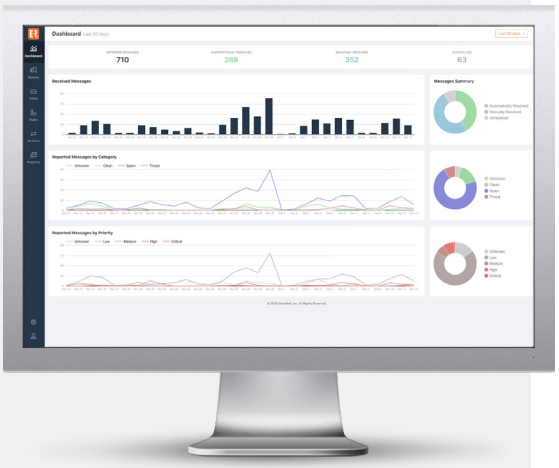
PhishER

KnowBe4
Human error. Conquered.



E-Mail-Bedrohungen schneller erkennen und richtig reagieren – mit PhishER

Da Phishing nach wie vor die am weitesten verbreitete Methode für Cyberangriffe darstellt, melden die meisten Nutzer:innen ihrem IR-Team (Incident Response) zahlreiche E-Mail-Nachrichten, die sie als potenziell schädlich einstufen. Unabhängig davon, ob Ihre Mitarbeiter:innen an einem Security Awareness Training teilnehmen oder nicht, nutzen sie wahrscheinlich bereits die in Ihrem Unternehmen, Ihrer Institution oder Ihrer Organisation zur Verfügung stehenden Kanäle, um potenziell gefährliche E-Mails zu melden. **Sie müssen den gestiegenen E-Mail-Traffic irgendwie in den Griff bekommen.**

Etwa 7 bis 10 % der schädlichen E-Mails und Spam-E-Mails schaffen es durch die Filter und landen bei den Nutzer:innen. Schätzungsweise stellt nur etwa eine von zehn gemeldeten E-Mails tatsächlich eine Bedrohung dar. Wie können Sie sich um die wirklich gefährlichen Phishing-Angriffe und Cyberbedrohungen kümmern und gleichzeitig die anderen 90 % der von Nutzer:innen gemeldeten Nachrichten präzise und effizient verwalten? **PhishER™.**

Was ist PhishER?

PhishER ist das zentrale Element in Ihrem Workstream für Cybersicherheit. Diese schlanke SOAR-Plattform unterstützt Sie beim Orchestrieren von Maßnahmen bei Bedrohungen und beim Verwalten der zahlreichen potenziell schädlichen E-Mail-Nachrichten, die Nutzer:innen melden. Dank der automatischen Priorisierung von E-Mails liefert PhishER Ihren für Datensicherheit und Sicherheitsabläufe zuständigen Teams schnell einen Überblick über den eingehenden Traffic, sodass diese schneller auf ernste Bedrohungen reagieren können.

Darüber hinaus können Sie mit PhishER einen automatisierten Workstream für die 90 % der gemeldeten E-Mails erstellen, die keine Bedrohung darstellen. Steigern Sie durch das orchestrierte Reagieren auf Vorfälle einfach und unmittelbar die Effizienz Ihres Sicherheitsteams und profitieren Sie von weiteren Vorteilen. Mit der richtigen Strategie und Planung kann Ihr Unternehmen, Ihre Institution oder Ihre Organisation ein vollständig orchestriertes und intelligentes Security Operations Center (SOC) einrichten, das den heutigen Bedrohungen gewachsen ist.

PhishER ermöglicht einen kritischen Workstream, mit dem Ihre IR-Teams gemeinsam die Risiken von Phishing-Angriffen mindern können. Das Tool eignet sich für alle Unternehmen, Institutionen und Organisationen, die nach einer präzisen und schnellen Lösung zum automatischen Priorisieren und Verwalten potenziell schädlicher Nachrichten suchen. PhishER ist als eigenständige Lösung oder als optionales Add-on für KnowBe4-Kunden erhältlich.

Gründe für PhishER

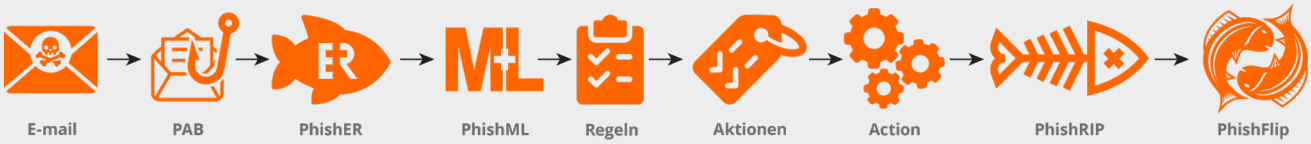
PhishER ist eine intuitive und benutzerfreundliche Webplattform mit wichtigen Workstreamfunktionen, auf der Sie Bedrohungen durch Phishing ermitteln und auf gemeldete Vorfälle reagieren können. Mithilfe von PhishER können Sie durch eine kurze Analyse ermitteln, welche Nachrichten legitim sind und welche nicht, und sie entsprechend priorisieren.

Außerdem kann Ihr Team mit PhishER hohe Volumen an E-Mails schnell ein- und zuordnen. Letztendlich sollen so viele Nachrichten wie möglich automatisch abgearbeitet werden. Sie können sich den von PhishER empfohlenen Schwerpunktbereichen annehmen oder andere gewünschte Aktionen durchführen.

Zentrale Vorteile

- Automatische Priorisierung von nicht bedrohlichen E-Mails über den Phish Alert Button von KnowBe4
- Übersicht im IR-Posteingang – schnelle und effiziente Reaktion auf tatsächliche Bedrohungen
- Mehr IR-Ressourcen zur Überprüfung von Spam-E-Mails und legitimen Anfragen (90 % der Nachrichten)
- Anzeige von Nachrichtenclustern oder -gruppen mit ähnlichem Muster zur Erkennung von großflächigen Phishing-Angriffen auf Ihr Unternehmen, Ihre Institution oder Ihre Organisation
- Einhaltung kritischer SLAs innerhalb Ihres Unternehmens, Ihrer Institution oder Ihrer Organisation bezüglich der Verarbeitung und Priorisierung von Bedrohungen und legitimen E-Mails
- Vorlagen für automatisierte E-Mail-Antworten zur schnellen Rückmeldung bei den Nutzer:innen
- Entlastung Ihres IR-Teams durch benutzerdefinierte Workflows für Aufgaben (z. B. Priorisierung und Warnungen)

PhishER – so funktioniert's



PhishER gruppiert und kategorisiert die von Nutzer:innen gemeldeten Phishing-E-Mails sowie andere verdächtige E-Mails anhand von Regeln, Tags und Aktionen. Das benutzerdefinierte Modul für maschinelles Lernen PhishML analysiert die Nachrichten und vergibt einen Konfidenzwert, um die Nachrichten entsprechend zu kennzeichnen. Mit PhishRIP können Sie mühelos verdächtige Nachrichten in den verschiedenen Posteingängen aufspüren und unter Quarantäne stellen. PhishFlip verwendet gemeldete Phishing-E-Mails in entschärfter Form automatisch für simulierte Phishing-Kampagnen.

Automatische Nachrichtenpriorisierung

Mit PhishER weisen Sie jede gemeldete Nachricht einer von drei Kategorien zu: unverdächtige Nachricht, Spam oder Bedrohung. Anhand der von Ihnen im integrierten Basiseditor festgelegten YARA-Regeln schlägt PhishER Prozesse vor, um automatisch so viele Nachrichten wie möglich ohne Nutzereingriff zu priorisieren.

Dank automatischer Priorisierung von nicht bedrohlichen E-Mails kann sich Ihr Team schneller auf tatsächliche Bedrohungen konzentrieren. PhishER lässt sich einfach über das Phish Alert Button (PAB)-Add-in von KnowBe4 integrieren. Verdächtige Nachrichten können an einen dedizierten Posteingang weitergeleitet werden.

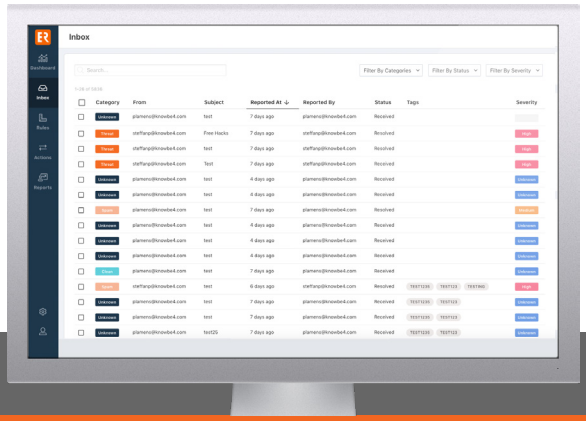
Emergency Rooms

In den „Emergency Rooms" von PhishER befinden sich ähnliche Nachrichten, die von Nutzer:innen gemeldet wurden. Die Emergency Rooms sind automatisch gefilterte Ansichten der unbearbeiteten Nachrichten in Ihrem PhishER-Posteingang. Diese Nachrichten werden dynamisch nach bestimmten Eigenschaften gruppiert. Die vom System gefilterten Ansichten führen Nachrichten nach „Häufigste Betreffzeilen", „Häufigste Absender:innen", „Häufigste Anhänge" und „Häufigste URLs" auf.

Die einzelnen Emergency Rooms sind interaktiv. Sie können die gefilterten Ansichten der Inbox eingehender untersuchen und gleichzeitig Maßnahmen für alle zugehörigen Nachrichten in die Wege leiten.

SIEM-Integrationen

PhishER speist Daten in beliebte SIEM-Plattformen wie Splunk und QRadar und kann so optimal in Ihr Unternehmen, Ihre Institution oder Ihre Organisation integriert werden. Dank Unterstützung für mehrere Syslog-Ziele können Daten auch in beliebig viele weitere Systeme übertragen werden.



PhishML™

PhishML ist ein PhishER-Modul für maschinelles Lernen, mit dem Sie verdächtige Nachrichten, die von Nutzer:innen gemeldet werden, am Anfang des Priorisierungsprozesses identifizieren und bewerten können. PhishML analysiert jede auf der PhishER-Plattform eingehende Nachricht und stellt Ihnen Informationen für einen schnellen, genauen und einfachen Priorisierungsprozess bereit.

PhishML entwickelt sich basierend auf den Nachrichten, die von Ihnen und anderen Nutzer:innen der PhishER-Community getaggt werden, kontinuierlich weiter. Das Modul wird dank der neu bereitgestellten Daten immer besser und genauer. So können in PhishER noch mehr Nachrichten automatisch kategorisiert werden.

PhishRIP™

PhishRIP ist eine Quarantänefunktion für E-Mails mit Unterstützung für Microsoft 365 und Google Workspace, dank der Ihr IR-Team schnell reagieren und Maßnahmen ergreifen kann.

Mithilfe von PhishRIP lassen sich identifizierte Bedrohungen aus allen Posteingängen Ihrer Nutzer:innen entfernen, nicht gemeldete Bedrohungen isolieren und zukünftige Bedrohungen vermeiden, indem legitime E-Mails gelöscht, unter Quarantäne gestellt oder wiederhergestellt werden.

PhishFlip™

PhishFlip ist eine Funktion von PhishER, bei der von Nutzer:innen gemeldete tatsächliche Phishing-Angriffe in einer sicheren Simulation für Phishing-Kampagnen auf Ihrer KnowBe4-Plattform eingesetzt werden. Mit PhishFlip können Sie einen gefährlichen Angriff unmittelbar in wirklichkeitsnahes Training „verwandeln".

Data Enrichment Intelligence

PhishER bietet Integrationen in externe Dienste wie VirusTotal, um Anhänge und schädliche Domains zu analysieren. Mithilfe von URL Unwinding werden verkürzte URLs automatisch erweitert, um die potenzielle Bedrohung der endgültigen Zieladresse einzustufen.

Weitere Informationen finden Sie auf www.KnowBe4.de.

KnowBe4 Germany GmbH | Rheinstraße 45/46 | 12161 Berlin – Deutschland | knowbe4.de | Tel.: +49 30 34 64 64 621 | kontakt@KnowBe4.com