HORNETSECURITY

INFOPAPER

AI EMAIL SECURITY ANALYST

CYBERTHREATS ARE DEVELOPING RAPIDLY MAKE YOUR EMPLOYEES SAFE DRIVERS IN THE RACE

Times have never been faster. Whether it's our internet connections, everyday gadgets, order delivery, or news distribution, it's becoming increasingly difficult to keep track of every way the world around us is changing.

Technology, and especially technology in the cybersecurity space is no different. We are in a constant race to develop the smartest and fastest ways to anticipate and battle all imaginable cyber threats (always in the race with us). And as we try everything to increase our odds of reaching and staying in first place, we must remember that it's not just our tech, but also our people being in the race with us.

The cybersecurity race isn't just about tech for fighting cyber threats; it's also about the people and how we can make them race together alongside technology.

And how to we accomplish this? By developing innovative technologies that create win-win situations where users get involved and empowered, effortlessly strengthening a company's security posture.

AND THE BEST STARTING POINT?

The same as for most cyber threats – the mailbox. Every user has the option of reporting emails they deem suspicious, which is an essential building block in any security structure.

But what happens to a reported email from the user's point of view? Nothing – That's the unfortunate most common answer. The user reports an email and receives no feedback, not knowing if the email was legitimate or malicious, and whether their report did anything at all.

This lack of feedback and transparency can be very discouraging and stops users from reporting emails altogether which comes with serious security implications:

- Users become desensitized to malicious emails.
- Users miss out on invaluable training on best security practices.
- SOC teams are unaware of malicious emails making it through to user mailboxes and can miss larger-scale attacks that target multiple users.

AI EMAIL SECURITY ANALYST

HOW DO WE SOLVE THE ISSUE?

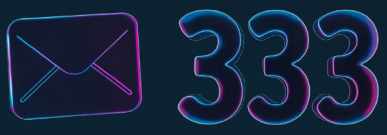
By making reporting emails valuable for both the company and, most importantly, for the users.

Hornetsecurity achieved this by introducing a solution that fully automates the analysis and response to user-reported emails.

LET **AI.MY** AUTOMATE THE ANALYSIS AND RESPONSE TO REPORTED EMAILS

Admins of a company with 1000 employees

Manually review about 333 reported emails per month



spending 55 hours on average

Whenever a user reports an email, Hornetsecurity's AI Email Security Analyst automatically analyzes it for malicious content and gives the user instant verdict. Whether the email is deemed malicious or safe, AI Email Security Analyst provides a detailed investigation of why, including advice on how to handle suspicious emails.

WITH THIS SIMPLE BUT POWERFUL SOLUTION, YOU ARE ONE CLICK AWAY FROM:

- Empowering employees to automatically receive a live and AI-powered analysis of their email reports.
- Training them in the best email security practices and expanding IT security knowledge.
- Freeing up invaluable SOC resources otherwise spent on manually reviewing emails.
- Improving email security services thanks to automation and instant feedback.

AI EMAIL SECURITY ANALYST

AI EMAIL SECURITY ANALYST IS PART OF THE NEW 365 TOTAL PROTECTION PLAN 4

The new 365 Total Protection Plan 4 is enhanced by AI Cyber Assistant, an automated security power-up that supports end users and admins in their day-to-day operations, ensuring secure communication and a lightened workload.

AI Cyber Assistant evolves continuously thanks to our machine learning technology, delivering invaluable support.

365 **TOTAL PROTECTION** PLAN 4

Unlock the future of cybersecurity today with a **free trial** of the most comprehensive solution for Microsoft 365 on the market.