

KI, die Vorfälle verhindert. Coaching, das Mitarbeitende vorbereitet.

Unverdächtige Akteurinnen und Akteure mit schlechten Absichten stellen heute die gefährlichste Bedrohung dar. KnowBe4 Defend, die Lösung von KnowBe4 für Sicherheit beim E-Mail-Empfang, trifft Entscheidungen nicht unverständlich in einer Blackbox. Stattdessen werden mithilfe von fortschrittlicher KI und Natural Language Processing (NLP) vergangene Kommunikationsmuster zugeordnet, um Anomalien sofort zu erkennen. Defend trifft autonom intelligenter, fundierter Entscheidungen und kann sich entwickelnde polymorphe Angriffe schneller stoppen als andere E-Mail-Sicherheitsebenen.



Defend

Highlights

- ▶ 30 % bessere Bedrohungserkennung
- ▶ 95 % weniger Zeitaufwand
- ▶ 1,4 Mrd. gefilterte Graymail-Mitteilungen pro Jahr

Defend-Kennzahlen für die mittlere Dauer (MTTX)

MTTD (Mean Time to Detect = Erkennen)
KI-gestützte Verhaltensanalyse erkennt Zero-Day-BEC-Angriffe sofort.

MTTT (Mean Time to Triage = Einordnen)
Ähnliche Warnungen werden in einer Ansicht gruppiert.

MTTI (Mean Time to Investigate = Untersuchen)
Erkannte Bedrohungen werden mit Microsoft Defender synchronisiert, um eine einheitliche Verteidigungsstrategie zu gewährleisten.

MTTC (Mean Time to Contain = Eindämmen)
Bedrohungen werden automatisch unter Quarantäne gestellt.

MTTR (Mean Time to Respond = Reagieren)
Verdächtige E-Mails sind mit einem Klick aus allen Posteingängen entfernt.

Zusammenspiel von Technologie und menschlicher Intelligenz

Technologie allein reicht nicht aus. Moderne Organisationen benötigen einen besseren ROI beim Sicherheitstraining, indem sie dieses in die vorhandene Technologie einbinden. Defend schließt die Lücke zwischen passivem Lernen und aktiver Abwehr.



Echtzeit-Coaching zu Risiken

Durch eine Kombination aus Security Awareness Training und Echtzeit-Coaching erhalten Ihre Mitarbeitenden die richtigen Tools *zum richtigen Zeitpunkt*. Diese zusätzliche Ebene befähigt Ihre Mitarbeitenden, auf Bedrohungen zu reagieren, die von Technologie allein nicht erkannt werden.



95 % weniger Zeitaufwand

Binden Sie Menschen in den Prozess ein („Human-in-the-Loop“). KI-Tools kümmern sich um Einordnung und Eindämmung, sodass Ihr SOC-Team entlastet wird (eine Organisation mit 1.000 Nutzerinnen und Nutzern kann dadurch 45 Stunden/Woche bei den Reaktionszeiten einsparen).



KI-native Erkennung von ausgefeilten Bedrohungen, die anderen Systemen entgehen

Entfernen Sie mehr nicht schädliche Mitteilungen und erkennen Sie mehr Bedrohungen durch eine vollständige KI-gestützte Erkennung ohne manuelle Konfiguration. Sicherheit beim E-Mail-Empfang von KnowBe4 erkennt Anomalien im Geflecht aus Absichten und Beziehungen, um komplexe BEC- und Supply-Chain-Angriffe zu stoppen, ohne dass eine manuelle Konfiguration erforderlich ist.

Wichtige Kennzahlen

Mit Defend können Sie Ihr Wachstum von den Risiken trennen. Denn bei einer steigenden Anzahl an Mitarbeitenden und einem höheren Umsatz sollten Sicherheitsvorfälle nicht zunehmen.

Mehr Vorfälle bei Unternehmenswachstum?

Mithilfe von KI-gestützter Verhaltensanalyse und Natural Language Processing (NLP) lassen sich 30 % mehr ausgefeilte, polymorphe Angriffe stoppen als mit anderen Systemen. So sind Sie bei Vergrößerung der Belegschaft nicht mit einer äquivalenten Flut an Datenschutzverletzungen konfrontiert.

Kapazitätsmanagement

Verhindern Sie, dass sich die Produktivität aufgrund der Menge an Warnmeldungen verringert. Da mehr als 1,4 Mrd. nicht schädlicher Graymail-Mitteilungen pro Jahr automatisch entfernt werden, kann sich Ihr SOC-Team auf strategisch wichtige Aufgaben konzentrieren.

Automatisierte Reaktion, menschliche Reaktion

Setzen Sie auf einen „Human-in-the-Loop“-Prozess, in dem Defend als intelligentes, autonomes System die mühsame Aufgabe der Einordnung übernimmt. Detaillierte Berichte geben Aufschluss darüber, welche Nutzerinnen und Nutzer ins Visier genommen werden und wo zielgerichtetes, wirkungsvolles Training sinnvoll ist.

Wichtige Produktfunktionen

KI-gestützte Phishing-Erkennung

Defend erkennt Bedrohungen effizient – durch eine Kombination aus selbstlernenden Verfahren, prägenerativer Modellierung, Verhaltensanalyse, Sprachverarbeitungsmodellen und Automatisierung.

Anpassungsfähige Architektur

Defend verbessert basierend auf Berechnungen aller von Defend verarbeiteten E-Mails automatisch die Erkennung von Bedrohungen für einzelne Nutzerinnen und Nutzer.

Umfassende Erkennung

Alle Bereiche einer eingehenden E-Mail werden gleichzeitig analysiert. Diese Herangehensweise ist viel effizienter als bei herkömmlichen Produkten zur Abwehr von Phishing und Malware mit isolierter Analyse.

Kontextuelle, lokalisierte Lernaspekte

Dynamische, lokalisierte Banner und Tags in verschiedenen Farben bieten verständliche Erläuterungen und ändern sich abhängig von der Risikostufe. Die Nutzerinnen und Nutzer erhalten E-Mails, in denen erklärt wird, warum eine Bedrohung entfernt wurde – das ist Coaching in Echtzeit.

Maschinelles Lernen und linguistische Analyse

Mithilfe von selbstlernenden Verfahren werden Baseline-Werte für das Verhalten Ihrer Nutzerinnen und Nutzer ermittelt und abweichendes Verhalten gekennzeichnet. Natural Language Processing (NLP) und Natural Language Understanding (NLU) bestimmen Emotion, Absicht und Kontext jeder E-Mail, um ungewöhnliches, verdächtiges und bedrohliches Verhalten zu erkennen.

Neutralisierung von schädlichem Code

Aktiver und schädlicher Code wird im HTML-Mitteilungstext und in E-Mail-Anhängen automatisch deaktiviert.

SSO-Integration

Defend lässt sich direkt in das Single Sign-On (SSO) Ihrer Organisation integrieren.

Absenderanalyse

Bei jeder Mitteilung werden die Absenderrichtlinien für SPF, DKIM und DMARC überprüft und validiert.

URL-Rewriting

Zeitbasierte Angriffe werden durch URL-Rewriting und Überprüfung zum Zeitpunkt des Klicks per SMTP-Bereitstellung gestoppt. Unsichere Links werden auf eine Warnseite mit verständlichen Kontextangaben weitergeleitet und als Lernaspekte zum Coaching Ihrer Nutzerinnen und Nutzer verwendet.

QR-Code-Erkennung

QR-Codes in E-Mails werden erkannt, um Ihre Nutzerinnen und Nutzer vor Quishing-Versuchen zu warnen.

Automatisierung der Abuse Mailbox

Verringern Sie Aufwand und Reaktionszeiten mit fortschrittlichen KI-gestützten Phishing-Analysen und -Abhilfemaßnahmen.

Intelligente Graymail-Erkennung

Erhöhen Sie die Produktivität Ihrer Nutzerinnen und Nutzer und entlasten Sie Ihre Admins, indem Graymail-Mitteilungen automatisch in einen separaten Ordner verschoben werden.

Nahtlose Integration in Microsoft 365

Profitieren Sie von der nahtlosen Integration in Ihre MS Outlook-Apps auf Windows Desktop und Mac sowie iOS- und Android-Geräten (inklusive Integration in sichere Links von Microsoft). Defend setzt nach Ihrem SEG und/oder nach der Durchführung einer Perimeteranalyse in Microsoft 365 ein.

Detaillierte Analyse

Das Security Center ist Ihr Portal für Risikoanalyse, Berichte und Eindämmung und Untersuchung von Vorfällen sowie Reaktion auf Vorfälle für all Ihre Produkte von KnowBe4 für E-Mail-Sicherheit in der Cloud (Defend, Prevent, Protect), inklusive Feed zu globalen Bedrohungen.

Wie funktioniert KnowBe4 Defend?



Analysieren

Defend erkennt im Geflecht aus Beziehungen geringfügige Änderungen in Tonfall oder Dringlichkeit: wichtige Kennzeichen kompromittierter Konten.



Warnen

Farbkodierte Outlook-Kategorietags oder interaktive Banner weisen die Nutzerinnen und Nutzer vor dem Lesen einer E-Mail auf Bedrohungen im Posteingang hin.



Coachen

Automatisierte E-Mails mit auf die einzelnen Nutzerinnen und Nutzer zugeschnittenen Lernaspekten enthalten Details zur Bedrohung.



Eindämmen

Ähnliche Bedrohungen werden in einer einzigen Ansicht zusammengeführt. Diese können mit einem Klick aus dem Weg geräumt werden.

„Wir haben erkannt, dass eine Ebene nicht ausreicht, um die Menge an fortschrittlichen Phishing-Bedrohungen zu neutralisieren, die GMMH tagtäglich begegnen. KnowBe4 Defend sorgt nicht nur für eine zusätzliche Abwehrebene, sondern ergänzt auch unser Security Awareness Training. Über die anklickbaren Defend-Banner wird das Sicherheitsbewusstsein unserer Mitarbeitenden fortlaufend geschult.“

- Kevin Orritt, Cyber Security Manager, Greater Manchester Mental Health (GMMH)

Mehr erfahren

knowbe4.com/products/defend

