

Case Study

Learn how IRONSCALES helps to protect Nium against advanced phishing attacks

NIUM

About Nium

Nium is the global platform for modern money movement. It provides banks, payment providers, and businesses of any size with access to global payment and card issuance solutions. Its modular platform powers frictionless commerce, helping businesses pay and get paid across the globe. Once connected to the Nium platform, businesses are able to pay out in more than 100 currencies to over 190 countries – 85 of which in real time. Funds can be received in 27 markets, including Southeast Asia, UK, Hong Kong, Singapore, Australia, India, and the US. Nium's growing card issuance business is already available in 34 countries, including Europe (SEPA), the UK, Australia and Singapore. Nium's license portfolio covers 11 of the world's jurisdictions, enabling seamless global payments and rapid integration, regardless of geography.

Challenges

- Rapidly growing Fintech organization with a wealth of sensitive data
- Sophisticated email threats impersonating company founders and employees

Solution

- IRONSCALES - the AI-driven, self-learning email security platform
- Regular phishing awareness campaigns for NIUM's employee base

Results (over a 12-month period)

- Inspected Emails: 11,147,232
- Total Remediated Emails: 7,901
- Resolved Phishing Incidents: 426

“Phishing attacks themselves are not new but using AI and ML has allowed attackers to be more sophisticated in their methods. In the past, phishing attempts were sent out at random and contained a lot of typos, so they were easy to identify. Now we're seeing more specific and targeted attacks that are far more convincing.

RAJ VISWANATHAN,
CHIEF INFORMATION SECURITY OFFICER (CISO) AT NIUM

The Problem

The financial services industry is consistently one of the most targeted by cyberattacks, with malicious actors constantly looking for ways to exploit the large amount of customer data and funds that the industry holds. And as a widely-used communication tool, email is a major attack vector; in the first six months of 2021 alone, [phishing attacks in the financial sector increased by 22%](#) from the same period in 2020.

In addition to an industry-wide increase in email threats, the NIUM security team noticed more sophisticated phishing attempts targeting their networks using AI (Artificial Intelligence) and ML (Machine Learning) to spoof the company founders' names and imitate their writing styles.

NIUM's existing SOC team was solely responsible for detecting and remediating phishing attacks reported by employees but lacked visibility into how many users were affected by any single threat. This made remediation a lengthy and labor-intensive process for the SOC team, with hours spent on understanding and correlating potential malicious emails.

With multiple phishing attempts making it past their existing email security tool, the NIUM team decided that to scale up safely the organization needed a solution that would evolve as phishing threats evolved and alleviate the pressure of remediation from the SOC team.



We made an evaluation sheet of all the solutions we were considering and gave each a score based on the key specifications we wanted including using AI/ML, easy implementation, and user education. When we calculated which solution hit all these parameters at the best cost, IRONSCALES was far ahead of the rest.

RAJ VISWANATHAN,
CISO AT NIUM

Solution

NIUM's security team wanted to find a solution that specifically used AI to identify complex, covert phishing threats seamlessly, without requiring more admin or overhead. The team was also looking for something to educate users on what to look for when they suspected a phishing attack, as well as a solution that would take the pressure of remediation off the SOC team and give them clear, actionable alerts on incoming threats. Any platform or service also needed to be simple to implement, with no impact on the users' workflow.

NIUM was recommended IRONSCALES through their partner named SRC Cyber Solutions. After considering multiple email security solutions on the market, both legacy and newer players, NIUM found that IRONSCALES was the most nimble, frictionless platform that best fit their organization's needs.

After conducting a two-month POC (Proof of Concept), NIUM implemented the full IRONSCALES solution into their staff base of 850 users in 2021. As well as benefitting from seamless implementation into their network, the team found IRONSCALES' additional support around integrations invaluable.

Outcomes

Since installing IRONSCALES' AI-powered anti-phishing solution, NIUM has experienced a significant change in the inboxes of employees and the productivity of the security team. In the 12 months since implementation, the IRONSCALES platform has inspected 11,147,232 emails and remediated a total of 7,901, resolving 426 phishing incidents and saving NIUM's analysts around 250 hours of remediation time.

The almost-immediate implementation saved NIUM's email administrators a significant amount of time on set-up and configuration and helped the SOC team become more agile in handling phishing alerts. Rather than tackling each potential phishing threat individually, IRONSCALES clusters identical and similar phishing attacks. This allows security professionals to see the correlation between various threats, the implications of each threat, and how many users have been impacted, so the SOC team can act accordingly. IRONSCALES' AI-driven platform automatically removes threats from the inboxes of NIUM's staff at scale, allowing the security team to focus on their day-to-day jobs, without the distraction of the vast majority of phishing-based security alerts.



We thought that our staff was well educated on phishing before running the first campaign, but the results were surprising! A lot of our employees were fooled by the phishing techniques we used, but that helped us come up with a benchmark to build on.

RAJ VISWANATHAN,
CISO AT NIUM

I have already recommended IRONSCALES to some of my fellow CISOs! It checks off the boxes of what we were looking for in an email security solution and we've been pleased with the **solution so far, so it should be a no-brainer..**




RAJ VISWANATHAN, CISO AT NIUM

Through IRONSCALES, NIUM has also been able to improve employees' overall phishing awareness, building longer-term organizational protection against future phishing attacks. IRONSCALES' training and phishing simulation features were a key selling point for the NIUM team, who have found the educational campaigns easy to run and vital in identifying gaps in organizational knowledge. With training managed within the IRONSCALES tool itself, NIUM started running simulations immediately and over time has begun to increase the ability of their employees to identify different types of phishing attacks.

Along with a positive improvement in their staff base's ability to identify phishing through the simulations, NIUM has seen a positive increase in their use of the IRONSCALES 'Report Phishing' button. The button has helped keep phishing top-of-mind for the entire employee network, even when users are looking at internal emails from familiar colleagues.

Looking Ahead

After seeing impressive results in phishing reports, employee awareness, and overall organization security, the NIUM security team is planning to continue their rollout of the IRONSCALES solution within their new and future business acquisitions. This involves expanding their user base, replacing acquisitions' legacy security systems with IRONSCALES where applicable, and running educational campaigns to ensure that phishing knowledge is aligned.

www.srccybersolutions.com | +91 120 232 0960 / 1 | sales@srccybersolutions.com   

ABOUT SRC CYBER SOLUTIONS LLP

At SRC Cyber Solutions LLP, we provide Next Generation, Automated and User-Friendly solutions in partnership with AUTOMOX for Patch and Endpoint Management, IRONSCALES for Comprehensive Email Security and Anti-Phishing Protection, THREATX for WAAP (WAF++) with an Attack-Centric approach for Web Application and API protection and Project Ares for Online Gamified Simulation-based Cyber Security Training.

ARPR Case Study

