AI-Driven Cloud Email Security

Protect your enterprise from evasive email threats with the power of a cloud-native AI threat prevention platform

Social Engineering: The Gateway to Enterprise Threats

The threat landscape is evolving rapidly, with attackers increasingly using evasive techniques to bypass traditional security technologies such as sandboxes, URL filtering, file-based machine learning, and signature-based detection. By combining these methods with sophisticated social engineering, they exploit human trust, emotions, and sentiments to launch attacks like phishing and ransomware. Social engineering threats involving conversational payloads, such as BEC, are becoming more challenging to detect due to the ease of generating variants with AI. Training users is also becoming less effective, as AI-enhanced emails introduce significant variations in writing style and payloads, allowing attackers to execute highly adaptive campaigns.

Legacy email security solutions—whether traditional gateway-based systems (Email Security 1.0) or the more recent platforms architected around 2018 (Email Security 2.0) relying on machine learning, behavior models, and pre-trained classifiers—are no longer sufficient against these advanced threats. These systems struggle to detect the endless evasive techniques attackers use and the significant semantic variations in social engineering attacks targeting human vulnerabilities.

What's needed is an AI-native solution purpose-built to confront these evolving threats. This is Email Security 3.0—powered by advanced AI technology and designed to defend against the next generation of attacks. This is Inception Cyber.ai.

Solution Benefits

30% More Effective Detection

- Detect what other technologies are missing.
- Fewer attacks reaching employee's mailbox.
- Reduce risk, i.e. SEC reporting.

Reduced Post Execution Detection Costs

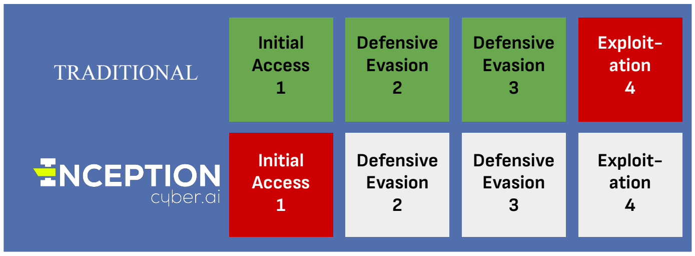
- Proactive detection reduces MDR/XDR burden.
- Avoids costly and time-consuming response and remediation.

Increased Accuracy

- Fewer False Positives/False Negatives reduce analyst workload.
- Reduces need for social engineering attack trainings.

The Native AI-Driven Expert System leverages LLMs (Meta - LLaMA3, CLIP), hierarchical topic modeling, and fine-tuned classifiers to deeply understand the semantic and thematic meaning of emails, along with file parsing results and URL structures, to make real-time decisions in classifying attachment, URL or email as benign or malicious.

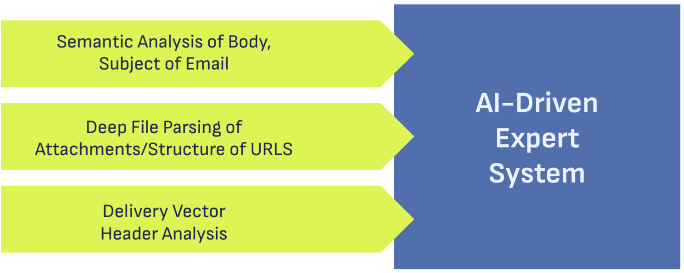
Radically Different Engine Design - Detection without the Malicious Payload



TRADITIONAL	Initial Access 1	Defensive Evasion 2	Defensive Evasion 3	Exploit-ation 4
INCEPTION cyber.ai	Initial Access 1	Defensive Evasion 2	Defensive Evasion 3	Exploit-ation 4

Leverages the **semantic** and **thematic** meaning of emails (words, sentences, phases) to detect malicious attachment and URLs at the initial stage making it Immune to Evasions

Unified Data for Maximum Context


Semantic Analysis of Body, Subject of Email
Deep File Parsing of Attachments/Structure of URLS
Delivery Vector Header Analysis
AI-Driven Expert System

Leverages three data sources for Expert System review vs separate engines losing context.

Zero-Shot Classification

Recognizes semantics without relying on pre-defined classifier, making it resilient to new semantic variants and understand different languages.

INCEPTION
cyber.ai

Core Features

Unlike legacy technologies like signature-based systems, sandboxes, machine learning, anomaly detection, and rule-based approaches — all of which rely on detecting malicious payloads — Inception Cyber identifies and blocks threats based on context.

Without the requirement of scanning or executing a malicious payload, Inception Cyber is immune to attackers' evasion techniques.

Decision Insights	Delivers clear, definitive insights into decision-making for both executives and analysts, including threat category, intent classification, meta tags, and account impersonation details.
Zero Trust BEC	Real-time SMS notification to the sender for emails that match threat intent but lack classification. Enhances accuracy in detecting Business Email Compromise (BEC). Used for detecting money transfer requests, gift card fraud, and aging report scams.
Zero Shot Semantic Analysis	Understands semantic variants introduced by threat actor or AI. The Inception Cyber NACE platform understands email intent and context, so iteration and rewording techniques cannot sneak past.

Deployment

Email Platforms	Microsoft 365, Google Workspace (G-Suite).
Modern Cloud-native, no MX record change	Fast deployment in minutes via Cloud-Native API, with no need for manual configuration, policy changes, or MX record modifications.
Traffic Processing	Inbound, outbound, and internal email traffic.
Journaling Mode	Ideal for evaluations and proofs of value. Email copies are reviewed and malicious emails are quarantined before end-users can click on them.
In-Line Mode	Ideal for production environments. Emails are analyzed, and threats stopped, before they reach the end-user's mailbox.
No Email Copies Stored	Emails are promptly deleted after review, with only non-PII summary metadata stored. Malicious emails are quarantined for analyst review.
Privacy	Operates on the AWS platform, with emails directed to the nearest Point of Presence (POP) and maintained within geographic boundaries.
Language Support	English, Hindi, German, French, Spanish, Chinese, Korean, Arabic.

Comprehensive Attack Type Coverage

Ransomware and Evasive Attachments	Covers threats like password stealers, HTML smuggling, downloaders, droppers, and other malware.
Phishing and Evasive Call-to-Action URLs	Includes QR codes, brand impersonation, and callback scams.
Business Email Compromise (BEC)	Detects initial lures, gift card scams, W-2 fraud, aging report fraud, wire transfers, invoice scams, acquisition scams, payroll scams, and VIP/CEO impersonation.
Account Compromise	Detects internal and external email account compromise as well as vendor account compromise.
AI-Generated Variations	Covers BEC, phishing, ransomware, and malware generated by AI.
Generic Scams and Other Conversational Payloads	Includes job scams and money laundering schemes.
Zero Trust BEC	Detects money transfer requests, gift card fraud, and aging report scams.

Inception Cyber has created a cloud-native deep learning platform called the Neural Analysis and Correlation Engine (NACE). This platform leverages large language models (LLMs) to deeply understand email, using this comprehension as a core feature to detect malicious attachments and URLs—such as ransomware, phishing, password stealers, QR codes, and more. i.e attacks relevant to the organization.

Learn more at inceptioncyber.ai

Inception Cyber
Palo Alto, CA