INCEPTION cyber.ai

Key Insights from Inception Cyber NACE™

Patent pending Neural Analysis and Correlation Engine is proven to stop what others miss

Industry-Recognized for Innovation

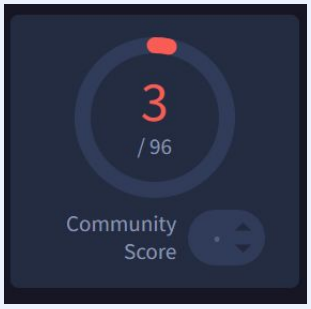
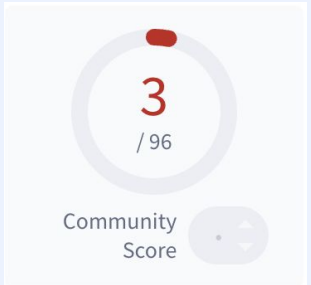
NACE™ was selected for presentation at the prestigious, peer-reviewed conferences AVAR 2024 and Black Hat MEA 2024

black hat MIDDLE EAST AND AFRICA

AVAR 2024 27th Annual Cyber Security Conference The Battle for Cyber Supremacy

Examples of Evasive Threats Caught by NACE™

In production environments, NACE™ is effectively detecting sophisticated phishing and BEC attempts—whether generated by AI or threat actors—that are constantly missed by over 95% of AV vendors and G-Suite.

Safeguarding from Real-World Attack	Attack Overview	Compared to 96 AV Vendors	
Phishing Targeting Finance Team DocuSign-Themed Campaign Exploits Trust in Legitimate Platforms	• Impersonating Docusign brand. • Hosted on jotform a legitimate service provider. • Employing several redirect and hidden behind CAPTCHA. • No "To" Header. Using SMTP Envelope for delivery. • Bypassed G-Suite defenses.	**0 out of 96** AV vendors detected the URL as malicious.	
Vendor Impersonation BEC Attacks to Trick Corporate Employees Vendor Impersonation and Fake Vendor Registration	• Impersonating brands like ExxonMobil, Larsen & Toubro, Dreistern. • Used TypoSquatting and Combosquatting to trick corporate employee to give sensitive information. • Hiding recipients and leveraging SMTP for delivery. • Used free email provider to evade SPF, DKIM, DMARC, G-Suite defenses.	Only **3 out of 96** AV vendors classified this URL as phishing.	
APT Phishing Designed for C- Level Executive Credential Phishing via Fake IT Communications	• Phishing hosted on JotForm legitimate service provider. • Multi Layer redirect employing CAPTCHA. • Leveraged SMTP header for delivery. • Bypassed G-Suite defenses.	Only **3 out of 96** AV vendors classified this URL as phishing.	

INCEPTION
cyber.ai

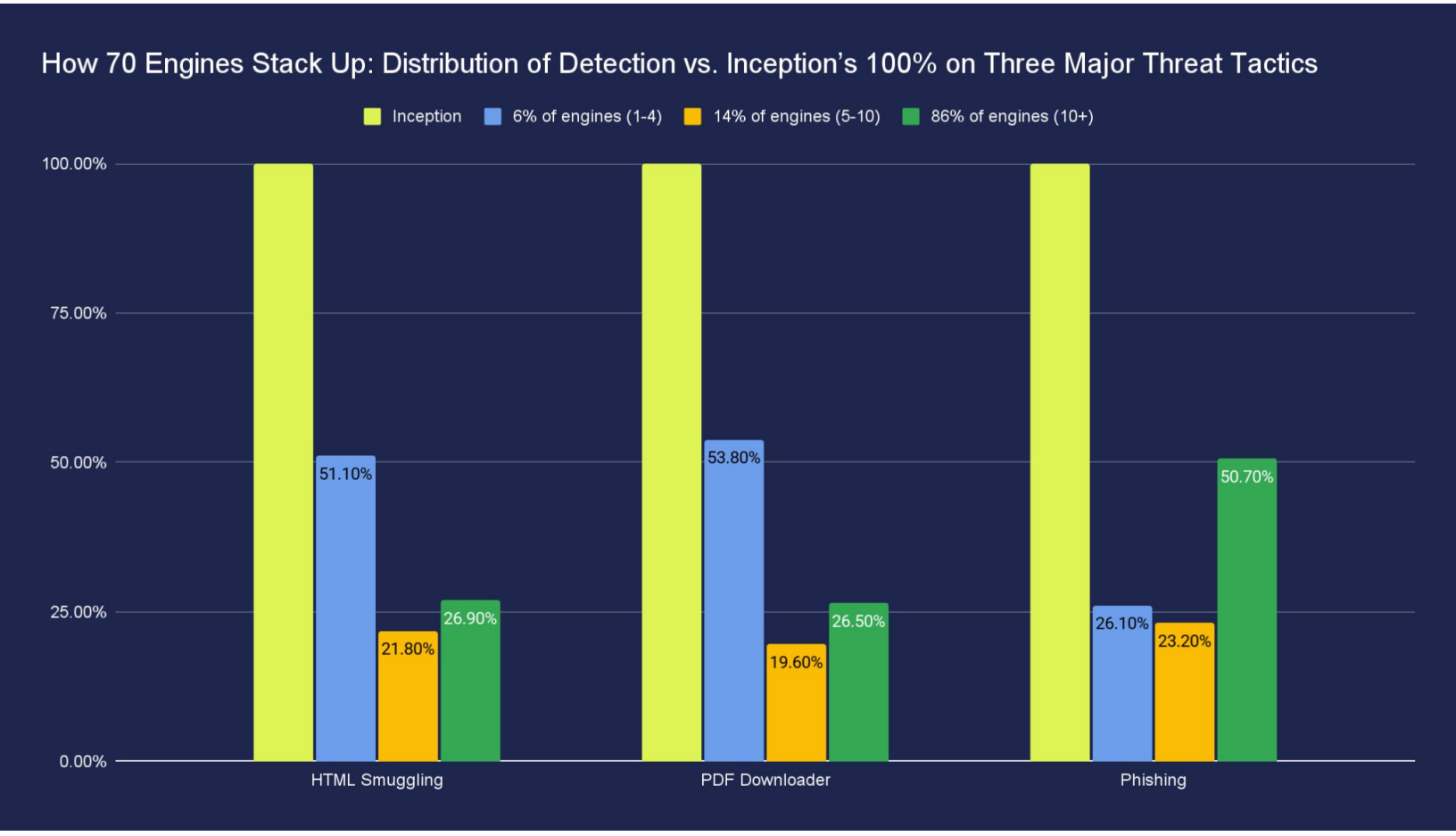
Inception detects ~50% more evasive threats

Chart shows how Inception compares to other detection engines. Three types of Threat Tactics are shown, for example HTML Smuggling is a common tactics for Ransomware.

Dataset for Benchmarking

VirusTotal 2024 Database

- ~ 13K Evasive emails
- 100k+ Clean Emails
- Vendors: ~ 70 AV Vendors, 70 URL BlackLists, 10 Sandboxes



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