Ahmed Moamer Mohamed Ali

Cairo, Egypt.

Mobile: (+20)01000787947

Email: ahmedmoamer519@gmail.com

LinkedIn: https://www.linkedin.com/in/ahmed-moamer 7a78b0172/

Military Status: Exemption

CAREER OBJECTIVE

A highly passionate, detail-oriented and self-motivated Information Security Analyst. Seeking for opportunity as GRC Consultant with skills in Handling PCI-DSS Certification and other Security Compliance, review policies, develop plans and IT audit and technically skills in Malware Analysis and knowledge in SIEM solution, Incident Response, Threat Intelligence.

EDUCATION

Bachelor of Computers and Artificial Intelligence | Fayoum University | 2018-2022

Work EXPERIENCE

Aug 2023 – Present
Information Security Analyst at **Basata**

- Handling PCI-DSS Certification and other Security Compliance
- Perform systems and network security hardening
- Perform security audit and identify/report information security gaps then follow-up till mitigation.
- Perform Threat Modeling according to STRIDE
- Perform Risk Assessment and Communicate the risk assessment findings and support relevant parties to tackle the risk and decide proper risk mitigation strategy
- Performed regular security audits of systems and networks to identify vulnerabilities.
- Performing GAP analysis for infrastructure assets; highlighting its vulnerabilities and recommending mitigation actions.
- Development of Information Security policies and processes, System Security Plans and Security baseline in accordance with PCI and NIST
- Develop Incident Response plan and process and Patch Management Policy
- Works with third-Party to facilitate our information security activities
- Reviewing Third-party/Vendors contractual agreements as per service provided from information security perspective
- Conduct third-party Penetration testing, and manage third-party Penetration testing and remediation
- Supervising the required penetration testing activities as per compliance
- Recognize potential, successful, and unsuccessful intrusion attempts and compromises thorough reviews and analyses of relevant event detail and summary information.
- Investigating, documenting, and reporting on any information security (InfoSec) issues as well as emerging trends
- Participated in regular meetings with management to discuss trends within the environment and provide recommendations for improvement where applicable.
- Executing corporate awareness activities in order to increase the awareness levels of business users with the growing security risks and its corresponding mitigations

PROFESSIONAL TRAININGS

Nov 2023 – Feb 2024

GRC Track at **WE Innovate Academy** in ITI Creativa

Introduction to Governance, Risk, and Compliance	Risk and Information Systems Control (CRISC)
Governance, Risk, and Compliance (ISC)²	EG Security & Privacy Regulations
Resilience	Security Risk Assessment
PCI-DSS Implementation Lead	ISO 27001/27017 Implementation lead
CISSP	

MAY 2023 – Jun 2023
Cyber Security Intern at **Telecom Egypt** in the Smart Village

- Practical on IBM-Qradar SIEM solution
- The ability to document Incident Response Activities, then write an incident response report
- Proven ability to effectively manage and triage, incidents
- Monitoring and responding to cyber threats

Feb 2023 – MAY 2023
Digital Egypt Youth Initiative, National Telecommunication Institute (NTI), New Capital(Advanced Cyber Security Track)

Technical Modules:

Linux Red Hat Administrator	Network Security
Cyber Ops Associate	Python for Security
CNP Security	

Business Skills Modules:

Business English	Soft Skills
Project Management	

Jun 2021 – Aug 2021

Incident Response Scholarships | CyberTalents&Trendmicro

A 3-month training program for 500 different talents in Arab and Africa brought by Trend Micro and CyberTalents in Incident Response that include the following topics[Reverse Engineering, Digital Forensics, Trend Micro solutions for deep analysis]

CERTIFICATES

Malware Analysis Fundamentals at MAHARA TECH	Practical Malware Analysis&Triage
TryHackMe Cyber Defense Path	

SKILLS

Technical:

- Good Understanding of Network Fundamentals || Solid knowledge of TCP/IP protocols
- Packet analysis in Wireshark
- Web application attacks (OWASP top 10)
- Deep Knowledge of Network security technologies (Firewalls, IDS/IPS, WAF, Antivirus …etc.)
- Good Understanding of OS (Windows - Linux)
- Knowledge in SIEM technologies
- Familiar with Intelligence Driven Defense, Cyber Kill Chain methodology, MITRE ATTACK framework.
- Profound Knowledge in threat intelligence || Digital forensics || cyber attacks
- Profound Knowledge in Malware analysis and Reverse Engineering
- Extract loC for malwares | Yara rules
- SANS SEC504 Hacker Tools, Techniques, and Incident Handling
- Assisted with the development of new security policies and procedures as well as providing ongoing training on current best practices related to information security.
- Investigate malicious phishing emails, domains and IPs using Open Source tools & recommend proper blocking based on analysis.
- Search firewall, email, web or DNS logs to identify and mitigate intrusion attempts.
- Research new and evolving threats and vulnerabilities with potential to impact the monitored environment
- Profound Knowledge in C/C++ || python

Interpersonal:

- Communication Skills
- Presentation Skills
- Team Work || Flexible || Research
- Analytical minded
- Ability to learn and learn New Technologies

Language:

- Arabic (Native)
- English (Intermediate)

CTFs and Projects

- 13th Place in ICMTC (**Military Technical College Competition**) Qualifications [2023]
- Spyware Detection Based on machine learning model **(Graduation Project)**
- Record the 16th place in Egypt and the 40th place personally on the qualifying rounds **CyberTalents**

VOLUNTEER EXPERIENCE

- [HR Member Team] | [IEEE Fayoum Student Branch] from Oct 2021– Aug 2022
- [Cyber Security Member] | [Cat Reloaded] from Oct2020 – Dec 2021
- [Academic Ambassador] |[CyberTalents] from Sep 2020 – Jun 2021
- [Marketing Member Team] | [IEEE Fayoum Student Branch] from Oct 2018– Jul 2019