PABLO PEREZ GARCIA

ANALISTA BLUE TEAM · SOC L1 · CIBERSEGURIDAD DEFENSIVA · FORENSE DIGITAL

+34 681279891 perez.gcia+job@gmail.com Madrid, Spain ppg92
papgar92 papgar92.github.io/whoami/

Técnico IT con base sólida en administración de sistemas (Windows y Linux) y experiencia práctica con herramientas de ciberseguridad. Actualmente formandome activamente en Blue Team con proyectos propios. Mi objetivo es incorporarme a un equipo SOC o Blue Team ; con foco en detección de intrusiones y respuesta ante incidentes.

HABILIDADES TÉCNICAS

- Blue Team: ▸ IDS/IPS — Snort (reglas, alertas) ▸ Firewall pfSense · WatchGuard ▸ MITRE ATT&CK Framework ▸ Log analysis: SSH, auth.log ▸ Wireshark — análisis de tráfico ▸ ISO 27000 · OT Security (ICS)
- Monitorización: ▸ Nagios Core — config y alertas ▸ Zabbix — monitorización SNMP ▸ Grafana + Prometheus ▸ PNP4Nagios ▸ Alertas SMTP automatizadas
- Sistemas & scripting: ▸ Python — seg. defensiva, logs ▸ Bash · PowerShell ▸ Windows Server 2022 + AD/GPO ▸ Proxmox VE · VMware · Azure ▸ Entra ID + Microsoft Intune ▸ Jira · Helix ITSM · Salesforce

PROYECTOS

Laboratorio SOC — Wazuh + Zeek + Proxmox VE

May 2026

SOC (Centro de Operaciones de Seguridad) montado íntegramente en un servidor Proxmox doméstico usando contenedores LXC ligeros. Cubre recogida de logs, detección de amenazas, análisis de tráfico de red y alertas en tiempo real — todo con herramientas open source y gratuitas.

Wazuh · Zeek · Proxmox
papgar92/soc-monitoring-lab

Detector de Fuerza Bruta SSH

May 2026

- Herramienta Python que analiza auth.log para detectar ataques SSH de fuerza bruta sin SIEM
- Identifica IPs atacantes, cuentas afectadas y patrones temporales; genera reportes de incidente exportables
- Habilidades demostradas: log analysis, detección de patrones de ataque, scripting de seguridad defensiva

Python · Log Analysis · MITRE ATT&CK T1110
papgar92/Detector-Fuerza-bruta-SSH

Red Segura para PYME — TFG ASIR

Sep 2025 - Dic 2025

- Diseño e implementación completa: firewall perimetral (pfSense), IDS con reglas Snort y monitorización Nagios
- Active Directory en Windows Server 2022, segmentación de red, pruebas de detección de intrusiones validadas
- Documentación técnica completa: topología, análisis de costes, procedimientos de prueba y resultados

pfSense · Snort IDS · Nagios · Windows Server 2022
papgar92/TFG-Arquitectura-Defensiva---Blue-Team

IDIOMAS Y FORMACIÓN COMPLEMENTARIA

- Inglés: B2 (MCER)
- ISO 27000 · MITRE ATT&CK · Linux · Forense Windows

EXPERIENCIA RELEVANTE

Técnico de Soporte IT dic 2025 - Present

Cartronic Group

• Administración de infraestructura IT en entorno PYME/corporativo: AD, GPOs, Proxmox/VMware, firewall WatchGuard
• Implementación de Nagios Core + Zabbix para monitorización de servicios críticos: SAP, servidores de dominio, red
• Resolución de incidencias N1-N2, administración de Google Workspace, despliegue de sistemas operativos

Técnico de soporte IT (prácticas) abr 2025 - jul 2025

Prosegur

• Migración On-Premise a cloud: Windows Server AD → Azure AD / Microsoft Intune (Entra ID)
• Despliegue de SSOO via PXE, gestión de inventario y GPOs; ticketing con Helix ITSM

Operador de STR feb 2017 - dic 2025

Movistar Prosegur Alarmas

• Resolución de incidencias en dispositivos de red (cámaras IP, NVRs): puertos, DNS, direccionamiento IP
• Gestión de tickets con Salesforce CRM y escalado via JIRA; experiencia que motivó el cambio deliberado hacia ciberseguridad

FORMACIÓN

FP Superior - ASIR sep 2023 - feb 2026

Ilerna Online

Master en ciberseguridad & IA abr 2026 - dic 2026

Evolve

CERTIFICACIONES

BTL1 — Blue Team Labs Level 1 En preparación - Q3 2026

Security Blue Team

SC-200 — Microsoft Security Operations Planificado - Q4 2026

Microsoft

IFCT0050 — Ciberseguridad en entornos OT Jul 2025 - Ago 2025

Grupo Hedima

IFCT0410 — Redes Departamentales Jun 2025 - Dic 2025

LideraK Formación

IFCT095PO — Python y Django Sep 2025 - Nov 2025

Campo Grande Formación