CASE STUDY

SLASHNEXT
NEXT GEN AI EMAIL+ SECURITY

Advanced Threats Stopped, Nearly $2.3 Million Annual Mitigations and 8+ Hours/Wk Saved in SOC Time

AMANA.
WE BUILD WITH YOU

Company

AMANA is the United Arab Emirate's trusted design-build company, specializing in industrial construction for over three decades. The company has locations in over seven countries, over 130 repeat clients, and over 8,000 employees. Its reputation is built on the ability to repeatedly provide turn-key solutions for fast-track projects.

Challenge

The Architecture, Engineering, and Construction (AEC) sector is a highly targeted industry for cybercriminals using email as the primary communication attack channel. As such, AMANA was experiencing a large amount of malicious emails within that attack surface. They needed protection against Business Email Compromise (BEC), vendor account takeovers, and other types of attacks. The existing approach and tooling created suboptimal results and a poor experience for the SOC team. The company investigated SlashNext, Abnormal Security, and Perception Point. AMANA chose SlashNext. AMANA Technology Manager Daniel Vargas said "SlashNext met our needs by having the highest level of efficacy when compared to the other two vendors."

Solution - Generative AI Powered Email, Mobile, and Browser Protection

- Stops credential stealing, BEC, spear-phishing, legitimate link compromise, social engineering scams, ransomware and malware in real time with fast 99.99% detection rates and a one in 1 million false positive rate.
- Five-minute set-up and deployment immediately demonstrates ROI by revealing compromised devices in the organization.
- Prevents smishing and BTC with zero-hour protection against the broadest range of link based and natural language threats in any mobile application.
- Integrated browser extension stops zero-hour link and exploit threats in all web messaging apps including email, ads, social, search, and collaboration.
- Educates employees at the point of click to reinforce training programs.

BUSINESS CHALLENGE

Company was experiencing a large amount of malicious BEC attacks; the existing tooling was suboptimal; and the SOC team needed a better experience

SOLUTION

SlashNext multi-channel Email+ mobile and browser phishing protection; gen AI security protects against BEC, smishing, QR Code attacks, social engineering attacks, and others

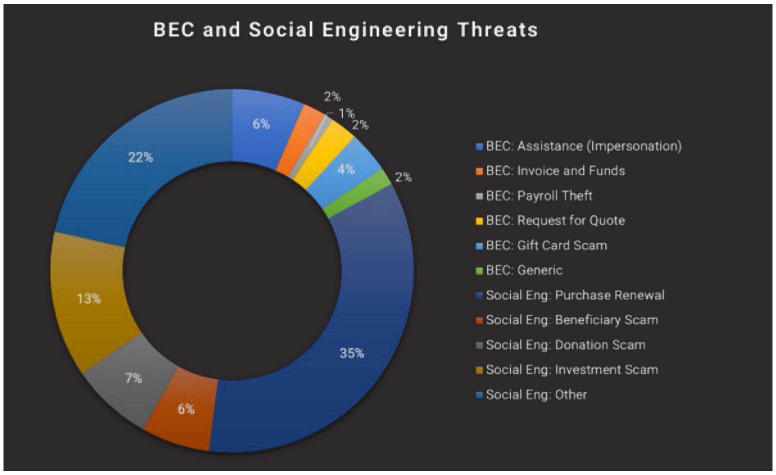
RESULTS

Saved company over $2 million from potential losses and SOC team over 8 hours per week in Operating Expenses

SlashNext Email+ Security immediately increased the security footprint with a more robust next-gen solution and detected more multi-stage BEC and natural language attacks. The types of attacks included malicious emails, QR Code attacks, and other known attack vectors. SlashNext met AMANA's needs and required less hands-on effort than other vendors when the product was configured.

According to a recent FBI IC3 report, the average cost of each successful BEC attack is $124K per attack. At AMANA, the number of attacks caught by SlashNext saved over $2.2 million dollars in mitigation the first year. SlashNext's intuitive and easy-to-use console not only thwarted zero-hour phishing attacks, it also saved security analysts over eight hours per week to perform other critical security job functions.

> ***"SlashNext met our needs by having the highest level of efficacy when compared to the other two vendors."***
>
> — Daniel Vargas, Technology Manager, AMANA



BEC Threat Types by Percentage – from SlashNext 2023 State of Phishing Report

The results align with our 2023 State of Phishing Report, which captured 12 months of customer data. In a SlashNext survey of cybersecurity professionals, 46% reported that they received a BEC attack.

The diversity and sophistication of BEC types (shown in the image on the left) have received a significant boost from the public availability of generative AI bots.

About SlashNext

SlashNext protects the modern workforce from malicious messages across all messaging channels. SlashNext Complete™ integrated cloud messaging security platform uses patented generative AI technology with 99.99% accuracy to detect threats in real time to stop zero-hour threats in email, mobile, and web messaging apps across M365, Gmail, LinkedIn, WhatsApp, Telegram, Slack, Teams, and many others messaging channels. Take advantage of SlashNext's Integrated Cloud Messaging Security for email, browser, and mobile to protect your organization from data theft and financial fraud breaches today.

For more information, visit www.SlashNext.com

Schedule a customized email risk assessment at https://slashnext.com/risk-assessment

6701 Koll Center Parkway 250, Pleasanton, CA 94566 | slashnext.com | info@slashnext.com | 800.930.8643