Amani Alshaikhi.
Amani.alshaikhi@icloud.com,
USA. 571-(205)-8564 KSA +966564748243

Professional Summary:

Database:	Management, Configuration, Monitoring, Optimization, Backup, Upgrade.
Developer:	Secure SDLC
Cyber Security:	Vulnerability Assessment, Penetration Testing, Security Audit, Compliance, SIEM, Data Loss Prevention, Malware Analysis**,** Endpoint Security
OS	Windows Client and Server, Linux Client and Server, MAC**,** Kali Linux
Networking:	TCP, UDP, IP, Router, Switches, Server, Network Troubleshooting
Security Devices:	Firewall, IPS & IDS, Update and Patch Management.

Training/ Certifications/ Education:

● PHD in Computer Science.	Howard University USA 3.70/4
● MSS in Cybersecurity.	Lewis University USA 3.67/4
● BS in Information Technology	UMM-Al Qura University 3.06/4
● Cybersecurity Certificate	

WORK EXPERIENCE

Cyber Security Consultant **Jan 2018- Dec 2021**
Nobel Data Solutions

- SOC analyst and SIEM experience with Splunk queries, create dashboards and reports and be familiar with Enterprise Security (ES).
- Analysis security events data from the network (IPS & IDS sensors, firewall traffic).
- Knowledge in **Carbon Black** always-on recording of activity from all monitored endpoints
- Experience with packet analysis tools such as **Wireshark**.
- Used **SERVICE+** tool created a ticket and (Assigned to tier2 team)
- Experience with scan/assessment tools such as Nmap, Nessus, Burp Suite, and Core Impact.
- Ability to monitor the security performance of enterprise systems
- Ability to continuously monitor systems to ensure security controls are implemented, operate as intended.
- Design and implement safety measures and data recovery plans.
- Act on privacy breaches and malware threats.

Dental IT Help Desk Support **Sep 2016 – May2022**
Millennium Dental Care, VA

- Security monitoring and incident response services required by the business.
- Intermediate experience with Wireshark.
- Knowledge in **McAfee** Dashboards and Monitors
- Involved in intrusion detection and incident response.
- Knowledge of FISMA and NIST 800 series standards.
- Knowledge of network mapping, vulnerability scanning, penetration testing, and Web Application testing.

- Analyses data collection and correlation that allow for detection and monitoring for profiles of suspicious internal threat activity.
- Comprehend and articulate the Security perspective and engage with Splunk Product teams on Splunk features and roadmap.
- Monitoring the system and managing alerts.

Additional Experience

- Experienced in Log analysis, proactive monitoring, mitigation, and response to network and security incident.
- Analysis security events data from the network (IPS & IDS sensors, firewall traffic).
- Perform static and dynamic malware analysis on virtual servers with proper documentation and steps for removal on infected systems.
- Experience with packet analysis tools such as **Wireshark**.
- Knowledge in **McAfee** Dashboards and Monitors
- Knowledge of FISMA and NIST 800 series standards.
- Experienced working in a SOC environment.
- Strong understanding of Microsoft Active Directory and Group Policies.

Reference: Available upon request.