Proofpoint Threat Response Auto-Pull

Mise en quarantaine automatique des emails malveillants après leur remise

PRINCIPAUX AVANTAGES

- Mise en quarantaine automatique des emails malveillants qui contournent les défenses périmétriques
- Réduction exponentielle du temps que les équipes chargées de la sécurité et de la messagerie consacrent à l'orchestration de la sécurité de la messagerie électronique et à la réponse aux incidents
- Classification des messages au moyen de la threat intelligence de Proofpoint
- Surveillance automatique des boîtes email de signalement d'abus
- Mise en quarantaine des messages transférés à d'autres personnes ou à des listes de distribution
- Traque des campagnes de phishing partiellement signalées et élimination du temps gaspillé dû aux messages signalés par erreur

Proofpoint Threat Response Auto-Pull (TRAP) permet aux administrateurs de la messagerie et de la sécurité d'optimiser le processus de réponse aux incidents. Lorsqu'un email malveillant est détecté, TRAP analyse les emails et supprime automatiquement les messages malveillants. Il met également en quarantaine les emails indésirables qui ont atteint les boîtes de réception des utilisateurs. TRAP est une puissante solution, qui permet de réduire de manière exponentielle le temps que vos équipes chargées de la sécurité et de la messagerie consacrent au nettoyage des emails malveillants et indésirables.

Plus de 90 % des compromissions de données commencent par la réception d'un email, le principal vecteur de menaces. Compte tenu de l'évolution des menaces propagées par email, les entreprises sont exposées à de plus en plus de messages malveillants. Les emails malveillants peuvent contenir des liens de phishing dont l'activité nocive peut être déclenchée après leur distribution, ou utiliser des techniques de contournement produisant des faux positifs et entraînant leur remise aux utilisateurs. Les équipes de sécurité de la messagerie électronique sont souvent chargées d'analyser les emails et de supprimer les messages malveillants et indésirables, afin de réduire l'exposition aux menaces et limiter les dommages potentiels. Si la mise en quarantaine d'un email unique est un processus relativement simple ne nécessitant que 10 à 15 minutes, elle peut vite se transformer en une tâche fastidieuse et chronophage dès lors que dix messages ou plus sont concernés.

Partage de threat intelligence sur plusieurs vecteurs grâce au graphique des menaces Nexus de Proofpoint

Le graphique des menaces Nexus de Proofpoint permet une agrégation et une corrélation de premier plan des données sur les menaces au niveau de la messagerie électronique, du cloud, du réseau et des réseaux sociaux. Il offre une protection et une réponse aux menaces en temps réel pour tous vos produits Proofpoint. Comme il est intégré à la plate-forme Proofpoint, vous n'avez rien à installer, à déployer ni à gérer.

En devenant membre de ce réseau et en conservant une longueur d'avance sur le paysage des menaces en constante évolution, vous bénéficiez des avantages suivants :

- Threat intelligence communautaire en temps réel issue de plus de 115 000 clients
- Visibilité sur plusieurs vecteurs, notamment la messagerie électronique, le cloud, le réseau et les réseaux sociaux
- Surveillance de plus de 100 cybercriminels afin de comprendre leurs motivations et les tactiques qu'ils utilisent pour une protection renforcée

TRAP tire parti du graphique des menaces Nexus pour mettre en correspondance les destinataires et les identités des utilisateurs, en identifiant les campagnes associées et en analysant les adresses IP et les domaines de l'attaque. Il exécute ensuite des actions automatisées en fonction des utilisateurs ciblés qui appartiennent à des départements ou à des groupes spécifiques bénéficiant d'autorisations spéciales.

Par ailleurs, si nous détectons un email contenant des liens ou des pièces jointes malveillantes, ou des adresses IP suspectes sur le site d'un client, nous partageons ces informations avec notre clientèle afin qu'elle puisse s'en protéger avant la remise de l'email. Nous supprimons et mettons en quarantaine les messages qui ont été remis dans les boîtes de réception des utilisateurs.

Identification et réduction des risques de phishing avec CLEAR

Un collaborateur informé peut constituer votre dernière ligne de défense contre une cyberattaque. Grâce à Proofpoint Closed-Loop Email Analysis and Response (CLEAR), le processus de signalement, d'analyse et de neutralisation des emails potentiellement malveillants est réduit de plusieurs jours à quelques minutes seulement. Enrichi par le système de veille de Proofpoint, CLEAR bloque les attaques actives en un clic. Votre équipe de sécurité peut ainsi économiser du temps et de l'énergie en mettant automatiquement en quarantaine les messages malveillants.

CLEAR est une solution complète, qui combine les fonctionnalités de PhishAlarm, le bouton de signalement d'emails, PhishAlarm Analyzer (la solution de catégorisation et de hiérarchisation s'appuyant sur la threat intelligence de Proofpoint) et TRAP, qui enrichit les messages et automatise la mise en quarantaine des messages malveillants.

Les messages signalés sont envoyés à une boîte email de signalement d'abus pour être analysés par CLEAR, et sont surveillés et traités de la même manière par TRAP. Ils sont ensuite analysés au moyen de la threat intelligence de Proofpoint et d'autres sources de renseignements tierces afin de déterminer si une partie du contenu comprend des marqueurs malveillants. Les messages sont automatiquement extraits de la boîte de réception du destinataire.

Gestion des emails en dehors des canaux habituels

TRAP prend également en charge les fichiers CSV et Proofpoint SmartSearch. Vous pouvez charger des résultats SmartSearch ou des fichiers CSV, ou encore saisir manuellement des incidents en renseignant quelques informations clés afin de lancer une action de mise en quarantaine pour un email ou des milliers de messages. Les emails qui enfreignent les règles ou qui présentent des menaces de sécurité peuvent être extraits des boîtes de réception en quelques instants. Une liste d'activités indique qui a lu les emails, ainsi que la réussite ou l'échec de la tentative de rappel du message.

Mise en quarantaine automatique des messages transférés

Les emails malveillants et indésirables peuvent être transférés à d'autres personnes, départements ou listes de distribution. De nombreux administrateurs rencontrent des difficultés pour supprimer ces messages après leur remise. TRAP résout le problème grâce à une logique métier et une veille intégrées qui détectent quand des messages sont transférés ou envoyés à des listes de distribution. Il effectue ensuite automatiquement le suivi des destinataires pour retrouver ces messages et les supprimer. Vous gagnez ainsi un temps précieux et évitez bien des frustrations.

Optimisation du triage

TRAP offre aux analystes des centres SOC un processus de triage amélioré des emails contenant des URL. Les URL peuvent être analysées en toute sécurité grâce à la technologie Proofpoint Browser Isolation. Les analystes peuvent ainsi procéder à une évaluation du contenu de l'URL, tout en protégeant l'entreprise contre les menaces.

EN SAVOIR PLUS

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