HORNETSECURITY

AI CYBER ASSISTANT

THE ULTIMATE SECURITY POWER UP FOR MICROSOFT 365

ALWAYS BY YOUR SIDE

AI Cyber Assistant is your vigilant AI security booster that empowers end users and admins in their day-to-day operations, ensuring secure communication and a lighter workload. Integrated seamlessly into Hornetsecurity solutions for Microsoft 365, AI Cyber Assistant evolves continuously thanks to our machine learning technology to instantly deliver the support you need most.

POWERING UP OUR LATEST SOLUTIONS

AI EMAIL SECURITY ANALYST

Unburden SOC resources while not only maintaining but also improving email security services thanks to automation and instant feedback!

Email Security Analyst automates responses to user queries about potential threats, replacing traditional manual analysis. Enriched with our latest security intelligence updates, end users automatically receive a live and AI-powered analysis of their email reports, including:

- An understandable decryption and description of legitimate or malicious indicators found in the reported email.
- A comprehensive level of caution and posture they should adopt on the reported email.
- Sanity check warning if obvious indications of compromise, or high-risk content are detected. (e.g., executable files).

Instant feedback and transparency encourages end users to remain vigilant and keep reporting emails without adding any extra burden on the SOC teams.

05-25

HORNETSECURITY

TEAMS PROTECTION

With more and more employees preferring instant messaging to email, Microsoft Teams can only continue to grow as an attack vector, with cyber criminals utilizing malicious links and malware sent by either externally open Teams or compromised internal accounts.

Teams Protection protects a tenant from internal compromised accounts by scanning all messages containing URLs, immediately issuing a warning message in the conversation through the AI Cyber Assistant bot. Teams Protection utilizes AI technology used in Hornetsecurity's Secure Links:

- Smart patterns analyze key features of URLs and pages (e.g. redirections, file paths, scripts, etc.) to identify malicious content.
- Supervised and unsupervised machine learning algorithms analyze more than 47 characteristics of URLs and web pages, scanning for malicious behaviors, obfuscation techniques, and URL redirects.
- Deep learning: Computer Vision models analyze images to extract relevant features used in phishing attacks, including brand logos, QR codes, and suspicious textual content embedded within images.

AI RECIPIENT VALIDATION

ENHANCED WITH SMART ALERTS

With the integration of the AI Cyber Assistant, our service AI Recipient Validation now features Smart Alerts:

- Intuitive side-panel warnings when a user is about to send an email to incorrectly selected recipients or when an email includes sensitive content.
- Smart Alerts enables seamless offline functionality, ensuring that AI Recipient Validation always remains reliably available. Users are empowered to work efficiently—regardless of connectivity.

With Smart Alerts, the user experience is further enhanced, making AI Recipient Validation an essential tool for increased productivity.

AVAILABLE IN

365 TOTAL PROTECTION PLAN 4

THE MICROSOFT 365 SECURITY, BACKUP & GRC POWERHOUSE

www.hornetsecurity.com | info@hornetsecurity.com | +49 511 515 464-0