MOHAMED AAKIF

Cyber Security Analyst | SIEM, Cloud & Infrastructure Security

Abu Dhabi, UAE | aakifcool1@gmail.com | +971563262846

https://www.linkedin.com/in/mohamedaakif | https://github.com/MohamedAakif

PROFESSIONAL SUMMARY

Cybersecurity professional with 3+ years of experience in enterprise healthcare environments, specializing in SIEM monitoring, incident response, vulnerability management, and threat detection across cloud and on-prem systems. Experienced in Microsoft Sentinel, NAC, privileged access management, and ADHICS regulatory compliance within healthcare operations. Strong hands-on background in security automation, malware analysis, and SOC-focused investigation workflows, with a proactive approach to reducing operational risk and improving security posture.

PROFESSIONAL EXPERIENCE

Cyber Security Analyst/ IT Support (Infrastructure & Healthcare Operations)
M42
May 2022 - Present

- Conducted vulnerability assessments and patch management for **20** servers (CCAD), reducing exposure risk by 90% quarterly.
- Managed and administered Genian NAC and ManageEngine PAM 360 for 300+ systems and 500+ users, strengthening privileged access management and network access controls.
- Supported annual ADHICS compliance audits, backend documentation, risk registers, BIA, policies, and asset inventories, reducing audit findings by **25%** YoY.
- Monitored vulnerability scans, threat intelligence feeds, and government advisories to identify and remediate 10–20 new vulnerabilities monthly, improving risk visibility and regulatory compliance readiness.
- Implemented PowerShell and Python automation scripts, reducing recurring incidents by **25–35%** and decreasing recurring tickets by 10–20 per month.
- Executed network segmentation for 100 printers and 300 systems (Printer VLAN segregation & Cerner printer builds), enhancing security isolation and reducing lateral movement risk by 90% through firewall rules.
- Supported enterprise-wide Active Directory migration from on-premises to Azure cloud across NRL and Healthpoint for **800+** devices and **1,000+** users, improving identity management efficiency.
- Contributed to infrastructure transformation initiatives including Windows 11 migration, ManageEngine Endpoint Central deployment, and Zscaler implementation for 300+ devices, achieving **99%** deployment success rate.
- Administered and supported 350+ Windows and Linux servers, Active Directory, Azure environments, and enterprise file systems, maintaining **99%** SLA compliance and high system availability.
- Managed identity and access controls across Crelio, Q-Pulse, Genian NAC, and Cisco Call Manager for 500+ users, strengthening access governance and reducing unauthorized access risks.
- Led end-to-end IT and infrastructure readiness for the Mubadala Dubai healthcare facility launch, supporting 200+ users and multiple clinical systems, achieving **99%** go-live availability, delivering 1 week ahead of deadline, with 0% downtime and less than 5 user complaints.
- Provided cross-site IT and security operational support across **9** core entities, primarily NRL, CCAD, Healthpoint, and Mubadala Dubai, maintaining production stability in a multi-entity healthcare environment.

SECURITY PROJECTS

Security Automation & SOAR – Wazuh, n8n, Gemini AI

- Designed and deployed an end-to-end SIEM + SOAR platform, automating **80%+** of alert triage tasks and reducing manual investigation time by 40% in a simulated SOC environment.
- Developed and tuned **10+** WQL detection rules with advanced log correlation, creating **2** custom dashboards to simulate enterprise SOC alert workflows and improve threat visibility.
- Developed **20+** custom detection rules mapped to MITRE ATT&CK, reducing false positives by 35% and improving high-severity alert visibility.
- Built automated IOC enrichment workflows integrating VirusTotal and threat feeds, decreasing analyst investigation time by 30%.
- Implemented severity-based response playbooks (IP blocking, user containment), reducing mean response time (MTTR) by **45%.**

Malware Analysis – FLARE VM & CAPEv2

- Analyzed **5+** real-world malware samples (AgentTesla, Zeus, WannaCry, Locky), extracting 100+ high-confidence IOCs for detection engineering use.
- Identified process injection, persistence, and C2 patterns mapped to MITRE ATT&CK techniques, improving threat detection coverage.
- Correlated host and network telemetry to simulate enterprise SOC investigations, enhancing behavioral detection accuracy.
- Produced structured threat reports enabling SIEM/EDR rule creation and proactive threat hunting simulations.

Cloud Infrastructure Deployment – AWS

- Designed and secured an AWS lab environment with EC2, IAM, VPC, and S3, implementing least-privilege access across **25+** IAM roles and policies.
- Applied network segmentation and hardening controls, reducing misconfiguration exposure risk by 50% (based on CIS benchmark checks).
- Configured centralized logging and monitoring to improve visibility across **99%** of deployed resources.
- Implemented infrastructure automation practices to improve deployment repeatability and reduce configuration errors.

Network Monitoring & Alerting – Security Onion

- Built a Security Onion lab integrating Suricata, Zeek, and Elastic Stack, generating and analyzing **500+** security events from malicious PCAPs.
- Detected and analyzed simulated C2 traffic and malware beaconing, improving network-based detection visibility.
- Tuned detection rules to reduce false positives by **30%,** improving alert prioritization accuracy.
- Produced structured SOC-style incident reports simulating enterprise incident response workflows.

CERTIFICATIONS

Automate Cybersecurity Tasks with Python - Google | 2025
Certified Ethical Hacker (CEH) - EC-Council | 2025
Practical Ethical Hacking (PEH) - TCM Academy | 2024
Microsoft Sentinel SIEM Certification - Microsoft | 2023
Ethical Hacking Essentials (EHE) - EC-Council | 2023
Threat Modeling and Hunting - LinkedIn Learning | 2023
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

SKILLS

Security Operations & Threat Management
Incident Response, SIEM Monitoring, Threat Hunting, Vulnerability Management, Malware Analysis, MITRE ATT&CK, Threat Intelligence, Detection Rule Development, ADHICS Compliance

Security Tools
Microsoft Sentinel, Splunk, Wazuh, Security Onion, Nessus, Qualys, Genian NAC, ManageEngine PAM360, Microsoft Sentinel (KQL), Log Correlation, Detection Rule Development, Alert Tuning

Cloud & Identity Security
AWS (EC2, VPC, IAM), Microsoft Azure, Active Directory & Azure AD, Identity & Access Management, Privileged Access Controls

Automation & Scripting
Python, PowerShell, Bash, Security Automation