Barracuda **Sentinel**

L'intelligence artificielle au service de la protection de la messagerie en temps réel

Les attaques d'e-mails frauduleux, le spear phishing et le piratage de comptes sont rapidement devenus les menaces les plus importantes pour les organisations. Ces attaques très ciblées appliquent des tactiques d'ingénierie sociale, conçues pour tromper les employés. Leurs conséquences peuvent être dévastatrices pour votre entreprise et pour votre marque.

Barracuda Sentinel combine l'intelligence artificielle, l'intégration en profondeur de Microsoft Office 365 et la protection des marques dans une solution cloud qui vous protège des attaques par e-mails frauduleux, du piratage des comptes, du spear phishing et d'autres cyberfraudes.

L'avantage Barracuda

- Une IA qui apprend vos modèles de communication pour détecter en temps réel les fraudes personnalisées
- La seule solution sur le marché avec une architecture basée sur les API capable de bloquer les menaces qui émanent de votre organisation et qui échappent aux passerelles classiques.
- Une solution complète pour détecter et bloquer le piratage des comptes

Caractéristiques du produit

- L'architecture avec API assure une connectivité directe à Office 365
- Une solution IA pour la protection en temps réel des attaques ciblées
- Protection des marques grâce au reporting et à la mise en application DMARC
- Fonctionne avec toutes les autres solutions de sécurité de la messagerie, y compris Barracuda Essentials, la sécurité intégrée à Office 365, etc.
- La configuration cloud s'effectue rapidement et ne nécessite pas de rediriger le trafic de la messagerie.

AI

Défense en temps réel contre le piratage de comptes professionnels

Le moteur IA qui constitue le cœur de Barracuda Sentinel détecte et bloque en temps réel les attaques par ingénierie sociale et identifie les employés les plus exposés

Son architecture unique basée sur des API permet au moteur IA de Sentinel d'accéder aux données historiques de la messagerie afin d'apprendre des habitudes de communication de chaque utilisateur. Le moteur s'appuie sur de multiples éléments de classement pour dresser la carte des réseaux sociaux de chaque membre de l'entreprise et il identifie tout signal anormal dans les métadonnées et dans le contenu des messages.

L'approche unique de Sentinel n'utilise pas de règles statiques pour détecter les attaques ciblées. Elle exploite les statistiques historiques de chaque organisation pour déterminer avec précision si un message fait partie d'une attaque par ingénierie sociale ou d'un piratage de compte.

Protection contre le piratage de compte et les risques internes

Tous les jours, des comptes professionnels sont piratés à l'aide d'informations d'identification volées. Le piratage de compte peut rester en sommeil plusieurs mois dans votre environnement, ce qui permet aux pirates d'étudier votre organisation avant de passer à l'attaque Les attaques internes lancées à partir d'un compte piraté ne passent en général pas par la passerelle et ne sont donc pas détectées.

La solution complète de Barracuda Sentinel pour lutter contre le piratage de compte s'articule autour de trois axes : prévention, détection et restauration. Barracuda Sentinel bloque les attaques par phishing (hameçonnage) ciblé qui contournent les passerelles classiques et peuvent déboucher sur la collecte d'informations d'identification. Si un compte a été piraté, Barracuda Sentinel détecte tout comportement anormal et alerte les services informatiques. Enfin, Barracuda Sentinel peut remédier à l'attaque en supprimant en un clic de la boîte aux lettres de l'employé tous les messages malveillants envoyés par le compte piraté.

Protection des marques et visibilité de la fraude au domaine

L'usurpation de domaine et le détournement de marque sont des techniques classiques employées par les pirates dans le cadre des attaques par ingénierie sociale. L'usurpation de domaine peut servir à cibler les employés, les clients et les partenaires de l'entreprise, ainsi que tout autre acteur qui accorde sa confiance à cette marque.

Barracuda Sentinel offre une protection complète contre la fraude au domaine de messagerie via le reporting, l'analyse et la visibilité DMARC (Domain-based Message Authentication Reporting and Conformance). Barracuda Sentinel comporte un assistant intuitif pour aider les entreprises à configurer facilement l'authentification DMARC Une fois DMARC configurée, elle assure une visibilité et une analyse précises des rapports DMARC. Les clients peuvent ainsi correctement mettre en œuvre la technologie DMARC et réduire les faux positifs.

Une fois l'application DMARC correctement configurée, les messages légitimes arrivent à leur destinataire et les messages d'usurpation non autorisés sont bloqués.

Principales caractéristiques

Intelligence artificielle pour la protection en temps réel

- Blocage des attaques de spear phishing en temps réel
- Utilisation de l'intelligence artificielle pour comprendre les modèles de communication propres à chaque entreprise
  - Cartographie des réseaux sociaux de l'entreprise pour comprendre les modèles de communication typiques
  - Identification des anomalies dans les métadonnées et le contenu
- Notification en temps réel
  - Mise en quarantaine automatique des messages
  - Alerte des administrateurs et des utilisateurs Notifications en temps réel
  - Visibilité sur les communications internes et l'historique des communications
- Protection complète contre les attaques personnalisées, appelées spear phishing, les attaques BEC, le whaling, les tentatives d'usurpation d'identité et/ou la fraude aux présidents

Protection contre le piratage de comptes

- Défense et restauration en temps réel

Protection contre l'usurpation de nom de domaine

- Authentification et analyse DMARC pour empêcher :
  - Le détournement de marque
  - L'usurpation de nom de domaine
- Assistant intuitif pour configurer l'authentification DMARC
- Analyse des rapports DMARC pour savoir qui envoie le courrier à partir de chaque domaine
- Livraison garantie des messages légitimes
- Procédure étape par étape permettant de respecter le protocole DMARC

Analyse des employés avec profil à haut risque

- S'appuyer sur l'intelligence artificielle pour identifier le personnel de l'entreprise qui présente un profil à haut risque

Déploiement et disponibilité

Disponible pour les utilisateurs de Microsoft Office 365 partout dans le monde

Solution 100 % cloud

- Ni matériel ni logiciel à installer ou gérer

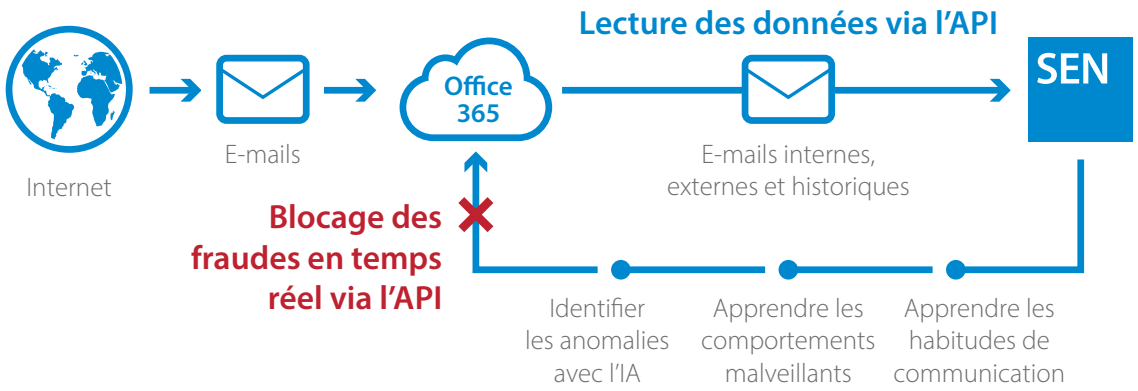
Compatible avec toutes les solutions de protection de messagerie

- Barracuda Essentials : protection, archivage et sauvegarde pour Office 365
- Barracuda Email Security Gateway
- Microsoft Exchange Online Protection (EOP)
- Autres

Architecture API

- Connectivité directe à Office 365
- Aucune incidence sur les performances réseau ou l'expérience utilisateur
- Configuration simple et rapide (moins de 5 minutes)

Fonctionnement de Sentinel



Tarification par utilisateur et par an. Des remises sont offertes aux clients de Barracuda Essentials et Barracuda Email Security Gateway. Les clients peuvent bénéficier de remises sur volume.