Aridañy Suárez

ANALISTA SOC · BLUE TEAM

CONTACTO

- aridanysuarezoj@gmail.com
- Las Palmas, España
- github.com/Arit0x
- linkedin.com/in/aridanysuarez
- arsosec.com

HABILIDADES

BLUE TEAM · SOC

SIEM · EDR / XDR · Threat Hunting · Incident Response · MITRE ATT&CK · Log Analysis

CTI · ANÁLISIS

Threat Intel · OSINT · IoC Investigation · Malware Analysis · TTP Mapping

SISTEMAS · REDES

Linux · Windows Server · Firewalls · Active Directory · Virtualización · TCP/IP

DESARROLLO

Python · TypeScript · Bash · SQL

IDIOMAS

Español	Nativo
Inglés	Intermedio

PERFIL PROFESIONAL

Analista SOC (Blue Team) con base en administración de sistemas. Especializado en monitorización, triage y respuesta a incidentes utilizando SIEM y EDR. Apasionado por la ciberseguridad defensiva, la inteligencia sobre amenazas y el análisis de malware. Enfocado en la detección de TTPs, correlación de eventos y mejora continua de la postura de seguridad. Comparto conocimiento y aprendizajes a través de **arsosec.com**.

EXPERIENCIA LABORAL

Analista de Ciberseguridad — SOC
Nov 2025 — Actualidad

Ackcent Cybersecurity

- Monitorización y análisis de alertas de seguridad con SIEM/EDR.
- Triage de incidentes, correlación de eventos y escalado según criticidad.
- Documentación de casos e identificación de IoCs y TTPs relevantes.

Administrador de Sistemas
Dic 2022 — Nov 2025

Cainser

- Administración de red y gestión de seguridad perimetral (firewalls SonicWall).
- Virtualización y administración de máquinas virtuales (VMware).
- Gestión de copias de seguridad con Acronis y NAS.
- Soporte técnico presencial y remoto, mantenimiento de infraestructura TI.

Técnico de Fibra Óptica
Nov 2021 — Dic 2022

Trirredes Solutions

- Instalación y mantenimiento de red de fibra óptica (Orange, Grupo MásMóvil).

Técnico de Operaciones de Red
Feb 2016 — Nov 2021

Sincatel Telecomunicaciones

- Instalación y mantenimiento de red FTTH en red propia de Movistar.
- Cableado estructurado, voz y datos en entornos residenciales y empresariales.

PROYECTOS

RansomVisor
github.com/Arit0x/RansomVisor · ransomvisor.streamlit.app

Python · Streamlit · Prophet · Threat Intelligence

Plataforma de análisis y predicción de ransomware en tiempo real. Dashboard interactivo con mapas de calor geográficos, análisis sectorial y modelado predictivo con Prophet, validación cruzada y regresores de CVE.

FORMACIÓN

CFGS — Administración de Sistemas Informáticos en Red (ASIR)
Jun 2022 — Jun 2025

IES El Rincón · Las Palmas, España

Curso de Ciencia de Datos con Python
Feb 2025 — Jun 2025

Escuela de Organización Industrial (EOI)

CERTIFICACIONES

Blue Team Level 1 (BTL1)
Security Blue Team · Oct 2025

SonicWall SNSA SonicOS 7.1
SonicWall · Jun 2025 (exp. Jun 2027)

IT Specialist — Cybersecurity
Certiport · Jan 2025

Google Cybersecurity Certificate
Google Career Certificates · Sep 2024

SOC Level 1 Certificate
TryHackMe · Jul 2025

SOC Analyst & SIEM Engineer Learning Path
LetsDefend · Feb 2025

CCST Cybersecurity & Junior Analyst
Cisco Networking Academy · Dic 2024

Google AI Essentials
Google Career Certificates · Sep 2024