KnowBe4
Human error. Conquered.

8 capacités essentielles pour évaluer les plateformes SOAR

Renforcer la sensibilisation à la sécurité devrait toujours être la priorité absolue des organisations qui cherchent à améliorer leurs défenses contre l'hameçonnage. Mais à mesure que les cybercriminels continuent d'affiner leurs tactiques, la nécessité d'une stratégie de défense robuste et complète contre l'hameçonnage est devenue primordiale. Les équipes du centre des opérations de sécurité (Security Operation Center, SOC) et de réponse aux incidents (Incident Response, IR) ont besoin d'outils leur permettant d'enquêter rapidement sur les attaques par hameçonnage et de les bloquer avant qu'elles ne causent des dommages.

Les produits anti-hameçonnage SOAR (Sécurité, Orchestration, Automatisation et Réponse) se sont imposés comme des outils puissants dans la lutte contre l'hameçonnage, offrant une approche unifiée qui combine technologie et expertise humaine. Ils constituent désormais un élément essentiel pour les professionnels de la sécurité informatique qui cherchent à contrer la menace croissante des attaques par hameçonnage et des campagnes d'harponnage ciblées.

Mais tous les produits SOAR ne se valent pas. Un bon produit SOAR doit avant tout automatiser l'analyse et la hiérarchisation des e-mails réellement malveillants afin d'éliminer la part d'incertitude dans l'identification des menaces d'hameçonnage à haut risque. En outre, au cours des dernières années, de nouvelles fonctionnalités puissantes ont permis aux produits SOAR de passer d'une analyse et d'une identification réactives à une atténuation proactive de l'hameçonnage. Il est important de comprendre ces capacités et ces avancées pour évaluer le marché.

Au moment de choisir un produit SOAR pour la défense anti-hameçonnage de votre organisation, voici les huit capacités que vous devez privilégier.

N°1 DONNER À VOS UTILISATEURS FINAUX LES MOYENS DE LUTTER

La défense d'une organisation contre les menaces d'hameçonnage et de piratage psychologique repose avant tout sur les utilisateurs finaux. C'est leur capacité à identifier et à signaler les cybermenaces qui permet à votre organisation de se protéger contre les attaques par hameçonnage et de réduire le risque qu'elles représentent. Un bon produit SOAR doit permettre à vos utilisateurs finaux d'accomplir cette tâche.

Il s'agit, dans un premier temps, de pouvoir signaler facilement les e-mails suspects. Un bouton de type « Phish Alert Button », intégré au client de messagerie de votre organisation, doit permettre aux utilisateurs de signaler les e-mails suspects à une boîte de réception informatique prédéfinie ou directement à la plateforme SOAR.

Deuxièmement, un produit SOAR doit inclure des modèles et des réponses par e-mail automatisées afin que votre équipe responsable de la sécurité de l'information puisse communiquer rapidement avec les employés au sujet des e-mails qu'ils ont signalés et déterminer ainsi si ces e-mails étaient en fait de simples courriers indésirables ou des messages légitimes (90 % du trafic).

N°2 APPRENTISSAGE AUTOMATIQUE ET IA

Une protection efficace contre l'hameçonnage est garantie par une plateforme SOAR qui tire parti de l'intelligence artificielle (IA) et de l'automatisation. Les équipes IR et SOC en sous-effectif ne peuvent agir seules. En s'appuyant sur l'IA et l'automatisation, elles peuvent identifier et hiérarchiser les menaces d'hameçonnage plus facilement, plus rapidement et avec plus de précision.

L'IA et l'automatisation accélèrent considérablement les capacités énumérées ci-dessous grâce à leur évolutivité, leur précision et leur atténuation proactive :

- analyse automatique et hiérarchisation des e-mails pour identifier rapidement les menaces d'hameçonnage à haut risque parmi tous les messages signalés par les utilisateurs ;
- automatisation du flux de travail de sécurité pour gérer les « 90 % restants » des e-mails signalés par les utilisateurs ;

- réponses par e-mail automatisées pour permettre au service informatique de communiquer rapidement avec les employés ;
- regroupement des messages grâce à une reconnaissance basée sur un modèle d'apprentissage automatique permettant aux équipes de réponse aux incidents d'identifier une attaque par hameçonnage à grande échelle ;
- liste de blocage automatisée, veille sur les menaces auprès de l'ensemble des utilisateurs et atténuation proactive de l'hameçonnage ;
- possibilité de sélectionner des attaques par hameçonnage réelles pour les transformer en modèles d'hameçonnage simulés afin de former vos employés.

N°3 ANALYSE ET HIÉRARCHISATION AUTOMATISÉES DES MENACES

De nombreuses équipes IR et SOC s'appuient encore sur des flux de travail manuels pour trier un e-mail suspect. En moyenne, 27 minutes sont nécessaires pour trier manuellement un e-mail d'hameçonnage [1]. Un délai de réponse trop long augmente le risque et les dommages potentiels d'une attaque par hameçonnage.

Pour protéger efficacement votre organisation et préserver la santé mentale de votre équipe de sécurité, mettez en œuvre un produit SOAR qui tire parti d'une analyse et d'une hiérarchisation des e-mails basées sur l'apprentissage automatique. Ainsi, plus aucune incertitude lorsqu'il s'agit d'identifier les menaces d'hameçonnage à haut risque parmi le flot d'e-mails signalés par les utilisateurs.

Assurez-vous que le produit que vous évaluez utilise l'apprentissage automatique pour hiérarchiser automatiquement les e-mails signalés sans interaction humaine. Il s'agit notamment de classer les e-mails dans différentes catégories, par exemple « Sain », « Spam » ou « Menace », et de classer les e-mails suspects par priorité en analysant un ensemble d'attributs, tels que l'objet, l'expéditeur, le destinataire, les pièces jointes, le corps du message, etc.

Comme son nom l'indique, une plateforme d'apprentissage automatique doit aussi apprendre. À mesure que de nouvelles données sont introduites dans le système, par exemple via les e-mails signalés par vos utilisateurs finaux, les données provenant de votre équipe SOC ou la veille sur les menaces vérifiées grâce à un flux d'intelligence tiers, la précision de la plateforme doit constamment s'améliorer. Elle pourra ainsi hiérarchiser automatiquement plus d'e-mails, avec encore plus de précision.

L'analyse et la hiérarchisation des e-mails constituent la base de tout bon produit SOAR. Les e-mails seront ainsi triés plus facilement, plus rapidement et avec plus de précision.

---

1 The Business Cost of Phishing, 2022 Report (Rapport 2022 sur le coût de l'hameçonnage)

N°4 MISE EN QUARANTAINE ET SUPPRESSION

Dès qu'une menace d'hameçonnage est identifiée, il est primordial de pouvoir mettre en quarantaine et de supprimer les e-mails d'hameçonnage similaires des boîtes de réception de tous les utilisateurs. Dans un monde où les menaces peuvent venir d'États et d'attaques par harponnage ciblées, il est crucial de pouvoir limiter l'hameçonnage à grande échelle.

Cette capacité de mise en quarantaine des e-mails doit être directement intégrée aux services de courrier électronique tiers tels que Microsoft 365 ou Google Workspace. Vous pourrez ainsi :

- **Supprimer**
  Une fois la menace identifiée, votre équipe SOC doit pouvoir supprimer les messages identiques ou similaires de tous les dossiers de messagerie : boîte de réception, messages envoyés, corbeille, etc.

- **Prévenir**
  Les utilisateurs finaux ne signalent pas tous les e-mails suspects. Pour ceux qui ne le font pas, vous devez être en mesure de surveiller et de détecter ces e-mails afin de les signaler, de les mettre en quarantaine et, enfin, de les analyser.

- **Protéger**
  Une analyse rétrospective est essentielle pour bloquer la prochaine attaque. Une fois les menaces immédiates atténuées, les capacités d'envoyer des communications de suivi aux utilisateurs concernés, de supprimer les messages des boîtes aux lettres de vos utilisateurs, de les maintenir en quarantaine ou de restaurer les messages identifiés comme légitimes sont autant de fonctionnalités qui devraient figurer sur votre liste de contrôle des capacités clés lors de l'évaluation d'un produit.

N°5 LISTE DE BLOCAGE

La mise en place d'une liste de blocage est la meilleure approche proactive pour empêcher les e-mails malveillants d'atteindre les boîtes de réception de vos utilisateurs. Les services de courrier électronique tels que Microsoft 365 et Google offrent une fonctionnalité de blocage de base, mais qui n'est pas suffisante pour bloquer les e-mails d'hameçonnage créés par l'intelligence artificielle.

Tout produit SOAR que vous évaluez doit renforcer les filtres de courrier électronique existants de votre organisation en offrant des capacités de blocage supérieures qui s'appuient sur les commentaires des utilisateurs finaux et l'analyse d'e-mails basée sur l'apprentissage automatique.

Il doit permettre aux équipes IR et SOC de bloquer les e-mails sur la base d'un ensemble d'attributs et de valeurs, tels que l'expéditeur, l'URL, les pièces jointes ou le hachage du fichier. En outre, la fonctionnalité de création de règles basées sur des conditions est plus efficace que celle des services de courrier électronique tiers.

Enfin et surtout, pour garder une longueur d'avance sur le paysage des menaces et atténuer de manière proactive les attaques par hameçonnage avant qu'elles ne frappent votre organisation, un produit SOAR de niveau entreprise doit permettre la mise en place d'une liste de blocage de haut niveau en exploitant la puissance de l'IA et la veille sur les menaces auprès de l'ensemble des utilisateurs. Pour plus d'informations, reportez-vous au point n°6.

N°6 VEILLE SUR LES MENACES AUPRÈS DE L'ENSEMBLE DES UTILISATEURS ET PROTECTION ANTI-HAMEÇONNAGE PROACTIVE

Même les équipes SOC et IR les plus importantes et les mieux dotées en ressources ne peuvent éviter d'être la cible de menaces d'hameçonnage et de pirates psychologiques. Les menaces sont trop diverses, en constante évolution, et de plus en plus sophistiquées. L'IA a permis aux cybercriminels de créer de nouveaux e-mails d'hameçonnage capables d'échapper aux filtres de sécurité traditionnels.

Dans le monde de la défense anti-hameçonnage, faire preuve de proactivité est donc le mot d'ordre. La plateforme SOAR que vous mettez en œuvre doit servir de vigie, en intégrant de manière transparente et en temps réel les données sur les menaces. Les dernières informations sur les menaces émergentes étant à portée de main, vous pouvez vous adapter et réagir rapidement.

C'est la raison pour laquelle les organisations font de plus en plus appel à des fournisseurs de cybersécurité sous la forme de hubs de veille sur les menaces. Votre fournisseur SOAR doit mettre en place une veille sur les menaces auprès des utilisateurs et des listes de blocage gérées par l'IA pour mettre en quarantaine et supprimer automatiquement les menaces d'hameçonnage des boîtes de réception de vos utilisateurs en se basant sur des menaces d'hameçonnage réelles vérifiées que des millions d'autres utilisateurs finaux ont déjà signalées.

La veille sur les menaces auprès des utilisateurs permet de repérer les menaces qui ont franchi tous les autres filtres. Elle fournit une couche supplémentaire de protection contre les e-mails malveillants qui échappent aux passerelles de courrier électronique sécurisées et se retrouvent dans les boîtes de réception de vos utilisateurs. Selon ArmorBlox, 56 % des attaques par courrier électronique ont contourné les filtres de sécurité traditionnels en 2022, et 18,8 % des e-mails d'hameçonnage ont contourné Microsoft Exchange Online Protection et Defender pour arriver dans la boîte de réception d'un utilisateur, selon un rapport de la Check Point Email Research Team [2].

N°7 FLUX DE TRAVAIL PERSONNALISABLES

Il n'existe pas de solution universelle en matière d'analyse et d'atténuation de l'hameçonnage. Les flux de travail et les processus varient d'une organisation à l'autre. Choisissez une plateforme SOAR qui offre la flexibilité nécessaire pour adapter les flux d'automatisation aux besoins spécifiques de votre organisation. Qu'il s'agisse d'analyser des e-mails suspects, de catégoriser des incidents ou de générer des réponses prédéfinies, la personnalisation est essentielle.

---

2 Check Point Microsoft Defender Report (Rapport Check Point Microsoft Defender)

N°8 TRANSFORMER LES ATTAQUES PAR HAMEÇONNAGE EN MATÉRIEL DE FORMATION

De nombreuses organisations soumettent les utilisateurs à des tests en leur demandant d'identifier et de signaler des e-mails d'hameçonnage qui ressemblent beaucoup à des menaces réelles. Un produit SOAR doit faciliter considérablement cette procédure en offrant la possibilité de « transformer » un e-mail d'hameçonnage malveillant en une opportunité de formation réelle pour vos utilisateurs. Cette capacité contribuera également à renforcer votre programme existant de formation sur la sensibilisation à la sécurité.

Les menaces par e-mail qui ont été signalées et supprimées doivent servir à créer une version « modifiée », puis à lancer automatiquement une simulation de campagne d'hameçonnage à l'intention des utilisateurs. Cela doit inclure la possibilité de remplacer les vrais e-mails d'hameçonnage arrivés dans la boîte de réception de vos utilisateurs (mais qui n'ont pas encore été ouverts) par la version « modifiée », permettant ainsi aux utilisateurs d'être plus vigilants face aux menaces réelles.

RÉSULTAT

Pour que votre organisation reste opérationnelle, la lutte contre les attaques par hameçonnage nécessite une stratégie globale. Les outils SOAR, avec leurs capacités d'orchestration, d'automatisation et de réponse, vous offrent une formidable ligne de défense.

Le marché des produits SOAR anti-hameçonnage est aussi diversifié que les menaces de piratage psychologique qu'ils sont censés atténuer. En fin de compte, le produit SOAR que vous mettez en œuvre devra réduire de façon optimale le temps moyen de réponse et atténuer les menaces d'hameçonnage avant qu'elles n'atteignent les boîtes de réception de vos utilisateurs, tout en renforçant les défenses existantes de votre organisation en matière de sécurité du courrier électronique. Il doit soulager votre équipe informatique en lui facilitant la tâche grâce à l'automatisation gérée par l'IA et à la veille sur les menaces auprès des utilisateurs, de sorte que vos équipes de sécurité puissent se concentrer sur l'orchestration et l'analyse tout en réduisant le risque que représente l'hameçonnage pour votre organisation.

KNOWBE4 PHISHER PLUS

PhishER Plus est un produit SOAR léger conçu pour orchestrer votre réponse aux menaces d'hameçonnage et pour booster les défenses de sécurité du courrier électronique de votre organisation. PhishER Plus combine une analyse efficace des e-mails basée sur l'apprentissage automatique, des capacités d'inoculation par ordre de priorité et de liste de blocage avec le flux de menaces global le plus puissant du secteur pour garantir une protection proactive contre l'hameçonnage.

PhishER Plus est alimenté par un flux de menaces global triplement validé qui bloque automatiquement les attaques par hameçonnage avant qu'elles n'atteignent les boîtes de réception de vos utilisateurs. Le flux de menaces global de PhishER Plus est alimenté par trois composants essentiels :

1. le réseau mondial KnowBe4, qui compte plus de 10 millions d'utilisateurs finaux ayant reçu une formation de pointe, ainsi que leurs administrateurs PhishER ;
2. PhishML, une intelligence artificielle entraînée à détecter les e-mails d'hameçonnage que les autres filtres n'ont pas repérés ;
3. des informations sur les menaces traitées par des êtres humains au sein du laboratoire d'identification des menaces KnowBe4.

Identifiez et répondez plus rapidement aux menaces d'hameçonnage avec PhishER Plus de KnowBe4.

En savoir plus

Demandez une démonstration de PhishER Plus de KnowBe4.

Demander une démonstration

Ressources supplémentaires

Test de sécurité gratuit relatif à l'hameçonnage
Découvrez le pourcentage de Phish-Prone (pourcentage de vulnérabilité à l'hameçonnage) de vos employés, en profitant de votre test de sécurité gratuit relatif à l'hameçonnage.

Programme automatisé de sensibilisation à la sécurité gratuit
Créez un programme de sensibilisation à la sécurité, personnalisé pour votre organisation.

Outil Phish Alert Button gratuit
Un seul clic suffit désormais à vos employés pour signaler les attaques par hameçonnage de manière sécurisée.

Outil Email Exposure Check (EEC) gratuit
Identifiez avant les pirates les adresses e-mail à risque de vos utilisateurs.

Outil Domain Spoof Test gratuit
Déterminez si les pirates peuvent usurper une adresse e-mail de votre domaine.

À propos de KnowBe4

KnowBe4 est le fournisseur de la plus grande plateforme de formation sur la sensibilisation à la sécurité et de simulation d'hameçonnage au monde. Née du constat selon lequel l'aspect humain de la sécurité était largement négligé, KnowBe4 a pour objectif d'aider les organisations à gérer la menace permanente de l'ingénierie sociale par le biais d'une approche globale et innovante de la formation sur la sensibilisation.

Cette méthode intègre un dispositif de test de référence basé sur des simulations d'attaques réelles, une formation interactive au contenu stimulant, un système d'évaluation continue reposant sur des simulations d'attaques par hameçonnage, ainsi qu'un état des lieux des points forts de l'entreprise. Elle a pour but de développer une organisation plus résiliente, ayant pour priorité la sécurité.

Dans le monde entier, des dizaines de milliers d'organisations de tous les secteurs d'activité utilisent la plateforme KnowBe4, y compris dans des domaines très réglementés tels que la finance, la santé, l'énergie, l'administration et les assurances. Elles mobilisent ainsi leurs utilisateurs finaux, qui constituent leur dernière ligne de défense, et leur permettent de prendre des décisions plus avisées en matière de sécurité.

Pour en savoir plus, consultez la page www.KnowBe4.com

KnowBe4
Human error. Conquered.

KnowBe4 NL, BV | Papendorpseweg 99, 3528 BJ Utrecht, Pays-Bas
Tél. : +31 (0)30 7996074 | www.KnowBe4.com | E-mail : Sales@KnowBe4.com

01D09K01