How Americanas Secured their Digital Platforms, Saving Millions, Boosting Productivity, and Overcoming a Secure Cyberattack.

Lojas Americanas successfully navigated a R$ 2 billion cyberattack targeted at their e-commerce platform, achieving and sustaining 100% availability across their digital platforms after this incident. These platforms generate an annual revenue of R$ 1.5 billion through 50 million customers.

1 Who is the Customer?

Lojas Americanas is one of the largest retailers in Brazil, with a strong presence in both e-commerce and physical stores. They stand out in the e-commerce landscape due to their market leadership through brands like Americanas, Submarino, and Shoptime. They offer a diverse and convenient platform, driven by digital marketing strategies, efficient logistics, and substantial investments in technology.

96 Years of History

49 Million Customers

44k + Employees

55.3 Billion in Revenues

162 Million Hits on eCommerce

87k Sellers Online Mkt place

2 Context and Challenges

The cybersecurity landscape in the Brazilian e-commerce sector in 2021 was challenging. Cyberattacks in Brazil surged by 62% compared to 2020, making it one of the most active years for attacks. Companies like Lojas Renner, CVC, Porto Seguro, Atento, Serasa Experian, as well as platforms like Facebook and LinkedIn, faced the repercussions of having their users exposed or their systems rendered inoperative.

Lojas Americanas themselves had experienced an almost 72-hour outage on their e-commerce platforms. Following this incident, the company began to seek a partner capable of implementing stronger and more appropriate security practices to safeguard sensitive customer data, financial information, and transaction systems . This also included compliance with data protection regulations such as the General Data Protection Law (GDPL).

With a presence in both e-commerce and physical stores, Lojas Americanas stand out in the retail sector by providing a diverse and convenient platform, driven by digital marketing strategies, efficient logistics, and technology investments.

They lead the Brazilian e-commerce market, consistently striving to enhance customer experience and adapt to online market changes.

3 Business Pain Points – Cyberattacks on eCommerce

1. **Decrease in Revenue:** Unfulfilled sales due to platform unavailability for customers.
2. **Storage Costs** for unmoved products (due to platform unavailability) + additional costs resulting from applied fraud.
3. **Loss of Brand Market Value** stemming from external mistrust generated
4. **High Costs** of ransom for kidnapped data or for restoring platform availability.
5. **Decreased Consumer Trust** and brand reputation among customers, suppliers, and business partners.
6. **Fines and Legal Actions** due to customer data breaches.

AMERICANAS CASE

In 2021, the e-commerce platforms Americanas, Submarino, and Shoptime experienced one of the largest e-commerce platform attacks in Brazil. This incident coincided with a major marketing campaign planned during a popular reality show on Brazilian broadcast TV. The attack led to the disruption of the live sales campaign, despite prior merchandising efforts.

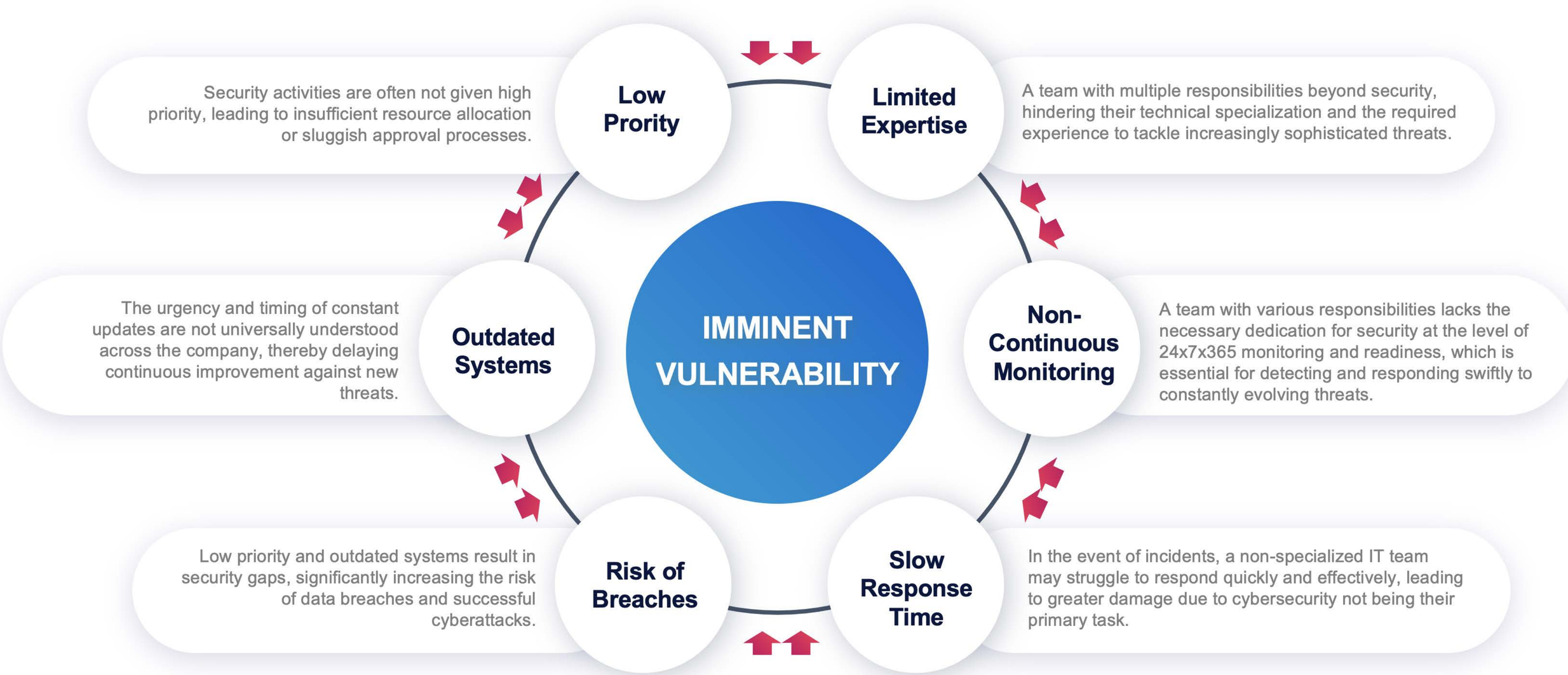
72 Hours of **Unavailability**

3 bi R$ **Millions in Market Value Loss** on the Bovespa (Brazilian stock exchange)

Loss in **Sales** and **Market Reputation**

Source: https://www.ibevar.org.br/blog/ataque-hacker-carregam-impactos-operacionais-e-financeiros-para-o-varejo/

Internal Company Challenges



4 Project Overview – Goals

Continuous Monitoring and Efficient Response

Achieve **uninterrupted monitoring** of network and system activities to identify real-time threats and ensure an immediate and coordinated response to security incidents, neutralizing or minimizing their impact.

Reputation Damage Prevention

Take **proactive measures** to strengthen data protection and prevent the exploitation of vulnerabilities that could lead to breaches, compromising customer trust and causing damage to the brand's reputation.

Alignment with Regulations

Ensure that security practices are aligned with specific regulations and continuously monitor compliance to **prevent violations and associated fines**.

Efficient Risk Management

Enhance the **identification, assessment, and management of cyber risks**, enabling the efficient allocation of resources to mitigate vulnerabilities and threats.

Agility and Scalability

Adapt services as the e-commerce expands, providing scalable support in monitoring and daily incident management.

Implemented Solution

GOVERNANCE, RISK& COMPLIANCE

- VULNERABILITY MANAGEMENT
- RISK & INCIDENT MANAGEMENT

PEOPLE

- TECHNICAL & PERSONAL DEVELOPMENT
- RECOGNITION & EVOLUTION
- COMMITMENT TO RESULTS
- TALENT ATTRACTIVENESS

PROCESS & METHODOLOGY

PYRAMID OF PAIN · CIS Controls · MITRE ATT&CK · ISO 27001 · NIST · INFOSEC WHEEL

TECHNOLOGY & INNOVATION

HYPERAUTOMATION and SCALABILITY

400 incidents/day - proactive and automated assessment and decision-making

REAL-TIME THREAT MONITORING · TECHNOLOGY AGNOSTIC · GLOBAL COVERAGE

4 Project Overview – Approach

For over 7 years, no client including the Stefanini Group, has experienced business interruptions.

stefanini GROUP

CYBERSECURITY

stefanini rafael

WAR COMBAT LEARNING:

Stefanini Rafael brings 60 years of experience in military defense and 20 years in global cybersecurity, including ongoing defense for the Israeli government. The developed Attack Innovation Mitigating Defense Model involves hands-on learning rooted in safeguarding against the latest cyberattack techniques. (For over 7 years, no clients, including the Stefanini Group, have experienced business interruptions)

Innovative Attack Mitigation Defense Model

Practical learning based on defending against the latest techniques of created cyberattacks.

5 Results and Business Impact

$50 Mil
Per Year saved from prevented attacks and data leaks

100%
Availability across all eCommerce platforms of the group

300%
Increase productivity of the client's internal IT team

Ongoing Gains
In consumer trust and brand value in the market

100x Payback
On the **security investment**