SECURONIX™

SOLUTION BRIEF

Securonix Phishing Analyzer

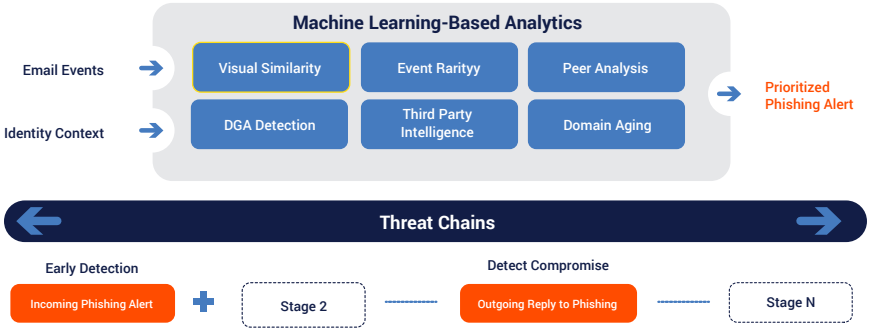
Email phishing attacks continue to rise in volume and sophistication. Attacks impersonating legit company domains (typosquatting) and company executives (business email compromise) have been highly successful at encouraging employees to click and respond.

Typosquatting – Attackers use domain names that appear the same but are spelled differently from the established name while still using the same character set.

Business email compromise (BEC) – Attackers use the identity of a legitimate user, typically an executive, to influence the target to respond with sensitive data or financial transactions.

Visual Similarity and Identity Analytics Detect Unknown Phishing Threats

Securonix Phishing Analyzer is designed to enhance the capabilities of an organization to detect unknown phishing threats. The solution uses visual similarity analytics that utilize identity context and machine learning to identify phishing attempts that may be otherwise missed.

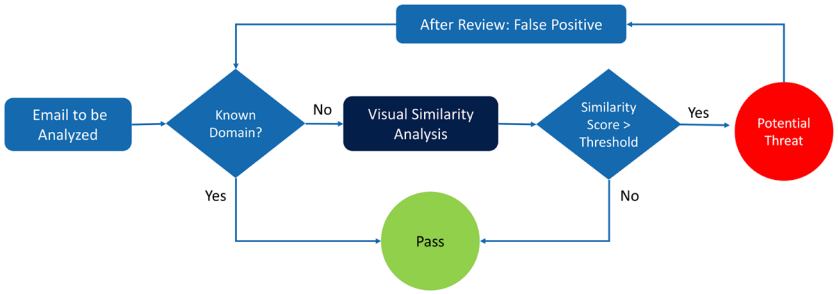


Solution Benefits

- Focus on unknowns. Machine learning-based visual similarity analysis identifies unknown domains using identity context.
- Identity context-based analysis prioritizes risk based on the chosen target's position within the organization.
- Threat chains prioritize high-risk attacks.

Visual Similarity Analytics

The solution uses a modified Levenshtein distance algorithm to detect visually similar domains. The solution assigns a similarity score based on the email domain name's similarity to legitimate domain names and name similarity to legitimate usernames. Emails that hit a threshold similarity value are tagged for review.

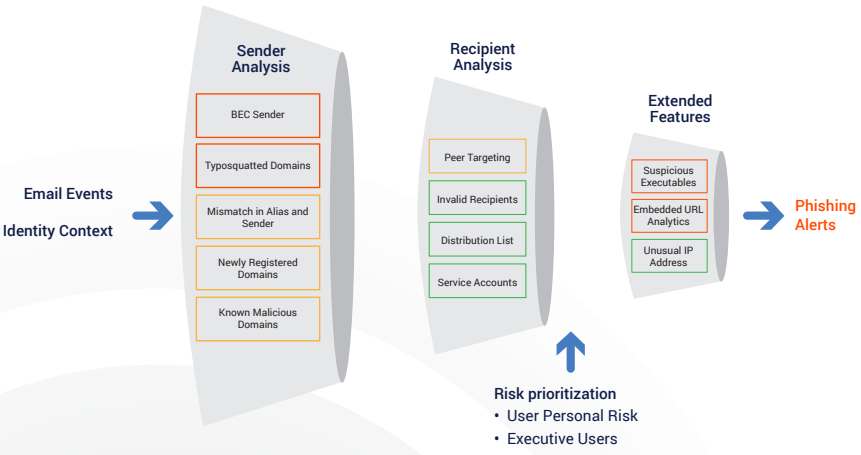


The parameters of the algorithm can be tuned based on an organization's needs to minimize false positives.

Multi-Stage Analysis

The phishing analyzer analyze email for threats in three stages.

- The first stage analyzes the sender's email address and checks for typosquatted domains or BEC. Analysis is also performed to detect newly created domains or known malicious domains.
- The second stage analyzes the recipient's email address to detect threats such as peer targeting (where a peer of the compromised user is emailed) or emails to service accounts.
- The third stage looks at additional suspicious indicators, such as suspicious executables or embedded URLs and the use of unusual IP addresses.



Key Use Cases

- Detect phishing campaigns that target top executives.
- Detect malicious emails purportedly sent from known, trusted domains.
- Detect other forms of attempted phishing fraud.

About Securonix

The Securonix platform delivers positive security outcomes with zero infrastructure to manage. It provides analytics-driven next-generation SIEM, UEBA, and security data lake capabilities as a pure cloud solution, without needing to compromise. For more information visit www.securonix.com.

SECURONIX™

LEARN MORE
www.securonix.com

LET'S TALK
+1 (310) 641-1000