

MOHAMED AAKIF

Abu Dhabi, UAE | aakifcool1@gmail.com | +971563262846 | [linkedin.com/in/mohamed-aakif](https://www.linkedin.com/in/mohamed-aakif) | github.com/mohamedaaakif

PROFESSIONAL SUMMARY

IT professional with over three years of experience supporting enterprise and healthcare environments. Strong background in Azure cloud operations, Windows and Linux server administration, infrastructure monitoring, incident response, and uptime management. Hands-on experience with automation using PowerShell, Python, and Bash to improve operational efficiency and reduce recurring issues. Proven contributor in regulated environments, supporting ISO 27001, ADHICS, CAP, and GCLP compliance alongside security and infrastructure teams.

PROFESSIONAL EXPERIENCE

IT Support Engineer – Infrastructure Operations M42

May 2022 - Present

- Led the launch of Mubadala Dubai healthcare facility, ensuring infrastructure readiness, system availability, access provisioning, and compliance alignment.
- Supported Azure-based environments, Active Directory, Windows file servers, and access controls across multiple M42 healthcare sites.
- Administered Windows and Linux servers, including user access, service troubleshooting, patch management and operational support.
- Implemented PowerShell and Python automation scripts to reduce recurring operational tickets and improve response time.
- Supported Linux-based systems across NRL, assisting departments with access, troubleshooting, and system stability.
- Managed enterprise tools including Microsoft Azure, Active Directory, Genian NAC, ManageEngine PAM 360, and file server permissions.
- Provided IT operations support across NRL, CCAD, Healthpoint, and Mubadala Dubai environments.

CERTIFICATIONS

Automate Cybersecurity Tasks with Python - Google | 2025
Microsoft Sentinel SIEM Certification - Microsoft | 2023
Certified Ethical Hacker (CEH) - EC-Council | 2025
Practical Ethical Hacking (PEH) - TCM Academy | 2024
Ethical Hacking Essentials (EHE) - EC-Council | 2023
Python Data Structures - LinkedIn Learning | 2023
Threat Modeling and Hunting - LinkedIn Learning | 2023
Cybersecurity Threat Landscape - LinkedIn Learning | 2023
Python Programming - SoloLearn | 2021
MITRE ATT&CK Defender Fundamentals - Cybrary | 2021

EDUCATION

Bachelor of Cyber Security (First Class Honours)
Solent University, United Kingdom | 2024

Advanced Diploma in Cyber Security
Winsys City Campus, Sri Lanka | 2022
Covered CEH, MCSA, CCNA, Linux Administration, Windows Networking, Python Programming

Higher National Diploma in Cyber Security
Qualifi, United Kingdom | 2021

PROJECTS

Cloud Infrastructure Deployment – AWS

Designed and deployed cloud infrastructure using AWS EC2, VPC, Security Groups, IAM, and S3 to simulate enterprise-grade environments. Provisioned and hardened Linux instances, configured network segmentation and access controls, and implemented monitoring to ensure availability and performance. Applied security best practices including least-privilege IAM policies, secure key management, and basic automation for repeatable deployments, aligning cloud operations with production-level workloads.

Log Monitoring & Incident Analysis – Splunk

Implemented a SOC lab using Splunk Enterprise to analyze security incidents. Configured log ingestion from Windows and developed SPL detections for brute-force attacks, lateral movement, privilege escalation, and data exfiltration. Created correlation searches and dashboards to track user anomalies and incident trends, enhancing skills in log analysis, threat hunting, and incident investigation.

Network Monitoring & Alerting – Security Onion

Built a malware detection lab using Security Onion. Replayed malicious PCAPs to detect malware patterns and beaconing. Developed custom Suricata and Zeek rules for threat identification, correlated alerts in Kibana, and enriched IOCs using VirusTotal API. Produced detailed incident reports simulating real SOC investigations.

SKILLS

Cloud & Infrastructure Operations

Azure & AWS (EC2, VPC, IAM, S3), Windows & Linux Server Administration, VMware, Proxmox, Firewall Management (FortiGate, pfSense, Azure Firewall), Network Access Control (NAC), Backup & Recovery (Veeam, Azure Backup), Infrastructure availability & uptime

Monitoring & Automation

Splunk, Microsoft Sentinel, Security Onion, Log monitoring, alerting, dashboards, PowerShell, Python, Bash (infrastructure automation), Identity & Access Management (Azure AD / IAM), ManageEngine PAM 360

Incident Response & Operational Support

Incident triage & escalation, Root Cause Analysis (RCA), Production issue resolution, Change & release support, Documentation & handover

Penetration Testing & Ethical Hacking

Web App Testing, Network Exploitation, XSS, SQLi, Burp Suite, Metasploit, Cobalt Strike, Core Impact