# Abdelwahab Ahmed Shandy

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

## SUMMARY

Information Systems student and Cybersecurity enthusiast with a dual focus on Security Operations (SOC) and Offensive Security. Proven track record in building automated security workflows, engineering SIEM ingestion pipelines, and conducting penetration testing through intensive national training programs.Passionate about continuous learning, technical documentation, and contributing to secure, scalable technology solutions.

## EDUCATION

- **BSc in Computer Systems and Information** *(In Progress)*
  MCI Academy — Aug 2022 – Jun 2026 (Expected)
- **Jalal Fahmy German Technical Secondary School** (*Five-Year Program*)
  Graduated: 2022

## WORK & INTERNSHIP EXPERIENCE

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

- Engineered end-to-end log ingestion pipelines for Windows and Linux using Winlogbeat, Filebeat, Logstash, and Elasticsearch.
- Centralized Windows event logs through Windows Event Forwarding (WEF) for SIEM use cases.
- Developed advanced SOAR workflows using n8n and AI agents to automate vulnerability discovery and remediation with human-approval gates.
- Automated security awareness and response based on CrowdStrike detections using AI-driven integrations.
- Executed Active Directory attack simulations from initial access to lateral movement with Sigma-based detections in ELK.
- Integrated multi-vendor security solutions for log forwarding, including Palo Alto Firewalls and Microsoft Sentinel.
- Troubleshot complex network and service-level issues, including Nginx web server optimization, in constrained environments.

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

- Executed comprehensive information gathering and vulnerability assessments as part of the ITI Cybersecurity program.
- Simulated real-world exploitation and post-exploitation scenarios focusing on web application security.
- Documented technical walkthroughs and write-ups for complex penetration testing labs and CTF challenges.

### WE INNOVATE | SOC Boot Camp | Giza, Egypt Sep 2025 – Oct 2025

- Deployed and optimized a fully functional SIEM system (ELK Stack) integrated with SOAR (n8n).
- Analyzed security events and conducted threat hunting to identify potential indicators of compromise (IOCs).
- Configured log collectors (Winlogbeat & Fluent Bit) to transform and ingest data from diverse network nodes.

### National Telecommunication Institute (NTI) | Windows Server Administration Boot Camp | Remote Aug 2025 – Sep 2025

- Administered Windows Server environments, including AD DS configuration and Group Policy (GPO) management.
- Configured critical network services such as DNS, DHCP, and Network Load Balancing (NLB).
- Implemented Failover Clustering and Disaster Recovery solutions in a virtualized lab environment.

### Information Technology Institute (ITI) | Network Infrastructure Boot Camp | Remote Jun 2025 – Jul 2025

- Established a solid foundation in networking and cloud fundamentals through theoretical and practical training.
- Utilized routing and switching concepts, network virtualization, and cybersecurity essentials.
- Completed technical essentials for cloud services and system administration through self-study and evaluation.
- Bridged the gap between infrastructure and security as a core step toward penetration testing.

### EraaSoft | Dotnet Developer Boot Camp | Giza, Egypt Nov 2024 – May 2025

- Developed backend applications using C#, SQL Server, and Entity Framework Core with MVC architecture.
- Applied SOLID principles and tiered architecture to ensure code maintainability and scalability.
- Built practical projects using object-oriented programming to organize code effectively.

### Programming Advices | Programming Foundations | Remote Aug 2024 – Jul 2025

- Developed a strong logical foundation through a structured roadmap in C++ and algorithmic thinking.
- Mastered programming foundations, flowcharts, and advanced problem-solving techniques.
- Implemented SQL databases and practiced real-world scenarios for database design and management.

### AMIT Learning | SOC Boot Camp | Cairo, Egypt Jun 2023 – Sep 2023

- Utilized security information and event management tools (IBM QRadar) for security operations and monitoring.
- Conducted incident triaging, response, and forensics to investigate attack patterns and indicators of compromise.
- Performed malware analysis and reverse engineering as part of a comprehensive defensive security track.
- Published a technical report on blue team challenges and investigative workflows.

### Information Technology Institute (ITI) | Network Security Boot Camp | Remote Aug 2023

- Served as the training leader, coordinating tasks and group activities during the intensive program.
- Studied advanced networking protocols, ethical hacking basics, and cybersecurity essentials.
- Gained exposure to industry-leading firewalls including Palo Alto Essentials and FortiGate.

---

## TECHNICAL SKILLS

- **Security Operations:** SIEM (ELK Stack, QRadar, Splunk), SOAR (n8n), AI Security Automation, Incident Response, Digital Forensics, Sigma Rules.
- **Offensive Security:** Pentesting Methodologies, Vulnerability Assessment (Nessus), Web Security, Ethical Hacking.
- **Systems & Networking:** Active Directory, Group Policy (GPO), Windows Server, Linux (Red Hat/Kali), CCNA Level Networking, Firewalls (Palo Alto, FortiGate).

## SOFT SKILLS

- **Analytical:** Critical Thinking, Computational Thinking, Attention to Detail.
- **Communication:** Public Speaking, Technical Writing, Leadership & Team Management.
- **Efficiency:** Time & Stress Management, Adaptability, Continuous Self-Learning.

---

## CERTIFICATIONS & PROJECTS

### Professional Certifications:

- Cybersecurity Foundations — **Infosec**.
- Google Cybersecurity — **Google**.
- Information Technology — **Google**.
- Cybersecurity Certificate for Beginners — **MaharaTech (ITI)**.
- Junior Cybersecurity Analyst Career Path — **Cisco Networking Academy**.

**Technical Projects:**

- **Enterprise Security Simulation** (Offensive & Defensive): Designed and implemented a zoned network architecture (External, DMZ, Internal) using pfSense, Active Directory, and ELK Stack to simulate real-world attack and defense scenarios.
- Movie Market (**Web Application**): Developed a full-featured cinema booking platform using ASP.NET Core MVC and 3-Tier Architecture, focusing on SOLID principles and SQL Server database management.
- **SIEM & SOAR Home Lab**: Built a centralized security monitoring environment integrating ELK Stack with n8n for automated detection and response.
- Database Design & SQL Implementation: Engineered comprehensive ERD/EERD designs and transformed them into relational schemas for practical SQL applications.
- Programming Challenges & OOP Collection: Solved complex algorithmic challenges and developed mini-projects in C++ and C# to master object-oriented programming.
- Arduino Calculator: Designed and programmed an embedded system project using Arduino Uno to perform multi-functional calculations.

**Technical Articles & Labs:**

**Security Lab Notes:** Published technical walkthroughs and documentation for penetration testing labs and CTF challenges on Hashnode.

**Cybersecurity Blog:** Authored professional articles on Medium covering blue team investigations and threat hunting workflows.

---

## LANGUAGES

Arabic: Native, English: Very Good / Professional Working Proficiency