

Qays Sarayra

info@qayssarayra.com • (+962) 792-785-506 • <https://qayssarayra.com> • LinkedIn

PROFILE SUMMARY

Security Engineer focused on SOC operations, cloud hardening, and SIEM/EDR deployments using ELK, Splunk and Wazuh. Experienced in building automated security workflows, WAF configuration, and developing security tools and platforms across cloud and on-premise environments.

EDUCATION

Bachelor's Degree in Cyber Security
Amman Arab University

Oct 2021 – Jun 2025

PROFESSIONAL CERTIFICATE

- ❖ CompTIA Security Analytics Professional (CSAP)
- ❖ CompTIA Cybersecurity Analyst (CySA+)
- ❖ CompTIA Certified: Security+ SY0-701
- ❖ HackTheBox Certified Defensive Security Analyst (CDSA)
- ❖ INE | Certified Incident Responder: eCIR
- ❖ INE | Certified Threat Hunting Professional: eCTHP
- ❖ Splunk Core Certified Power User (SPLK-1002)
- ❖ Splunk Enterprise Certified Admin (SPLK-1003)
- ❖ Microsoft Certified: Security Operations Analyst Associate (SC-200) (soon)

PROFESSIONAL EXPERIENCE

SMT Group – *Cyber Security Analyst (Full-Time)*

Jan 2026 - Present

- Monitored security alerts using SIEM
- Investigated to incidents
- Coordinated with response teams
- Documented findings and stayed updated

TECHNICAL SKILLS

- Security Tools: ELK, Wazuh, Splunk, Azure Sentinel, Snyk, AlienVault OTX, Wireshark/Tshark, Snort, Suricata, Autopsy, FTK Imager, Volatility, Nmap, Nessus, Burp Suite, Metasploit.
- Programing language and Framework: Python, PowerShell, C++, Laravel, FastAPI, Node JS, GO, MySQL, PostgreSQL.
- Specialties: Security Engineering, Hardening Cloud Security, Building SOAR, WAF, SIEM, EDR, Threat Hunting, Incident Response, Malware Analysis, Security Tool Development, Cybersecurity, Full-Stack Development.
- Platforms: Linux, Windows, Cloud environments (Hostinger VPS, Azure)

PROJECTS

- ❖ Cyber Security Services – securevista.net
One platform for cybersecurity competitions and organization training.
- ❖ Cyber Security Competition and Training Platform – ctfs.fun
Cybersecurity services: security solutions, products and competitions built around community needs.
- ❖ ELK SIEM Setup
This guide provides comprehensive instructions for building a Security Information and Event Management (SIEM) system using the ELK Stack (Elasticsearch, Logstash, Kibana) with network traffic analysis and Windows endpoint monitoring.
- ❖ VPS Security Blueprint
Blueprint provides automated VPS security by protecting SSH, adding DDoS and firewall defenses, running IDS/IPS and WAF, syncing threat data, and sending real-time alerts.
- ❖ SecureHome – Wazuh SIEM
This lab provides a comprehensive SIEM solution with EDR capabilities for learning security operations, threat hunting, and incident response in a controlled environment.
- ❖ SecureVPS – Splunk & IDS/IPS
VPS servers managed by a load balancer, structured for security even with public IPs. Hardened with Splunk, Snort IDS/IPS, EDR, firewall, secure coding, and real-world attack-defense testing.
- ❖ Perflect – SecOps tool for server Management
a security operations tool designed to simplify and automate server management tasks
- ❖ DockerRunKit API – Docker Runner on VMs by API
an api service to run docker containers on virtual machines programmatically
- ❖ XenoTrojan – Trojan
a trojan malware project used for research or testing security defenses
- ❖ VirusGuard - Malware Analysis
a tool or system designed for analyzing and detecting Linux malware threats inside sandbox
- ❖ SiteLaunch-v2 - network administrators
a tool to help network administrators deploy and manage websites efficiently
- ❖ OpenVPN Generator
a utility to create and configure openvpn profiles easily

HONORS & AWARDS

- 🏆 Cyber Security Competition System Administrator IEEE CyberSecurity 2025
- 🏆 Coordinating and Managing Aliens-CTFv1 Event
- 🏆 Coordinating and Managing AAU-CTFv1, AAU-CTFv2, AAU-CTFv3 Event
- 🏆 Cyber Security Competition System Administrator LesCTF (hybrid)
- 🏆 Cyber Security Competition System Administrator TuxCTFv2 (onsite)
- 🏆 Certificate of Achievement ICPC 2022
- 🏆 Certificate of Achievement NCSC Advance Training
- 🏆 Participant Queen Rania Entrepreneurship Competition at Business Park ZINC 2023