DANIEL MARTÍNEZ PASCUAL

Aspirante a Analista SOC (N1) · Blue Team · Ciberdefensa

Oviedo, España · linkedin.com/in/danimarpas4 · github.com/danimarpas4 · martinezpascual.es

RESUMEN PROFESIONAL

Aspirante a **Analista SOC N1** con 8 años en el Ejército de Tierra (misiones NATO/UE), donde he trabajado bajo presión y en equipos multinacionales usando inglés operacional (SLP 2.2.2.2). Me formo en monitorización y respuesta a incidentes con **TryHackMe SOC Level 1** (en curso) y Cyber Security 101 (completado). Administro servidores Linux en producción (hardening, SSH por clave, fail2ban, UFW) y analizo logs de Nginx para detectar accesos anómalos y aplicar bloqueos. Curso el BSc in Applied Computing (UWTSD).

EXPERIENCIA

Cabo de Infantería Ligera — Operaciones Multinacionales · Ejército de Tierra Nov 2018 – Actualidad

Presencial · Misiones NATO y UE

- Operé en entornos de alta presión durante 3 despliegues NATO/UE, desarrollando toma de decisiones rápida bajo incertidumbre y gestión de incidentes críticos — habilidades centrales en respuesta a incidentes de seguridad (IR).
- Mantuve protocolos de seguridad operacional (OPSEC) y comunicaciones cifradas en misiones internacionales, aplicando principios de necesidad de saber (need-to-know) y mínimo privilegio en la práctica.
- Obtuve certificación de inglés operacional SLP 2.2.2.2, habilitando lectura de threat intelligence, documentación técnica y colaboración en equipos SOC internacionales.
- Coordiné con fuerzas de +8 países en entornos multinacionales, desarrollando capacidad de trabajo en equipo bajo presión aplicable a turnos de guardia SOC 24/7.

PROYECTOS TÉCNICOS — ENFOQUE SEGURIDAD

Administración y Securización de Infraestructura Web | promilitar.es | martinezpascual.es

Entornos en producción: Servidor VPS (Hetzner) · Nginx · Django · React · Linux Hardening

- **Gestión de Servidores:** Despliegue y administración de aplicaciones SaaS en servidores VPS. Configuración y securización de Nginx como proxy inverso.
- **Seguridad y Hardening:** Implementación de control de acceso SSH por clave, fail2ban, configuración de firewalls (UFW/iptables) y gestión automatizada de certificados SSL/TLS (Let's Encrypt).
- **Monitorización:** Análisis de logs de acceso/error (Nginx) para detectar patrones anómalos o intentos de acceso no autorizados, aplicando bloqueos reactivos.

Automatización y Desarrollo Backend (Bots Telegram eb Python) | app.promilitar.es

Desarrollo: Python asíncrono · Bases de Datos Relacionales (SQL) · APIs

- **Bots de Automatización:** Desarrollo y mantenimiento de bots de Telegram en Python asíncrono para el envío automatizado de contenido, integrando manejo robusto de excepciones, logging estructurado para resolución de incidentes (troubleshooting) y alertas de estado del servicio.
- **Gestión de Bases de Datos:** Diseño y operación de bases de datos relacionales (SQL/MySQL/SQLAlchemy) para la gestión de usuarios de la academia y para la aplicación de seguimiento de personal militar (*app.promilitar.es*), garantizando la integridad relacional de los datos.
- **Pipeline CI/CD:** Implementación de flujos de trabajo en GitHub Actions para la validación y despliegue continuo del código en los servidores de producción.

FORMACIÓN

Bachelor of Science in Applied Computing · University of Wales Trinity Saint David (UWTSD) 2026 – 2029 (En curso)

Grado oficial acreditado UK cursado vía CESTE. Base académica con especialización en ciberseguridad.

Máster en Desarrollo Full-Stack · Conquer Blocks Ago 2025 – Ago 2026

Python - Django · Linux · Nginx · Docker · CI/CD · SQL · APIs REST — comprensión profunda del stack que los SOC defienden.

HABILIDADES TÉCNICAS

Sistemas & Redes: Linux/Ubuntu · Nginx · SSH · TCP/IP · Firewalls · VPS · DNS · SSL/TLS · Wireshark

Monitorización & Logs: Logs web (Nginx) · GitHub Actions alerts · SQLite event logging · Análisis de tráfico

Scripting & Automatiz.: Python (asíncrono, POO) · Bash · SQL · CI/CD

Seguridad aplicada: Hardening de servidores · Gestión de certificados · Control de acceso · OPSEC militar

Desarrollo (stack def.): Django · HTML5/ CSS3 · Git · Docker

Herramientas de Seguridad: TryHackMe (Top 5%) · Conceptos SIEM · MITRE ATT&CK · Splunk

Idiomas: Español (nativo) · Inglés B2 operacional (SLP 2.2.2.2)

CERTIFICACIONES Y FORMACIÓN COMPLEMENTARIA

- TryHackMe: Pre Security (Completado)
- TryHackMe: Cyber Security 101 (Completado)
- TryHackMe: SOC Level 1 (En curso)
- Big Data aplicado al negocio (FADE – Empresas de Asturias, Nov 2025)

Próximas certificaciones objetivo: CompTIA Security+ · AWS Academy Cloud Foundations · Blue Team Level 1 (BTL1)