KnowBe4
Human error. Conquered.

Acht wichtige Funktionen, auf die Sie bei der Beurteilung von SOAR-Plattformen achten sollten

Unternehmen, Institutionen und Organisationen, die sich effektiver vor Phishing schützen möchten, sollten der Verbesserung der Security Awareness stets oberste Priorität einräumen. Cyberkriminelle setzen immer ausgefeiltere Taktiken ein. Daher ist eine robuste, umfassende Strategie zur Phishing-Abwehr von entscheidender Bedeutung. Security Operation Center (SOC)- und Incident Response (IR)-Teams benötigen Tools, mit denen sich Phishing-Angriffe schnell untersuchen und unterbinden lassen, bevor sie Schaden anrichten.

Anti-Phishing Security, Orchestration, Automation and Response (SOAR)-Produkte haben sich mit ihrem Konzept, Technologie und Know-how zu verknüpfen, als leistungsstarke Tools zur Phishing-Abwehr erwiesen. Sie sind für IT-Sicherheitsteams unverzichtbar, die die wachsende Bedrohungslage in Zusammenhang mit Phishing-Angriffen und gezielten Spear-Phishing-Kampagnen in den Griff bekommen möchten.

Doch SOAR-Produkt ist nicht gleich SOAR-Produkt. Gute SOAR-Produkte müssen in erster Linie eine automatische E-Mail-Analyse sowie eine entsprechende Priorisierung tatsächlich schädlicher Nachrichten bieten, sodass menschliches Versagen bei der Erkennung von Phishing-Bedrohungen, die ein hohes Risiko darstellen, ausgeschlossen ist. Dank zusätzlicher, in den letzten Jahren entwickelter leistungsstarker Funktionen bieten SOAR-Produkte mittlerweile einen proaktiven Phishing-Schutz, der über die reaktive Analyse und Identifizierung hinausgeht. Bei der Suche nach einer geeigneten Lösung ist es wichtig, mit diesen Funktionen und Fortschritten vertraut zu sein.

Achten Sie bei der Auswahl eines SOAR-Produkts für die Phishing-Abwehr in Ihrem Unternehmen, Ihrer Institution oder Ihrer Organisation vor allem auf folgende acht Funktionen.

1. EMPOWERMENT VON ENDNUTZERN UND ENDNUTZERINNEN

Endnutzern und Endnutzerinnen kommt eine tragende Rolle bei der Verteidigung von Unternehmen, Institutionen und Organisationen gegen Phishing- und Social-Engineering-Bedrohungen zu. Nur wenn sie Cyberbedrohungen erkennen und melden können, können sich Unternehmen, Institutionen und Organisationen vor Phishing-Angriffen schützen und das damit verbundene Risiko verringern. Ein gutes SOAR-Produkt ermöglicht es den Endnutzern und Endnutzerinnen, zu diesem Schutz beizutragen.

Hierzu gehört zunächst die Möglichkeit, verdächtige E-Mails problemlos melden zu können. Ein in den E-Mail-Client Ihres Unternehmens, Ihrer Institution oder Ihrer Organisation integrierter Phish Alert Button sollte es Nutzern und Nutzerinnen ermöglichen, verdächtige E-Mails an eine voreingestellte E-Mail-Adresse der IT-Abteilung oder direkt an die SOAR-Plattform zu melden.

Außerdem sollte ein SOAR-Produkt Vorlagen und eine Funktion zur automatischen Beantwortung von E-Mails umfassen, sodass das Sicherheitsteam die Mitarbeitenden rasch über gemeldete E-Mails sowie nach der Prüfung darüber informieren können, ob es sich bei diesen einfach nur um Spam oder unbedenkliche Nachrichten handelt (90 % aller Meldungen).

2. MASCHINELLES LERNEN UND KI

SOAR-Plattformen gewährleisten zuverlässigen Schutz vor Phishing, wenn sie künstliche Intelligenz (KI) und Automatisierung einsetzen. IR- und SOC-Teams sind häufig unterbesetzt und verfügen nicht über die Kapazität, ohne Hilfe für Sicherheit zu sorgen. KI und Automatisierung wirken als Multiplikatoren, die die Identifizierung und Priorisierung von Phishing-Bedrohungen einfacher, schneller und genauer machen.

KI und Automatisierung ermöglichen und beschleunigen die unten aufgeführten Funktionen erheblich, da sie Skalierbarkeit, Genauigkeit und proaktive Risikominderung ermöglichen:

- Automatische Analyse und Priorisierung von E-Mails, sodass menschliches Versagen bei der Ermittlung von Phishing-Bedrohungen in gemeldeten Nachrichten ausgeschlossen ist
- Automatisierung des Sicherheitsworkflows für den Umgang mit den 90 % der unbedenklichen gemeldeten E-Mails

- Automatisierte Beantwortung von E-Mails, sodass die IT-Abteilung die Mitarbeitenden zeitnah informieren kann
- Gruppierung oder Clustering von Nachrichten auf Basis von Mustererkennung durch maschinelles Lernen, sodass IR-Teams umfassende Phishing-Angriffe erkennen können
- Automatisiertes Blocklisting, über Crowdsourcing gewonnene Bedrohungsdaten und proaktive Phishing-Abwehr
- Möglichkeit, Vorlagen für Phishing-Simulationen zu Trainingszwecken anhand von realen Phishing-Angriffen zu erstellen

3. AUTOMATISIERTE ANALYSE UND PRIORISIERUNG VON BEDROHUNGEN

Zahlreiche IR- und SOC-Teams prüfen verdächtige E-Mails nach wie vor manuell. Das dauert pro E-Mail im Durchschnitt 27 Minuten.[1] Ist die mittlere Reaktionszeit zu lang, erhöht dies das Risiko für Phishing-Angriffe und mögliche Schäden.

Zum Schutz Ihres Unternehmens, Ihrer Institution oder Ihrer Organisation vor Phishing-Angriffen und Ihres Sicherheitsteams vor Überlastung sollten sie sich für ein SOAR-Produkt entscheiden, das die Analyse und Priorisierung von E-Mails auf Basis von maschinellem Lernen ermöglicht. Auf diese Weise schließen Sie aus, dass es bei der Identifizierung von Phishing-Bedrohungen mit hohem Risiko in den zahlreichen von Nutzern und Nutzerinnen gemeldeten E-Mails zu Fehlern kommt.

Achten Sie darauf, dass sämtliche Produkte, die Sie in Erwägung ziehen, gemeldete E-Mails automatisch und ohne Nutzereingriff anhand von maschinellem Lernen priorisieren. Hierzu gehören auch die Einteilung von E-Mails in unterschiedliche Kategorien, beispielsweise „Unverdächtig“, „Spam“ oder „Bedrohung“, sowie das Ranking verdächtiger E-Mails nach Priorität. Letzteres sollte anhand Reihe von E-Mail-Attributen wie Betreff, Absender, Empfänger, Anhänge, Text usw. erfolgen.

Selbstverständlich muss die Plattform lernen. Die Präzision des Systems sollte anhand von eingespeisten neuen Daten fortlaufend verbessert werden. Hierzu zählen beispielsweise gemeldete verdächtige E-Mails, Daten Ihres SOC-Teams oder verifizierte Bedrohungsdaten aus dem Feed eines Drittanbieters.

Analyse und Priorisierung von E-Mails sind das Fundament jedes guten SOAR-Produkts, da sie den Prozess einfacher, schneller und präziser machen.

---

1 The Business Cost of Phishing, Report (2022)

4. QUARANTÄNE UND ENTFERNUNG

Im Anschluss an die Identifizierung von Phishing-Bedrohungen ist es von entscheidender Bedeutung, dass ähnliche Phishing-E-Mails in Quarantäne verschoben und aus den Posteingängen sämtlicher Nutzer und Nutzerinnen entfernt werden können. In einem Umfeld, in dem Bedrohungen von staatlich unterstützten Hackergruppen ausgehen und gezielte Spear-Phishing-Angriffe erfolgen, ist diese Fähigkeit zur umfassenden Eindämmung von Phishing unerlässlich.

Diese E-Mail-Quarantäne sollte direkt in E-Mail-Dienste von Drittanbietern wie Microsoft 365 oder Google Workspace integriert werden und Folgendes ermöglichen:

- **Entfernen**
  Das SOC-Team sollte im Anschluss an die Identifizierung einer Bedrohung diese und ähnliche Nachrichten aus allen E-Mail-Ordnern (Posteingang, gesendete E-Mails, Papierkorb usw.) entfernen können.
- **Isolieren**
  Nicht alle Endnutzer und Endnutzerinnen melden verdächtige E-Mails. Sie müssen auch diese nicht gemeldeten verdächtigen E-Mails im Blick behalten können, damit sie gemeldet, in Quarantäne gestellt und analysiert werden können.
- **Schützen**
  Die Post-Mortem-Analyse ist unerlässlich für den Schutz gegen zukünftige Angriffe. Im Anschluss an die Entschärfung unmittelbarer Bedrohungen sollten Follow-ups an betroffene Nutzer und Nutzerinnen versendet, Nachrichten aus den Posteingängen der Nutzer und Nutzerinnen gelöscht, die fortgesetzte Quarantäne gewährleistet und als unbedenklich identifizierte Nachrichten wiederhergestellt werden können. All diese Funktionen sollten Sie bei der Bewertung von Produkten im Hinterkopf behalten.

5. BLOCKLISTING

Blocklisting ist ein wichtiges proaktives Verfahren, um zu verhindern, dass schädliche E-Mails in den Posteingängen von Nutzern und Nutzerinnen landen. E-Mail-Dienste wie Microsoft 365 und Google bieten grundlegende Blocklisting-Funktionen. Diese sind vor dem aktuellen Hintergrund einer Flut an KI-generierten Phishing-E-Mails jedoch bei weitem nicht ausreichend.

Alle SOAR-Produkte, die Sie in Erwägung ziehen, sollten die vorhandenen E-Mail-Filter Ihres Unternehmens, Ihrer Institution oder Ihrer Organisationen durch weiterreichende Blocklisting-Funktionen ergänzen, die auf Endnutzerfeedback und der auf maschinellem Lernen basierenden Analyse von E-Mails beruhen.

Die Produkte müssen IR- und SOC-Teams ermöglichen, E-Mails auf der Grundlage einer Reihe von Attributen und Werten zu blockieren, darunter Absender, URL, Anhänge oder Datei-Hash. Achten Sie außerdem darauf, dass eine zuverlässige Funktion vorhanden ist, mit der sich anhand von Bedingungen Regeln erstellen lassen und die entsprechenden Funktionen herkömmlicher E-Mail-Dienste überlegen ist.

Der letzte und vielleicht wichtigste Punkt, wenn Sie die Bedrohungslage bewältigen und Phishing-Angriffe proaktiv entschärfen möchten, bevor diese Schaden anrichten: SOAR-Produkte sollten Unternehmen, Institutionen und Organisationen umfassendes Blocklisting auf Basis von KI und über Crowdsourcing gewonnene Bedrohungsdaten ermöglichen. Den Grund hierfür erfahren Sie unter Punkt 6.

6. ÜBER CROWDSOURCING GEWONNENE BEDROHUNGSDATEN UND PROAKTIVER SCHUTZ VOR PHISHING

Nicht einmal die größten und am besten ausgestatteten SOC- und IR-Teams können der Bedrohungslage in Zusammenhang mit Phishing und Social Engineering immer einen Schritt voraus sein. Die Bedrohungen sind zu vielfältig, entwickeln sich ständig weiter und werden immer raffinierter. Mithilfe von KI können Cyberkriminelle neuartige Phishing-E-Mails erstellen, die herkömmliche E-Mail-Sicherheitsfilter umgehen.

Daher kommt es bei der Phishing-Abwehr auf proaktives Handeln an. Die gewählte SOAR-Plattform sollte stets auf dem neuesten Stand sein und Echtzeit-Bedrohungsdaten nahtlos integrieren. So erhalten Sie zuverlässig aktuelle Erkenntnisse über neue Bedrohungen und können entsprechende Anpassungen und Reaktionsmaßnahmen einleiten.

Aus diesem Grund setzen Unternehmen, Institutionen und Organisationen bei Bedrohungsdaten zunehmend auf Anbieter von Cybersicherheitslösungen. Ihr SOAR-Anbieter sollte anhand von Millionen von Endnutzern und Endnutzerinnen gemeldeten Daten zu verifizierten Bedrohungen und KI-gestützten Blocklisting-Funktionen Phishing-Bedrohungen automatisch unter Quarantäne stellen und aus den Posteingängen Ihrer Nutzer und Nutzerinnen entfernen.

Über Crowdsourcing gewonnene Bedrohungsdaten enthalten Informationen zu Bedrohungen, die es durch alle aktivierten Sicherheitsfilter geschafft haben. Somit steht eine zusätzliche Ebene zum Schutz vor schädlichen E-Mails zur Verfügung, die selbst durch sichere E-Mail-Gateways in die Posteingänge von Nutzern und Nutzerinnen gelangen. Laut einem Report des Check Point Email Research Team von ArmorBlox wurden 2022 56 % der E-Mail-Angriffe von herkömmlichen Sicherheitsfiltern nicht erfasst und bei Einsatz von Exchange Online Protection und Defender von Microsoft gelangten 18,8 % der Phishing-E-Mails in Posteingänge der Nutzer und Nutzerinnen.[2]

7. ANPASSBARE WORKFLOWS

Es gibt keine Universallösung für Phishing-Analyse und -Schutz. Unternehmen, Institutionen und Organisationen haben jeweils eigene Workflows und Prozesse. Entscheiden Sie sich für eine flexible SOAR-Plattform, bei der Automatisierungsworkflows individuell angepasst werden können. Das ist bei der Analyse verdächtiger E-Mails, der Kategorisierung von Vorfällen und der Einleitung vordefinierter Maßnahmen gleichermaßen von Bedeutung.

---

2 Check Point Microsoft Defender Report

8. TRAININGSVORLAGEN AUS ECHTEN PHISHING-ANGRIFFEN

Viele Unternehmen, Institutionen und Organisationen möchten anhand von simulierten Phishing-E-Mails, die realen Bedrohungen entsprechen, testen, ob Nutzer und Nutzerinnen diese erkennen und melden. SOAR-Produkte sollten daher schädliche Phishing-E-Mails problemlos unschädlich machen, damit diese als Vorlagen für Trainingszwecke eingesetzt werden können. Diese Funktion ergänzt Ihr vorhandenes Security Awareness Training Program.

Aus gemeldeten und entfernten E-Mail-Bedrohungen sollten sich „entschärfte" Versionen erstellen und automatisch in simulierten Phishing-Kampagnen für Nutzer und Nutzerinnen einsetzen lassen. Außerdem sollten sich hierbei echte Phishing-E-Mails, die in Posteingängen gelandet sind (jedoch noch nicht geöffnet wurden), durch die „entschärfte" Version ersetzen lassen. Dadurch schulen Sie die Aufmerksamkeit der Nutzer und Nutzerinnen für reale Bedrohungen.

FAZIT

Der ungehinderte Betrieb von Unternehmen, Institutionen und Organisationen lässt sich nur mithilfe einer umfassenden Strategie zur Bekämpfung von Phishing-Angriffen sicherstellen. SOAR-Tools ermöglichen dank ihrer Orchestrierungs-, Automatisierungs- und Reaktionsfunktionen eine umfassende Verteidigung.

Der Markt für SOAR-Produkte zur Phishing-Abwehr ist so vielfältig wie die entsprechenden Social-Engineering-Bedrohungen. Das SOAR-Produkt, für das Sie sich entscheiden, muss letztlich die mittlere Reaktionszeit optimal verkürzen und Phishing-Bedrohungen entschärfen, bevor diese in die Posteingänge ihrer Nutzer und Nutzerinnen gelangen. Zugleich muss es vorhandene Maßnahmen zur Gewährleistung der E-Mail-Sicherheit ergänzen. Das Produkt sollte Ihr IT-Team mithilfe von KI-gestützter Automatisierung und über Crowdsourcing gewonnene Bedrohungsdaten entlasten, damit es sich auf die Orchestrierung und Analyse konzentrieren und so das Phishing-Risiko reduzieren kann.

KNOWBE4 PHISHER PLUS

PhishER Plus ist ein unkompliziertes SOAR-Produkt, mit dem sich die Reaktion auf Phishing-Bedrohungen orchestrieren und die E-Mail-Sicherheit in Unternehmen, Institutionen und Organisationen erhöhen lässt. PhishER Plus vereint eine zuverlässige, auf maschinellem Lernen basierende E-Mail-Analyse, prioritätsabhängige Isolierung und Blocklisting-Funktionen mit dem branchenweit leistungsstärksten Feed zu globalen Bedrohungen für proaktiven Phishing-Schutz.

Der Feed zu globalen Bedrohungen von PhishER Plus ist dreifach validiert und blockiert Angriffe mit Phishing-E-Mails, bevor diese in die Posteingänge Ihrer Nutzer und Nutzerinnen gelangen. Dieser Feed umfasst drei wichtigen Komponenten:

1. Ein globales KnowBe4-Netzwerk mit mehr als 10 Millionen bestens geschulten Endnutzern und Endnutzerinnen sowie PhishER-Administratoren und -Administratorinnen
2. PhishML, eine einzigartige KI-Engine, gespeist mit Phishing-E-Mails, die alle anderen Filter nicht erkannt haben
3. Von Menschen ausgewählte Bedrohungsdaten aus dem Threat Research Lab von KnowBe4

Beschleunigen Sie mit PhishER Plus von KnowBe4 die Identifizierung von Phishing-Bedrohungen sowie die entsprechende Reaktion.

Mehr erfahren

Vereinbaren Sie eine Demo.

Demo vereinbaren

Weitere Ressourcen

Kostenloser Phishing Security Test
Wie anfällig sind Ihre Mitarbeitenden für Phishing? Unser kostenloser Phishing Security Test verrät es Ihnen.

Kostenloses Automated Security Awareness Program
Erstellen Sie ein auf Ihr Unternehmen, Ihre Institution oder Ihre Organisation abgestimmtes Security Awareness Program.

Phish Alert Button (kostenlos)
Mit diesem Tool können Mitarbeitende ab sofort Phishing-Angriffe mit nur einem Klick sicher melden.

Email Exposure Check (kostenlos)
Welche Ihrer E-Mail-Anmeldedaten wurden bereits offengelegt? Werden Sie aktiv, bevor es die Kriminellen tun.

Domain Spoof Test (kostenlos)
Finden Sie heraus, ob Hacker E-Mail-Adressen Ihrer Domain spoofen können.

Über KnowBe4

KnowBe4 ist der Anbieter der weltweit größten integrierten Plattform für Security Awareness Training und Phishing-Simulationen. Der Faktor Mensch wurde bei Sicherheitstrainings bisher deutlich vernachlässigt. In den umfangreichen KnowBe4-Programmen werden Mitarbeitende über die fortlaufenden Gefahren von Social Engineering aufgeklärt und erfahren, wie sie Ihr Unternehmen, Ihre Institution oder Ihre Organisation schützen können.

Der neue Ansatz kombiniert elementare Tests auf Basis realer Angriffsszenarien, kurzweilige interaktive Trainings, kontinuierliches Assessment anhand von simulierten Phishing-Versuchen sowie aussagekräftige Reports, um Unternehmen, Institutionen oder Organisationen durch sicherheitsbewusstes Handeln besser vor tatsächlichen Angriffen zu schützen.

Weltweit nutzen Zehntausende Unternehmen, Institutionen oder Organisationen aus unterschiedlichsten Branchen – darunter auch stark reglementierte Bereiche wie das Finanzwesen, das Gesundheitswesen, die Energiebranche, die öffentliche Verwaltung und das Versicherungswesen – die KnowBe4-Plattform, um Nutzer und Nutzerinnen in die Lage zu versetzen, kompetente Entscheidungen hinsichtlich Cybersicherheit zu treffen.

Weitere Informationen finden Sie auf www.KnowBe4.de.

KnowBe4
Human error. Conquered.

KnowBe4 Germany | Rheinstr. 45/46 | 12161 Berlin – Deutschland
Tel.: +49 30 34 64 64 60 | knowbe4.de | Email: kontakt@knowbe4.com

04D09K01