Cómo transformar el hallazgo de vulnerabilidades en la máxima tranquilidad para sus clientes

Tras superar con éxito su etapa de lanzamiento, Zeronet, la firma de software que está redefiniendo el ecosistema Green ITOps desde su fundación en 2024, ha completado una exhaustiva reingeniería de sus capacidades de análisis de datos.

Con un ecosistema digital maduro y un volumen creciente de clientes corporativos, la tecnológica ha dado un giro estratégico al evolucionar desde el diagnóstico ambiental estático hacia la mitigación activa y automatizada del consumo en la nube. De este modo, permite a las grandes corporaciones aligerar drásticamente el impacto ecológico de sus sistemas informáticos mediante software puro, prescindiendo de sensores costosos o equipamiento físico, lo que a su vez maximiza el ahorro de costes energéticos y acelera sus metas ESG.

EL RETO

Antes de integrarse al programa de hacking ético de Secur0, Zeronet carecía de auditorías formales de seguridad, por lo que la protección de su plataforma dependía exclusivamente de las buenas prácticas de su equipo de desarrollo. Esta falta de validación externa dejaba expuestos riesgos críticos, tanto lógicos como de infraestructura, que resultaban indetectables mediante los análisis internos automatizados.

El verdadero reto consistía en evaluar de forma independiente y rigurosa la resistencia del sistema. Zeronet necesitaba descubrir de manera proactiva cualquier vulnerabilidad que pudiera comprometer la confidencialidad, integridad o disponibilidad de sus servicios, neutralizando las amenazas antes de que pudieran ser explotadas por actores maliciosos.

SOLUCIÓN PLANTEADA

La estrategia para blindar la plataforma se articuló mediante la puesta en marcha de un Programa de Divulgación de Vulnerabilidades (VDP) respaldado por analistas de hacking ético, cuyo propósito principal fue descubrir fallos de seguridad complejos que habían pasado completamente desapercibidos para las herramientas automáticas de la

compañía. Este enfoque proactivo permitió auditar a fondo el código y la arquitectura de la nube, simulando ataques reales para evaluar la resistencia del software sin alterar la operatividad de los clientes que ya utilizaban el servicio.

IMPACTO

Gracias a la detección temprana de estas debilidades críticas, Zeronet logró neutralizar amenazas graves antes de que causaran daños reales, transformando esos riesgos en una clara ventaja competitiva. Al corregir los fallos lógicos en la confidencialidad del sistema, se evitó por completo el espionaje corporativo y la filtración de registros de consumo energético o costes operativos, garantizando el blindaje absoluto de la información estratégica de las empresas.

Asimismo, solventar los problemas de integridad y suplantación en los paneles de configuración impidió el secuestro de claves API o la desactivación de las alarmas de monitorización, lo que reforzó la confianza de los clientes en la estabilidad de la plataforma. Finalmente, al subsanar la vulnerabilidad en las funciones de diagnóstico, se previno un posible colapso digital a gran escala y la caída simultánea de las conexiones de red de múltiples organizaciones. Como resultado directo, Zeronet no solo protegió la continuidad del negocio de sus usuarios, sino que consolidó su reputación en el mercado corporativo como un socio tecnológico maduro, seguro y plenamente alineado con los más altos estándares de ciberseguridad.

> “Sabíamos que un pentest encontraría fallos en el sistema, y esa era exactamente la idea. En lugar de temer a los resultados, vimos esta prueba como el camino más rápido para mejorar nuestro producto y dar total tranquilidad a nuestros clientes.”