



## AI EMAIL SECURITY ANALYST

Das Bewusstsein der Endbenutzer für schädliche E-Mails nimmt zu. Während dies für die Sicherheit eines Unternehmens vorteilhaft ist, bedeutet es zugleich eine zusätzliche Belastung für SOC- und Service-Desk-Teams, die sich mit jeder gemeldeten E-Mail einzeln auseinandersetzen müssen. Ob False Negatives (FNs) oder False Positives (FPs) – jede markierte E-Mail verbraucht Ressourcen und erhöht somit die **Kosten**. Gleichzeitig fehlt es Endbenutzern an Transparenz und Rückmeldung zu den von ihnen gemeldeten E-Mails.

### PAIN POINTS:

- » **Mangel an Informationen und Transparenz für Endbenutzer:** Sofern sie sich nicht an ihr Security Operation Center oder ihre Administratoren wenden, erhalten Endbenutzer keine Rückmeldung oder Einblicke beim Melden von E-Mails, ebenso wenig wie eine Einschätzung zur Legitimität der E-Mail nach deren Meldung.
- » **Sicherheitsteams verbringen viel Zeit mit der Untersuchung, Behebung und Individualisierung von Antworten** auf die Meldungen oder Fragen der Benutzer zu den E-Mails in ihren Postfächern – ein erheblicher Zeitaufwand, der zu steigenden **Kosten** führt.



### OPTIMIEREN SIE IHRE ABLÄUFE MIT AI EMAIL SECURITY ANALYST, SORGEN SIE FÜR MEHR TRANSPARENZ UND SPAREN SIE KOSTEN.

**AI Email Security Analyst** ist eine KI-gesteuerte E-Mail-Sicherheitslösung, die Antworten auf Benutzeranfragen zu potenziellen Bedrohungen automatisiert und die herkömmliche manuelle Analyse ersetzt. Die Lösung ist das, was jedes SOC-Team braucht, um den Aufwand bei der Bearbeitung von FN-/FP-Meldungen erheblich zu reduzieren. Sie bietet dem Endbenutzer dringend benötigte Transparenz – unabhängig davon, ob die gemeldete E-Mail bösartig war oder nicht – sowie die Begründung des Analyseergebnisses.



**AI Email Security Analyst** teilt Endbenutzern verständlich mit, welche Vorsichtsmaßnahmen sie im Umgang mit der gemeldeten E-Mail treffen sollten. Zudem liefert das Feature eine verständliche Entschlüsselung und Erklärung legitimer oder bösartiger Indikatoren innerhalb der Nachricht. Die Hinweise von **AI Email Security Analyst** tragen dazu bei, das Sicherheitsbewusstsein der Nutzer zu stärken und sie indirekt darin zu schulen, künftig Anzeichen einer möglichen Kompromittierung selbstständig zu erkennen.

## TOP FUNKTIONEN:

- » **Basierend auf unseren neuesten Security-Intelligence-Erkenntnissen** erhalten Endbenutzer automatisch eine KI-gestützte Live-Analyse ihrer gemeldeten E-Mails. Die Bewertung basiert auf der Analyse der gesamten E-Mail: Header, Inhalt und Anhänge.
- » Die Rückmeldung an den Endbenutzer kann enthalten:
  - » Konkrete Handlungsempfehlungen, wie mit der gemeldeten E-Mail umzugehen ist.
  - » Eine verständliche Entschlüsselung und Beschreibung legitimer oder bössartiger Indikatoren, die in der gemeldeten E-Mail gefunden wurden.
  - » Eine Sanity-Check-Warnung, falls offensichtliche Anzeichen für eine Kompromittierung oder hochriskante Inhalte erkannt wurden (z. B. ausführbare Dateien).
- » **Einfach durch Administratoren einzurichten und zu aktivieren** sowie für Endbenutzer über eine intuitive Benutzeroberfläche zugänglich, die keine zusätzliche Schulung erfordert.
- » **AI Email Security Analyst ist der erste Baustein** in einer Reihe von Funktionen, die die Arbeit von SOC-Teams mit Benutzerberichten automatisieren und erleichtern sollen.
- » Die Lösung lernt kontinuierlich mit dem Benutzerfeedback, wobei die LLM-Modelle die Qualität der gelieferten Antworten verbessern.
- » Administratoren können **AI Email Security Analyst** im **Email Live Tracking** verwenden, wo sie auf Abruf eine aktuelle Analyse, eine Risikoeinschätzung und eine KI-gestützte Begründung erhalten, um Benutzer-E-Mails zu untersuchen und zu bearbeiten.

## WICHTIGSTE VORTEILE:

- » Deutliche Zeitersparnis für das SOC-Team bei der Bearbeitung potenzieller False Negatives (FNs) oder False Positives (FPs).
- » Ressourcen werden entlastet, während die E-Mail-Sicherheit dank Automatisierung und unmittelbarem Feedback sogar über das bisherige Niveau hinaus optimiert wird.
- » **Wachsamer Endbenutzer:** Direktes Feedback und Transparenz fördern proaktives Meldeverhalten – ohne SOC-Teams zusätzlich zu belasten.
- » **Indirektes Security-Awareness-Training** für Endbenutzer durch regelmäßige Rückmeldungen, die verdächtige oder legitime Merkmale in ihren gemeldeten E-Mails erklären und einordnen.
- » **Erhöhte Sicherheit** durch steigendes Bewusstsein und sofortiges Feedback – was Endbenutzer motiviert, verdächtige E-Mails häufiger zu melden.