Yahya Mortahil Elaaouad

Técnico Superior en Administración de Sistemas Informáticos en Red

yahyamortahilelaaouad@gmail.com | 632 08 79 97 | linkedin.com/in/yahya-mortahil-elaaouad

PERFIL

Técnico Superior en ASIR con experiencia práctica en seguridad defensiva, hardening de infraestructuras y monitorización de amenazas. Sólida capacidad demostrada en el diseño e implementación de soluciones de seguridad perimetral, despliegue de entornos SIEM y ejecución de campañas de concienciación en ingeniería social. Perfil proactivo con dominio de herramientas Open Source y enterprise, y un firme compromiso con la mejora continua en un sector en constante evolución.

EXPERIENCIA PROFESIONAL

Ulandu, Formación en prácticas 12/2025 – 06/2026

- Aseguramiento y control de la totalidad de la red corporativa mediante la configuración e intercepción de tráfico NAT con pfSense, gestionando el enrutamiento seguro de 10 usuarios simultáneos y logrando un uptime del 99% sin registrar fugas de información.
- Despliegue e integración de un sistema de filtrado DNS perimetral centralizado con pfBlockerNG, dando cobertura a más de 20 dispositivos en la oficina y reduciendo el tráfico de red no deseado en aproximadamente un 30%.
- Implementación de controles avanzados de seguridad perimetral con pfBlockerNG, logrando el bloqueo proactivo de más de 5.000 consultas DNS maliciosas y mitigando amenazas a nivel de IP y dominio.
- Implementación integral de un entorno SIEM basado en Wazuh, abarcando la configuración del servidor central y el despliegue de agentes en 15 endpoints, lo que permitió centralizar los logs y reducir el tiempo de detección de incidentes a tiempo real.
- Diseño y ejecución de campañas de phishing simulado con Gophish dirigidas a 10 empleados, evaluando el nivel de concienciación interno y reduciendo la tasa de clics en enlaces maliciosos en un 40% tras las acciones formativas.

PROYECTOS

Marshall: Plataforma de monitorización y Análisis del tráfico de red

- Desarrollo de una plataforma de monitorización y detección de amenazas en tiempo real orientada a pequeñas y medianas empresas, integrando Suricata como motor IDS para el análisis de tráfico de red y un backend en Flask para la centralización, correlación, filtrado y generación de alertas sobre eventos sospechosos.
- Diseño de pipeline de procesamiento de logs capaz de gestionar grandes volúmenes de datos de red, reduciendo el tiempo de triaje de incidencias mediante una interfaz orientada a la eficiencia operativa del SOC.
- Stack: Suricata, Flask, Python, análisis de tráfico de red, IDS/IPS, detección de amenazas, SIEM, correlación de eventos, monitorización en tiempo real.

COMPETENCIAS Y TECNOLOGÍAS

Seguridad y Hacking Ético: Seguridad perimetral, análisis de vulnerabilidades, hardening, mitigación de amenazas, SIEM, SOC, IDS/IPS, pentesting, ingeniería social, respuesta ante incidentes.

Herramientas de Seguridad: pfSense, pfBlockerNG, Wazuh, Gophish, Suricata, Nmap, SQLmap, Metasploit, Sn1per, OpenVAS, Nessus.

Redes e Infraestructura: TCP/IP, DNS, DHCP, NAT, routing, firewalls, filtrado DNS, VPN, segmentación de red.

Sistemas Operativos y Servidores: Linux, Windows Server, hardening de sistemas, SSL/TLS, Docker, Apache.

Scripting y Desarrollo: Python, Bash, Flask, bases de datos.

Competencias Transversales: Capacidad analítica, trabajo en equipo, proactividad, aprendizaje rápido.

EDUCACIÓN

IES Ribera del Tajo 09/2024 – 05/2026
Ciclo Formativo de Grado Superior en Administración de Sistemas Informáticos en Red (Modalidad Bilingüe)

CERTIFICADOS

- Ciberseguridad en la Empresa
- Especialista en Hacking Ético
- Curso de análisis de malware
- Python Essentials 1
- Python Essentials 2

IDIOMAS

Español (Nativo), **Inglés** (Intermedio - B1)