### **Asim Kalla**

[122344@gmail.com](mailto:122344@gmail.com) | Franklin Square, NY | (123456789 | in/abdul-w-mian

**Cyber Incident Management Specialist**

I am an experienced Cyber Incident Responder expert on Identifying and managing key data points regarding information security incidents, such as root-cause analysis, possible attack methods and techniques, malware infection and persistence methods. I have a strong understanding of life cycle of an Incident and tools used to determine root cause during an incident and prevent recurrence. Currently I hold security+ certification by CompTIA and preparing for CEH certification by EC-Council.

**TECHNICAL SKILLS**

* **IT Security**

Digital forensics (EnCase, FTK imager), Incident response (The Hive, ServiceNow), Security Information and Event Management (IBM Qradar, Splunk), Endpoint Detection and Response (FireEye HX, Carbon Black), Threat Intelligence (Socradar.io) Log analysis, Phishing analysis, Malware analysis (Cuckoo Sandbox), Ransomware IOCs, IAM, OSINT resources Virus-Total, Any-Run, MX toolbox, and Mitre att&ck framework etc.

* **Networking**

Enterprise Network Security, Packet Analysis (Wireshark, Tcpdump), NGFW (Fortinet), TCP/IP, Intrusion Detection/Intrusion Prevention Systems (IDS/IPS), DNS, Nmap and OSI Model.

* **Vulnerability**

Vulnerability Management (Nessus Tenable.io), System Hardening, Compliance with Risk Management Framework NIST 800-37 and Application Security (OWASP).

* **Systems**

Windows, Unix/Linux, IOS, VMware, SDLC (System Development Life Cycle).

**PROFESSIONAL EXPERIENCE**

**CyberSecurity Analyst Apr 2020 to Present**

**CyberNow Labs, Chantilly, VA**

Job Responsibilities:

* Monitor the SIEM (Splunk ES) for notable events and work with customers to investigate and remediate those events. Analyze notable events in Splunk ES and determine if notable events need to become incidents.
* Responding security incidents using network forensics, endpoint forensics, root cause analysis and malware analysis.
* Participate in the creation and maintenance of use cases for recurring investigation/incident triggers in support of Cyber Threat Operations and Cyber Threat Management program.
* Interface with other teams in Information Security e.g. Network Operations Center (NOC), Cyber Threat Operations Center (CTOC), vulnerability management and along with information and liability risk officers and technology management to help guide cyber security strategy.
* Adhere to all policies, standards and regulatory requirements regarding reporting and escalations.
* Identify new threat tactics, techniques and procedures used by cyber threat actors.

**Network Operations Analyst Sept 2018 to Mar 2020**

**Links International, Ashburn, VA**

Job Responsibilities:

* Monitoring the network with network monitor (OP5, SolarWinds)
* Monitor network for connectivity and security issues.
* Integration of new network devices and technologies.
* Configuring network devices.

**Electronics Technician Dec 2008 to Oct 2018**

**Self Employed, Woodside, New York**

* Electronic devices repair, reimaging, reverse engineering, JTAG interface for debugging, reading for memory errors, writing flash memory and file system data recovery.
* DIY script kiddie project: Attempt to decrypt AES-256 encryption using side channel analysis, tool of interest was ChipWhisperer by NewAE Technology Inc.

**EDUCATION**

* University of Punjab 1997-1999

**B.S (Biological Sciences)**

**CERTIFICATIONS**

* **CompTIA Security+** (6TLY8MPMV341QS5N) Expires July,2023
* Splunk 7.x Fundamentals
* CEH (In Progress)

*Authorized to work in the US for any employer without sponsorship (US citizen).*

*References available upon request!*