Youssef Chalghoumi

+216 21 629 389 | chalghoumi.youssef@gmail.com | linkedin.com/in/youssef-chalghoumi | cyberv3.vercel.app

Professional Summary

Cloud Security Engineer with experience in AWS security, DevSecOps, SOC operations, and infrastructure automation. Skilled in designing hardened cloud architectures, building secure CI/CD pipelines, automating incident response workflows, and implementing scalable security monitoring solutions. Currently focused on developing AI-driven security systems leveraging GraphRAG, VectorRAG, and Model Context Protocol (MCP) for contextual cloud threat analysis and autonomous remediation.

Skills & Certifications

- **Cloud & Infrastructure:** AWS (Shield Advanced, WAF, FMS, GuardDuty, ECS, Lambda, IAM, Route53), Terraform, Docker, Kubernetes.
- **DevSecOps & Automation:** GitLab CI/CD, Ansible, Python, Bash, tfsec, Trivy, SonarQube, detect-secrets, n8n.
- **AI Security & Agentic Systems:** GraphRAG, VectorRAG, Neo4j, ChromaDB, LangChain, MCP (Model Context Protocol), Ollama, Streamlit, AI Agents, LLM Tool Routing.
- **Security Operations:** Trend Micro XDR, TheHive, MITRE ATT&CK, Elasticsearch, Grafana, Splunk, Incident Response, Threat Detection.
- **Networking & Systems:** Fortinet (SD-WAN, NSE 1–3), Cisco ASA, Wireshark, Zabbix, Linux (RedHat, Ubuntu).
- **Certifications:** AWS Solutions Architect – Associate, AWS Cloud Practitioner, Google Cybersecurity Professional, Fortinet NSE 1–3, AWS Academy Machine Learning Foundations.

Key Achievements

- Architected automated AWS Shield Advanced and WAF deployments using Terraform and Firewall Manager, reducing manual deployment time by 90%.
- Developed an autonomous cloud security AI agent leveraging **GraphRAG**, **VectorRAG**, and **MCP-based** orchestration, reducing cloud investigation time and minimizing LLM hallucinations during infrastructure analysis workflows.
- Led remediation initiatives for a major energy services provider by optimizing Trend Micro XDR policies and eliminating critical security exposures.
- Reduced infrastructure misconfiguration risk by integrating automated DevSecOps security gates into GitLab CI/CD pipelines, eliminating repetitive manual validation workflows across cloud deployments.

Experience

Pwn & Patch Feb 2024 – Present
Cloud Security Engineer

- Architected a hardened multi-account AWS Shield Advanced strategy through Terraform and Firewall Manager (FMS), integrating Route53 health checks for automated DDoS mitigation workflows.
- Implemented hardened GitLab CI/CD pipelines integrating tfsec, Trivy, detect-secrets, and SonarQube, reducing manual security review overhead and preventing insecure Terraform deployments before production release.
- Engaged with a major energy services provider to redesign endpoint security posture through deployment and tuning of Trend Micro XDR detection and response policies.
- Automated cloud incident response workflows through CloudWatch and AWS Lambda integrations, significantly reducing alert triage and Mean-Time-To-Respond (MTTR) during infrastructure security events.
- Conducted AWS Well-Architected Reviews and CIS Benchmark audits, delivering actionable remediation roadmaps for cloud environments.

OneTech Business Solutions Feb 2023 – Jun 2023
Network Security Intern

- Deployed Fortinet SD-WAN infrastructures with IPS, HA, and ADVPN configurations to ensure resilient inter-site connectivity.
- Configured FortiManager and FortiAnalyzer platforms for centralized security policy management and monitoring.

- Hardened Cisco ASA firewall policies aligned with enterprise security and compliance requirements.

KEYSTONE Group Dec 2022 – Jan 2023
Cyber Security Intern

- Built a CTF-based cybersecurity training platform focused on penetration testing and vulnerability exploitation scenarios.
- Supported internal red team simulations to evaluate employee awareness and SOC response effectiveness.

TOPNET Jan 2022 – Mar 2022
Network Administrator Intern

- Deployed monitoring infrastructures using Zabbix and Azure Monitor to track bandwidth, uptime, and network health metrics.
- Created automated operational dashboards improving infrastructure visibility and incident tracking capabilities.

Highlighted Projects

Snock – Autonomous Cloud Security AI Agent 2026 – Present

- Architected a hybrid **GraphRAG + VectorRAG** security platform using **Neo4j** and **ChromaDB** to analyze AWS attack paths and retrieve CIS / MITRE ATT&CK remediation guidance.
- Engineered an **agentic AI pipeline** leveraging **Model Context Protocol (MCP)** for deterministic tool routing, significantly reducing LLM hallucinations during cloud infrastructure investigations by isolating graph analysis from semantic retrieval workflows.
- Developed a YAML-driven cloud detection engine capable of identifying **multi-hop attack paths** including IAM privilege escalation, SSRF pivot chains, exposed workloads, and lateral movement scenarios.
- Integrated live AWS telemetry ingestion through **Boto3**, enabling real-time infrastructure graph mapping and accelerated attack-path investigations across interconnected cloud assets.
- Automated Terraform remediation generation by correlating graph-discovered vulnerabilities with context-aware remediation guidance retrieved through VectorRAG pipelines, decreasing manual remediation effort for cloud security findings.

SpecterHeal – AI Self-Healing Infrastructure Platform

- Developed an autonomous remediation engine leveraging **Lynis** for security auditing and **Ollama** for AI-driven remediation analysis.
- Integrated **Ansible** automation to dynamically generate and execute remediation playbooks based on AI-generated findings.
- Built a **Streamlit** interface enabling centralized infrastructure visibility and autonomous remediation orchestration.

SOC Automation & Visualization Platform

- Engineered a dockerized SOC stack integrating **TheHive**, **Elasticsearch**, and **Grafana** for centralized security operations and attack visualization.
- Implemented automated alert routing and response orchestration using **n8n** workflows.

Education

TEK-UP University Tunis, Tunisia
Engineer's Degree in Cybersecurity

ISET Charguia Tunis, Tunisia
Bachelor's Degree in Networking and Cybersecurity Engineering