KnowBe4

AIDA – Tools von KnowBe4 für das Human Risk Management

Inhaltsverzeichnis

Einführung

Die Bedrohung durch KI-gestützte Cyberangriffe nimmt zu. Fachkräfte aus der Informationssicherheit blicken sorgenvoll auf diese Entwicklung. Branchenstudien belegen, dass über 95 % der Fachkräfte aus dem Bereich Cybersicherheit davon ausgehen, dass mit KI-generierter Content das Erkennen von Phishing erschwert.

Akteurinnen und Akteure mit schlechten Absichten sind aufgrund dieser technologischen Weiterentwicklung in der Lage, absolut überzeugende Social-Engineering-Angriffe zu erstellen. Ein allgemeines, unspezifisches Security Awareness Training (SAT) reicht nicht mehr aus.

Ab sofort können Sie dieses Problem mit KI bekämpfen, genauer gesagt mit AIDA von KnowBe4, Ihren Artificial Intelligence Defense Agents. AIDA ist eine Suite mit KI-gestützten Agenten und hilft Ihnen dabei, Ihr Human Risk Management (HRM) deutlich zu verbessern. Mithilfe verschiedener KI-Technologien erstellt AIDA für alle Nutzerinnen und Nutzer personalisierte, anpassungsfähige und hoch effektive Trainings, die eine nachhaltige Verhaltensänderung bewirken.

In diesem Whitepaper erfahren Sie, wie Sie mit diesen ersten vier AIDA-Agenten das Risiko durch den Faktor Mensch in den Griff bekommen. Darüber hinaus werden Anwendungsbeispiele erläutert.

Was ist AIDA?

AIDA ist eine umfassende KI-Suite mit Agenten, die Ihre Organisationen bei der Transformation des SAT-Konzepts unterstützen. Mithilfe von KI stellt AIDA personalisiertes, effizientes und anpassungsfähiges Training bereit, das die Risiken der Organisation reduziert und nachhaltige Verhaltensänderungen bewirkt.

Im Gegensatz zu herkömmlichen SAT-Tools lernt AIDA von KnowBe4 kontinuierlich dazu und passt sich den spezifischen Anforderungen Ihrer Organisation an. Dadurch wird eine maximale Wirkung und ein maximaler ROI in Bezug auf Ihr Security Awareness Training gewährleistet. Ein Beispiel: Ihre Administratorinnen und Administratoren benötigen mit AIDA nicht mehr durchschnittlich sieben Tage, um Training Content zu erstellen, sondern nur noch wenige Augenblicke. Daher entlastet AIDA Ihr Sicherheitsteam deutlich.

Im Folgenden finden Sie einen ersten Überblick über die ersten vier AIDA-Agenten:

Agent für automatisiertes Training: Verwendet KI mit 316 Indikatoren, die 37 Faktoren in 7 Wissensgebieten beeinflussen, um die Lernkurve, die Rolle, den Risk Score, die Verhaltensmuster und sogar die bevorzugten Sprachen Ihrer Nutzerinnen und Nutzer zu analysieren, sodass AIDA automatisch relevanten und motivierenden Content zuweisen kann. Dadurch wird sichergestellt, dass Nutzerinnen und Nutzer ungeachtet von Position oder Standort Training erhalten, das auf die jeweiligen Bedürfnisse und Lernstile abgestimmt ist. Dies trägt dazu bei, die Wissensvermittlung und Anwendung in der Praxis Ihrer bewährten Sicherheitsmethoden zu maximieren.

Agent für Vorlagengenerierung: Mithilfe von generativer KI erstellt AIDA anhand von aktuellen Angriffsvektoren besonders realistische Phishing-Vorlagen. Social-Engineering-Indikatoren oder Warnsignale basieren auf dem NIST Phish Scale.

Agent für Auffrischungsübungen: AIDA generiert in optimalen Zeitintervallen passende Auffrischungsübungen, damit die Nutzerinnen und Nutzer kritische Sicherheitskonzepte auch tatsächlich anwenden.

Agent für Richtlinienquiz: AIDA generiert intelligente Quiz basierend auf den spezifischen Sicherheits- und Compliance-Richtlinien Ihrer Organisation. Dadurch wird sichergestellt, dass Ihre Nutzerinnen und Nutzer die Vorgaben, an die sie sich halten sollen, zur Kenntnis nehmen und wirklich verstehen.

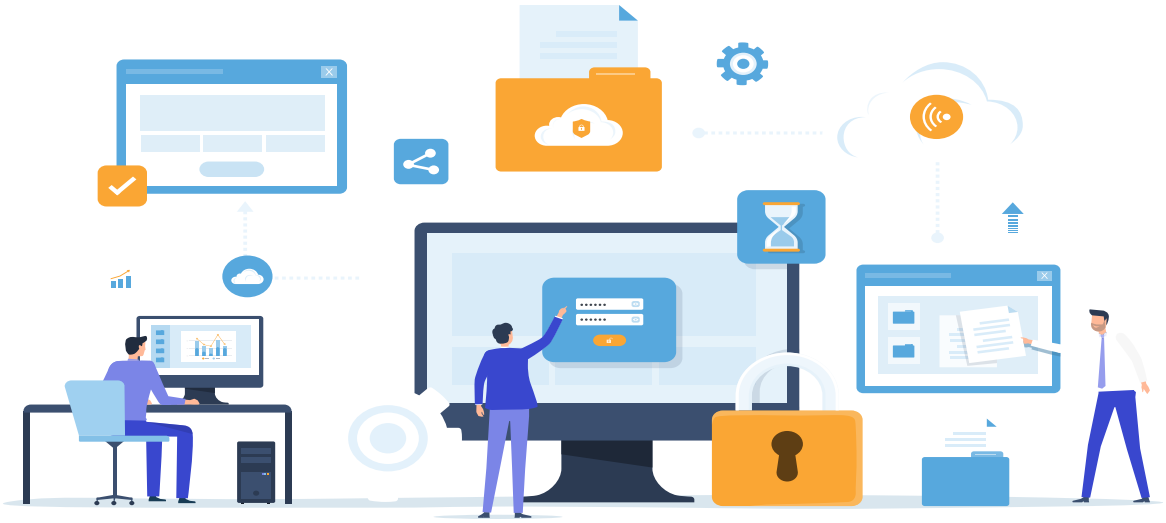
Vorteile für das Human Risk Management

HRM ist ein moderner Ansatz, den fortlaufenden Bedarf an starken Sicherheitskulturen in Organisationen jeder Größe zu befriedigen. Es geht nicht mehr nur darum, SAT regelmäßig anzubieten. Vielmehr soll eine positive Sicherheitskultur etabliert werden. Dieses Ziel wird mit den folgenden drei Haupttaktiken verfolgt:

1. Quantifizierung des Risikos durch den Faktor Mensch durch Erfassen und Messen der Verhaltensweisen
2. Bereitstellung von relevantem, angepasstem Training Content
3. Durchführung von Auffrischungsübungen, damit die Nutzerinnen und Nutzer wissen, wie sie sich vor häufigen und schwerwiegenden Cyberrisiken schützen können

Herkömmliches SAT ist in komplexem Arbeitsumgebungen nicht mehr effektiv. Ein jährliches Training reicht bei Weitem nicht mehr aus. Ihre Nutzerinnen und Nutzer haben bereits viel zu tun. Das angebotene Training muss daher darauf ausgelegt sein, die Zeit optimal zu nutzen. Mit der richtigen HRM-Strategie können Sie relevante und motivierende Inhalte für verschiedene Rollen, Abteilungen und Sprachen bereitstellen, die das Verhalten von Nutzerinnen und Nutzern nachhaltig verändern. AIDA steht bei diesen Bemühungen im Mittelpunkt.

Im Folgenden gehen wir auf die ersten vier AIDA-Agenten näher ein. Im Anschluss blicken wir in die Zukunft.



Die ersten vier AIDA-Agenten

Hinter diesen ersten vier Agenten steht eine zentrale KnowBe4-Funktion: der SmartRisk Agent™. Diese Funktion stellt verwertbare Daten und Kennzahlen (den Risk Score) bereit, mit denen Sie einen besseren Einblick in die Stärken und Schwächen der Sicherheit Ihrer Organisation erhalten können.

Der SmartRisk Agent berechnet anhand von Verhaltensdaten der Endnutzerinnen und Endnutzer aller KnowBe4-Produkte das Risiko, das durch den Faktor Mensch entsteht. Die multidimensionalen Risk Scores dieses Agenten sollen es Ihnen erleichtern, potenzielle Probleme auf Nutzer-, Gruppen- und Organisationsebene zu erkennen. Je mehr Produkte von KnowBe4 Sie verwenden, desto tiefgreifendere Einblicke erhalten Sie.

Funktionsumfang unserer ersten vier Agenten:

Agent für automatisiertes Training

Funktion

Der Agent für automatisiertes Training analysiert mehrere Datenpunkte, darunter Risk Scores, Phishing-Testergebnisse und individuelle Lernvorlieben, und stimmt das Training so auf die einzelnen Nutzerinnen und Nutzer ab. Wissenslücken werden ermittelt und mit Lernmodulen aus der umfangreichen Inhaltsbibliothek im ModStore von KnowBe4 gezielt beseitigt.

Verwendungsweise

Konfigurieren Sie den Agenten so, dass er den spezifischen Anforderungen Ihrer Organisation entspricht. In der KnowBe4-Konsole können Sie Kriterien für die Registrierung, die Dauer des Trainings und Benachrichtigungs-einstellungen festlegen. Im Testmodus des Agenten können Sie die Trainingsempfehlungen vor der Bereitstellung als Vorschau anzeigen, um sicherzustellen, dass geeignete Trainingsmodule automatisch zugewiesen werden.

Sie möchten die Performance im Blick behalten? Sie haben Zugriff auf Tracking-Kennzahlen wie Abschlussquoten von Trainingsmodulen und Umfrageergebnisse, um die Effektivität Ihres Trainingsprogramms zu messen.

Anwendungsbeispiele

Beseitigung von Phishing-Schwachstellen: Anhand von Reaktionen oder Fehlern Ihrer Nutzerinnen und Nutzer in bestimmten simulierten Phishing-Tests können Sie Training automatisch zuweisen. Die Nutzerinnen und Nutzer werden darin über Phishing-Strategien und -Taktiken aufgeklärt.

Onboarding neuer Mitarbeitender: Bewerten Sie den Risk Score neuer Mitarbeitender und bieten Sie SAT an, das auf den vorhandenen Wissensstand abgestimmt ist, indem Sie gezielt Smart Groups einsetzen.

Agent für Vorlagengenerierung

Funktion

Der Agent für Vorlagengenerierung erstellt mithilfe der integrierten generativen KI absolut überzeugende Phishing-E-Mails, die auf die spezifischen Anforderungen und das Risikoprofil Ihrer Organisation abgestimmt sind. Verschiedene Phishing-Szenarien mit unterschiedlichem Schwierigkeitsgrad, Tonfall und Angriffsvektor können in mehreren Sprachen erstellt werden. Ihre Nutzerinnen und Nutzer werden so auf das gesamte Spektrum potenzieller Bedrohungen vorbereitet.

Verwendungsweise

Sie können die Sprache, das Gebietsschema, den Tonfall und den gewünschten Angriffsvektor in wenigen Augenblicken festlegen. Stimmen Sie den Schwierigkeitsgrad simulierter Phishing-E-Mails durch die Auswahl bestimmter Social-Engineering-Indikatoren (SEI) ab oder wählen Sie einen vordefinierten Schwierigkeitsgrad aus. Die erstellten Vorlagen können als Vorschau angezeigt, bearbeitet und für die künftige Verwendung gespeichert werden. Sie sparen dadurch wertvolle Zeit beim Erstellen und Verwalten eines robusten Phishing-Simulationsprogramms.

Anwendungsbeispiele

Simulation von Business Email Compromise (BEC): Lassen Sie eine Woche pro Monat oder einmal im Quartal spezifische BEC-E-Mails erstellen, die den Anschein erwecken, von Ihrer CEO oder Ihrem CEO oder anderen Führungskräften zu stammen. Der Agent kann mithilfe von generativer KI den Schreibstil von Führungskräften imitieren und um eine Überweisung oder eine andere dringende Angelegenheit bitten.

Phishing-Tests in mehreren Sprachen: Stellen Sie für Ihre internationale Belegschaft Phishing-E-Mails in mehreren Sprachen bereit. Die Vorlagengenerierung kann den E-Mail-Text sogar sprachlich und kulturell an eine bestimmte Region anpassen.

Schnelle Reaktion auf neue Bedrohungen: Es tauchen immer wieder neue Cyberangriffe auf. Mit der Vorlagengenerierung können Sie in wenigen Minuten einen doppelten simulierten Phishing-Angriff erstellen und Ihre Mitarbeitenden auf neue Bedrohungen vorbereiten.

Agent für Auffrischungsübungen

Funktion

Der Agent für Auffrischungsübungen hilft Nutzerinnen und Nutzern dabei, ihre Kenntnisse in Bezug auf Cybersicherheit aufzufrischen und sich Abzeichen zu verdienen, indem sie Quizfragen zu bestimmten Szenarien beantworten. KI-generierte Auffrischungsübungen bieten eine unterhaltsame und schnelle Möglichkeit, die wichtigsten Erkenntnisse aus dem zurückliegenden Training zu wiederholen.

Verwendungsweise

Aktivieren und konfigurieren Sie die Funktion auf der Registerkarte „AIDA-Training“ oder beim Erstellen einer neuen Trainingskampagne. Hier können Sie Parameter wie das Zeitintervall zwischen dem Trainingsabschluss und der Verfügbarkeit von Auffrischungsübungen festlegen. Nach der Aktivierung stehen die Auffrischungsübungen im Nutzerbereich zur Verfügung. Ihre Nutzerinnen und Nutzer können ihren Lernprozess dadurch optimieren.

Anwendungsbeispiele

Stärkung des Bewusstseins für Phishing: KI-generierte Auffrischungsübungen, in denen verschiedene Szenarien thematisiert werden, können im Rahmen von unterstützendem Training eingesetzt werden, wenn Nutzerinnen und Nutzer auf eine simulierte Phishing-E-Mail geklickt haben. Dieses kontinuierliche Training stärkt die Wachsamkeit gegenüber neuen Phishing-Taktiken.

Wissensvermittlung durch Compliance-Training: Durch regelmäßige, gezielte Auffrischungsübungen zu wichtigen Compliance-Themen können Organisationen, die bestimmte gesetzliche Anforderungen erfüllen müssen, ihrer Sorgfaltspflicht nachkommen und eine Compliance-Kultur etablieren, wodurch die Haftbarkeit verringert und die Ergebnisse von Audits verbessert werden können.

Agent für Richtlinienquiz

Funktion

Dieser KI-gestützte Agent für Richtlinienquiz generiert automatisch Quiz basierend auf den spezifischen Richtlinien Ihrer Organisation. Es wird darauf geachtet, dass die Mitarbeitenden wichtige Informationen nicht nur lesen, sondern auch verstehen und sich daran halten.

Verwendungsweise

Fügen Sie die Richtlinie Ihrer Organisation in Ihrer KnowBe4-Konsole als PDF-Datei hinzu. Danach können Sie Quizfragen zur Richtlinie bearbeiten und verwalten und dann eine Trainingskampagne erstellen, um die Richtlinie Ihren Nutzerinnen und Nutzern zuzuweisen. Nachdem Sie die Richtlinie einer Kampagne zugewiesen haben, können Sie den Fortschritt und die Kenntnisnahmen der Nutzerinnen und Nutzer verfolgen.

Anwendungsbeispiele

Onboarding neuer Mitarbeitender: Stellen Sie mithilfe von individuell erstellten Richtlinienquiz sicher, dass neue Mitarbeitende die Richtlinien nicht nur lesen, sondern auch verstehen. Nehmen Sie dieses Ergebnis als Maßstab für das erste Compliance-Training und reduzieren Sie das Risiko von Richtlinienverstößen aufgrund von Missverständnissen.

Jährliche Richtliniendurchsicht: Optimieren Sie den Prozess der jährlichen Richtliniendurchsicht. Der Agent für Richtlinienquiz erstellt schnell aktualisierte Quiz, in denen Änderungen an den Richtlinien und Regeln der Organisation berücksichtigt werden. Richtlinienbasierte Trainingskampagnen optimieren die Wissensvermittlung und liefern Administratorinnen und Administratoren klare Kennzahlen über das Verständnis der Richtlinien der Organisation. Es können Bereiche ermittelt werden, in denen zusätzliches Training erforderlich ist.

Blick in die Zukunft

Die Funktionen dieser vier Agenten werden im Laufe der Zeit immer besser. Es kommt ein KI-gestütztes Orchestrierungsmodell zum Einsatz, das mit einem zielbasierten, fortlaufenden Ansatz die Risiken durch den Faktor Mensch in Ihrer Organisation deutlich verringert.

Dies ist jedoch erst der Anfang. Neue Agenten sind in Planung:

- **Agent für Orchestrierung:** Dieser KI-gestützte Agent übernimmt die Rolle einer SAT-Administratorin bzw. eines SAT-Administrators und verwaltet Phishing-Simulationen, Bereitstellung und Reporting.
- **Agent für Zielerreichung:** Dieser Agent optimiert die Zielbestimmung, Angriffsvektoren und Trainingshäufigkeit, um die Risiken durch den Faktor Mensch in Ihrer Organisation zu verringern.
- **Agent für anpassungsfähige Abwehr:** Dieser Agent setzt Trainingseinheiten unter Berücksichtigung von Arbeitsplänen und aktuellen Bedrohungen zum geeignetsten Zeitpunkt an und stimmt den Content auf neue Risiken ab.
- **Agent für SAT-Assessments:** Dieser Agent erstellt individuelle SAT-Assessments basierend auf den spezifischen Richtlinien und Verfahren Ihrer Organisation.

Fazit

AIDA ist nicht einfach der nächste Schritt von KnowBe4 in Sachen Human Risk Management, diese Suite an KI-Agenten ist ein echter Quantensprung. Mit AIDA und der Möglichkeit, KI-Bedrohungen mithilfe von KI zu begegnen, ist Ihre Organisation der Zeit voraus.

Vorteile von AIDA für Ihre Organisation:

- AIDA ist auf den NIST Phish Scale abgestimmt. Dadurch entspricht Ihr SAT den Anforderungen allgemeiner Sicherheitsinitiativen Ihrer Organisation.
- Ihre Administratorinnen und Administratoren benötigen mit AIDA nicht mehr durchschnittlich sieben Tage, um Training Content zu erstellen, sondern nur noch wenige Augenblicke. Daher entlastet AIDA Ihr Sicherheitsteam in großem Maße.
- Verbessern Sie die Zusammenarbeit zwischen Ihrem Sicherheitsteam und anderen Abteilungen, indem Sie sicherstellen, dass alle Nutzerinnen und Nutzer die Sicherheitsziele kennen. Dadurch stärken Sie die Sicherheitskultur Ihrer Organisation.
- Indem Sie die Risiken durch den Faktor Mensch aktiv und effizient im Griff behalten, können Sie Ihr Budget für Sicherheit flexibel für andere wichtige Initiativen einsetzen.
- Maximieren Sie durch eine problemlose Integration von AIDA den Wert Ihres vorhandenen Security Tech Stack.

KnowBe4 ist der einzige Anbieter, der Security Awareness, Verhalten und Sicherheitskultur berücksichtigt, sodass Organisationen durch den Faktor Mensch verursachte Cybersicherheitsrisiken mindern können. KnowBe4 hilft Organisationen durch datengestütztes Human Risk Management beim Aufbau einer starken Sicherheitskultur.

AIDA in Aktion

Weitere Ressourcen

Kostenloser Phishing Security Test
Finden Sie mit dem kostenlosen Phishing Security Test heraus, wie viele Mitarbeitende auf eine Phishing-Simulation hereinfallen (Phish-prone Percentage).

Kostenloses Automated Security Awareness Program (ASAP)
Erstellen Sie ein individuelles Security Awareness Program für Ihre Organisation.

Kostenloser Phish Alert Button
Bieten Sie Ihren Mitarbeitenden die Möglichkeit, Phishing-Angriffe mit einem Klick zu melden.

Kostenloser Email Exposure Check
Finden Sie heraus, welche E-Mail-Adressen Ihrer Organisation offengelegt wurden, bevor es Cyberkriminelle tun.

Kostenloser Domain Spoof Test
Finden Sie heraus, ob Hackerinnen oder Hacker eine E-Mail-Adresse Ihrer Domain spoofen können.

Über KnowBe4

KnowBe4 befähigt Ihre Mitarbeitenden, jeden Tag intelligente Sicherheitsentscheidungen zu treffen. Zehntausende von Organisationen weltweit stärken mit der KnowBe4-Plattform ihre Sicherheitskultur und reduzieren menschliche Fehler. KnowBe4 stärkt die Abwehrkräfte von Organisationen durch den Aufbau einer zuverlässigen Human Firewall mit New-School Security Awareness and Compliance Training.

KnowBe4 sorgt dafür, dass Nutzerinnen und Nutzer wachsam sind und Phishing, Ransomware sowie andere Social-Engineering-Bedrohungen abwenden möchten. Auf der Plattform steht Ihnen ein umfassendes Angebot zur Verfügung: Security Awareness and Compliance Training, Coaching in Echtzeit, KI-gestützte Social-Engineering-Simulationen und Phishing-Abwehr mithilfe der Crowd.

Die Inhalte werden in mehr als 35 Sprachen lokalisiert. Damit bietet KnowBe4 die weltweit größte Bibliothek mit stets aktuellen und ansprechenden Inhalten zur Stärkung Ihrer Human Firewall.

Weitere Informationen unter www.KnowBe4.com

KnowBe4

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

04F01K01