Gabriel Manuel Vega Domínguez

Especialista Blue Team

Datos de contacto

- vegadominguezg@gmail.com
- 637 066 163
- Vecindario, Gran Canaria
- linkedin.com/in/gabriel-vega-domínguez-6021352a3

Idiomas

Español — Nativo
Inglés — B1

Aptitudes técnicas

- Threat Detection & Response
- Incident Response (IR)
- SIEM: Splunk, IBM QRadar
- Log Analysis & Correlation
- SOC Operations (Tier 1/2)
- Network Traffic Analysis
- Wireshark / Tcpdump
- Vulnerability Assessment
- Malware Analysis (básico)
- OSINT & Threat Hunting
- MITRE ATT&CK Framework
- Firewall SonicWall
- Windows Server / AD
- GNU/Linux (Kali, Ubuntu)
- VMware · Virtualización
- Gestión de NAS
- HackTheBox · LetsDefend
- TryHackMe
- Análisis de logs Windows
- Active Directory Security
- Email Analysis / Phishing
- IOC Investigation
- Python (scripting básico)
- Gestión de incidencias

Otros

- Carnet de conducir tipo B
- Vehículo propio
- Plena disponibilidad para viajar

Resumen profesional

Técnico de Ciberseguridad con sólida orientación Blue Team y más de 2 años de experiencia en entornos empresariales reales. Especializado en operaciones SOC, detección y análisis de amenazas, respuesta a incidentes y gestión de infraestructura de seguridad. Certificado BTL1 (Blue Team Level 1), CCST Cybersecurity, SOC Level 1 (TryHackMe) y SOC Analyst (LetsDefend). Activo en plataformas de práctica continua como LetsDefend, HackTheBox y TryHackMe, con foco en threat hunting, análisis de logs SIEM, análisis de tráfico de red y respuesta a incidentes. Comprometido con la mejora continua y orientado a crecer en roles de Analista SOC, Incident Responder o Threat Intelligence Analyst. Comprometido con las buenas prácticas de seguridad, documentación de incidentes y trabajo en equipo dentro de entornos SOC.

Experiencia laboral

Técnico Informático, Cainser S.A.
Enero 2024 – Actualidad · Polígono de Arinaga, Agüimes

- Administración e implantación de sistemas operativos Windows Server (2016/2019) y GNU/Linux en entorno de producción empresarial.
- Configuración, gestión y monitorización de firewall SonicWall: reglas de acceso, túneles VPN site-to-site, filtrado de contenido y alertas de seguridad.
- Administración de cortafuegos SonicWall: gestión de políticas de seguridad, control de aplicaciones, IPS/IDS y reporting de eventos de red.
- Supervisión y análisis de logs de red y sistema para detección temprana de anomalías y comportamientos sospechosos.
- Gestión de infraestructura LAN/WAN: switching, routing, VLANs y resolución de incidencias de conectividad.
- Administración de NAS corporativo: control de accesos, políticas de backup y retención de datos.
- Soporte técnico presencial y en remoto (teleasistencia), gestión de incidencias y coordinación con proveedores.
- Elaboración de documentación técnica: procedimientos de operación, inventario de sistemas y registros de incidencias.
- Aplicación de políticas de seguridad, actualizaciones y parcheo de sistemas para minimizar la superficie de ataque.

Técnico de Sistemas, Desic S.L.
Prácticas curriculares · Las Torres, Las Palmas de Gran Canaria

- Administración de sistemas operativos Windows y Linux, servicios de red y gestión de usuarios en Active Directory.
- Instalación, configuración y puesta en marcha de equipos de escritorio, portátiles y periféricos corporativos.
- Gestión de firewall y segmentación de red mediante VLANs para mejorar el aislamiento y la seguridad perimetral.
- Colaboración en tareas de supervisión de sistemas, detección de fallos y aplicación de parches de seguridad.
- Soporte a usuarios finales, resolución de incidencias hardware/software y gestión del inventario de equipos.

Licencias y certificaciones

Certificación	Emisor
★ **BTL1 — Blue Team Level 1**	Security Blue Team
SOC Level 1	TryHackMe
SIEM Engineer Career Path	LetsDefend
SOC Analyst Learning Path	LetsDefend
IT Specialist – Cybersecurity	Pearson
CCST Cybersecurity	Cisco Networking Acad.
Jr. Cybersecurity Analyst	Cisco Networking Acad.
Ciencia de Datos con Python	Escuela de Organización Industrial (EOI)

Estudios

BTL1 — Blue Team Level 1
Security Blue Team
2026

Especialización en Ciberseguridad en Entornos TI
CIFP Villa de Agüimes
2023 – 2024

CFGS — Administración de Sistemas Informáticos en Red (ASIR)
CIFP Villa de Agüimes
2021 – 2023

Curso de Ciencia de Datos con Python — Certificado oficial
Escuela de Organización Industrial (EOI)
Feb. 2025 – Jun. 2025

Curso de Sistemas Microinformáticos y Redes
Liceo 2000, Las Palmas de Gran Canaria
2020 – 2021

Bachillerato Científico/Tecnológico
IES Santa Lucía, Santa Lucía de Tirajana
2018 – 2020