Barracuda Sentinel

L'intelligence artificielle au service de la protection des e-mails en temps réel.

Le piratage de comptes professionnels (BEC), le spear phishing et le piratage de comptes sont actuellement les menaces les plus courantes pesant sur les messageries électroniques. Ces attaques très ciblées poussent les employés à commettre des erreurs extrêmement coûteuses.

Barracuda Sentinel combine l'intelligence artificielle, l'intégration avancée à Office 365 et la protection des marques dans une solution cloud complète pour fournir une défense efficace contre ces attaques potentiellement dévastatrices.

Défense en temps réel contre le piratage de comptes professionnels

L'architecture API exceptionnelle de Sentinel permet à son moteur IA d'étudier l'historique des messages électroniques et d'en déduire les modèles de communication propres aux différents utilisateurs. Ce qui lui permet ensuite d'identifier les anomalies dans les métadonnées et le contenu des messages, afin de détecter et de bloquer les attaques par ingénierie sociale en temps réel.

Cette approche fondée sur des modèles historiques est beaucoup plus précise que les stratégies traditionnelles fondées sur des politiques pour détecter les attaques par ingénierie sociale et le piratage de comptes.

Protection contre le piratage de comptes et les risques internes

Le piratage de comptes permet aux pirates d'étudier secrètement leur cible et de planifier leur attaque. Les défenses des passerelles ne voient jamais les attaques internes lancées à partir de ces comptes piratés, et ne peuvent donc pas les détecter.

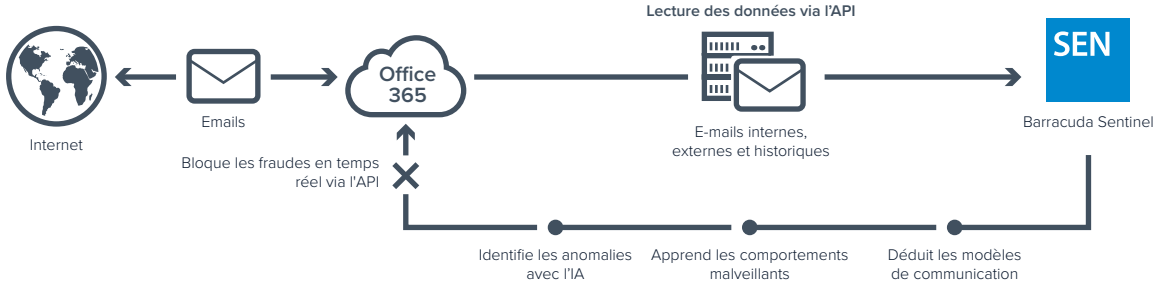
Sentinel bloque les attaques de phishing utilisées pour collecter les informations d'identification permettant le piratage de comptes. La solution détecte les comportements anormaux et alerte le service informatique, puis identifie et supprime tous les e-mails frauduleux envoyés à partir des comptes piratés.

Protection des marques et visibilité de l'usurpation de nom de domaine

L'usurpation de nom de domaine est un type courant d'attaque par ingénierie sociale qui cible les employés, les clients et les partenaires des entreprises. Barracuda Sentinel contribue à lutter contre la fraude au nom de domaine de messagerie grâce au reporting et à l'analyse DMARC (Domain-based Message Authentication Reporting and Conformance).

Sentinel aide à configurer l'authentification DMARC. La visibilité et l'analyse granulaires des rapports DMARC permettent ainsi de réduire le nombre de faux positifs, de protéger les e-mails légitimes et d'empêcher les usurpations.

Principe de fonctionnement de Sentinel



Barracuda Sentinel

Défense de la boîte de réception ✓

Barracuda Total Email Protection est une solution de protection de messagerie multicouche, par laquelle Sentinel utilise l'IA pour contrecarrer les tentatives de spear phishing, de piratage de comptes et d'attaques BEC.

Protection de messagerie multicouche Barracuda Total Email Protection

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 types
  - 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
  - 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 des e-mails contre le chantage et l'extorsion

Protection contre le piratage de comptes

- Défense et restauration en temps réel
- Détection des activités de piratage de comptes/ des emails piratés et envoi d'alertes
- Notification des utilisateurs externes et suppression des emails piratés
- Blocage de l'accès aux comptes piratés pour les attaquants
- Visibilité des modifications des règles des boîtes de réception
- Alerte sur les connexions suspectes

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 connaître l'expéditeur 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

Identification, basée sur l'intelligence artificielle, du personnel de l'entreprise qui présente un profil à haut risque

Création de rapports

- Analyse de l'environnement de menaces
- Attaques détectées au fil du temps
- Informations sur l'usurpation d'identité et les attaques BEC

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)

Les tarifs sont proposés par utilisateur et par année. Des réductions sont disponibles pour les clients Barracuda Essentials et Barracuda Email Security Gateway. Des remises quantitatives sont également applicables. Les prix peuvent varier selon les pays. Pour plus d'informations, rendez-vous sur barracudasentinel.com.

Barracuda
Your journey, secured.