Ahmad Abdul Rahman Wakkaf
Cybersecurity Analyst

Saint Petersburg, Russia
+7 999 862-56-58 | ahmadwakkaf@yandex.com
https://www.linkedin.com/in/ahmad-wakkaf

SUMMARY

- An ambitious and hardworking individual with a keen interest in cyber security and a solid understanding of reviewing SIEM logs and security Events from variety of devices and solutions such as Firewalls, IDS/IPS, Antiviruse, EDR, Sysmon, Syslog, Proxy Server and more.
  Beside his good knowledge in Network Forensics, Packets Analysis, Vulnerability Assessment, Phishing and Email Analysis he knows how to implement and use the different types of Cyber Defense Frameworks and using Threat Intelligence Methods for APTs, plus identify their TTPs. All of that for the benefit of the Organization.
- To him, Life is a journey worth exploring every aspect and failure just like success, makes for a stronger personality and leads to a better outcome, hence he had always been a positive and optimistic person believeing in fullfilling his dreams no matter the difficulties and circumstances, so he believeing in self-learning and he didn't waste one single day without learning a new thing, You can consider him a flame of passion and enthusiasm regarding any resource will develop his hard and soft skills in order to develop his career in the cyber security field.

INDUSTRY KNOWLEDGE

- Monitoring and Investigating Suspicious Network and Devices Logs Utilizing a variety of Tools and Solutions SIEM: SPLUNK- ELK, QRadar, EDR: Wazuh - Sysmon - Sysinternals - Osquery
- Performing a Security Assessment and Vulnerability Management on the Network Using: Nessus - OpenVAS - Nmap
- Investigating Phishing and Malicious Emails, Domain and IP Addresses Using: URL Scan - AbuseIPDB - Any.Run - VirusTotal - Talos Reputation Center
- Deep Understanding of Networking Concepts Like: Protocols, OSI and TCP/IP Models, DNS, DHCP, VPN, Proxy and Active Directory
- GOOD Knowledge With Cyber Defense Frameworks and Models: Cyber Kill Chain - Unified Kill Chain - Diamond Model
- Threat Intelligence for APTs Groups and Identify their TTPs Using MITRE ATT&CK - MISP
- Knowledge of Forensics investigation Techniques in Windows Forensics, Memory Forensics and fundamental Linux Forensics Using: FTK - Volatility - Autopsy - Redline
- Perform Network Forensics and Packets Analysis in order to looking for Malicious activities in the Network Using Wireshark - Tcpdump
- Basics of Malware Analysis

PROFESSIONAL EXPERIENCE

- **CyberTalents** 07/2022 - 09/2022
  Cyber Security Intern
  - Web Application Security
  - Data Encryption Techniques
  - Network Security
  - Digital Forensics

- **Masar Center Education** 01/2022 - 08/2022
  IT Support Specialist
  - Performing PCs and Computers installation, setup, and maintenance of hardware and software for new and existing users.
  - Tracking of complex software and hardware issues of networking and applications to meet business needs.
  - Checking antivirus status, storage space, network activity and adjusting network equipments and settings to improve system performance.

- **ACM ICPC-Syrian Collegiate Programming Contest** 07/2019 - 06/2020
  IT Network Technician
  - Providing technical assistance and application support while adhering to established processes and procedures to ensure a reliable workplace.

- Troubleshooting hardware and software issues and recommendation for necessary upgrades and configuration for implementation.
- Analyzing and diagnosing wired and wireless local area networks and repairing any failures related to these networks.

EDUCATION

- Master's Degree, Information Security - ITMO University 02/2024 - 06/2026
- Russian Language - ITMO University 10/2022 - 06/2024
- Bachelor's Degree, Computer Systems and Networks Engineering - Tishreen University 09/2015 - 03/2021
  Grade: 80.24% - GPA: 3.2/4.0

CERTIFICATIONS

- Google IT Support Professional
  Issued by Google via Coursera, Sep 2022
- NSE 1 Network Security Associate
  Issued by Fortinet, May 29, 2022 - May 29, 2024
- NSE 2 Network Security Associate
  Issued by Fortinet, June 3, 2022 - June 3, 2024
- NSE 3 Network Security Associate
  Issued by Fortinet, October 22, 2022 - October 22, 2024

COURSES

- Introduction to Cyber Security Learning Path
  TryHackMe
- Complete Beginner Learning Path
  TryHackMe
- Pre Security Learning Path
  TryHackMe
- Python Training Program
  DataFlair
- Web Penetration Testing
  Tera Courses
- Cyber Security Specialization
  Edraak
- MITRE ATT&CK DEFENDER™ (MAD) ATT&CK® Fundamentals
  Cybrary
- MITRE ATT&CK DEFENDER™ (MAD) ATT&CK® SOC Assessments
  Cybrary
- CompTIA Security+
  Netriders Academy
- eLearnSecurity Certified Incident Responder - eCIR
  Netriders Academy

LANGUAGES

- **Arabic**
  Native Proficiency
- **English**
  Limited Working Proficiency
- **Russian**
  Limited Working Proficiency

SOFT SKILLS

- Critical Thinking
- Problem Solving
- Teamworking
- Scheduling