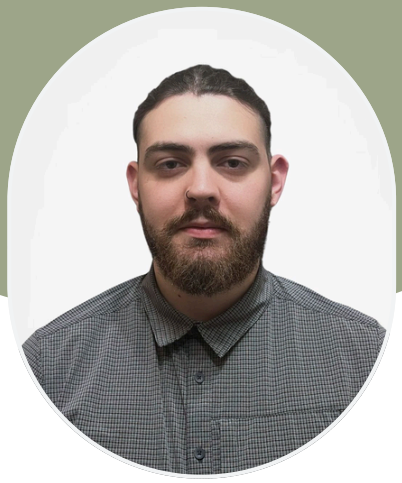
ALBERT
PALAZÓN VILLARINO

Cybersecurity Analyst

albertpalazon.github.io



About me

IT professional with more than 6 years of experience in enterprise environments, supporting Level 1 and Level 2 operations and contributing to team training. Specialized in identity management and incident analysis in critical infrastructures.

Master's degree in Cybersecurity and certifications including CCSP (ISMS Forum) and eJPT (INE Security).

Currently focused on Cybesecurity Analyst SOC and Threat Hunting roles, combining hands-on technical experience with vulnerability management and cloud security environments.

Contact

652 950 346

albertpalazon97@gmail.com

linkedin.com/in/albertpalazon

Badalona, Barcelona (open to remote work)

github.com/albertpalazon

Certifications

- eJPTv2 - Junior Penetration Tester
- CCSP - Certified Cyber Security Professional
- eCPPTv3 - Certified Professional Penetration Tester – In progress

Languages

Spanish	Catalan	English
100%	100 %	80 %
Native	Native	Advanced C1

Education

- Higher Degree in Network & Systems Administration
- Higher Degree in Systems & Network
- Master's degree Cybersecurity & Ethical Hacking - UCAM
  Master's Thesis: Development of a Linux distribution for OSINT research

Professional Experience

NTT Communications - Europe LTD

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

- Technical lead within the team, responsible for validation and approval of operational changes. Training of a 10-member analyst team.
- Incident management in Low Priority Cloud environments (Teams, SIP, CUCM) across multiple ITSM platforms (ServiceNow, Salesforce, Agora) and corporate customer portals.
- Administration of corporate portals and IAM in Azure AD.
- Resolution and analysis of technical incidents in critical infrastructure environments.

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

- Level 2 support in enterprise environments for incidents related to Fortinet Firewalls, NetScaler SSL, DNS, Load Balancers and NetBackup.
- Storage management: NetApp Filers, SAN, NAS, CIFS, NFS, LUN.
- Investigation and resolution of recurring incidents, implementing permanent technical solutions.
- Technical documentation and standardization of procedures and runbooks.

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

- Incident and resolution within the Service Desk.
- Monitoring and alert management for hosting environments, with training for escalation to Level 2.
- Resolution of issues related to storage and networking infrastructure.
- Helpdesk Level 2 support for external clients.

Technical Skills

- SIEM & Event Analysis: 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 & Security Tools: Microsoft Defender, CrowdStrike, Firewalls (Fortinet)
- Detection & Monitoring: SIEM use cases, alert tuning, rule improvement
- Systems & Infrastructure: Windows, Linux, Cloud, AWS, Azure AD (IAM / MFA)
- Offensive Security: eJPT, eCPPT, web, AD & network Pentesting, OWASP
- Scripting: PowerShell, Python & Exploits