Abdelwahab Ahmed Shandy

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

SUMMARY

Abdelwahab Shandy is an Information Systems student with a strong passion for cybersecurity and software development , Driven by curiosity, he continually explores how technology works beneath the surface from defending systems and analyzing threats to building secure and efficient backend solutions , He has gained hands-on experience through national and institutional training programs in Security Operations (SOC), Penetration Testing, and .NET Development, and holds professional certifications from **Google**, **Cisco**, **TryHackMe**, **Infosec**, **ITI**, **NTI , CyberTalents** and **WE INNOVATE** , Abdelwahab believes in continuous learning, knowledge sharing, and collaboration, and is always eager to connect with professionals, contribute to real-world projects, and grow within the global tech and cybersecurity community.

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

Experience

On-Job Training (OJT) Trainee

ZeroSploit MEA · Training Program
Oct 2025 – Jul 2026 | Hybrid | El Agouza , Egypt
Selected as one of 15 trainees out of 400 total applicants from NTI graduates and the WE INNOVATE program
Completed General Track :

- Designed and implemented **end-to-end log ingestion pipelines** across Windows and Linux environments using **Winlogbeat, Filebeat, Fluent Bit, Logstash, and Elasticsearch**.
- Centralized Windows event logs using **Windows Event Forwarding (WEF)** with **WinRM / WS-Management**, optimizing delivery latency for SIEM use cases.
- Parsed and normalized **Linux authentication, syslog, and auditd (admin activity: create, delete, update)** logs and ingested them into Elasticsearch.
- Built **Elasticsearch Ingest Pipelines** (multi-processor) for data enrichment, normalization, and improved detection quality.
- Created **Kibana dashboards** to visualize security events and operational insights with before/after pipeline validation.
- Implemented **automated data retention enforcement** using **n8n + Elasticsearch**, including index size monitoring, conditional deletion, and email reporting.
- Developed **SOAR-style automations** with n8n:
  - Security awareness email automation from **CrowdStrike detections**, translated into user-friendly language using AI.
  - Vulnerability discovery and remediation workflow integrating **Nessus, AI agents, human approval gates, and MCP-based execution**.

Advanced to Specialized Tracks after passing General Track technical evaluation.

Specialized Hands-on Labs & Projects

- Autonomous vulnerability analysis and remediation with full auditability (Nessus + AI + n8n).
- Detection coverage mapping to **MITRE ATT&CK**, including rule feasibility validation against available telemetry.
- Active Directory attack simulation (Initial Access → Privilege Escalation → Credential Dumping → Lateral Movement) with **ELK-based detections written in Sigma**.
- **Web Server Troubleshooting** – Investigated Nginx connectivity issues on port 8000 without restarting services or modifying configurations; successfully retrieved HTML content using **curl**, demonstrating root-cause analysis and non-intrusive resolution skills.
- SIEM integrations and log forwarding (Palo Alto Firewall → Linux → Microsoft Sentinel).
- Advanced troubleshooting of network and service-level issues in constrained environments.

Penetration Testing Bootcamp

CyberTalents · Internship
Oct 2025 – Nov 2025 | Remote
Completed Phase 03 of the **ITI Universities Cybersecurity Training Program**, organized by **CyberTalents**. Focused on developing offensive security skills through practical labs, CTF-style challenges, and real-world exploitation scenarios.
Key Topics: Penetration Testing, Information Gathering, Vulnerability Assessment, Web Application Security, Exploitation, and Post-Exploitation.

SOC Engineering and Analysis Trainee

WE INNOVATE · Internship
Sep 2025 – Oct 2025 | Hybrid
Cybersecurity Boot Camp (in collaboration with WE, ITI, Zerosploit MEA , EG-CERT, NTRA , Xceed and NTRA):
SOC Engineering : SIEM deployment, configuration, log management, and automation(SOAR) .
SOC Analysis : Security monitoring, alert investigation, threat hunting, and incident triage.
Incident Response : Attack pattern analysis, data correlation, and reporting workflows.
Threat Intelligence : Real-world simulations, vulnerability management, and detection use cases.

Windows Server Administration Intern

National Telecommunication Institute (**NTI**) · Internship
Aug 2025 – Sep 2025 | Remote
120-hour Summer Training:
Soft Skills: communication, teamwork, business writing, freelancing basics.
Windows Server Administration: AD DS, Group Policy, DHCP, DNS, NLB, Failover Clustering, Disaster Recovery.

Networks Infrastructure Summer Bootcamp

Information Technology Institute (ITI) · Internship
Jun 2025 – Jul 2025 | Remote
120-hour Summer Training:
Completed Phase 02 of the **ITI Universities Cybersecurity Training Program**, organized by **ITI**. **Prerequisite :** Completing the Cybersecurity For Beginners Certification from MaharaTech – ITIMooca . **Covered Topics :** Computer Networks & Cloud, Routing & Switching , Cybersecurity Basics, Ethical Hacking , and HCCDA – Tech Essentials (Huawei Cloud Self-Study Course).

Backend Development Intern

EraaSoft · Internship
Nov 2024 – May 2025 | On-site | Giza, Egypt
Backend Development Track (C#/.NET):
C#, OOP, Intro SOLID Principles, LINQ, Entity Framework Core, SQL Server.
ASP.NET MVC architecture: building structured and maintainable backend applications.
After completing my course: I developed projects using a 3-tiered architecture to better organize code and implement practical OOP.

Programming Basics (Self-Study)

Programming Advices · Self-employed
Aug 2024 – Jul 2025 | Remote
Stage 1 : General programming, flowcharts, problem-solving techniques, C++ foundations
Stage 2 : Intermediate C++ algorithms, basic database concepts, SQL projects & practice

Network Security Intern (Summer Training Team Leader)

Information Technology Institute (ITI) · Internship
Aug 2023 | Remote
120-hour Summer Training:
Prerequisite: Completed Some courses on MaharaTech - ITIMooca platform
Topics: Computer Network Fundamentals, Advanced Networking (CCNA200-301), Cybersecurity Essentials, Intro to Ethical Hacking (CEH), Palo Alto Essentials (PCCET), FortiGate NSE4

SOC (Security Operations Center) Intern

AMIT Learning · Internship
Jun 2023 – Sep 2023 | Nasser City, Cairo, Egypt
Scored 100% on final assessment .
Courses & Workshops: Cybersecurity Fundamentals, Cybersecurity Operations Assistant, Intro Threat and Vulnerability Management, Security Operations and Monitoring, Threat Simulation, Introduction to Incident Response and Forensics, Introduction to Malware Analysis and Reverse Engineering, Introduction to QRadar and SOAR.

CERTIFICATIONS :

HCCDA - Tech Essentials	Huawei ICT Academy-Egypt | link	Jul 2025
Cybersecurity Certificate for beginners	MaharaTech - ITIMooca | link	Feb 2024
Cybersecurity Professional Certificate	Google Career Certificates | link	Jul 2023
Information Technology Professional Certificate	Google Career Certificates | link	Feb 2023
Cybersecurity Foundations	Infosec | link	Jul 2023

PROJECTS & TECHNICAL REPORTS

Movie Market (Web Application)

May 2025 – Jul 2025 | ASP.NET Core MVC | link

- Full-featured cinema ticket booking platform with admin panel, pricing control, and user reviews
- Implemented 3-Tier Architecture (**Presentation, BLL, DAL**)

Skills: ASP.NET Core, C#, OOP, MVC, SOLID Principles, Microsoft SQL Server, ER-Diagrams, Bootstrap, HTML5, CSS3

Arduino Calculator 4x4 Keypad LCD

May 2025 | University Project | link

- Built a simple calculator using Arduino Uno, 4x4 keypad, and I2C LCD
- Users can perform basic operations (+, -, *, /) and view results on LCD

Skills: Arduino, Embedded Programming, Logic Design

Database Design with ERD, EERD, Relational Schemas & SQL Implementation

Dec 2024 – Jan 2025 | link

- The project includes examples of how ERD and EERD designs are transformed into relational diagrams (relational diagrams) for students using SQL.

Skills: Microsoft SQL Server, ER-Diagrams, Relational Schema , SQL

OOP Mini Projects

Nov 2024 – Feb 2025 | link

- A collection of mini projects built using basic OOP concepts in C# and C++, designed to apply OOP principles to a practical context.

Skills: C++, C#, Object-Oriented Programming

Programming Challenges Multi Language

Jan 2024 – Jun 2025 | link

Curated collection of programming challenges solved in multiple languages

- **Skills:** Algorithms, C++, C#, OOP, Critical Thinking, Problem Solving

---

Technical Articles & Labs

- **Enterprise Offensive & Defensive Security Simulation | link**
  - **Designed and built a fully isolated enterprise-like network using zoned architecture (External, DMZ, Internal) with pfSense, Active Directory, SIEM (ELK/Wazuh), and SOAR automation.**
  - **I practice offensive tactics (pivoting, lateral movement, exploitation) and defensive tactics (central recording, detection, linking, and automatic response), and I'm still working on this lab.**

- **SIEM & SOAR Home Lab (Build & Detection) | Link**
- **Collection of CTF challenges, hands-on and cybersecurity articles | Link**
- **Cybersecurity Articles | Medium , Blog.**

SKILLS

❖ **Soft Skills:** Leadership, Public Speaking & Communication, Time Management & Analytical Thinking, Analytical Thinking, Computational Thinking & Problem Solving.

❖ Programming & Development:

✔ **Languages:** C++, C# , OOP
✔ **Database Design:** ERD, EERD, Relational Schemas, SQL Implementation
✔ ASP.NET Core , Entity Framework, LINQ
✔ Algorithms & Problem Solving , Flowchart Design
✔ **Version Control:** Git
✔ **Front-end basics:** HTML5, CSS3, Bootstrap

❖Cybersecurity & Network:

✔ Network Fundamentals (CCNA level)
✔ Linux & Windows OS knowledge
✔ Bash Scripting
✔ Cloud & Virtualization Concepts

LANGUAGES

ARABIC |ENGLISH