaque alerte est une véritable indication d'une tentative de déplacement latéral par une personne inconnue dans le réseau.

« Les données capturées par Proofpoint nous fournissent des informations à valeur ajoutée exploitables qui constituent un puissant outil de reconstitution des événements. »

RSSI

Les résultats

Élimination de l'accès au domaine

Dès son déploiement, Proofpoint Spotlight a mis au jour et amplifié des failles inconnues liées aux bonnes pratiques, telles que des erreurs de configuration et des problèmes de contrôle d'accès. La plate-forme propose des fonctionnalités de découverte perpétuelle et d'automatisation sélective, ce qui permet d'identifier et d'éliminer facilement les voies d'accès à haut risque. Proofpoint a non seulement identifié les comptes disposant de privilèges trop élevés, mais il a également mis au jour les chemins réseau réels qu'un cybercriminel pourrait emprunter pour accéder aux ressources stratégiques de la banque. Grâce à cette visibilité, l'équipe du RSSI a obtenu le contexte nécessaire pour comprendre exactement comment des connexions apparemment anodines exposaient la banque à des déplacements latéraux par des cybercriminels. Ces informations lui ont permis de supprimer les points de connexion inutiles en fonction des indicateurs de risque et de l'impact sur les opérations et les workflows de l'entreprise. En outre, le RSSI a collaboré avec l'équipe informatique pour réduire les privilèges de façon stratégique et supprimer progressivement tous les privilèges d'accès à l'échelle de l'infrastructure.

« Nous avons affiné nos règles et réduit les privilèges administrateur de domaine de 350 à zéro », explique le RSSI. « En cas d'urgence, l'accès de secours n'est ouvert que pour une durée limitée. »

La capacité d'identifier rapidement et facilement les failles exploitables donne à l'équipe de sécurité un avantage préventif sur les cybercriminels. Lorsqu'un collaborateur quitte l'entreprise, celle-ci utilise les identifiants de connexion de cet ancien collaborateur pour déterminer où il les a utilisés et combler les failles qui n'auraient peut-être pas été identifiées autrement.

Obtention —et conservation — de la confiance du conseil d'administration

En plus de détecter efficacement les déplacements latéraux et d'aider l'équipe à renforcer la sécurité de l'environnement, la plate-forme Proofpoint Identity Threat Defense offre une valeur considérable en termes de communication. Les données télémétriques étoffées et les rapports fournis par la solution Proofpoint ont permis au RSSI de fournir aux dirigeants de la banque et aux membres du conseil d'administration des explications visuelles claires de la façon dont les cybercriminels opèrent, des raisons pour lesquelles les déplacements latéraux sont si graves et de la manière dont les défenses de la banque protègent l'environnement.

Même si la banque disposait déjà d'une infrastructure de cybersécurité robuste, Proofpoint a amélioré le contrôle, la visibilité et la capacité de communication du RSSI. La possibilité d'identifier les vulnérabilités, de les corriger et de démontrer l'efficacité des contrôles a considérablement renforcé la sécurité de la banque.

« Grâce à Proofpoint Identity Threat Defense, nous avons beaucoup plus confiance dans nos contrôles de sécurité », commente le RSSI. « Nous avons constaté une amélioration quantifiable de la qualité globale de la protection. »

EN SAVOIR PLUS

Pour plus d'informations, visitez notre site à l'adresse : **proofpoint.com/fr**.

proofpoint.

0613-002-03-01 06/24