MOHAMED KHALIL GAMMAR

Germany (+49)15216228373 gammarkhalil@gmail.com
mohamed-khalil-gammar https://khalil-420.github.io

SUMMARY

Graduate Engineer with 2 years of experience in DevSecOps, penetration testing and secure SDLC. Managed Kubernetes clusters and built infrastructures from scratch. Conducted pentest assessments, integrated security testing into CI/CD pipelines, and collaborated with engineering teams to remediate vulnerabilities. Researcher and top-10 global CTF competitor.

PROFESSIONAL EXPERIENCE

Elumia - Remote, Tunisia
Automation Intern (Graduate Engineering Project) **Feb 2026 – Jun 2026**

- Engineered a GDPR-compliant data protection architecture for an AI email platform, building a 3-stage PII masking pipeline that securely anonymized live mailbox content prior to third-party LLM inference.
- Orchestrated secure infrastructure on a Kubernetes cluster, utilizing CI/CD pipelines to automate workflows, configuration updates, and deployments.
- Enforced shift-left security by integrating SAST, dependency checking, and secret-scanning gates into the CI/CD pipeline, backed by centralized monitoring.
- **Environment**: Python, K3s, GitHub Actions, Azure,Sonarqube, OWASP Dependency Check,Gitleaks, Prometheus, Loki, Grafana

Kian Technology - Ariana, Tunisia
DevSecOps Engineer (Full Time) **May 2025 – Jan 2026**

- Automated pre-release security testing by embedding SAST, DAST, SCA, and secret scanning into pipelines.
- Centralized vulnerability management by consolidating 5 different scanners into a single dashboard with MS Teams alerts, providing a prioritized security backlog.
- Architected an automated testing framework from scratch and integrated it into CI/CD pipelines, significantly improving regression coverage and release reliability.
- Managed and hardened Kubernetes environments, troubleshooting containerized applications to improve workload reliability and resolve infrastructure bottlenecks.
- Executed internal penetration tests on a multi-tenant platform, uncovering critical tenant isolation flaws (IDOR, JWT vulnerabilities); developed PoCs and integrated regression checks directly into the pipeline.
- **Environment:** Kubernetes, Helm, Semgrep, OWASP ZAP, Trivy, Gitleaks, Jenkins, DefectDojo, Playwright, Python, Burp Suite

Penetration Tester (Internship) **Jul 2024 – Aug 2024**

- Discovered and published **CVE-2025-9094** (client-side template injection) while assessing an IoT platform prior to production rollout.
- Identified critical infrastructure flaws, including cross-tenant data exposure, RBAC bypasses, exposed messaging tokens, and a race condition circumventing device provisioning limits.
- **Environment:** ThingsBoard, MQTT, Burp Suite, Python, Nuclei, Microsoft Word

DevSecOps (Internship) **Jun 2024 – Jul 2024**

- Deployed SIEM across 14 endpoints, establishing baseline security event visibility and monitoring where none previously existed.
- Implemented a vulnerability management platform, successfully establishing it as the engineering team's single source of truth.
- **Environment:** Wazuh, DefectDojo, Linux

Intellisec Solutions - Remote, Canada
Cyber Security Consultant (Full Time) **Feb 2025 – May 2025**

- Delivered full-scope, black-box penetration tests for 15+ clients, comprehensively assessing web applications and APIs for authentication, authorization, injection, and business logic flaws.
- Authored actionable, PTES-aligned remediation reports for non-technical stakeholders, mapping CVSS v3.1 ratings to direct business impact to drive prioritized security spending.
- **Environment:** Burp Suite, PTES Framework, Postman, Pwndoc, Microsoft Powerpoint, Nuclei, Kali Linux Tools

EDUCATION

Hochschule Schmalkalden — **Schmalkalden, Germany**
Two-Semester Academic Mobility Program — **April 2026-March 2027**

TEK-UP University (Night Courses) — **Ariana, Tunisia**
Master's Degree: Engineering in Information Systems & Networks — **Sep 2021-July 2026**

CERTIFICATIONS

- **eWPTX – Extreme Web Penetration Tester**
- **CKA – Certified Kubernetes Administrator**
- **PCAP – Certified Python Associate**
- **eWPT - Web Penetration Tester**
- **eJPT – Junior Penetration Tester**

TECHNICAL SKILLS

- **DevOps & Cloud:** Kubernetes, K3s, Docker, Helm, ArgoCD, GitOps, Jenkins, GitHub Actions, AWS, Azure, CI/CD
- **QA & Test Automation:** Playwright, Manual QA, Automated Testing, Regression Testing, API Testing, Test Automation
- **Security:** Application Security, Web & API Security, Penetration Testing, Secure Code Review, SAST, DAST, SCA, Container Security

KEY TECHNICAL PROJECTS

GitOps-Driven Cloud-Native CI/CD Infrastructure

- Containerized an existing Django/React restaurant management application and deployed it on AWS EC2 using a k3s Kubernetes cluster. Designed a GitHub Actions CI/CD pipeline to build Docker images, execute automated tests, integrate security checks (Trivy, Gitleaks), and publish versioned images to DockerHub.
- Implemented GitOps-based continuous deployment using ArgoCD and Helm charts, enabling automated synchronization between Git repositories and the Kubernetes cluster while managing application deployments and configuration updates.

SOC/SOAR & Scalable CTF Infrastructure

- Deployed a local SOC/SOAR environment using virtual machines, integrating Wazuh, Suricata, Shuffle, MISP, and TheHive. Configured automated incident response workflows where Wazuh and Suricata alerts triggered Shuffle playbooks for IoC enrichment through MISP, case creation in TheHive, email notifications, and automated response actions such as IP blocking. Managed Wazuh agents across multiple endpoints and monitored security events through dashboards.
- Managed CTF infrastructure hosted on OVH VPS using CTFd, Nginx, and Cloudflare, implementing challenge deployment automation with ctfcli and managing isolated challenge instances and replicas to support competitive security events.

ACHIEVEMENTS & ASSOCIATIVE WORK

- **Vulnerability Research:** Discovered and published CVE-2025-9094 (Client-Side Template Injection vulnerability in Thingsboard).
- **Industry Contribution:** Selected as the official challenge author for the Intigriti Monthly Challenge (June 2026).
- **Competitive Experience:** Active competitor with team L3ak with a Top 10 worldwide ranking on CTFtime; 1st place in the CyberSphere Congress Advanced CTF; Top 15 placement in the Blackhat MEA International CTF.
- **Securinets Association:** Core infrastructure lead responsible for deploying, scaling, and managing environments for international and local CTF competitions.

LANGUAGES

- English (Fluent), French (Fluent), Arabic (Native),German (Basic)