

MOHAMED KHALAF HAMMAD

Cybersecurity & Security Infrastructure Engineer

Doha, Qatar | +974 30019938 | m.khalafhammad@gmail.com | linkedin.com/in/m-khalafhammad | mkhalafhammad.com

Born in Qatar | B.Sc. Computer Science (Cybersecurity), Qatar University

PROFESSIONAL SUMMARY

Cybersecurity engineer working across SIEM and other security tools, endpoint security, and network design, with solid networking fundamentals and a software development background applied to security work. Also comfortable with Linux and Windows infrastructure.

CORE SKILLS

SIEM & Security Operations: Splunk Enterprise (SPL, Universal Forwarder, indexer and search head clustering, Cluster Manager, Deployer, License Manager, Monitoring Console), CIM normalization and parser development, CIM compliance auditing, syslog ingestion, Wazuh.

Endpoint & Identity Security: TrendMicro Vision One (agent onboarding, policy exclusion management), Microsoft Entra ID, Microsoft Defender.

Networking & Network Design: Network fundamentals, routing and switching, VLANs and subnetting, secure network design, firewall policy on pfSense, Suricata IDS/IPS deployment.

Systems & Platforms: Linux, Windows Server, Proxmox VE.

Development & Automation: Python, Bash, SQL, JavaScript and TypeScript, Django, FastAPI, Next.js, Docker, Git and GitHub.

PROFESSIONAL EXPERIENCE

Security Infrastructure Engineer Intern

02/2026 - Present

Meeza (Managed IT Services Provider) | Doha, Qatar

- Administer a production Splunk Enterprise distributed deployment: indexer clustering, search head clustering, and the full management tier (Cluster Manager, Deployer, License Manager, Monitoring Console).
- Onboard and troubleshoot log sources across syslog and universal forwarder, including Universal Forwarder deployments on Linux and Windows.
- Audit CIM compliance, measuring field-level coverage per sourcetype and separating real mapping gaps from fields a source does not carry.
- Build SPL searches and reporting for host inventory and asset classification, including a license utilization calculator used for capacity planning.
- Manage endpoint protection policy in TrendMicro Vision One, including a exclusion audit across Windows and Linux servers that produced a three-tier policy model (universal baseline, and role-specific children) with a vendor cited justification behind every exclusion.
- Designed an enterprise network security architecture: dual NGFW high-availability perimeter with WAF and inline IPS/IDS, VLAN segmentation with NAC and 802.1X, an isolated management plane with PAM and PKI, security tool placement across zones (NDR, EDR/XDR, deception, DNS security), and a mirrored DR site.

IT Administrator

02/2025 - 04/2025

The Commercial Avenue | Doha, Qatar

- Administered identity and endpoint security across the enterprise fleet using Microsoft Entra ID, Intune, and Defender.
- Resolved endpoint, account, and access issues for employees across enterprise systems.
- Developed features and improvements for the company loyalty application.

Full Stack Developer

07/2024 - 12/2024

Sidra Holding (Bawaba LLC) | Doha, Qatar

- Deployed and maintained Odoo ERP in Docker on Linux servers, handling server administration and availability.
- Built and maintained production web applications using Next.js.
- Hardened systems and provided operational support for hosted services.

Penetration Testing Intern

06/2024

Sidra Holding (Sidra Chain) | Doha, Qatar

- Conducted web application vulnerability assessments using Burp Suite and custom Python scripts.
- Identified and documented application security issues, including a file upload bypass, and supported exploit validation and assessment reporting.

PROJECTS

SannadHealth: AI Clinical Scribe (Hackathon Winner)

09/2026

1st Place, McKinsey Qatar AI Hackathon (McKinsey & QuantumBlack AI) | Doha, Qatar

- Won first place with a seven-person cross-functional team over a two-day build, owning the agentic architecture and defending the design decisions to the judging panel.
- Built a real-time clinical documentation system that listens to a doctor and patient consultation and drafts the clinical note, ICD-10 diagnostic codes, and follow-up actions during the appointment rather than after it.
- Designed a five-agent runtime (transcript builder, scribe, coder, differential, question suggester) coordinating through a shared version-stamped session draft, with per-agent concurrency slots and stale-result guards instead of an orchestration framework. Built on FastAPI with WebSockets, Next.js, Azure OpenAI, and Whisper for chunked audio ingestion.
- Prevented hallucinated diagnostic codes by constraining the coding agent to a deterministically retrieved ICD-10 shortlist through schema-enforced enums, and kept evidence verification and the clinician review gate as deterministic code rather than model output.

STAM: Security Tool Asset Manager (Personal Project)

2026 - Present

- Design and build an on-prem, multi-tenant platform that gives a managed service provider one auditable record of every security tool running across its clients: what is deployed, on which assets, under which license, and where coverage is missing.
- Built around SecOps accountability: changes are tied to a ticket, and the audit trail is append-only, so tool ownership, version drift, and license renewals stay traceable during audits and incident reviews.

Enterprise SOC Home Lab (Personal Project)

2025 - Present

- Built a multi-VLAN SOC lab on Proxmox VE with pfSense, Splunk Enterprise, and Wazuh, segmented into 5 zones (attacker, DMZ, internal, management, Splunk).
- Integrated Pfsense, and Suricata IDS/IPS and centralized log collection, with Splunk.
- Currently integrating Splunk with n8n to build agents that investigate logs and raise alerts automatically.

DGM Platform: Self-Evolving AI System (Personal Project)

2025 - Present

- Architected and built a full-stack platform for LLM-driven optimization of code and prompts: Next.js and TypeScript frontend, FastAPI control plane, isolated Docker runtimes orchestrated through the Docker SDK, PostgreSQL, MinIO, and real-time WebSocket progress streaming.
- Implemented the sandbox security controls for running untrusted LLM-generated code: network-isolated containers, CPU and memory limits, read-only input artifacts, no shell execution, and output sanitization, the same controls needed to run AI-assisted automation safely in a SOC.

EDUCATION

B.Sc. Computer Science, Cybersecurity Concentration

08/2019 – 05/2024

Qatar University | Doha, Qatar | Dean's List (Spring 2022)

CERTIFICATIONS

- TrendAI Vision One: Platform Certified Practitioner; Endpoint Security Certified Practitioner
- Kaspersky Next EDR Certified Professional: Foundation, Optimum, Expert Administration
- Google Security Operations Engineer Certification (in progress, expected 2026)
- CCNAv7: Introduction to Networks, Cisco Networking Academy | Samsung Innovation Campus: Artificial Intelligence Course