

Die HRM+ Plattform von KnowBe4 ist eine innovative Ressource für das Human Risk Management. Es handelt sich um eine umfangreiche Best-of-Suite-Plattform mit KI-Unterstützung, die Nutzerinnen und Nutzer auf die Abwehr aktueller Cyberbedrohungen vorbereitet.

Als einzige globale Sicherheitsplattform ihrer Art sorgt HRM+ dafür, dass Ihre Mitarbeitenden von der größten Angriffsfläche zur größten Stärke werden, indem sie Ihre Organisation aktiv vor Cybersicherheitsbedrohungen schützen.



HRM+ umfasst die folgenden Produkte:



Security-Awareness-Training

Mit KI-gestütztem New-School Security-Awareness-Training und Phishing-Simulationen können Unternehmen und Organisationen Mitarbeitende sensibilisieren und Verhaltensänderungen herbeiführen.



E-Mail-Sicherheit in der Cloud

Die einzige E-Mail-Sicherheitsinfrastruktur, die das Risiko durch den Faktor Mensch kontinuierlich bewertet und Sicherheitskontrollen dynamisch anpasst.



Phishing-Abwehr

Sicherheitsorchestrierung und proaktive Phishing-Abwehr, damit Ihre Incident-Response- und Sicherheitsorchestrierungs-Teams Phishing-Bedrohungen erkennen und abwenden können, bevor sie in den Posteingängen Ihrer Nutzerinnen und Nutzer landen.



Echtzeit-Coaching

Das erste Echtzeit-Sicherheitscoaching, das riskantes Verhalten von Nutzerinnen und Nutzern erkennt und sofort Feedback bereitstellt.



Compliance-Training

New-School Compliance-Training mit stets aktuellem Content. Ihre Organisation kann mit diesem Produkt einen umfassenden Ansatz für Security-Awareness-Training und Compliance-Training verfolgen.



Artificial Intelligence Defense Agents

AIDA ist eine Suite fortschrittlicher KI-gestützter Agenten, mit denen Sie Ihre Strategie für das Human Risk Management auf die Zukunft ausrichten können.

Bewusstsein schaffen und Verhalten ändern

Sicherheitskontrollen dynamisch anpassen

Phishing-Bedrohungen identifizieren und stoppen

Erkennen und reagieren

New-School Training Content

Human Risk Management auf die Zukunft ausrichten

KnowBe4 HRM+ Personalisiert. Relevant. Anpassungsfähig.

Wesentliche Vorteile

Mit HRM+ bekommen Organisationen schwierige Herausforderungen im Bereich der Cybersicherheit in den Griff:



Social-Engineering- und Phishing-Angriffe stellen das größte Cyberrisiko für Organisationen dar und sind der primäre Angriffsvektor in Bezug auf Datenschutzverletzungen und Ransomware.



Akteurinnen und Akteure mit schlechten Absichten nutzen KI, um komplexe Phishing- und Social-Engineering-Angriffe in großem Maßstab zu erstellen.



Das Phishing-Risiko von Organisationen erhöht sich, wenn IT-/Sicherheitsteams personell unterbesetzt und unzureichend ausgestattet sind sowie wenn veraltete Strategien zur Analyse und Abwehr von Phishing-E-Mails zum Einsatz kommen.



Führungskräfte sind sich einig, dass der Aufbau einer Sicherheitskultur hohe Priorität hat. Unklarheit herrscht jedoch darüber, wie der erfolgreiche Aufbau aussehen soll und wie das Risiko durch den Faktor Mensch gemessen werden kann.



Die gesetzlichen Vorgaben hinsichtlich der Offenlegung des Cybersicherheitsstatus sowie der entsprechenden Berichterstattung werden zunehmend strenger.



Herkömmliches Security-Awareness-Training führt zu keiner Verhaltensänderung bei Nutzerinnen und Nutzern. Hierfür sind regelmäßige Tests mit simulierten Phishing-Versuchen und entsprechendes Echtzeit-Coaching erforderlich.



Mir bereitet in Bezug auf KI und Cybersicherheit wirklich große Sorgen, dass Cyberkriminelle, extrem überzeugende Phishing-Angriffe erstellen können, die nur noch anhand weniger Warnsignale erkennbar sind.“

– **Leiter eines Teams für Informationssicherheit**



Social-Engineering- und Phishing-Angriffe bedrohen die Cybersicherheit immens. Sie stellen das größte Cyberrisiko für meine Organisation dar. Diese Bedrohungen sind die Hauptursache für Datenschutzverletzungen, Ransomware-Angriffe und Malware-Infektionen.“

– **CISO**



Wir haben uns das Angebot auf dem Markt genau angesehen. Vielen SAT-Produkten fehlt die Vielfalt, die Benutzerfreundlichkeit und eine gewisse Breite der Inhalte. All dies ist jedoch erforderlich, um das Verhalten der Mitarbeitenden wirklich zu ändern.“

– **IT-Admin**

Produktfunktionen

Security Awareness Training

KnowBe4 bietet das weltweit größte Angebot an Security-Awareness- und Compliance-Training sowie Social-Engineering-Simulationen. Die Plattform umfasst die branchenweit umfangreichste Bibliothek mit ansprechenden, in 35 Sprachen lokalisierten Inhalten, Phishing-Simulationen auf Basis von KI und Training, das sich an die Nutzerinnen und Nutzer anpasst, umfangreichem Reporting sowie robusten Nutzertests und Assessments, die für Sensibilisierung sorgen und Verhaltensänderungen bewirken. Im Schnitt reduziert sich der Phish-prone™ Percentage einer Organisation durch das Security Awareness Training von KnowBe4 nach 12 Monaten von über 30 % auf unter 5 %.

[Mehr erfahren](#) →

AIDA

AIDA (Artificial Intelligence Defense Agents) ist die innovative Suite von KnowBe4 mit KI-gestützten Sicherheitsagenten, die das Human Risk Management erleichtern und automatisieren. AIDA bietet umfangreiche und anpassungsfähige Funktionen, die sich mit der Bedrohungslage weiterentwickeln. Durch den Einsatz mehrerer KI-Technologien vereint AIDA menschliche und künstliche Intelligenz, um das Risiko durch den Faktor Mensch zu reduzieren. AIDA umfasst erweitertes Reporting nach Rolle, Reports für Führungskräfte und mehr.

[Mehr erfahren](#) →

Compliance Plus

Compliance Plus ist eine umfassende Bibliothek für professionelles Compliance-Training. Die mehr als 700 Module mit weltweit einsetzbarem, laufend aktualisiertem, ansprechendem, relevantem, prägnantem und anpassbarem Content vermitteln den Mitarbeitenden, wie sie die auf der jeweiligen lokalen Ebene gültigen Vorschriften ihrer Organisation einhalten.

Die enge Integration von Compliance Plus in das KSAT-Training von KnowBe4 ermöglicht Ihrer Organisation beim Sicherheits- und Compliance-Training einen umfassenden Ansatz, durch den sich das Risiko von Geldbußen, Rufschädigung, Kundenabwanderung und weiteren Problemen mindern lässt.

[Mehr erfahren](#) →

SecurityCoach

SecurityCoach ist das erste Echtzeit-Sicherheitscoaching, das IT- und SOC-Teams dabei unterstützt, die größte Angriffsfläche Ihrer Organisation zu schützen – Ihre Mitarbeitenden. SecurityCoach stärkt Ihre Sicherheitskultur, indem Ihre Nutzerinnen und Nutzer bei riskantem Verhalten ein Echtzeit-Sicherheitscoaching erhalten.

In dem Moment, in dem riskantes Nutzerverhalten erkannt wird, erhalten die entsprechenden Nutzerinnen und Nutzer über Microsoft Teams, Slack, Google Chat oder per E-Mail einen Echtzeit-SecurityTip von SecurityCoach. Diese Sofortbenachrichtigungen sind eine wirkungsvolle Erweiterung zu jedem Security-Awareness-Programm.

[Mehr erfahren](#) →

Produktfunktionen (Fortsetzung)



PhishER ist ein schlankes SOAR-Produkt, das gemeldete E-Mail-Nachrichten automatisch analysiert und kategorisiert, um schädliche E-Mails zu identifizieren und unter Quarantäne zu stellen. Darüber hinaus werden gemeldete Phishing-E-Mails in entschärfter Form für Phishing-Simulationen verwendet.

PhishER Plus stellt eine KI-validierte Blockliste und PhishRIP-Funktionen bereit, mit denen sich aktuelle Phishing-E-Mails, die durch die Filter gelangt sind, proaktiv blockieren und entfernen lassen, BEVOR diese in die Posteingänge von Nutzerinnen und Nutzer gelangen. Das SOC-Team hat weniger Aufwand bei der Bedrohungsabwehr, was zu deutlichen finanziellen Einsparungen und der Freisetzung von InfoSec-Kapazitäten führt.

Maschinelles Lernen sowie die KI-gestützte Analyse und Priorisierung von E-Mails sorgen dafür, dass bei der Ermittlung der hochriskanten Phishing-Bedrohungen in der Gesamtheit der von den Nutzerinnen und Nutzer gemeldeten Mitteilungen nicht länger auf Mutmaßungen zurückgegriffen werden muss. Zugleich ermöglichen sie die Automatisierung des Sicherheitsworkflows für den Umgang mit den 90 % der unbedenklichen gemeldeten E-Mails. So kann Ihre Organisation ein vollständig orchestriertes und hocheffektives SOC-Teams aufbauen, das Social-Engineering-Bedrohungen nahezu in Echtzeit erkennen und abwehren kann.

Mehr erfahren →



Ein neuer Ansatz für E-Mail-Sicherheit. KnowBe4 ist das einzige E-Mail-Sicherheitsprodukt, das Ihnen bei der Bewertung des menschlichen Risikos hilft und die Richtlinienkontrollen dynamisch anpasst, um Schutz vor fortschrittlichen Phishing-Angriffen und Datenschutzverletzungen bei ausgehenden Mitteilungen zu bieten. Mithilfe von kontextbezogenem maschinellem Lernen und neuronalen Netzwerken sowie einer nahtlosen Integration über eine cloudnative API-Architektur profitieren Sie von einem verbesserten E-Mail-Schutz, einem umfassenden Einblick in das Risiko durch den Faktor Mensch und einer schnellen Amortisierung Ihrer Investition.

Mehr erfahren →

Weitere Informationen auf

KnowBe4.de →