

MOHAMED SABRY

SOC Analyst | Blue Team | DFIR

+201144661053 | mohamedsabry01144@gmail.com | [LinkedIn](#) | [GitHub](#) | Egypt

PROFESSIONAL SUMMARY

SOC Tier 1 Analyst with hands-on experience in SIEM operations, alert triage, and incident response across Splunk, ELK, Wazuh, and Microsoft Sentinel environments. Skilled in IOC extraction, log analysis, and adversary behavior mapping using the MITRE ATT&CK framework. Practical background in digital forensics and incident response through structured internship programs. Currently reinforcing blue team expertise as a Cybersecurity Instructor. Seeking a SOC Analyst role to apply detection and response skills in a production security environment.

CORE COMPETENCIES

SIEM & Monitoring: Splunk, Elastic (ELK), Wazuh v4.14.4, Microsoft Sentinel, Alert Triage, Correlation Rules, False Positive Reduction

Incident Response: Triage Workflow, IOC Extraction, Containment Steps, Escalation Procedures, Incident Documentation

Threat Analysis: MITRE ATT&CK, STIX 2.1, Sigma Rules, Attack Timeline Building, VirusTotal, AbuseIPDB

Network & Endpoint: Wireshark, TCP/IP, Packet Analysis, Windows Event Logs, Linux, Endpoint Monitoring

Tools & Scripting: Python, ThreatScope, Autopsy 4.22.1, FTK Imager, Volatility, Hydra, VS Code, Git/GitHub

Digital Forensics: Disk Image Analysis, Malware Analysis, Evidence Handling, PCAP Analysis, Report Writing

Cloud & Identity Security: Microsoft Azure, Azure Active Directory, RBAC, Microsoft Defender for Endpoint, IAM

PROFESSIONAL EXPERIENCE

Zero2Aura | Cybersecurity Instructor & Founder *Oct 2025 – Present*

- Delivered SOC fundamentals training covering SIEM concepts, alert triage workflow, log analysis, and incident handling to entry-level cybersecurity learners
- Developed practical exercises and structured walkthroughs to build hands-on blue team investigation skills
- Founded Zero2Aura, a cybersecurity training and software services company offering courses, penetration testing, and web development

Digital Egypt Pioneers Initiative (DEPI) | Digital Forensics Investigator Intern *Nov 2025 – Present*

- Practiced digital forensics workflows through hands-on CTF challenges, TryHackMe labs, and scenario-based investigations
- Conducted network forensics analysis using Wireshark and Tshark — capturing, filtering, and dissecting packet captures to identify suspicious traffic patterns
- Performed disk and memory forensics using Autopsy, FTK Imager, and Volatility across evidence acquisition and artifact analysis scenarios
- Applied evidence handling and chain-of-custody documentation standards throughout structured investigation exercises

Digital Egypt Pioneers Initiative (DEPI) | Incident Response Analyst Intern *Oct 2024 – May 2025*

- Investigated security alerts and log data to identify Indicators of Compromise (IOCs) across simulated enterprise environments
- Executed structured incident response workflows covering detection, triage, containment, and documentation phases
- Analyzed security events using Wazuh SIEM, Splunk, and TryHackMe SOC lab environments
- Documented investigation findings and produced incident reports aligned with SOC operational standards

British University | Cybersecurity & Penetration Testing Training *Jul 2024*

- Completed intensive on-site training covering cybersecurity fundamentals, Linux and Windows OS administration, and networking concepts
- Gained hands-on experience in introductory penetration testing techniques including reconnaissance, vulnerability identification, and basic exploitation
- Practiced in live lab environments simulating real-world attack and defense scenarios

PROJECTS

SOC Lab — Automated Threat Detection & Incident Response *Mar 2026*

Hands-on SOC lab simulating real-world attack scenarios with full detection and incident response workflow.

- Executed 3 attack scenarios: SSH Brute Force (Hydra), PowerShell Fileless Attack (IEX), and Privilege Escalation via Sudo Abuse
- Deployed Wazuh SIEM v4.14.4 for real-time endpoint monitoring; detected 400+ security events across all scenarios
- Applied ThreatScope (custom Python engine) to analyze 17,000+ log lines using 144 detection rules

- Extracted 57+ IOCs and exported STIX 2.1 threat intelligence bundles
- Mapped all findings to 12 MITRE ATT&CK techniques across 6 tactics

Tools: Wazuh, ThreatScope, Hydra, MITRE ATT&CK, STIX 2.1, Ubuntu Server, Python

ThreatScope — Log Intelligence & Threat Detection Engine *Mar 2026 – Present*

Open-source Python-based SOC/DFIR tool for advanced log analysis and threat detection. Available on GitHub.

- 308 detection rules with 274 MITRE ATT&CK technique mappings covering all 14 tactics
- STIX 2.1 IOC export, Sigma rule support, and full JSON structured reporting
- Supports .log, .txt, .evtx, .csv, .json formats with 8-Tab Premium GUI and CLI Mode
- 35-rule correlation engine with Threat Score (0-100%), File Integrity Monitoring, and Rule Browser

Tools: Python, Sigma Rules, MITRE ATT&CK, STIX 2.1

Digital Forensics — Malware Disk Image Investigation *Mar 2026*

Static digital forensics investigation on a malware disk image (.img) using Autopsy 4.22.1.

- Identified JavaScript file masquerading as PDF via filename spoofing (MIME type: text/javascript)
- Discovered malware delivered inside ISO container to bypass Windows Mark-of-the-Web (MOTW) — T1553.005
- Detected multi-layer code obfuscation: hex encoding and character replacement to evade AV detection — T1027
- Identified WScript.CreateObject usage for system-level execution via Windows Script Host — T1059.007
- Uncovered likely Registry-based persistence mechanism via REG_SZ write — T1547

MITRE ATT&CK: T1566, T1027, T1059.007, T1547, T1553.005 | **Tools:** Autopsy 4.22.1, VS Code, Deobfuscator.io

CERTIFICATIONS & TRAINING

- Google Cybersecurity Professional Certificate (Coursera — Google)
- Microsoft Cybersecurity Analyst Professional Certificate (Coursera — Microsoft)
- Cisco Security Operations Center (Coursera — Cisco)
- SOC Level 1 (TryHackMe)
- Incident Handling & Response (MaharaTech — ITI MOOC)
- Junior Cybersecurity Analyst (Cisco NetAcad)
- CCNA 7 (Cisco NetAcad)
- Threat Intelligence 101 with Cisco Talos (Cisco NetAcad)
- Certified in Cybersecurity — CC (ISC2)

EDUCATION

Egyptian E-Learning University | BSc, Information Technology *2022 – 2026*

University of Tokyo | Data Science & AI Program — Matsuo-Iwasawa Lab *Apr 2026 – Jul 2026*

14-week intensive program covering Python, Machine Learning, SQL, time series analysis, and business analytics

LANGUAGES

Arabic (Native) | English (Professional Working Proficiency)