Moetez AFIF *DevSecOps Engineer*

✉ moetezafif@gmail.com   🔗 https://www.linkedin.com/in/moetez-afif   ⭘ Github   ●● Medium

---

🪪 PROFILE

Experienced DevSecOps Engineer specializing in designing and deploying secure, scalable Kubernetes environments with service mesh solutions like HashiCorp Consul. Successfully streamlined CI/CD pipelines and automated vulnerability assessment workflows, enhancing risk management and system compliance. Leverage deep expertise in infrastructure and cybersecurity to deliver secure, efficient, and innovative solutions in complex, high-demand environments.

💼 PROFESSIONAL EXPERIENCE

DevSecOps Engineer   2023 July – present | Tunis, Tunisia
Cytailor

CI/CD & DevSecOps Pipelines
- Designed and deployed secure CI/CD pipelines for 7+ microservices on Amazon EKS using GitHub Actions, ArgoCD, Helm, and Git, integrating **Semgrep** (SAST), **Trivy** (container scanning), and **OWASP ZAP** (DAST), achieving ~90% compliance with the DoD DevSecOps Playbook.
- Accelerated deployments by 40% and reduced pipeline failures by 25% through **GitOps practices**, continuous drift detection, and automated secrets management with **HashiCorp Vault**.
- Centralized credential handling using Vault and Vault Secrets Injection (Vault SCI), eliminating hardcoded secrets and enforcing secure, automated secrets distribution across microservices.

Cloud Migration & Infrastructure
- Led the migration of multiple microservices from AWS to OVH, contributing to the design of a scalable, reliable, and secure infrastructure architecture.
- Deployed and operated HashiCorp Consul across multi-cluster Kubernetes environments on AWS (EKS) and OVH, reducing microservice latency by 30% and enforcing mTLS, RBAC, and ACL-based security.
- Designed and enforced Consul ACL policies with least-privilege access control, improving cluster security and compliance posture.

Security Consulting & Workshops
- Participated in a security consulting engagement for a French client, improving security posture through policy enforcement and governance controls.
- Designed and implemented a lightweight automated mini-SOC using Make automation and Google GAT+, enabling continuous monitoring and security reporting.
- Built an automated reporting mechanism delivering weekly summaries of high-risk or non-compliant activities for administrative review, aligned with organizational data protection policies.
- Conducted a workshop for a French 5G client on microservices security, covering secure API gateway configuration, HashiCorp Consul implementation, and best practices for securing their Dockerized 5G environment.
- Led DevSecOps security consulting for a French 5G organization, securing Docker and Kubernetes architectures with HashiCorp Consul for PKI, automated certificate management, and mTLS.

Knowledge Base / AI Integration
- Developed a cybersecurity knowledge base using a Retrieval-Augmented Generation (RAG) architecture, generating vector embeddings with Amazon Bedrock and storing them in Amazon Aurora PostgreSQL with pgvector to enable LLM-powered semantic search and querying.

Internship   2023 September – present
6NLG(2SB) - SUP'COM   Tunis, Tunisia
- Secured cloud services using **Reverse Proxy** and **Cloud Access Security Broker (CASB)** solutions.
- Implemented robust **cloud security, data protection, and access control** leveraging **Netskope CASB, SWG, and ZTNA** technologies.
- Developed, enforced, and monitored **security policies** to ensure compliance, reduce risk, and protect sensitive data.

Technical Team   2023 March – 2023 June | Tunis, Tunisia
Hackfest
Preparing challenges for the CTF competition (Web Exploitation , Cryptograhy)

🎓 EDUCATION

ICT engineering
Higher School Of Communication Of Tunis

2021 September – present
Ariana, Tunisia

Information and communication technology engineering program, with a focus on network infrastructure, cybersecurity, cloud computing, software engineering, database management, data science and artificial intelligence.

Preparatory Cycle
Monastir Preparatory Engineering Institute

2019 September – 2021 June
Monastir, Tunisia

studied the basics of mathematics and physics. rank: 19/900

🧠 SKILLS

DevOps & nfrasctructure
Jenkins, Kubernetes (**AWS EKS, OVH**), GitHub Actions, ArgoCD, HashiCorp Vault & Vault SCI, Docker, Terraform, Helm, Ansible, CI/CD Pipeline Design, GitOps, Microservices Architecture, PKI & mTLS, Infrastructure Design & Migration

Monitoring & Automation
OpenSearch, Logstash, Beats (Filebeat), Grafana, Prometheus, Wazuh, Netskope Solutions, AWS CloudWatch, Make Automation, n8n, Real-Time Alerting, Custom Correlation Rules, Security Reporting

Programming and Script Languages
Python, JavaScript, TypeScript, C++, Bash, PowerShell

Cybersecurity
Wireshark & Network Protocols, CASB, Firewalls (FW), EDR/XDR, VPN, SAST (Semgrep), DAST (OWASP ZAP), Trivy, SonarQube, Secure Coding, Web Application Penetration Testing, Linux & Windows Security, Infrastructure Security, RBAC, ABAC, Role Binding, Security Policy Enforcement, Vulnerability Management (CVSS, NIST & CISA feeds)

Design and Modeling Tools
UML, System Design, Distributed Systems, Databases (**SQL & NoSQL**), SDLC, Infrastructure as Code (IaC), Service Mesh, Risk Visualization & Dashboards

📑 CERTIFICATES

ISC2 Certified In Cybersecurity (CC) 🔗 — Knowledge about Network Security, Risk management, Threat Identification, Incident Response

Cybersecurity Bootcamp By CyberTalents & TrendMicro 🔗 — A 2-month program to start your career as a Cybersecurity Engineer.

🌐 LANGUAGES

Anglais — Fluent
TOEIC 880/990

Français — Native/Bilingual

Arabe — Native/Bilingual

📁 PROJECTS

ELK Stack Security Monitoring in Dockerized Environment
- Designed and deployed an **ELK Stack (Elasticsearch, Logstash, Kibana)** using **Docker** to monitor infrastructure logs and metrics.
- Centralized logs from containerized services to enable **real-time visibility and analysis**.
- Simulated **cybersecurity attacks** (e.g. brute force, suspicious access patterns) to validate detection capabilities.
- Implemented **custom detection rules and dashboards** in Kibana to identify security events.
- Evaluated alert accuracy and system effectiveness in detecting anomalous behavior.

Keywords: Docker, Elasticsearch, Logstash, Kibana, Linux, Security Monitoring

Intrusion Detection Using Machine Learning 🔗
- Analyzed **network traffic data** to detect malicious activities using **supervised machine learning models**.
- Designed, trained, and evaluated **Random Forest** and **Convolutional Neural Network (CNN)** models on a **labeled intrusion detection dataset**.
- Performed **data preprocessing, feature engineering, and model evaluation** to identify patterns and behaviors associated with known cyberattacks.
- Visualized model performance and traffic patterns to assess detection accuracy and false positives.

Keywords: Python, JupyterLab, Scikit-learn, Pandas, NumPy, Matplotlib, Machine Learning, Intrusion Detection