Alphonse Joseph

+46 764319646 | alphonse.joseph@proton.me | LinkedIn | GitHub | Portfolio | Trollhättan, Sweden

PROFILE

Junior Security Operations Engineer and Cybersecurity Master's student with a passion for threat intelligence, penetration testing, OSINT, and security architecture. Experienced in building hands-on home lab environments, IoT security analysis, cloud network security, and CTF competitions . Combines a strong computer science foundation with practical offensive and defensive security skills, with a growing focus on IoT and automotive cybersecurity.

TECHNICAL SKILLS

Offensive Security: Penetration Testing, Web Exploitation (SQLi, XSS), OSINT & Recon, CTF Methodology
Defensive Security: SIEM (Wazuh, Splunk), Incident Response, Security Architecture, IDS/IPS, Pi-hole
Home Lab & Infra: Raspberry Pi 5 (Pi-hole, WireGuard, nftables, Fail2ban, Cowrie SSH Honeypot, CrowdSec)
Cloud & Network: Azure (NSG, VNet, Network Security), VPN (WireGuard, OpenVPN), Docker, Portainer
Monitoring & Logging: Grafana, Prometheus, Loki, Promtail, Discord Webhook Alerting, Heimdall Dashboard
Scripting & Tools: Python, Bash, Git, Jupyter Notebook, Flipper Zero (Momentum firmware)
IoT & Automotive: IoT Vulnerability Analysis, ISO/SAE 21434, TARA, Threat Modeling

SECURITY PROJECTS

Master's Thesis: Comparative Evaluation of Open-Source SOAR Tools Feb 26 – Ongoing
Shuffle vs. Wazuh/Cortex/TheHive,with Fortigate 50G Integration SOAR,Python,tpotce

- Built hybrid security architecture combining FortiGate NGFW and T-Pot honeypot to generate real attack data.
- Developed standardized playbooks for automated response and measured key performance metrics.
- Created Python scripts for metrics analysis – first empirical benchmark of open-source SOAR tools.

Raspberry Pi 5 Cybersecurity Home Lab 2026 – Ongoing
Raspberry Pi 5, Pi-hole, WireGuard, nftables, Docker, Grafana, Prometheus, CrowdSec

- Built a full-stack home lab with Pi-hole DNS ad-blocking/filtering, WireGuard VPN server (PiVPN), and nftablesfirewall rules for network hardening.
- Deployed Cowrie SSH honeypot alongside CrowdSec for real-time threat detection and automated IP banning withcommunity threat intelligence.
- Implemented full observability stack: Prometheus + Grafana dashboards, Loki + Promtail log aggregation, andDiscord webhook alerting across all services.
- Containerised services using Docker (Portainer management) with Heimdall dashboard for unified access; configuredremote access from Sweden to India home network via DDNS and Tailscale fallback.

IoT Security Analysis – Smart Devices 2024
IoT, Threat Modeling, Security Analysis, Vulnerability Assessment

- Analysed 15+ smart siren and light devices, identifying 12 critical vulnerabilities including exposed misconfigurationsand attack surfaces.
- Produced a structured security report with threat models and remediation recommendations.

Network Worm Containment with Azure NSGs 2026
Azure, NSG, Network Segmentation, Cloud Security

- Demonstrated worm containment through Azure Network Security Group segmentation across 3 attack scenarios,achieving 95% containment rate.
- Documented architecture and published findings on GitHub.

ISO/SAE 21434 Automotive Cybersecurity Review 2025

Automotive Security, Compliance, TARA, Research

- Reviewed 20+ academic and industry papers on automotive cybersecurity standard implementation.
- Identified 5 key gaps between standard requirements and real-world TARA process adoption.

Cybersecurity Labs – Network Security & Monitoring 2025

OpenVAS, Nessus, Splunk, FortiGate, Honeypots, Web Security

- Conducted vulnerability assessments using OpenVAS and Nessus with professional remediation reporting.
- Deployed honeypots and Splunk SIEM for attack detection; configured FortiGate WAF and tested SQLi/XSSdefences.

EDUCATION

Master in Cybersecurity Aug 2025 – Jun 2026 (Expected)

Högskolan Väst, Trollhättan, Sweden

- Specialisation in security operations, threat intelligence, IoT security, and automotive cybersecurity.
- Thesis focused on comparative evaluation and empirical benchmarking of open-source SOAR tools.

WORK EXPERIENCE

Cyber security Intern Apr 2023 – Jun 2023

Cisco Networking Academy

- Gained hands-on experience with cybersecurity tools and concepts, including network security, threat detection, and incident response procedures.

CERTIFICATIONS

Cisco CyberOps Associate 2025

SOC operations, incident response, and security monitoring.

Google Cybersecurity Professional 2023

Security operations, incident response, and foundational security tools.

CTF & COMMUNITY

- **Medium Blog:** Security write-ups on cybersecurity frameworks, breaking into cybersecurity, and hands-on experiments.
- **Flipper Zero:** Hardware security research and BadUSB/RF tooling with Momentum firmware.

PERSONAL QUALITIES

Analytical · **Curious** · **Collaborative** · **Proactive** · Genuine passion for emerging security technologies, IoT, and automotive security. Loves flight simulators, tech tinkering, and making complex security topics accessible.

LANGUAGES

Swedish: Basic (spoken and written) · English: Fluent (spoken and written)