

Cloudflare Area 1 – Solution de sécurité des e-mails

Déployez une protection préventive de vos utilisateurs contre l'hameçonnage, la compromission des adresses e-mail professionnelles et les attaques par e-mail sur la chaîne logistique.



L'hameçonnage est l'une des cybermenaces les plus fréquentes et coûteuses auxquelles sont confrontées les organisations.

Cloudflare Area 1 est une plateforme cloud-native de sécurité des e-mails, qui identifie et bloque les attaques avant qu'elles n'atteignent les boîtes de réception des utilisateurs, offrant ainsi une protection plus efficace contre l'hameçonnage ciblé, la compromission des adresses e-mail professionnelles et d'autres menaces avancées qui échappent aux défenses existantes.

Le service Area 1 renforce la sécurité nativement proposée par les fournisseurs de messagerie dans le cloud grâce à l'intégration en profondeur aux environnements et aux flux de production Microsoft et Google.

Area 1 fait partie de nos services Zero Trust.

Arrêtez les menaces liées à l'hameçonnage ciblé

Area 1 offre une protection contre un large éventail d'attaques par hameçonnage, des campagnes à grande échelle aux tentatives de compromission par e-mail de la chaîne logistique très ciblées, préparées depuis des mois.



Hameçonnage

Le rapport Verizon DBIR de 2021 cite l'hameçonnage comme la tactique de violation la plus courante. En associant l'indexation à très grande échelle du web, l'analyse de données reposant sur des petits modèles et des détections améliorées, Area 1 peut arrêter les attaques par hameçonnage plusieurs jours avant qu'elles n'atteignent les boîtes de réception des utilisateurs.



Compromission des adresses e-mail professionnelles et menaces reposant sur l'ingénierie sociale

Lors de la compromission des adresses e-mail professionnelles, les auteurs d'une attaque se font passer pour des entités de confiance ou compromettent celles-ci avec l'objectif de dérober de l'argent et des données. Area 1 analyse le contenu et le contexte des communications par e-mail afin de mettre un terme à ces menaces « indétectables ».



Attaques par e-mail sur la chaîne logistique

Les auteurs d'une attaque compromettent le compte de messagerie d'un fournisseur, observent les modèles d'envoi et de réception d'e-mails et interceptent les conversations existantes pour exécuter une fraude à la facture. Area 1 analyse les fils de messages, le sentiment des messages et les graphes sociaux pour arrêter ces attaques sophistiquées.



E-mails d'extorsion et contenant des rançongiciels

Gartner estime que 40 % des attaques par rançongiciel commencent par un e-mail. Area 1 contribue à offrir une protection proactive contre les e-mails contenant un rançongiciel avant qu'ils n'atteignent les utilisateurs finaux, et supprime également les messages malveillants avant qu'ils ne se propagent.

Une solution supérieure aux passerelles e-mail traditionnelles



Préventive

Identifiez à l'avance l'infrastructure et les mécanismes de diffusion employés par les auteurs d'attaques afin d'arrêter l'hameçonnage dès les premières étapes du cycle d'une attaque.



Contextuelle

Tirez profit de techniques de détection avancées (analyse du langage, vision artificielle, analyse graphique sociale, etc.) pour arrêter la compromission des adresses e-mail professionnelles, l'utilisation frauduleuse des adresses e-mail de fournisseurs et les autres menaces sans charge utile.



Complet

La solution couvre l'intégralité des types d'attaques reposant sur les e-mails (URL, charges utiles, compromission des adresses e-mail professionnelles), des vecteurs (e-mail, web, réseau) et des canaux d'attaque (externe, interne, partenaires de confiance).



Continue

Déployez une défense approfondie avec des couches de protection contre les menaces placées avant, pendant et après la réception d'un e-mail.

Avantages

Améliorez la sécurité native de votre messagerie

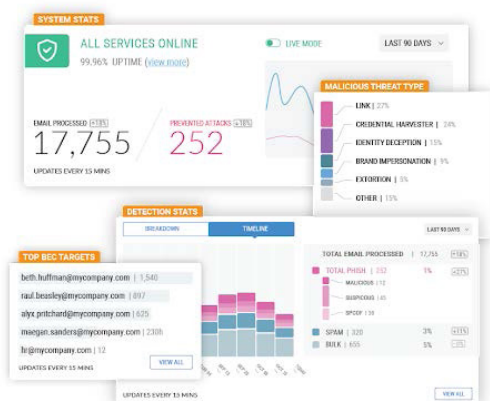
Évitez que les attaques avancées par hameçonnage et par compromission des adresses e-mail professionnelles n'échappent à vos couches de sécurité intégrées. Tirez parti d'intégrations profondes dans les environnements de messagerie dans le cloud, avec un impact minime, voire nul sur la productivité de la messagerie.

Adoptez une architecture orientée cloud

Évitez la lourdeur et le manque de flexibilité d'une passerelle de messagerie traditionnelle et optez plutôt pour une architecture moderne et évolutive. Réduisez les dépenses liées aux couches de sécurité qui dédoublent les fonctionnalités natives de sécurité des e-mails.

Un gain de temps pour l'équipe du centre d'opérations de sécurité

Déployez la solution en quelques minutes, sans installer d'équipements physiques ni d'agents. Libérez du temps qui serait autrement consacré à la création et la configuration de politiques. Accélérez les enquêtes du centre d'opérations de sécurité grâce aux intégrations SIEM et SOAR.



Demandez une évaluation des risques d'hameçonnage

Demandez l'exécution du service de sécurité des e-mails Area 1 en conditions réelles sur le trafic de vos e-mails de production et découvrez, en temps réel, quelles attaques par e-mail parviennent à franchir vos mesures de sécurité existantes.

L'évaluation ne requiert aucune installation d'équipements physiques ou logiciels et n'aura aucune incidence sur la transmission de vos e-mails.

Demandez votre évaluation [ici](#).