

KI-gestützte Phishing-Angriffe abwenden und SOC-Effizienz erhöhen – dank Incident-Response-Automatisierung

PhishER Plus

Wesentliche Vorteile

- ▶ Bedrohungen automatisch kategorisieren
- ▶ Sofortiges Feedback für Reports bereitstellen
- ▶ Verdächtige E-Mails mit einem Klick aus allen Posteingängen entfernen
- ▶ E-Mails basierend auf Expertenwissen, Daten von über 13 Millionen Nutzerinnen und Nutzern weltweit sowie Integrationen mit führenden Sicherheitsplattformen analysieren und klassifizieren

PhishER Plus ist eine SOAR-Plattform mit Incident-Response-Automatisierung, die Sicherheitsteams entlastet und für eine effizientere Ressourcennutzung sorgt.

PhishER Plus priorisiert Bedrohungen anhand der weltweit umfangreichsten Datenbank zu Bedrohungen und dämmt diese sofort ein. Dabei werden KI-Tools, deren Training auf 15 Jahren menschlichen Verhaltens basiert, Analysen aus dem Threat Research Lab von KnowBe4 sowie Feeds zu Bedrohungen von integrierten Drittanbietern kombiniert. Die Plattform stellt eine umfassende Ansicht bereit, über die Risiken bewertet und schnell Maßnahmen in allen Posteingängen ergriffen werden können.

Risiko von menschlichen Fehlern reduzieren

PhishER Plus verhindert Zero-Day-Bedrohungen durch Übernahme der Funktion einer zusätzlichen Sicherheitsebene in Ihrer technologischen Infrastruktur. Mithilfe der globalen PhishRIP-Funktion und globalen Blocklisten werden gemeldete Bedrohungen automatisch in drei Schritten validiert und eingedämmt. Bedrohungen werden gleichzeitig aus allen Posteingängen der Mitarbeitenden entfernt. Die Reaktionsdauer verringert sich von Stunden auf Minuten und begrenzt die möglichen Auswirkungen des Angriffs erheblich.

Arbeitsaufwand für Ihr SOC-Team und Zeitaufwand für die Analyse gemeldeter E-Mails verringern

PhishER Plus verringert den Zeitaufwand für die Analyse von E-Mails und entfernt riskante E-Mails automatisch aus den Posteingängen der Nutzerinnen und Nutzer. PhishER Plus stützt sich auf E-Mail-Bedrohungsdaten aus dem Threat Research Lab von KnowBe4 sowie Daten aus branchenweit einzigartigen Drittanbieterintegrationen. Im Schnitt realisieren Kunden einen ROI von über 360 % im ersten Jahr und reduzieren den Zeitaufwand für die manuelle Überprüfung von E-Mails um 99 %.

Fortschritte und Chancen im Bereich Security Awareness für Ihre Mitarbeitenden anzeigen

Mit PhishER Plus als Integration in KnowBe4 Security Awareness Training (SAT) und Phishing-Simulationen können Führungskräfte nachvollziehen, wer E-Mails gemeldet hat und wer auf einen simulierten Phishing-Angriff, der mithilfe von PhishFlip unschädlich gemacht wurde, hereingefallen ist. Zusätzlich können PhishER Plus-Aktionen und -Tags eingerichtet werden, mit denen sich unbedenkliche E-Mails und Spam schnell identifizieren und nachverfolgbares Echtzeit-Coaching ohne Eingreifen des SOC-Teams bereitstellen lassen. Einer Nachricht zugewiesene Tags legen fest, wie die Nachricht in PhishER Plus verarbeitet wird. Die Aktionen geben dabei vor, wie PhishER Plus die Nachricht behandelt.

Wichtige Funktionen

Drei Schritte zur Validierung gemeldeter Bedrohungsdaten

- **Abwehrnetzwerk:** Bedrohungsdaten aus einem Netzwerk mit über 13 Millionen Nutzerinnen und Nutzern weltweit, die täglich neue Bedrohungen melden
- **Einblicke aus proprietären KI-Tools:** Unsere Trainingsdaten basieren auf 15 Jahren menschlichen Verhaltens – für herausragenden Zero-Day-Schutz
- **Expertenwissen:** Unter Einbezug von Branchenkenntnissen und Echtzeit-Analysen aus dem Threat Research Lab von KnowBe4
- **Drittanbieter-Integrationen:** Kombination aus internen Daten und Feeds zu Bedrohungen integrierter Drittanbieter, darunter CrowdStrike Falcon Sandbox, VirusTotal und Threat Intel Powered by Webroot

Incident-Response-Automatisierung und Eindämmung

- **Globale PhishRIP-Funktion:** Gleichzeitige Entfernung zugestellter, schädlicher E-Mails aus den Posteingängen aller Mitarbeitenden basierend auf den von der Community gemeldeten Bedrohungen
- **Globale Blockliste von Microsoft 365:** Sofortige Einleitung der Eindämmung – bekannte Bedrohungen werden blockiert, bevor diese in Ihre Microsoft 365-Umgebung gelangen
- **PhishML-KI-Klassifizierung:** Automatische Klassifizierung von bis zu 90 % der gemeldeten E-Mails als „Unbedenklich“, „Spam“ oder „Bedrohung“ – weniger Aufwand für die manuelle Überprüfung
- **Korrektur mit einem Klick:** Eine Ansicht, über die schnell Maßnahmen in allen Posteingängen ergriffen und Bedrohungen eingedämmt werden können

SOC-Effizienz und Transparenz

- **Präzise Automatisierung:** Individuelle Schwellenwerte für PhishML-Automatisierungen basierend auf den Anforderungen
- **PhishML-Einblicke:** Ausführliche Erläuterungen der Klassifizierung von Nachrichten mithilfe von KI – für eine transparente KI-Entscheidungsfindung
- **Echtzeit-Feedback:** Bereitstellung von sofortigem Feedback und Informationen für die Nutzerinnen und Nutzer bei der Meldung von E-Mails über den Phish Alert Button (PAB)
- **Detaillierte Reports und Analysen:** Umfassende Transparenz von Sicherheitsentscheidungen und ROI – genaue Angaben zu den gestoppten Bedrohungen

Motivation der Mitarbeitenden und Training

- **PhishFlip:** Umwandlung gemeldeter echter Phishing-Versuche in harmlose Trainingssimulationen: Welche Nutzerinnen und Nutzer wären darauf hereingefallen?
- **Stärkung sicherer Verhaltensweisen:** Mensch-KI-Ansatz, bei dem Nutzerinnen und Nutzer wachsam bleiben und positive Verhaltensweisen gestärkt werden

Mehr erfahren

knowbe4.com/de/products/phisher-plus



knowbe4

KnowBe4 Germany | Rheinstr. 45/46, 12161 Berlin – Deutschland
+49 30 34 64 64 60 | [KnowBe4.de](https://knowbe4.de) | kontakt@knowbe4.com

Andere genannte Produkt- und Firmennamen sind eventuell Marken und/oder eingetragene Marken ihrer jeweiligen Unternehmen.