HORNETSECURITY

# AI CYBER ASSISTANT

## DER ULTIMATIVE SECURITY-BOOSTER FÜR MICROSOFT 365

## IMMER AN IHRER SEITE

Der AI Cyber Assistant ist Ihr neuer, aufmerksamer KI-Sicherheitsassistent. Er unterstützt Endbenutzer bei der sicheren Kommunikation und reduziert gleichzeitig den Arbeitsaufwand für Administratoren erheblich. Nahtlos in die Hornetsecurity-Lösungen für Microsoft 365 integriert, entwickelt sich der AI Cyber Assistant dank unserer Machine-Learning-Technologie kontinuierlich weiter – und liefert genau dann Unterstützung, wenn Sie sie am dringendsten benötigen.

### AI CYBER ASSISTANT STELLT NEUE LÖSUNGEN BEREIT


AI EMAIL SECURITY ANALYST

Entlasten Sie Ihre SOC-Ressourcen, ohne dabei Kompromisse bei der E-Mail-Sicherheit einzugehen. Im Gegenteil: Verbessern Sie diese dank Automatisierung und sofortigem Feedback für Endbenutzer!

Der AI Email Security Analyst automatisiert die Analyse und Beantwortung von gemeldeten, potenziell gefährlichen E-Mails und ersetzt damit die herkömmliche manuelle Analyse. Basierend auf den neuesten Security-Intelligence-Updates erhalten Nutzer automatisch eine KI-gestützte Echtzeit-Analyse ihrer gemeldeten E-Mails – inklusive:

- Verständlicher Entschlüsselung und Erläuterung legitimer oder bösartiger Hinweise in der gemeldeten E-Mail
- Konkreter Handlungsempfehlung und Sicherheitsbewertung für die gemeldete E-Mail
- Warnhinweis bei offensichtlichen Anzeichen einer Kompromittierung oder hochriskantem Inhalt (z. B. ausführbare Dateien)

Das sofortige Feedback und die hohe Transparenz motivieren Endbenutzer, wachsam zu bleiben und verdächtige E-Mails weiterhin zu melden – ohne zusätzliche Belastung des SOC-Teams.

05-25

HORNETSECURITY

## TEAMS PROTECTION

Da immer mehr Mitarbeiter Instant Messaging der E-Mail vorziehen, steigt die Gefahr, dass Microsoft Teams als Angriffsvektor genutzt wird und Cyberkriminelle bösartige Links oder Malware per Chatnachricht versenden.

Teams Protection schützt Ihre Umgebung vor schädlichen Nachrichten von intern kompromittierten Konten oder aus Teams-Konversationen, die mit externen Gesprächspartnern initiiert wurden. Dies geschieht, indem Nachrichten, die URLs beinhalten, gescannt und verdächtige Inhalte sofort per Warnmeldung über den AI Cyber Assistant Bot in der Unterhaltung angezeigt werden. Dabei kommt dieselbe KI-Technologie wie bei Hornetsecuritys Secure Links zum Einsatz:

- Intelligente Musteranalyse prüft wichtige URL- und Seitenmerkmale (z. B. Weiterleitungen, Dateipfade, Skripte), um schädliche Inhalte zu identifizieren
- Machine-Learning-Algorithmen analysieren über 47 Merkmale von URLs und Webseiten, um schädliches Verhalten, Verschleierungstechniken und Weiterleitungen zu erkennen.
- Deep Learning: Computer-Vision-Modelle analysieren Bilder, wie z. B. Markenlogos, QR-Codes und verdächtige Textinhalte in Bildern, um relevante Merkmale für Phishing-Angriffe zu identifizieren.

## AI RECIPIENT VALIDATION

JETZT MIT SMART ALERTS

Mit dem AI Cyber Assistant erhält AI Recipient Validation das Smart Alerts-Feature.

- Smart Alerts sind intuitive Warnhinweise am Seitenrand, die erscheinen, wenn der Nutzer im Begriff ist, z.B. eine E-Mail an versehentlich ausgewählte Empfänger oder mit sensiblen Inhalten zu versenden.
- Zusätzlich ermöglicht Smart Alerts eine nahtlose Offline-Funktionalität. Dadurch ist sichergestellt, dass AI Recipient Validation jederzeit zuverlässig verfügbar ist – für effizientes und sicheres Arbeiten.

Mit AI Cyber Assistant und den Smart Alerts wird das Nutzererlebnis weiter optimiert und AI Recipient Validation zu einem unverzichtbaren Tool für mehr Produktivität.

VERFÜGBAR IN

**365 TOTAL PROTECTION PLAN 4**

DIE ULTIMATIVE LÖSUNG FÜR SECURITY, BACKUP & GRC IN MICROSOFT 365