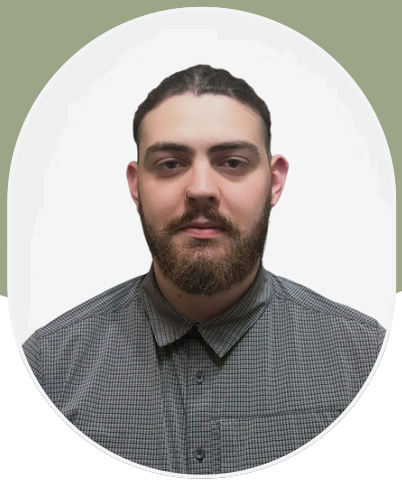
ALBERT
PALAZÓN VILLARINO

Cybersecurity Analyst

albertpalazon.github.io



Sobre mí

Profesional IT con más de 6 años de experiencia en entornos empresariales internacionales (L1, L2 y formación del equipo), especializado en gestión de identidades y análisis de incidencias en infraestructuras críticas.

Máster en Ciberseguridad y certificados CCSP (ISMS Forum) y eJPT (INE).

Enfocado a roles de Cybesecurity Analyst, SOC y Threat Hunting , combinando experiencia real y base técnica en gestión de vulnerabilidades, alertas y seguridad en entornos cloud.

Contacto

652 950 346

albertpalazon97@gmail.com

linkedin.com/in/albertpalazon

Badalona, Barcelona (abierto a trabajo remoto)

github.com/albertpalazon

Certificaciones

- eJPTv2 - Junior Penetration Tester
- CCSP - Certified Cyber Security Professional
- eCPPTv3 - Certified Professional Penetration Tester – En progreso

Idiomas

Español	Catalán	Inglés
100%	100 %	80 %
Nativo	Nativo	Advanced C1

FORMACIÓN

- Grado superior de Administración de Sistemas y Redes
- Grado medio de Sistemas Microinformáticos y Redes
- Máster en Ciberseguridad y Hácking Ético - UCAM

  TFM - Desarrollo de una distribución Linux para la investigación OSINT.

EXPERIENCIA LABORAL

NTT Communications - Europe LTD

BH Senior Service Desk Analyst **2022-2024**

- Referente técnico del equipo, responsable de validación y aprobación de Change Requests. Formación de equipo de 10 analistas.
- Gestión de incidencias en entornos VoIP y Cloud (Microsoft Teams, SIP, Cisco CUCM), mediante múltiples plataformas ITSM (ServiceNow, Salesforce, Angora) y portales propios de clientes y carriers.
- Administración del portal corporativo y gestión de identidades y permisos en Azure AD.
- Resolución y análisis de incidencias técnicas en infraestructuras críticas.

24x7 Service Desk Analyst **2019 – 2022**

- Soporte L2 en entornos enterprise para incidencias relacionadas con Fortinet Firewall, NetScaler SSL, DNS, Load Balancers y NetBackup/Veritas.
- Gestión de almacenamiento: NetApp Fillers, SAN, NAS, CIFS, NFS, LUN.
- Investigación y resolución de incidencias recurrentes, implementando soluciones permanentes.
- Documentación técnica y estandarización de procesos y runbooks. .

24x7 Service Desk Operator **2018-2019**

- L1 de Incidencias y solicitudes en el Service Desk
- Gestión de alertas y hosting, con formación para el Nivel 2 de escalado.
- Resolución básica de problemas relacionados con Storage y Networking.
- Helpdesk L2 para clientes externos.

HABILIDADES TÉCNICAS

- Análisis SIEM y de eventos: Splunk, ELK Stack, log analysis & correlation
- Incident Response: alert triage, incident investigation, root cause analysis
- Threat Detection & Hunting: suspicious activity, IoCs, TTPs, MITRE ATT&CK
- EDR y Herramientas de Seguridad: Microsoft Defender, CrowdStrike, Firewalls
- Detección y Monitorización: casos de uso SIEM , alert tuning, rule improvement
- Sistemas e Infraestructura: Windows, Linux, Cloud, AWS, Azure AD (IAM / MFA)
- Seguridad Ofensiva: eJPT, eCPPT, web, AD y network Pentesting, OWASP
- Scripting: PowerShell, Python y Exploits