SECURONIX™

SOLUTION BRIEF

Securonix Phishing Analyzer

Effective Threat Detection for Business Email Compromise

Significant Upsurge in Phishing Attacks

As more organizations allow work from home, a spike in phishing attacks has occurred. According to the GreatHorn 2020 Phishing Attack Landscape Report, organizations saw an average of 1,185 phishing attacks every month. Furthermore, employees often fall prey to phishing emails that use typo squatting, mimic legitimate company domains, or impersonate company executives in order to encourage employees to click on a malicious URL.

Although email gateways are the first line of defense, more recent attacks use machine learning that is difficult for these solutions to detect. This upsurge in sophisticated cyberattacks calls for new, cutting edge detection. Securonix Phishing Analyzer uses machine learning-based analytics to uncover stealthy phishing attacks and mitigate further damage.

Detect Sophisticated Phishing Threats with Machine Learning

Many phishing detection solutions are limited to alphanumeric correlations. However, Securonix Phishing Analyzer uses visual similarity and identity analytics, as shown in Figure 1 below, to detect hidden phishing threat vectors. Phishing Analyzer detects phishing campaigns by analyzing inbound email gateway logs and applying machine learning-based analytics techniques. Threat chains stitch together related alerts to prioritize alerts for security teams. Machine learning and threat chains work in tandem so that security teams can quickly detect and respond to phishing threats.

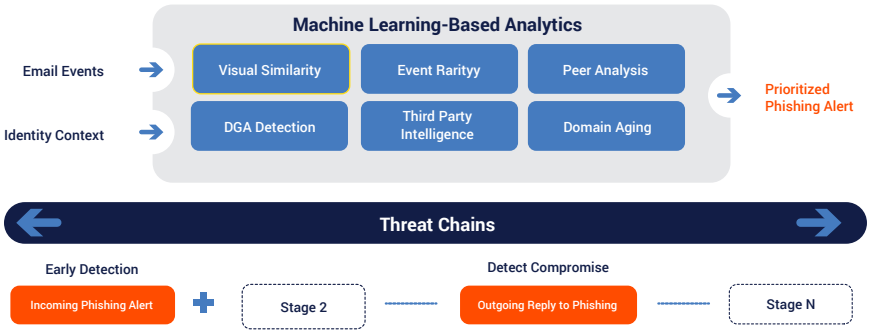

Figure 1: Machine Learning-Based Analytics and Threat Chains Provide Prioritized Alerts

Visual Similarity Analytics

Securonix uses visual similarity analytics, which utilizes identity context and machine learning, to identify phishing attempts that may be otherwise missed (as shown in Figure 2).

Solution Benefits

- Identify unknown phishing domains using visual similarity analytics.
- Detect hidden phishing attacks that bypass latent detection using machine learning-based analytics.
- Prioritize and respond to sophisticated phishing attacks based on risk score using context-based identity analysis and threat chains.

The solution uses a modified Levenshtein distance algorithm to detect visually similar domains. Phishing Analyzer then assigns a score based on the similarity to legitimate domain names or usernames. Emails that are too similar are flagged for review as a potential threat. The parameters of the algorithm can be tuned, depending on an organization's needs, to minimize false positives.

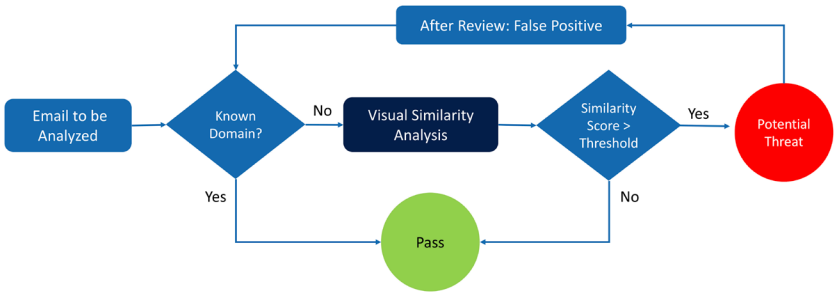

Figure 2: Visual Similarity Analytics Logic Flow

Multi-Stage Analysis

Securonix Phishing Analyzer evaluates emails for threats in three stages.

1. The sender's email address is inspected for typosquatted domains or business email compromise. Analysis is also performed to detect newly created domains or known malicious domains.
2. The recipient's email address is examined to detect threats such as peer targeting, where a peer of the compromised user is emailed, or emails to service accounts.
3. Other suspicious indicators are investigated, such as suspicious executables or embedded URLs and the use of unusual IP addresses.

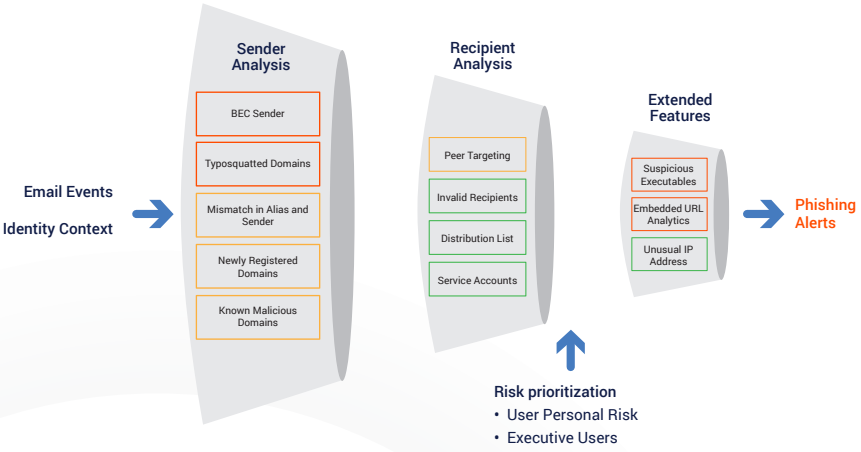

Figure 3: Multi-Stage Analysis

Securonix Equips Your SOC to Detect Sophisticated Phishing Threats

Securonix Phishing Analyzer identifies advanced phishing techniques using multistage analysis, visual similarity analytics, machine learning-based algorithms, and threat chain models. With Securonix Phishing Analyzer your organization is protected from advanced phishing attacks without adding another product to your security technology stack.

Key Use Cases

- **Typo Squatting**
  Attackers use domain names that appear similar to established domains.
- **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.
- **Impersonation**
  Involves an email that seems to come from a trusted source, like from a trusted colleague, a third-party vendor, or other well-known person.
- **Phishing Campaigns** and other forms of phishing attacks like spear phishing, malware phishing, whaling, vishing, and email phishing.

For more information about how Securonix can improve your search and threat hunting capabilities visit us at www.securonix.com or schedule a demo www.securonix.com/request-a-demo.

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