MOHAMED AAKIF

Abu Dhabi, United Arab Emirates

+971 56 326 2846

Aakifcool1@gmail.com

Dear Hiring Manager,

I am writing to express my interest in any IT or Cyber Security position. With over three years of hands-on experience as a Cyber Security Analyst / IT Support Engineer, I bring strong technical expertise in threat detection, incident response, and malware analysis. My experience with tools such as Microsoft Sentinel, Splunk, CrowdStrike Falcon, Genian NAC, and ManageEngine PAM360 has equipped me to effectively monitor, analyze, and mitigate complex security threats across enterprise environments.

In my current role at M42, I actively manage and respond to cyber threat intelligence (CTI) alerts, conduct vulnerability assessments, and develop SIEM correlation rules to improve incident visibility and reduce false positives. I regularly analyze system and network logs to identify the root causes of security events, providing timely and effective resolutions. To increase operational efficiency, I have built automation scripts in Python, PowerShell, Bash, and CMD, streamlining repetitive processes, enhancing workflows, and improving threat detection accuracy.

My hands-on expertise extends beyond daily operations. I have designed and maintained advanced home labs to simulate real SOC environments for continuous learning and experimentation. These labs integrate Splunk and Security Onion for SIEM and network traffic analysis, alongside Suricata and Zeek for intrusion detection. For malware analysis and behavioral investigation, I leverage FLARE VM, REMnux, CAPEv2, and attacker systems running Kali Linux to perform both static and dynamic analysis of malicious samples. Through these environments, I've gained deep insight into attack chains, command-and-control communication, beaconing, and data exfiltration techniques, while improving my ability to create and test detection rules aligned with MITRE ATT&CK tactics and techniques.

I take pride in maintaining a balance between technical proficiency and analytical thinking. My experience has strengthened my ability to collaborate across teams, handle multiple incident queues efficiently, and align technical remediation with organizational security objectives. I've contributed to achieving over 90% compliance in ISO 27001, ADHICS, CAP, and GCLP audits by ensuring effective security controls, user awareness, and proactive monitoring. These experiences have shaped me into a well-rounded analyst capable of operating across both SOC operations and security engineering functions.

Beyond detection and analysis, I focus on continuous improvement and automation. I believe every detection can be optimized, every workflow simplified, and every alert made more actionable. I constantly seek ways to integrate scripting and automation into SOC operations, reducing response times while minimizing analyst fatigue. This mindset has enabled me to deliver more consistent, data-driven results while maintaining a strong focus on operational resilience and security posture improvement.

What excites me most about this opportunity is the chance to contribute my technical knowledge, passion for cybersecurity, and proactive problem-solving approach to a forward-thinking security team. I thrive in environments that value both precision and adaptability where detecting, analyzing, and responding to emerging threats makes a real impact on business continuity and defense readiness.

Thank you for considering my application. I would welcome the opportunity to discuss how my experience in SOC operations, malware analysis, and security automation can contribute to strengthening your organization's cybersecurity capabilities and overall resilience.

Thank you,
Mohamed Aakif