ALEJANDRO SÁNCHEZ MORENO

Administrador de Sistemas y Técnico de Ciberseguridad



sanchezalexmoreno16@gmail.com
634761208
Toledo
credly.com/users/alex16
linkedin.com/in/alexitosm16
github.com/alexitocvf16
alexitocvf16.github.io

OTROS DATOS

Discapacidad reconocida del 33%
Plenamente apto para el ejercicio de la profesión y las funciones del puesto.

IDIOMAS

Inglés: nivel medio

SKILLS

SOFT SKILLS

- Trabajo en equipo y comunicación profesional
- Documentación técnica y redacción de informes
- Capacidad analítica y resolución de problemas
- Capacidad para recibir y aplicar feedback
- Aprendizaje continuo
- Responsabilidad, compromiso y discreción

PERFIL PROFESIONAL

Técnico en formación en Administración de Sistemas Informáticos en Red, enfocado en la ciberseguridad defensiva (Blue Team) y la respuesta ante incidentes. Tengo formación básica en SIEM con Splunk y me estoy preparando la certificación Blue Team Level 1 (BTL1). Cuento con una base práctica en administración de Linux, Windows Server y Active Directory, análisis de tráfico con Wireshark y automatización de tareas con Python, n8n e inteligencia artificial. Además, la eJPTv2 me da conocimiento de las técnicas de ataque, útil para saber qué buscar al defender. Busco unas prácticas en un SOC o departamento de Seguridad TIC para crecer en monitorización, triaje de alertas, gestión de incidentes y documentación técnica.

EDUCACIÓN

Administración de Sistemas Informáticos en Red
FP Euroformac · 2025 – Actual

Bachillerato
I.E.S. El Greco

CERTIFICACIONES Y FORMACIÓN

- **Blue Team Level 1 (BTL1)** · en preparación
- Curso de introducción a Splunk (SIEM)
- Junior Penetration Tester (eJPTv2)
- Cisco Certified Support Technician Cybersecurity (CCST Cybersecurity)
- Microsoft Certified: Security, Compliance, and Identity Fundamentals (SC-900)
- Microsoft Certified: Azure AI Fundamentals (AI-900)
- Artificial Intelligence Fundamentals (IBM)

PROYECTOS PRÁCTICOS · HOMELAB

- **Monitorización y análisis:** análisis de tráfico de red con Wireshark y revisión de registros de sistemas Windows y Linux en el laboratorio para detectar actividad anómala.
- **Perspectiva del atacante:** creación de máquinas vulnerables y ejercicios de hacking ético en entorno controlado (Kali Linux, Burp Suite) para entender las técnicas de ataque y cómo detectarlas; documentación de hallazgos.
- **Administración segura de sistemas:** despliegue de Active Directory y Windows Server, gestión de usuarios, grupos y permisos, y revisión de configuraciones en Linux y Windows.
- **Automatización e IA:** flujos de automatización con n8n y scripts en Python, apoyándome en herramientas de IA para agilizar tareas repetitivas, analizar información y documentar; servicios desplegados en Docker.

COMPETENCIAS TÉCNICAS

Blue Team: monitorización y análisis
Splunk (nivel básico), Wireshark, análisis de logs y tráfico de red

Sistemas, redes y virtualización
Windows Server, Active Directory, Linux, Cisco Packet Tracer, VirtualBox, VMware

Conocimiento ofensivo (apoyo a la defensa)
Kali Linux, Burp Suite, herramientas de pentest

Cloud, identidad y cumplimiento
AWS, Microsoft Azure, Microsoft Entra ID; fundamentos de cumplimiento normativo (SC-900)

IA y automatización
Python, n8n, Docker, MySQL; uso de IA generativa para scripting, análisis y documentación