**Mohamed Suliman**

**Security Operations Center (SOC) Analyst**

Tel Aviv, Israel

+972525591751; [fitijoe@gmail.com](mailto:fitijoe@gmail.com)

https://www.linkedin.com/in/mohamed-suliman-138994249

|  |
| --- |
| **PROFESSIONAL SUMMARY:** |

Innovative, technically-oriented, and self-driven professional with extensive experience in driving business solutions and optimizing cyber-threat monitoring, security operations and solutions, and security architectures. Provide front-line support of cyber defense, detecting and responding to cyber attacks as they happen. Familiarity with many fields in the worlds of CyberSecurity and Information Security. Skilled in investigating, documenting, and reporting on any information security (InfoSec) issues as well as emerging trends. Provide analysis and response to previously unknown hardware and software vulnerabilities. Knowledgeable in preparing disaster recovery plans. Proven success in conducting tests to identify system vulnerabilities, prevent future security breaches, and ensure the overall systems are secured and protected from cyber-attacks. Evaluate the cybersecurity posture, vulnerabilities, and potential impact of all mission related control systems. Collaborate with other team members to detect and respond to information security incidents, develop and follow security events such as alerts, and engage in security investigations. In-depth Familiarity With Communication Models and Many Network Protocols IT Systems: Virtualization, Linux, Windows, and Active Directory

|  |
| --- |
| **PROFESSIONAL QUALIFICATIONS, KNOWLEDGE, SKILLS, AND ABILITIES:** |

* Identify the root of the attack, implement the required security actions to counter the attack, and restore system operations.
* Responsible for investigating and generating reports on information security issues.
* Carries out vulnerability assessments and penetration tests to assess the resilience of the organization and to isolate areas of weakness that need attention. Reviews alerts, threat intelligence, and security data.
* Maintain security systems up to date and contribute to ongoing security approaches to secure the organization against further attacks.
* Abreast of most tools and resources that are used for cybersecurity, such as antivirus software, firewalls, vulnerability scanning, system-wide operating systems.

|  |
| --- |
| **EXPERTISE:** |

|  |  |  |
| --- | --- | --- |
| * Security Architecture | * Cybersecurity Roadmaps | * Vulnerability Management |
| * Systems Security | * Business Development | * Network Architectures |
| * Security Program Development | * Cyber Threat Intelligence | * Security System |
| * Cyber Intelligence | * Cybersecurity Frameworks | * Intrusion Detection and Mitigation |
| * Problem-Solving | * Communication | * Cyber Incident Response |

|  |
| --- |
| **PROFESSIONAL EXPERIENCE:** |

JANUARY 2023 **Business Solution**

**Ness Technologies, Tel Aviv**

JAN 2008 — DEC 2010 **Computer Technician/ Help Desk**

**Hotline, Tel Aviv**

Responsible for the maintenance of the organization's Computers, Operation of Office Systems, Data Management, Research, Analysis of Information

Translator From Fur Language To English And English to Arabic And Hebrew To English And Arabic & Fur Languages.

|  |
| --- |
| **EDUCATION:** |

**Cairo University, Cairo**

FEBRUARY 2004 — OCTOBER 2005

**San Andrew, Cairo**

FEBRUARY 2004 — AUGUST 2005

**Python & Web Design Courses at ARDC**

MARCH 2022

Self-study on the above sites: TryHackME.com, HackTheBox Academy, Let'sDefend.io Bugcrowd.com, PicoCTF.org, Portswigger.net

**Kernelios College**

2021-2022

Graduated From a Course Applying CyberSecurity Defense (500 Hours Total)

Course that Includes a Government Certification Certificate, Containing a lot Of Theoretical And Practical knowledge in CyberSecurity

|  |
| --- |
| **SKILLS:** |

Network Traffic Analysis (wireshark, NMAP, NC), Password cracking and Mitigation, Intelligence Collection Methods, Experience with VMware, Kali

Linux: Terminal and tools, Proxy- Burpsuite, Metasploit. DDOS, MIDM, Malware analysis, Criptography, Web

App Security System Installing and Configuring Windows 10, Windows Server 2012r, 2016, 2019 tools,

Roles and Add-ons Active Directory, Domain Controler, DNS, DHCP Networking OSI, TCP/IP Models.

Protocols: HTTP, DNS, DHCP, FTP, SSH

|  |
| --- |
| **LANGUAGES:** |

English, Hebrew, Arabic, Fur Languages

|  |
| --- |
| **REFERENCES:** |

**Available Upon Request**