Proofpoint Domain Discover

Identification des domaines frauduleux et intervention

FONCTIONNALITÉS DU PRODUIT

- Découverte
- Classification
- Investigation
- Notification
- Intervention
- Rapports

Proofpoint Domain Discover vous permet d'identifier les domaines frauduleux qu'utilisent les cybercriminels pour tromper vos collaborateurs, clients et partenaires, puis de prendre les mesures appropriées. Proofpoint Domain Discover analyse en continu les nouveaux domaines enregistrés à l'aide d'un système de détection hautement évolutif. S'il découvre un domaine qui constitue un risque pour votre sécurité ou votre marque, par exemple, il vous alerte et vous permet d'intervenir.

La qualité de notre cyberveille et l'étendue de notre couverture contribuent à une identification précise des domaines et des URL qui présentent des risques pour votre entreprise et vos clients, notamment en termes de sécurité et de marque commerciale. Notre visibilité étendue sur tous les canaux numériques, notamment la messagerie électronique, vous permet de faire le lien entre les domaines suspects et les attaques actives telles que le phishing, le piratage de la messagerie en entreprise, les malwares, etc.

Voici une vue d'ensemble des fonctionnalités de Proofpoint Domain Discover :

Découverte

La solution identifie les domaines associés à votre entreprise.

- Elle surveille les sources de données WHOIS, en analysant plus de 350 millions d'URL par jour.
- Elle utilise un système de détection automatisé (piloté par l'intelligence artificielle, l'apprentissage automatique et le traitement du langage naturel) pour analyser les domaines en continu afin de repérer les fraudes, les domaines usurpés et le typosquattage.

Classification

La solution détecte et balise les risques liés aux domaines pour vous offrir une meilleure visibilité sur les menaces potentielles. Proofpoint Domain Discover classe les domaines par niveau de risque pour vous aider à identifier rapidement les domaines à risque moyen ou haut.

De plus, il analyse les données Proofpoint sur les activités email et les attaques actives afin de détecter rapidement les domaines impliqués dans des campagnes de phishing ou d'autres attaques.

- Domaines défensifs appartenant à la marque
- Domaines frauduleux récupérés par l'entreprise
- Score de risque (haut, moyen)
- État du domaine (actif, inactif, en sommeil, inconnu ou supprimé)
- Etc.

Investigation

La solution collecte des informations détaillées sur les domaines.

Par exemple :

- Nom et adresse email du titulaire
- Bureau d'enregistrement
- Données d'enregistrement
- Numéro ASN
- Enregistrements MX
- Détails du certificat de sécurité
- Instantanées du contenu Web
- Etc.

Notification

La solution envoie des alertes instantanées lorsqu'elle détecte des domaines à risque.

Vous pouvez créer des messages de notification et des listes de destinataires personnalisés en fonction de facteurs tels que :

- Type de classification du domaine
- État d'origine et état modifié (actif, inactif, en sommeil, inconnu ou supprimé)
- Ajout d'enregistrements MX
- Etc.

Intervention

Vous pouvez agir contre les domaines malveillants grâce à des workflows intégrés, disponibles en option :

Module complémentaire Virtual Takedown (offre Proofpoint) :

- Placez rapidement sur liste de blocage les domaines les plus risqués afin de limiter l'exposition de vos collaborateurs, partenaires et clients.
- Bloquez l'accès grâce à des listes de blocage HTTP/HTTPS, DNS et SMTP largement utilisées.
- Aucune intervention n'est nécessaire auprès de l'hébergeur ou du bureau d'enregistrement.

Module complémentaire de mise hors service traditionnelle (solution partenaire) :

- Désactivez et mettez hors service de façon permanente les domaines illicites.
- Intervenez auprès du bureau d'enregistrement et/ou de l'hébergeur afin de désactiver l'infrastructure d'hébergement et de supprimer le domaine de façon définitive.
- Lancez une procédure UDRP/URS pour contrefaçon de marque.

Parmi les options de correction supplémentaires, citons l'exportation de listes de domaines à bloquer au niveau de la passerelle de messagerie, etc.

Rapports

La solution permet d'évaluer et de détailler les menaces liées aux domaines, ainsi que les mesures prises, grâce à des rapports clairs.

EN SAVOIR PLUS

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