///AXUR

Naranja X automates 100% of exposed card and credential mitigation with Axur

About the company

NaranjaX

With 38 years of history, Naranja X has evolved to support everyday financial activity by offering savings, payments, credit, and collection solutions. The company provides interest-bearing accounts, cards, loans, transfers, and more than 5,000 services, including top-ups, insurance, and billing.

Problem

Naranja X faced targeted attacks against its assets and customers, including phishing, fake social media profiles, identity impersonation, fraudulent mobile applications, leaked credit and debit card data, and exposed credentials belonging to both customers and employees.

An additional challenge came from fraudulent activity across the Deep & Dark Web, where incident detection, validation, and remediation are inherently limited by the nature of these environments. The company needed robust monitoring tools to effectively detect and respond to these threats.

Solution

To strengthen its cybersecurity strategy, Naranja X integrated Axur's solutions, gaining regional focus and broader coverage.

Axur's ability to detect exposed debit/credit cards and leaked credentials across the web—combined with a stable and powerful API—enabled the company to automate 100% of its mitigation processes.

Impact at a glance

- 249K signals monitored between March 2023 and January 2024
- 1.8K threats detected during the period
- 33 incidents recorded and handled
- 70% of exposed debit/credit cards detected
- 50% of leaked customer credentials detected
- 100% automation across mitigation workflows

> "With the goal of strengthening our cybersecurity strategy, we recently added Axur's solutions, which allow us to achieve regional focus and coverage."
>
> **Leonardo Chiodin**
> Senior Information Security Analyst at Naranja X

> “Axur’s ability to detect exposed debit/credit cards and customer credentials across the web, along with the effectiveness of its stable and powerful API, enabled us to automate 100% of our mitigation processes.”
>
> Leonardo Chiodin
> Senior Information Security
> Analyst at Naranja X

Automated response and efficient mitigation

Axur’s integration into Naranja X’s cyber defense framework strengthened threat detection and mitigation through fast takedowns and efficient follow-up. Early browser-based mitigation helps protect customers while internal response workflows are completed.

Surface, Deep & Dark Web monitoring

Axur provides visibility into phishing, fake profiles, brand abuse, and the sale of compromised cards or credentials—helping prevent more severe attacks such as ransomware.

Large-scale detection and 360° visibility

The platform enabled a proactive and automated operating model, reducing analysts’ operational workload. By monitoring over 9,000 internet providers, bots detect fraud, data leaks, and Deep & Dark Web incidents at scale.

> “For us, it is impossible to think about Naranja X without a Digital Brand Protection program, and Axur is a key tool in making that possible.”
>
> Leonardo Chiodin
> Senior Information Security
> Analyst at Naranja X

Powerful API enabling full automation

Axur’s API made 100% mitigation automation possible, triggering real-time responses and automated takedowns 24/7. The integrated workflow of monitoring, detection, analysis, and remediation dramatically reduces Mean Time to Containment (MTTC).

Start protecting your business and your customers with Axur today

BOOK A DEMO

Gartner
Peer Insights 4.9 ★★★★★

Discover all our solutions: **axur.com**

///AXUR