Omar Kamand

Cybersecurity Engineer

okomarok10@gmail.com

+39 350 857 6155

Erba (CO), Italy

EU Italian citizenship

linkedin.com/in/omar-kamand-988a4721b

diseico.com

EDUCATION

Degree in Informatics Engineering
Universidad de las Islas Baleares (UIB)
09/2018 – 06/2022 | Mallorca, Spain

SKILLS

Cybersecurity Skills
Threat hunting - Alerts & Log Management - Code Analysis - Incident Response - Cybersecurity Documentation - Encryption Algorithms - Playbooks

Cybersecurity tools
Splunk - Sekoia - FortiGate - Sonicwall - FortiSOAR - Crowdstraike - FortiEDR - FortiAnalyzer - FortiMail - Avanan - Wireshark - Cisco Packet Tracer

Programming Languages:
Python - Javascript - C - C# - C++ - Golang - Java - Ada - Prolog

Database Management Systems
Postgresql - MySQL - MongoDB

Operating Systems, Virtualisation & Infrastructure
Windows - Linux Based OS - Docker - Oracle Virtual Box - Vagrant - Ansible

PROFILE

Detail-oriented Cybersecurity Engineer specializing in Threat Hunting, Security Software Development, API integration and security operations automation. Worked in a SOC from its beginning and built it alongside the team to make the service become reliable, efficient and effective.

PROFESSIONAL EXPERIENCE

Cybersecurity Engineer
OmniAccess
07/2022 – Present
Mallorca, Spain (Remotely from Erba, Italy)

Threat hunting and analysis. Incident response covering a wide variety of customers with different systems and environments. EDR management. SOAR and SIEM management and development. Automation and software development for Cybersecurity Tools. Cybersecurity documentation and reporting for customers.

Fullstack Developer
GoDevel
09/2021 – 02/2022 | Mallorca, Spain

Develop solutions and softwares for customers to optimise backend and improve frontend.

PROJECTS

SOAR Development
09/2022 – 01/2025
The quantity of Cybersecurity tools in the SOC made it difficult to keep up with the security incidents and reduced the quality of the serves. To solve that, I led a team of 2 engineers and designed and developed a fully functional SOAR that smoothly integrates different SIEMs, EDRs and Email protection systems into one platform with customized UI/Dashboards and playbooks. This project was the backbone to the department during its beginnings and greatly helped improve the quality of the service.

LANGUAGES

- **English** - Native
- **Italian** - Native
- **Spanish** - Native
- **Arabic** - Native
- **Catalan** - Conversational
- **French** - Beginner

Automated Reporting System

07/2022 – Present

Developed an internal reporting system that creates monthly and weekly statistical reports. These reports are based on 10+ security tools, such as SIEMs, SOARs, EDRs, Firewalls and Email Protection Systems all from different providers. The software made a massive impact on customers by serving as a bridge from the Cybersecurity department to the customer, by showing the result of the team's work through data, charts and personalized recommendations.

Automated Firewall Blocklist/Allowlist Management System — FortiSOAR to FortiGate Integration

09/2024 – 05/2025

Developed an integration between FortiSOAR and FortiGate that automates firewall policy enforcement based on analyst threat verdicts. In this project, then a SOC analyst classifies an indicator (IP address, URL/domain, or file hash) as malicious or legitimate during an investigation or while managing incidents, the tool automatically routes it to the appropriate blocklist or allowlist and pushes the update to the customer FortiGate firewalls. This project was built for a multi-tenant environment, allowing consistent, auditable enforcement across multiple customer firewall deployments.

Containerized Web Application Firewall with Automated Attack Simulation

04/2026 – 08/2026

Developed a containerized Web Application Firewall using ModSecurity and the OWASP Core Rule Set, deployed via Docker Compose in front of a deliberately vulnerable app (OWASP Juice Shop). For testing, I developed a Python harness to simulate real attacks (SQLi, XSS, path traversal, command injection) and measure block rates with and without the WAF in place, visualized results in a lightweight JS dashboard.

CERTIFICATES

- CompTIA Security+