Barracuda Sentinel

Künstliche Intelligenz (KI) für E-Mail-Schutz in Echtzeit.

Business Email Compromise (BEC), Spear Phishing und Account Takeover (ATO) sind heute die häufigsten Bedrohungen per E-Mail. Die sehr zielgerichteten Angriffe täuschen Mitarbeiter böswillig, um sie zu kostspieligen Fehlern zu verleiten.

Barracuda Sentinel kombiniert künstliche Intelligenz (KI), eine tiefe Integration in Microsoft Office 365 und Brand Protection zu einer umfassenden, Cloud-basierten Lösung zum Schutz gegen diese potenziell verheerenden Angriffe.

Echtzeitschutz vor Business-Email-Compromise

Dank der einzigartigen API-basierten Architektur analysiert das KI-Modul von Sentinel die historischen E-Mails und erlernt die typischen Kommunikationsmuster der einzelnen Benutzer. Dadurch lassen sich Anomalien in den Metadaten und im Inhalt von Nachrichten identifizieren und Social Engineering-Angriffe in Echtzeit ermitteln und blockieren.

Dieser auf historischen Mustern basierende Ansatz ist erheblich genauer als herkömmliche richtlinienbasierte Strategien zur Erkennung von Social Engineering- und Account Takeover-Angriffen.

Schutz vor Account Takeover und Bedrohungen durch Insider

Durch einen Account Takeover können Hacker ihr Ziel unbemerkt ausspähen und ihren Angriff planen. Mit Abwehrmaßnahmen an Gateways lassen sich keine internen Angriffe erkennen, die von kompromittierten Konten ausgehen.

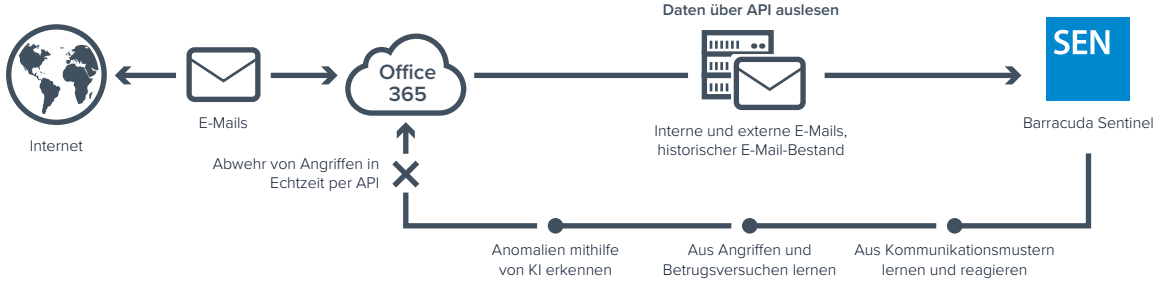
Sentinel stoppt Phishing-Angriffe und verhindert dadurch, dass Mitarbeiter ihre Anmeldedaten versehentlich für einen Account Takeover preisgeben. Die Lösung erkennt anomale E-Mail-Verhaltensweisen und benachrichtigt die IT-Sicherheitsexperten im Unternehmen. Anschließend werden alle von kompromittierten Konten gesendeten betrügerischen E-Mails ermittelt und gelöscht.

Schutz der Unternehmensmarke und Erkennung von Domain-Betrug

Domain-Spoofing ist ein gängiger Social Engineering-Angriff auf Ihre Mitarbeiter, Kunden und Partner. Sentinel trägt mit DMARC-Berichten (Domain-based Message Authentication Reporting and Conformance) und Analysen zum Schutz vor E-Mail-Domain-Betrug bei.

Barracuda Sentinel erleichtert das Einrichten der DMARC-Authentifizierung. Durch detaillierte Transparenz und Analysen von DMARC-Berichten können Sie Fehlalarme minimieren, legitime E-Mails schützen und Spoofing verhindern.

Funktionsweise von Sentinel



Barracuda Sentinel

Schutz von Posteingängen ✓

Barracuda Total Email Protection ist eine mehrstufige Email Protection-Lösung mit Sentinel für KI-basierten Schutz vor Spear Phishing, Account Takeover und Business Email Compromise.

Barracuda Total Email Protection – mehrstufige Email Protection-Lösung

Hauptmerkmale

Echtzeitschutz durch KI

- Stoppt Spear Phishing-Angriffe in Echtzeit
- Lernt die individuellen Kommunikationsmuster jedes Kunden mithilfe von KI
  - Zuordnung und Abbildung sozialer Netzwerke im Unternehmen, um typische Kommunikationsmuster verstehen zu können
  - Identifizierung von Anomalien in Metadaten und Inhalten
- Echtzeit-Benachrichtigung
  - Stellt verdächtige E-Mail-Nachrichten automatisch in Quarantäne
  - Benachrichtigt Administratoren und Benutzer
  - Analysiert historische und interne Kommunikationsdaten und -muster
- Schützt umfassend vor personenbezogenen betrügerischen Täuschungsangriffen wie Spear Phishing, Business Email Compromise (BEC), Whaling, Identitätsbetrug und CEO Fraud
- Schutz vor E-Mail-basierter Erpressung

Schutz vor Account Takeover

- Echtzeitschutz und Schadensbehebung
- Erkennt und meldet Account Takeover-Aktivitäten und kompromittierte E-Mails
- Benachrichtigt externe Benutzer und löscht kompromittierte E-Mails
- Blockiert den Zugriff von Angreifern auf kompromittierte Konten
- Bietet einen transparenten Einblick in Änderungen der Posteingangsregeln
- Meldet verdächtige Anmeldungen

Schutz vor Domain-Betrug

- DMARC-Authentifizierung und -Analyse zum Schutz vor:
  - Brand Hijacking (Marken- bzw. Domain-Hijacking)
  - Domain-Spoofing
- Intuitiver Setup-Assistent zum Einrichten der DMARC-Authentifizierung
- Transparenter E-Mail-Verkehr durch DMARC-Berichtsanalysen
- Zuverlässige Zustellung legitimer E-Mails
- Detaillierte umsetzbare Informationen zur Einhaltung der DMARC-Richtlinie

Analyse zur Erkennung von Personen mit hohem Risikopotenzial

Identifiziert mithilfe von künstlicher Intelligenz Mitarbeiter mit hohem Risiko

Reporting

- Analyse der Bedrohungsumgebung
- Protokollierung aller erkannten Angriffe
- Einblick in Angriffe durch Identitätsbetrug und BEC

Deployment und Verfügbarkeit

Weltweit für Microsoft Office 365-Benutzer verfügbar

100 % Cloud-basiert

Keine Hardware oder Software erforderlich

Mit beliebigen E-Mail-Security-Lösungen kompatibel

- Barracuda Essentials – E-Mail-Security, Archivierung und Backup für Office 365
- Barracuda Email Security Gateway
- Microsoft Exchange Online Protection (EOP)
- Und viele mehr

API-basierte Architektur

- Direkte Verbindung zu Office 365
- Keine Auswirkung auf Netzwerk-Performance oder Benutzererfahrung
- Schnelle, einfache Einrichtung (in weniger als 5 Minuten)

Die Abrechnung erfolgt pro Benutzer und Jahr. Rabatte für Kunden von Barracuda Essentials und Barracuda Email Security Gateway. Mengenrabatte verfügbar. Internationale Preise können variieren.
Weitere Informationen erhalten Sie unter barracudasentinel.com.

Barracuda
Your journey, secured.

DATENBLATT • DE 1.3 • Copyright 2019 Barracuda Networks, Inc. • barracuda.com
Barracuda Networks und das Logo von Barracuda Networks sind eingetragene Marken der Barracuda Networks, Inc. in den USA. Alle anderen Namen sind Eigentum der jeweiligen Inhaber.