

Vigilancia perimetral inteligente para un laboratorio farmacéutico

IThink 
One Step Ahead
in the Digital World



Gracias a nuestra solución de **vigilancia perimetral inteligente**, un destacado laboratorio farmacéutico de Barcelona ha dado un **salto cualitativo en su ciberseguridad**: ahora detecta, prioriza y actúa frente a vulnerabilidades de forma más rápida y eficaz, **minimizando el riesgo de ciberataques**.

El reto

En un contexto donde la ciberseguridad es crítica, especialmente en sectores tan regulados y sensibles como el farmacéutico, uno de nuestros clientes, un laboratorio farmacéutico de referencia de Barcelona, se enfrentaba al reto de gestionar de forma eficiente un **volumen creciente de vulnerabilidades** en sus sistemas conectados. Algunas de ellas ya estaban siendo explotadas, lo que exigía una respuesta ágil y eficaz.

La creciente complejidad de su infraestructura digital requería una visibilidad total para detectar riesgos y anticiparse a posibles ataques. Para lograrlo, el laboratorio confió en IThinkUPC, con el objetivo de **identificar y gestionar proactivamente estas amenazas**, reduciendo así su exposición y garantizando la continuidad segura de sus operaciones.

Para responder al desafío, aplicamos un enfoque basado en datos reales, inteligencia artificial y una visión práctica de la seguridad, que prioriza las amenazas críticas y optimiza los recursos de remediación.

El proyecto

El objetivo principal del proyecto fue reducir el riesgo de exposición a ciberataques y optimizar la gestión de remediación, permitiendo al equipo del laboratorio centrarse en lo que realmente importa. Para ello, desarrollamos un plan de acción en cuatro fases:

1. **Análisis exhaustivo de la infraestructura.** Se realizó un escaneo detallado del entorno tecnológico del laboratorio para detectar todas las vulnerabilidades presentes. Este diagnóstico inicial permitió establecer una visión completa y realista del estado de seguridad.
2. **Priorización basada en riesgo real.** En lugar de seguir la metodología tradicional basada únicamente en la severidad teórica (CVSS), aplicamos el modelo **EPSS (Exploit Prediction Scoring System)**. Esto nos permitió priorizar las vulnerabilidades con mayor probabilidad de ser explotadas, optimizando los esfuerzos del equipo y reduciendo significativamente la carga de trabajo en tareas poco relevantes.
3. **Recomendaciones personalizadas y plan de remediación.** Elaboramos un plan de remediación adaptado al contexto y recursos del laboratorio, con medidas concretas y eficientes. Estas recomendaciones incluían no solo parches, sino también mitigaciones prácticas alineadas con su presupuesto y prioridades de negocio.
4. **Seguimiento continuo y visión proactiva.** Establecimos una monitorización constante para detectar nuevas amenazas, asegurar la implementación efectiva de las acciones recomendadas y ajustar el plan cuando fuera necesario. Esto permitió mantener la protección activa y alineada con la evolución del entorno digital.

Un enfoque basado en datos reales

Uno de los elementos clave del proyecto fue la adopción del modelo **EPSS (Exploit Prediction Scoring System)**, un sistema estadístico que predice la probabilidad de que una vulnerabilidad sea explotada próximamente.

A diferencia de enfoques tradicionales, esta metodología se basa en datos reales y dinámicos, combinando inteligencia artificial y aprendizaje automático para ofrecer predicciones ajustadas a la realidad. Gracias a ello, el laboratorio pudo tomar decisiones mejor fundamentadas, priorizando remediaciones críticas y reduciendo el tiempo de exposición a posibles ataques.



EPSS vs. enfoque tradicional: una comparación clave

La siguiente tabla resume las diferencias entre la metodología utilizada por IThinkUPC (EPSS) y el enfoque tradicional (CVSS):

Funcionalidad	Análisis con IThinkUPC	Análisis tradicional
Objetivo principal	Probabilidad de explotación, según riesgo real documentado	Severidad teórica de la vulnerabilidad
Factores de contexto	Con Threat Intelligence y patrones activos de explotación	Sin explotabilidad basada en hechos reales. Solo contempla riesgos teóricos
Casos de uso	Priorización de amenazas fundamentadas	Comprender la gravedad y el posible impacto
Fortalezas	Enfoque en acciones inmediatas y remediaciones de riesgo	Evaluación integral de la gravedad
Cobertura y eficiencia	Excelente cobertura con una eficiencia mucho mayor	Cobertura media-baja

Los resultados

Gracias a este enfoque, el laboratorio consiguió:



Reducir drásticamente el riesgo de ciberataques, con un enfoque más eficaz y focalizado.



Incrementar la confianza en su postura de seguridad, tanto interna como de cara a clientes y organismos reguladores.



Mejorar su cumplimiento normativo, mostrando una actitud proactiva ante auditorías y estándares del sector.



Optimizar recursos, dedicando tiempo y esfuerzo solo a las amenazas relevantes.