Abdelwahab Ahmed Shandy

(+20) 1017417103 abdelwahabshandy@gmail.com Cairo - Egypt
linkedin.com/in/abdelwahab-ahmed-shandy abdelwahabshandy.hashnode.dev

SUMMARY

Information Systems student focused on Defensive Security, with hands-on experience in SOC operations, network security, and IT fundamentals, seeking an entry-level role in SOC, Network Engineering, IT or Network security.

EDUCATION

B.Sc. in Computer Systems and Information | MCI Academy | Aug 2022 – Jun 2026 *(Expected)*
Diploma in Technology (5-Year Program) | Jalal Fahmy German Technical Secondary School
Graduated: 2022 | Graduation Project Team Lead coordinated team tasks and project delivery

INTERNSHIP EXPERIENCE

ZeroSploit MEA | On-Job Training Trainee | El Agouza(Hybrid) Oct 2025 – Jan 2026

- **Log Engineering**: Designed end-to-end pipelines using ELK Stack, centralizing Windows (WEF) and Linux logs for enhanced security monitoring.
- **Security Automation (SOAR):** Developed AI-driven n8n workflows for automated vulnerability remediation (Nessus) and CrowdStrike incident response.
- **Detection & Defense**: Executed Active Directory attack simulations to build Sigma-based detections aligned with the MITRE ATT&CK framework.
- **Infrastructure Integration**: Integrated multi-vendor solutions (Palo Alto to Microsoft Sentinel) and optimized Nginx server performance in production-like environments.

CyberTalents | Penetration Testing Boot Camp | Oct 2025 – Nov 2025

- Gained a foundational understanding of offensive security by practicing information gathering, web vulnerability assessments, and documenting technical walkthroughs for CTF challenges.

WE INNOVATE | SOC Boot Camp (Creativa Hub)| Sep 2025 – Oct 2025

- Deployed and optimized a SIEM system (ELK Stack) with SOAR (n8n), analyzed security events, and configured log collectors to ingest data from multiple network nodes

National Telecommunication Institute (NTI) | Windows Server Admin| Aug 2025 – Sep 2025

- Gained hands-on experience in Windows Server administration, including AD DS, Group Policy, DNS, DHCP, NLB, and implemented failover clustering and disaster recovery in a virtualized lab environment.

Information Technology Institute (ITI) | Network Infrastructure | Jun 2025 – Jul 2025

- Completed the Cybersecurity Certificate for Beginners (MaharaTech) as a prerequisite, followed by hands-on training in routing, switching, and cloud fundamentals to bridge the gap between infrastructure and security

AMIT Learning | SOC Boot Camp | Jun 2023 – Sep 2023

- Gained hands-on experience in SOC operations using IBM QRadar, including alert monitoring, incident analysis, and basic malware investigation, and documented findings in a technical report

Information Technology Institute (ITI) | Network Security | Aug 2023

- Training Team Lead: Coordinated group activities while mastering network security protocols and gaining hands-on exposure to Palo Alto and FortiGate firewalls

TECHNICAL SKILLS

Cybersecurity : SIEM (ELK, QRadar), SOAR (n8n), Basic Incident Response, Basic Digital Forensics

Windows Server: Active Directory, Group Policy (GPO), DNS, DHCP, basic failover configuration
Linux: User & permission management, system monitoring, basic shell scripting
Networking: CCNA-level knowledge – TCP/IP, routing & switching, VLANs, subnetting
Firewalls & Security Devices: Intro to FortiGate & Palo Alto – rules creation, traffic monitoring

SOFT SKILLS

Problem solving, Team management (Graduation Project Lead), Public speaking, Documentation & technical reporting (Hashnode author), Continuous self-learning

---

CERTIFICATIONS & PROJECTS

Professional Certifications:

- Cybersecurity Foundations — **Infosec**.
- Google Cybersecurity & Information Technology — **Google**.
- Junior Cybersecurity Analyst Career Path — **Cisco Networking Academy**.

Technical Projects:

Enterprise Security Simulation : Built a personal lab with a zoned network (External, DMZ, Internal) to practice attack and defense scenarios, and security monitoring, with full documentation published on my blog

Link : sec-lab-notes.hashnode.space/abdelwahabshandy-notes/enterprise-offensive-defensive-security-simulation-lab/objective

SIEM & SOAR Home Lab: Built a centralized monitoring system with automated alert analysis, user-friendly email notifications, and a simple dashboard.

Link : sec-lab-notes.hashnode.space/abdelwahabshandy-notes/siem-home-lab/pre-lab-overview

Movie Market Web App : Developed a cinema booking platform using ASP.NET Core MVC, 3-Tier Architecture, and SQL Server

Database & Programming Projects : Engineered ERD/EERD schemas, solved algorithmic challenges, and developed C++/C# mini-projects

Arduino Calculator : Embedded system project for multi-functional calculations

Link Programming projects : github.com/abdelwahab-ahmed-shandy

---

LANGUAGES

Arabic: Native English: Very Good(Professional Working Proficiency)