

# 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 la réponse aux incidents
- Classification des messages au moyen du système de veille de Proofpoint
- Surveillance automatique des boîtes aux lettres 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

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.

### Mise en quarantaine automatique des emails malveillants

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 d'autres 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.

### Utilisation d'informations de cyberveille enrichies

Le système de veille de Proofpoint couvre de nombreux vecteurs de menaces : emails, réseaux sociaux, appareils mobiles, cloud et réseaux. Nous bénéficions ainsi d'une visibilité unique sur les dernières menaces et les tactiques utilisées par les cybercriminels. TRAP vous permet d'utiliser le système de veille de Proofpoint ainsi que des sources de cyberveille tierces, dont les flux STIX/TAXII, WHOIS, VirusTotal, Soltra et MaxMind.

Vous pouvez ainsi identifier les personnes, les données et les systèmes ciblés par les attaques, trier et hiérarchiser rapidement les alertes et vous libérer des tâches répétitives.

Une fois qu'un email est détecté, il est enrichi par les sources de cybersécurité susmentionnées. TRAP relie également les destinataires et les identités des utilisateurs, identifie les campagnes associées et analyse les adresses IP et les domaines de l'attaque. Vous bénéficiez ainsi d'une classification extrêmement précise des messages. En outre, vos équipes de sécurité peuvent se consacrer à d'autres tâches et n'ont plus à analyser manuellement chaque message détecté.

## 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 le système de veille 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 aux lettres 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 du système de veille de Proofpoint et d'autres sources de cybersécurité 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. Les utilisateurs peuvent 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 unique 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.

## EN SAVOIR PLUS

Pour plus d'informations, visitez notre site à l'adresse : [proofpoint.com/fr](https://www.proofpoint.com/fr)

### À PROPOS DE PROOFPOINT

Proofpoint, Inc. (NASDAQ:PFPT) est une entreprise leader dans le domaine de la cybersécurité qui protège les ressources les plus importantes et les plus à risques des entreprises : leurs collaborateurs. Grâce à une suite intégrée de solutions cloud, Proofpoint aide les entreprises du monde entier à stopper les menaces ciblées, à protéger leurs données et à rendre leurs utilisateurs plus résistants face aux cyberattaques. Les entreprises de toutes tailles, y compris plus de la moitié des entreprises de l'index Fortune 1000, font confiance aux solutions de sécurité et de conformité de Proofpoint centrées sur les personnes, pour diminuer leurs risques les plus critiques via les emails, le cloud, les réseaux sociaux et le Web. Pour plus d'informations, rendez-vous sur [www.proofpoint.com/fr](https://www.proofpoint.com/fr).

©Proofpoint, Inc. Proofpoint est une marque commerciale de Proofpoint, Inc. aux États-Unis et dans d'autres pays. Toutes les autres marques citées dans ce document sont la propriété de leurs détenteurs respectifs.