proofpoint

TÉMOIGNAGE CLIENT

Une société de distribution d'énergie renforce ses défenses avec Proofpoint

Le défi

- Accroître la visibilité sur les menaces ciblant l'infrastructure et les ressources stratégiques
- Accélérer l'identification des menaces et améliorer la réponse aux incidents
- Améliorer la collecte des données d'investigation numérique

La solution

Proofpoint Identity Threat Defense

- Proofpoint Shadow

Les résultats

- Absence de faux positifs
- Visualisation de l'activité cybercriminelle en temps réel
- Réduction de deux tiers des délais d'investigation
- Réception instantanée de données d'investigation numérique détaillées pour une prise de décision reposant sur des preuves incontestables
- Établissement d'un véritable partenariat avec Proofpoint tout au long du déploiement

L'entreprise

Cette entreprise distribue de l'énergie et offre des services connexes à des millions de clients et partenaires dans le monde entier. Cette multinationale mène également des opérations d'exploration et de production d'énergie. Du fait du caractère stratégique de l'énergie pour la vie et la sécurité nationale, l'entreprise s'appuie sur l'innovation technologique pour développer des produits, applications et services de pointe. Compte tenu de la priorité qu'elle accorde à la sécurité, l'entreprise s'est rapprochée de Proofpoint pour bénéficier de fonctionnalités uniques lui permettant de détecter toute activité malveillante et de bénéficier d'informations d'investigation numérique en temps réel.

Le défi

Pour une société de distribution d'énergie, la protection de sa surface d'attaque complexe est un enjeu de sécurité majeur. Cette entreprise dispose d'une infrastructure sur site et dans le cloud, ainsi que d'un réseau stratégique de contrôle et d'acquisition de données en temps réel (SCADA) et de terminaux. Son association avec de multiples partenaires externes exige de nombreuses connexions réseau entrantes et sortantes. L'accent mis sur les opérations de développement (DevOps) va de pair avec la protection des endpoints d'une large communauté de développeurs, ainsi que du code applicatif et des systèmes de test. En sa qualité de fournisseur d'énergie, l'entreprise a besoin d'une parfaite visibilité sur l'infrastructure de sécurité et doit pouvoir collecter des données télémétriques en cas de détection de menace afin de se conformer aux réglementations sectorielles, au règlement général sur la protection des données (RGPD) et aux autres exigences de sécurité.

L'entreprise avait déjà adopté une approche de défense en profondeur en matière de sécurité et s'emploie à mettre en œuvre et à améliorer en permanence les bonnes pratiques. Avant l'intervention de Proofpoint, des utilisateurs internes avaient déjà déclenché des alertes dans les systèmes de sécurité de l'entreprise. À chaque alerte, l'équipe SOC devait récupérer l'ordinateur portable de l'utilisateur et mener des investigations manuelles, telles que des recherches approfondies dans les registres système et la collecte minutieuse d'une quantité suffisante de données d'investigation numérique pour pouvoir reconstituer l'événement. Même en récupérant rapidement l'ordinateur portable, ces investigations pouvaient prendre des heures. Pour améliorer sa réactivité, l'entreprise a lancé une initiative de sécurité focalisée sur la protection des ordinateurs portables et postes de travail.

La solution

Dans le cadre de sa recherche d'une solution, l'entreprise s'est d'abord intéressée à la technologie de honeypots, puis a découvert Proofpoint Identity Threat Defense et sa technologie de leurres basée sur les endpoints. Son choix s'est porté sur Proofpoint Shadow.

« Au départ, je pensais que Proofpoint Shadow n'était qu'un honeypot », explique le responsable de la sécurité des informations. « Mais je me suis vite aperçu que l'approche de Proofpoint était bien plus sophistiquée. »

Les leurres sans agent de Proofpoint Shadow, pilotés par la threat intelligence et installés sur chaque endpoint, sont conçus pour ressembler à de véritables données, identifiants et connexions. Désormais, lorsqu'un cybercriminel, ou un utilisateur interne malveillant disposant d'un accès légitime au réseau, tente de s'implanter dans les systèmes, il découvre de nombreuses fausses ressources très crédibles. Il est alors presque impossible d'emprunter une voie sûre et indétectable, le moindre faux pas alertant le SOC. Une fois le leurre activé, le système commence à collecter de riches informations d'investigation numérique dans les systèmes où le cybercriminel s'est introduit pour fournir des données précises en temps réel permettant de prendre rapidement des mesures informées.

« Proofpoint réduit de deux tiers les délais d'investigation. Le tableau de bord graphique indique à quel endroit le cybercriminel a été en contact avec les ressources stratégiques de l'entreprise. Nous pouvons rapidement examiner en détail des informations spécifiques. Le système nous fournit automatiquement le déroulé de l'événement au niveau de l'endpoint. Cette aide est inestimable. »

Responsable de la sécurité des informations, fournisseur d'énergie

Le fournisseur d'énergie a déployé Proofpoint Identity Threat Defense dans son environnement à l'aide de son MSP et des Services professionnels Proofpoint. La solution a immédiatement identifié des voies d'accès aux données les plus précieuses de l'entreprise et plusieurs vulnérabilités dues à des erreurs de configuration du système existant.

« Proofpoint Identity Threat Defense nous a été d'une aide précieuse », affirme le responsable de la sécurité. « La solution collecte des informations sur les endpoints et suggère plusieurs leurres appropriés, ce qui nous fait gagner du temps et améliore considérablement nos défenses. L'équipe Proofpoint nous a particulièrement impressionnés. Elle est à l'écoute de nos besoins, nous aide à adapter nos défenses à notre environnement et fait preuve d'une grande réactivité. »

Les résultats

Après son déploiement, la solution Proofpoint a immédiatement détecté des instances de tentatives d'intrusion de cyberadversaires inconnus, piégés par des leurres. Désormais, l'équipe SOC peut identifier et surveiller en temps réel l'activité des cybercriminels. Simultanément, une investigation numérique en temps réel met à disposition de l'équipe SOC des renseignements sur la cyberattaque, ce qui lui permet d'examiner rapidement en détail des informations spécifiques, à l'insu du cybercriminel. L'équipe de réponse aux incidents est maintenant en mesure de prioriser rapidement ses investigations, sachant quels sont les outils utilisés par le cybercriminel. Les alertes Proofpoint sont simultanément envoyées au système ServiceNow de l'entreprise, ce qui optimise l'attribution des tâches aux analystes, la hiérarchisation des réponses et la gestion des tickets.

« Auparavant, nous n'aurions pas eu connaissance de cette activité », déclare le responsable de la sécurité. « Il nous aurait fallu attendre d'être alertés par plusieurs couches de sécurité pour être sûrs qu'il ne s'agissait pas d'un faux positif, puis de mettre en quarantaine et de confisquer l'ordinateur portable pour pouvoir mener nos investigations et collecter des preuves. »

Une vraie révolution

« Les données télémétriques ont changé la donne », ajoute-t-il. « Proofpoint Identity Threat Defense réduit de deux tiers les délais d'investigation. Le tableau de bord graphique indique à quel endroit le cybercriminel a été en contact avec les ressources stratégiques de l'entreprise. Nous pouvons rapidement examiner les informations en détail. La solution nous fournit automatiquement le déroulé de l'événement au niveau de l'endpoint. Cette aide est inestimable. »

Les données télémétriques de la solution fournissent également des preuves irréfutables. Si la cyberattaque est le fait d'un utilisateur interne malintentionné, l'entreprise peut apporter des preuves incontestables de l'incident et prendre les mesures nécessaires. En cas de tentatives d'attaque d'origine externe, plus fréquentes, l'entreprise dispose désormais de données détaillées sur les objectifs et les techniques du cybercriminel, ce qui lui permet de renforcer ses défenses le cas échéant.

Le socle de l'avenir

Le fournisseur d'énergie, qui doit protéger ses sites distants, son environnement SCADA et ses terminaux IoT, envisage d'utiliser Proofpoint Identity Threat Defense pour étendre son approche de défense en profondeur à ces ressources.

« Proofpoint Identity Threat Defense est un outil fondamental », souligne le responsable de la sécurité. « Il est d'une grande efficacité. S'il nous fallait rationaliser nos outils de sécurité, ce serait le dernier dont nous nous séparerions. »

EN SAVOIR PLUS

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