Taha Abdelhady Abu Khalil

Sheikh Zayed, Egypt
+20 109 223 1129
tahaabukhalil60@gmail.com
LinkedIn https://www.linkedin.com/in/taha-abu-khalil-

Cybersecurity Engineer | Network Security Specialist | Information security

Dedicated and detail-oriented **Cybersecurity & Network Engineer** with a strong academic background and hands-on experience in securing and managing IT infrastructure. Equipped with certifications such as **CCNA, CCNA Security, MCSA, ITIL Foundation, and SOC Analyst**, and a proven track record in **threat detection, incident response, firewall management**, and **network hardening**. Passionate about staying ahead of cyber threats and continuously improving security posture in dynamic environments.

Education

B.Sc. in Computer and Information Systems – IT Track
Menoufia University – Egypt | **Graduated: 2021**

Relevant Professional Experience

Senior IT – Kheyoot for Clothes Cotton, Smart Village, Egypt

Dec 2024 – Present

- Implemented and managed **pfSense firewall**, defining user permissions and network segmentation.
- Deployed a **load balancing solution** between two ISPs for high availability.
- Managed IT infrastructure for **28 retail branches across Egypt**, including POS and CCTV systems.
- Ensured secure network connectivity and minimal downtime through proactive monitoring.
- Evaluated new technologies and maintained endpoint security measures.

- Device maintenance (software and hardware), including barcode and regular printers; troubleshooting internet and file sharing issues; providing technical support for sales staff in malls and resolving any sales system problems; onboarding employees and streamlining their daily tasks; software and network monitoring; performing regular backups to protect data; and maintaining and improving the efficiency of devices.

- Responsible for the cPanel mail server used by sales representatives in the branches where they sell, and for employee emails. Responsibilities include: website creation, email creation, database management, uploading website files, backups, domain management, and adding and removing employees.

IT Specialist – Al Fahd Steel Import & Export, Egypt

Dec 2023 – Aug 2024

- Administered IT security protocols including antivirus, endpoint protection, and strong password policies.
- Monitored and maintained all IT infrastructure including servers, PCs, and printers.
- Ensured system hardening, software patching, and malware prevention strategies.
- Conducted internal audits and routine security updates across the network.

Network Engineer – MISR Rotogravure, Egypt

Oct 2021 – Sep 2022

- Maintained and configured routers, switches, and secured internal networks.
- Supported database access and implemented basic cybersecurity measures.
- Conducted troubleshooting and performance monitoring for critical systems.

Cybersecurity Training & Certifications

🎓 Cyber Security Analyst & Responder (SOC) Diploma – CyberGuardX Academy

Start Date: September 22, 2025 — *Currently in progress*
Duration: 176 Hours

Key Focus:
Comprehensive, hands-on cybersecurity training preparing for SOC (Tier 1 & 2) roles. Covers advanced topics in network security, ethical hacking, incident response, and SIEM management.

Main Modules:

- **Network Fundamentals (CCNA Fast Track):** Networking, routing, VLANs, secure topology design.
- **Operating Systems (Windows & Linux):** System administration, hardening, Active Directory, SELinux, firewalls.
- **Network Security:** Firewalls, IDS/IPS, VPNs, encryption, FortiGate, and Snort configuration.
- **Attack Concepts:** Threat hunting, malware analysis, phishing simulations, MITRE ATT&CK framework.
- **Security Operations Tools:** Log analysis, Wireshark, Nmap, digital forensics (FTK Imager, Autopsy), threat intelligence (MISP, OpenCTI).
- **SIEM & Incident Response:** Splunk, QRadar, ELK Stack, playbook design, SOAR basics, and real-world attack simulations.

Certifications Alignment:
Prepares for **Cisco CyberOps Associate**, **eCIR**, **CompTIA Security+**, and **ISC² CC**.

Practical Skills:
Incident detection & response, network defense, digital forensics, SOC workflows, and threat intelligence analysis.

Cybersecurity Diploma (SOC Track) – AMIT

Dec 2023 – Apr 2024

- Hands-on training in **incident response**, **SIEM (QRadar)**, **threat detection**, and **digital forensics**.
- Tools: **Wireshark, Metasploit, XSOAR, ASA Firewall, IDS/IPS**, Linux (Kali, Parrot).
- Worked on **FortiGate F60/F61 v7** configurations and firewall policy management.
- Covered topics from Cisco CyberOps, Cybersecurity Essentials & Introduction to Cybersecurity.

Cybersecurity Diploma – NTI

Aug 2024

- Covered **Blue Team vs Red Team roles**, **penetration testing**, **social engineering defense**, and **QR code-based threats**.
- FortiGate configuration and CLI proficiency developed in lab simulations.

CompTIA Security+ (SY0-601) – Prep Course – NetRiders Academy2024

Covered Topics:

- Attacks, Threats & Vulnerabilities
- Secure Network Architecture & Design
- Cryptography & PKI
- Incident Response & Operations
- Governance, Risk & Compliance

IT Diploma – Creative Group

Feb 2020 – May 2020

- Foundation training in **networking, system administration, and security**.
- Studied **CCNA**, **CCNA Security**, **MCSA**, and **ITIL Foundation** modules.

Technical Skills

1. Active Directory (windows server 2019&2021)
2. Microsoft 365 (Excel & word & power point & PDF)
3. Tryhackme
4. Cyberdefinders
5. Cisco Networking Academy
6. CTF Player

Cybersecurity Tools & Concepts

- Threat Detection & SIEM (QRadar, XSOAR)
- Network Firewalls (pfSense, FortiGate, ASA)
- IDS/IPS (Snort, Zeek)
- Malware Analysis & Forensics
- Incident Response (SOC Operations)
- Cryptography & Secure Protocols
- Network Hardening & Secure Design
- Vulnerability Scanning (Nessus, Nmap)
- Log Analysis, Packet Capturing (Wireshark)
- Cybersecurity Frameworks (MITRE ATT&CK, YARA)
- Scripting with Python for Security Tasks
- OS Platforms: Windows Server, Linux (Kali, Parrot)
- Cloud Security Fundamentals (AWS)

Soft Skills

- Analytical Thinking & Problem Solving
- Team Collaboration & Communication
- Adaptability & Self-Motivation
- Creativity in Cyber Defense Strategy
- Strong Work Ethic & Time Management
- Continuous Learning and Training

Languages

- **Arabic** – Native
- **English** – B2 (Upper-Intermediate)