Vigilància perimetral intel·ligent per a un laboratori farmacèutic

IThink UPC
One Step Ahead
in the Digital World

Gràcies a la nostra solució de **vigilància perimetral intel·ligent**, un destacat laboratori farmacèutic de Barcelona ha fet un **salt qualitatiu en la seva ciberseguretat**: ara detecta, prioritza i actua davant de vulnerabilitats de manera més ràpida i eficaç, **minimitzant el risc de ciberatacs**.

El repte

En un context on la ciberseguretat és crítica, especialment en sectors tan regulats i sensibles com el farmacèutic, un dels nostres clients, un laboratori farmacèutic de referència de Barcelona, s'enfrontava al repte de gestionar de manera eficient un **volum creixent de vulnerabilitats** en els seus sistemes connectats. Algunes d'aquestes ja estaven sent explotades, fet que exigia una resposta àgil i eficaç.

La creixent complexitat de la seva infraestructura digital requeria una visibilitat total per detectar riscos i anticipar-se a possibles atacs. Per aconseguir-ho, el laboratori va confiar en IThinkUPC, amb l'objectiu d'**identificar i gestionar proactivament aquestes amenaces**, reduint així la seva exposició i garantint la continuïtat segura de les seves operacions.

Per respondre al desafiament, vam aplicar un enfocament basat en dades reals, intel·ligència artificial i una visió pràctica de la seguretat, que prioritza les amenaces crítiques i optimitza els recursos de remediació.

El projecte

L'objectiu principal del projecte va ser reduir el risc d'exposició a ciberatacs i optimitzar la gestió de remediació, permetent a l'equip del laboratori centrar-se en allò que realment importa. Per aconseguir-ho, vam desenvolupar un pla d'acció en quatre fases:

1. **Anàlisi exhaustiva de la infraestructura**. Es va dur a terme una anàlisi detallada de l'entorn tecnològic del laboratori per detectar totes les vulnerabilitats presents. Aquest diagnòstic inicial va permetre establir una visió completa i realista de l'estat de la seguretat.

2. **Priorització basada en el risc real**. En lloc de seguir la metodologia tradicional basada únicament en la severitat teòrica (CVSS), vam aplicar el model **EPSS (Exploit Prediction Scoring System).** Això ens va permetre prioritzar les vulnerabilitats amb més probabilitat de ser explotades, optimitzant els esforços de l'equip i reduint significativament la càrrega de treball en tasques poc rellevants.

3. **Recomanacions personalitzades i pla de remediació**. Vam elaborar un pla de remediació adaptat al context i als recursos del laboratori, amb mesures concretes i eficients. Aquestes recomanacions incloïen no només pegats, sinó també mitigacions pràctiques alineades amb el seu pressupost i les seves prioritats de negoci.

4. **Seguiment continu i visió proactiva**. Vam establir una monitorització constant per detectar noves amenaces, assegurar la implementació efectiva de les accions recomanades i ajustar el pla quan fos necessari. Això va permetre mantenir una protecció activa i alineada amb l'evolució de l'entorn digital.

Un enfocament basat en dades reals

Un dels elements clau del projecte va ser l'adopció del model **EPSS (Exploit Prediction Scoring System)**, un sistema estadístic que prediu la probabilitat que una vulnerabilitat sigui explotada properament.

A diferència dels enfocaments tradicionals, aquesta metodologia es basa en dades reals i dinàmiques, combinant intel·ligència artificial i aprenentatge automàtic per oferir prediccions ajustades a la realitat. Gràcies a això, el laboratori va poder prendre decisions més ben fonamentades, prioritzant remediacions crítiques i reduint el temps d'exposició a possibles atacs.

EPSS vs. enfocament tradicional: una comparació clau

La taula següent resumeix les diferències entre la metodologia utilitzada per **IThinkUPC (EPSS)** i l'**enfocament tradicional (CVSS)**:

Funcionalitat	Anàlisi amb IThinkUPC	Anàlisi tradicional
Objectiu principal	Probabilitat d'explotació, segons risc real documentat	Severitat teòrica de la vulnerabilitat
Factors de context	Amb Threat Intelligence i patrons actius d'explotació	Sense explotabilitat amb fets reals. Només contempla riscos teòrics
Cas d'ús	Prioritzar amenaces fonamentades	Entendre la gravetat i el possible impacte
Fortaleses	Focus en accions immediates i remediacions de risc	Avaluació integral de la gravetat
Cobertura i eficiència	Cobertura excel·lent amb una eficiència molt més gran	Mitjana-Baixa

Els resultats

Gràcies a aquest enfocament, el laboratori va aconseguir:

- **Reduir dràsticament el risc de ciberatacs**, amb un enfocament més eficaç i focalitzat.
- **Incrementar la confiança en la seva postura de seguretat**, tant interna com de cara a clients i organismes reguladors.
- **Millorar el seu compliment normatiu**, mostrant una actitud proactiva davant d'auditories i estàndards del sector.
- **Optimitzar recursos**, dedicant temps i esforç només a les amenaces rellevants.

IThink UPC
One Step Ahead in the Digital World

Per a més informació, contacta amb nosaltres.

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