Cofense Reporter™

LES VRAIES MENACES EN TEMPS RÉEL GRÂCE AUX EMPLOYÉS

Même si Cofense Cofense aide vos employés à résister aux tentatives de phishing, s'abstenir de cliquer ne suffit pas. Pour contrer une attaque de phishing, une détection précoce est essentielle. Cette visibilité est cruciale pour permettre aux équipes de sécurité et de réponse aux incidents de limiter le temps passé par un attaquant sur votre réseau. Cof Reporter™ offre aux entreprises un moyen simple et économique de générer des rapports utilisateurs sur les e-mails suspects, qui peuvent contribuer à la détection précoce des cyberattaques.

Pourquoi choisir Cofense Reporter™ ?

Cofense a démontré sa capacité à réduire le risque que les employés soient victimes de cyberattaques de 95 %, préparant ainsi votre ligne de défense ultime pour repérer les tentatives de phishing les plus subtiles et y faire face.

Principaux avantages

- Standardise et organise le processus de signalement par les utilisateurs
- Détecte les menaces par e-mail et y répond plus rapidement grâce aux signalements effectués par les utilisateurs
- Analyse les URL et les pièces jointes malveillantes au moyen d'intégrations tierces
- Réduit l'impact des failles de sécurité grâce à une réponse proactive et à une visibilité accrue
- Le retour d'information personnalisé à l'utilisateur encourage le personnel à prendre part aux procédures de sécurité

En quoi consiste Cofense Reporter™ ?

Lorsque les défenses techniques comme le filtrage proxy, la réécriture d'URL et le DLP échouent, les utilisateurs constituent l'ultime défense face aux attaques. S'ils sont correctement formés, ils peuvent fournir à temps des informations précieuses en identifiant et en signalant simplement les e-mails suspects. Les entreprises ont tenté d'exploiter cette ressource, en vain. Par conséquent, les activités malveillantes perdurent souvent pendant des semaines, voire des mois sur leur réseau.

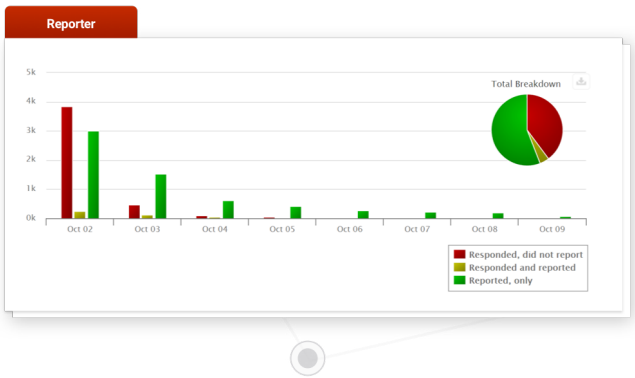
Cofense Reporter rationalise le processus de signalement en installant un module d'extension dans la barre d'outils de la messagerie des utilisateurs. Lorsqu'ils cliquent dessus, le système envoie l'e-mail suspect concerné à votre service de sécurité, avec les informations pertinentes nécessaires pour procéder à une analyse et répondre à la menace.

Reporter fait automatiquement la différence entre les e-mails signalés à partir des scénarios de Cofense PhishMe et les e-mails signalés par des sources inconnues, ce qui garantit que seuls les signalements d'e-mails potentiellement malveillants sont envoyés au personnel approprié ou à Cofense Triage pour analyse.

Amélioration du signalement

Que vous ayez ou non mis en place des procédures de signalement, Reporter vous aide de la manière suivante :

- **en conservant l'en-tête complet des e-mails signalés, ce qui permet aux spécialistes de bloquer et de supprimer les messages similaires ;**
- **en garantissant que les pièces jointes et les URL sont incluses ;**
- **en complétant les campagnes Simulator par le suivi des réponses des utilisateurs et le temps passé par l'entreprise à réagir.**



Cet e-mail est-il un scénario Cofense ?

OUI.

ENREGISTRER LE SIGNALEMENT UTILISATEUR DANS COFENSE

« REMERCIER » L'UTILISATEUR

CLIC !

« Que se passe-t-il lorsque je clique sur le bouton ?... »

NON, IL S'AGIT D'UNE MENACE RÉELLE.

SIGNALER L'E-MAIL À L'ÉQUIPE DE RÉPONSE AUX INCIDENTS

« REMERCIER » L'UTILISATEUR

ENVOYER À TRIAGE OU À L'ÉQUIPE DE SÉCURITÉ INTERNE POUR ANALYSE ET DÉTERMINATION DE LA MARCHE À SUIVRE

E-mails Cofense PhishMe

Reporter récupère les signalements d'e-mails envoyés à partir de Simulator, y compris l'utilisateur à l'origine du signalement, et lui confirme de manière personnalisée qu'il a bien été reçu. L'envoi d'une confirmation permet d'améliorer la capacité du personnel à identifier avec précision les cyberattaques. Ces informations font l'objet d'un suivi et sont intégrées aux mesures de signalement complètes de Cofense.

E-mails inconnus suspects

Les signalements d'e-mails inconnus suspects sont transmis à un emplacement désigné ou à Triage. Ils y sont analysés par l'équipe de sécurité interne de l'entreprise. Les e-mails suspects sont envoyés avec leur en-tête d'origine et des informations contextuelles pour une analyse rapide. Lors de l'utilisation de Triage, les équipes de sécurité et de réponse aux incidents peuvent organiser leur analyse selon divers facteurs, notamment la capacité de l'utilisateur à identifier avec précision les tentatives de phishing.

Cofense™, anciennement PhishMe®, est le leader mondial, dirigée par l'être humain, de solutions de défense contre le Phishing des entreprises qui craignent d'être compromises par des cyberattaques sophistiquées. Cofense met en œuvre une démarche collaborative en matière de cybersécurité en permettant à l'ensemble de votre organisation de réagir face au vecteur d'attaque le plus courant : le Phishing. Cofense répond aux besoins d'organisations diverses de toutes tailles, notamment dans les secteurs des services financiers, de l'énergie, de l'administration, de la santé, de la technologie, de la production et bien d'autres encore, figurant parmi les 1000 sociétés les plus grandes du monde. Ces entreprises perçoivent l'impact considérable du changement des comportements des utilisateurs pour améliorer la sécurité, réagir rapidement aux incidents et réduire le danger de pénétration

COFENSE

Pour en savoir plus, contactez :

Site Web : cofense.com/contact Tél. : 703 652 0717
Adresse : 1608 Village Market Blvd, SE #200
Leesburg, VA 20175, États-Unis