HORNETSECURITY

VALUE
PROPOSITION

AI EMAIL SECURITY ANALYST

Thanks to growing media attention, end users are becoming increasingly suspicious of incoming emails. While this is great for a company's security, it does add to the burden of SOC and Service Desk teams who must deal with each reported or questioned email on a case-by-case basis. Whether False Negatives or False Positives, each flagged email drains resources and increases costs. At the same time, end users lack transparency and feedback on the emails they report.

CUSTOMER AND PARTNER PAIN POINTS:

- Lack of information and transparency for end users: Unless they reach out to their security operation center or admins, end users do not receive tailored feedback or insights when reporting emails, nor do they receive guidance on an email's legitimacy after reporting it.
- Security teams spend time investigating, remediating, and customizing responses to users' reports or questions about the email in their inboxes which takes up a substantial amount of time leading to increased costs.

OPTIMIZE YOUR OPERATIONS WITH AI EMAIL SECURITY ANALYST, ENSURE GREATER TRANSPARENCY, AND SAVE COSTS.

AI Email Security Analyst is an AI-driven email security solution that automates threat detection and response, replacing traditional manual analysis. The solution is what every SOC team needs to significantly reduce the time spent on FN/FP reports. It provides much needed transparency to the end user whether the email they reported was malicious or not, and the reasoning behind the analysis.

AI Email Security Analyst provides the end user with different measures of caution they should apply on the reported email as well as a decryption and description of legitimate or malicious indicators inside the reported email. The content of AI Email Security Analyst can sensibilize and indirectly train users to detect indicators of compromises in the future.

HORNETSECURITY

VALUE PROPOSITION

TOP FEATURES

- Enriched with our latest security intelligence updates, end users automatically receive a live and AI-powered analysis of their email reports. The verdict is done by analyzing the entirety of an email: headers, contents, and attachments.
- The feedback message to the end user can contain:
  - A comprehensive level of caution and posture they should adopt on the reported email.
  - An understandable decryption and description of legitimate or malicious indicators found in the reported email.
  - Sanity check warning if obvious indications of compromise, or high-risk content are detected. (e.g., executable files).
- Effortless to set up and activate by admins, and easily accessible to the end user with an intuitive interface that does not require additional training.
- AI Email Security Analyst is the first brick of a set of features that will automatize and facilitate the way SOC teams are dealing with user reports.
- The solution continuously learns with user feedback, with the LLM models improving the quality of the responses provided.
- Admins can utilize AI Email Security Analyst in Email Live Tracking, where they receive, on demand, an up-to-date analysis, a level of caution, and AI-Powered reasoning to help them investigate and handle user emails.

TOP BENEFITS

- Significant reduction of the time a SOC team spends responding to potential FNs or FPs.
- Freeing up resources while not only maintaining but also improving email security services thanks to automation and instant feedback.
- Empowered end user: Instant feedback and transparency encourages end users to remain vigilant and keep reporting emails without adding any extra burden on the SOC teams.
- Indirect security awareness training for end users thanks to regular exposure to content describing legitimate or malicious indicators inside the email they receive and report.
- Increased security thanks to growing awareness and instant feedback, making end users more eager to report suspicious emails.