Intelligent Perimeter Monitoring for a Pharmaceutical Laboratory

IThink UPC
One Step Ahead in the Digital World

Thanks to our **intelligent perimeter monitoring** solution, a leading pharmaceutical laboratory in Barcelona has made a **qualitative leap in its cybersecurity**: it now detects, prioritizes, and responds to vulnerabilities more quickly and effectively, **minimizing the risk of cyberattacks**.

The Challenge

In a context where cybersecurity is critical, especially in highly regulated and sensitive sectors like pharmaceuticals, one of our clients, a benchmark pharmaceutical laboratory in Barcelona, was facing the challenge of efficiently managing a **growing volume of vulnerabilities** in its connected systems. Some of these were already being exploited, demanding a swift and effective response.

The increasing complexity of its digital infrastructure required full visibility to detect risks and anticipate potential attacks. To achieve this, the laboratory relied on IThinkUPC, with the aim of **proactively identifying and managing these threats**, thereby reducing its exposure and ensuring the secure continuity of its operations.

To address the challenge, we applied a data-driven approach based on real-world intelligence, artificial intelligence, and a practical view of security, which prioritizes critical threats and optimizes remediation resources.

The Project

The main goal of the project was to reduce the risk of exposure to cyberattacks and optimize remediation management, allowing the laboratory's team to focus on what truly matters. To achieve this, we developed a four-phase action plan:

1. **Thorough analysis of the infrastructure**. A detailed analysis of the laboratory's technological environment was carried out to detect all existing vulnerabilities. This initial diagnosis provided a complete and realistic view of the security status.

2. **Prioritization based on actual risk**. Instead of following the traditional methodology based solely on theoretical severity (CVSS), we applied the **EPSS (Exploit Prediction Scoring System)** model. This allowed us to prioritize vulnerabilities with a higher probability of being exploited, optimizing the team's efforts and significantly reducing the workload on low-relevance tasks.

3. **Tailored recommendations and remediation plan**. We created a remediation plan adapted to the laboratory's context and resources, with concrete and efficient measures. These recommendations included not only patches but also practical mitigations aligned with its budget and business priorities.

4. **Ongoing monitoring and proactive insight**. We implemented continuous monitoring to detect new threats, ensure the effective implementation of the recommended actions, and adjust the plan as needed. This ensured active protection aligned with the evolving digital landscape.

A Data-Driven Approach

One of the key elements of the project was the adoption of the **EPSS (Exploit Prediction Scoring System)** model, a statistical system that predicts the likelihood of a vulnerability being exploited in the near future.

Unlike traditional approaches, this methodology relies on real and dynamic data, combining artificial intelligence and machine learning to offer predictions that reflect reality. Thanks to this, the laboratory was able to make better-informed decisions, prioritizing critical remediations and reducing the time of exposure to potential attacks.

EPSS vs. Traditional Approach: A Key Comparison

The table below summarizes the differences between the methodology used by **IThinkUPC (EPSS)** and the **traditional approach (CVSS)**:

Functionality	Analysis with IThinkUPC	Traditional Analysis
Main Objective	Exploitation probability, based on documented real-world risk	Theoretical severity of the vulnerability
Contextual Factors	With Threat Intelligence and active exploitation patterns	No exploitability based on real evidence. Only considers theoretical risks
Use Case	Prioritization of well-founded threats	Understanding severity and potential impact
Strengths	Focus on immediate actions and risk remediations	Comprehensive severity assessment
Coverage and Efficiency	Excellent coverage with much higher efficiency	Medium-low coverage

The Results

Thanks to this approach, the laboratory achieved the following:

- **Dramatically reduced the risk of cyberattacks**, with a more effective and focused approach.
- **Increased confidence in its security posture**, both internally and from the perspective of clients and regulatory bodies.
- **Improved regulatory compliance**, demonstrating a proactive attitude toward audits and industry standards.
- **Optimized resources**, dedicating time and effort only to relevant threats.

IThink UPC
One Step Ahead in the Digital World

For more information, get in touch with us.

Marc Lapuente
Cybersecurity Business Developer
m.lapuente@ithinkupc.com