# SHADY EHAB ASSAD

JUNIOR SOC ANALYST (TIER 1 / L1)

*shady.ehab.assad@gmail.com*
*+974 66776962*
Doha, QA
linkedin.com/in/shady-ehab-07666a255
github.com/shady202


## Summary


Junior SOC Analyst (Tier 1/L1) with hands-on SOC experience monitoring SIEM and SOAR (Cortex XSOAR) for continuous alerting, Level 1 triage, incident response, and threat hunting. Skilled in log and packet analysis (Windows Event Logs, Sysmon, Wireshark/tcpdump), EDR telemetry, IOC enrichment, and mapping TTPs to MITRE ATT&CK to support investigations and playbook-driven containment. Practical experience with Splunk (SPL), basic scripting (Python, PowerShell, Bash), asset auditing, and compliance-ready incident documentation. Doha-based with valid QID; immediately available and comfortable with shift work.


## Work Experience

### SOC / IT Support Intern

Jan 2025 – May 2025

*Ali Bin Ali Technology Solutions (ABATS)*

- Monitored alerts and endpoint telemetry each shift using Cortex XSOAR and SIEM dashboards; performed Level 1 triage to assess priority and initial risk, and escalated confirmed incidents to senior analysts with enriched IOC evidence and contextual analysis to accelerate investigations and support containment/remediation.
- Built and executed Splunk SPL searches and correlation queries to validate detections; extracted source/destination IPs, file hashes, and user accounts and enriched indicators via VirusTotal and AbuseIPDB to inform root-cause investigations.
- Inspected Windows Event Logs, Sysmon, EDR telemetry and packet captures (Wireshark, tcpdump) to investigate anomalies across DNS, DHCP, SMTP and SMB; validated brute-force attempts, lateral movement, and suspicious process activity and supported directed threat-hunting tasks.
- Supported development and testing of SOAR playbooks and automated response steps using Cortex XSOAR and basic Python/PowerShell scripts to accelerate containment and evidence collection.
- Managed IT asset inventory with Lansweeper; audited Active Directory and Windows Server accounts and remediated permissions to enforce least privilege and reduce attack surface.
- Documented incidents in an ITSM ticketing system with timelines, triage steps, evidence chains and audit trails; prepared clear handoff notes to support senior analyst investigations and maintain compliance-ready records for internal investigations.

## Education

### Asia Pacific University of Technology and Innovation, Malaysia

Mar 2023 – May 2026

**Cyber Security** | Bachelor of Science (Honours)

GPA: 3.35 / 4.00

## Skills

**Security Operations**

SOC, cybersecurity operations, security monitoring, SIEM, Splunk Enterprise, Splunk SPL, Security Orchestration, Automation, and Response (SOAR), Cortex XSOAR, EDR, endpoint security, alert triage, incident management, incident response, threat intelligence, OSINT, threat hunting, log analysis, digital forensics, playbooks, MITRE ATT&CK, information security, IT security

**Networking and Systems**
Network fundamentals, TCP/IP, OSI model, DNS, DHCP, SMTP, SMB, network devices, network architecture, network security, firewalls, traffic logs, Wireshark, tcpdump, packet inspection, Nmap, operating systems (Windows, Windows Server, Ubuntu Linux, Kali Linux, Red Hat Enterprise Linux), Active Directory

**Scripting and Tools**
Python, TensorFlow, Git, Docker, Burp Suite, Metasploit, Nessus, Aircrack-ng, Cisco Packet Tracer, Lansweeper, Microsoft Office 365, Bash scripting

**Professional**
Written and verbal communication, critical thinking skills, analytical thinking, ability to multitask, accountability, accuracy, confidentiality, ethical conduct, timely resolution, attention to detail, working under pressure, motivated, enthusiasm for cybersecurity

## Project

### Blockchain E-Voting Platform
2026

- Built and tested Solidity smart contracts and Web3 interfaces for an Ethereum e-voting prototype; documented smart contract vulnerabilities and secure deployment practices.

### BlackCat/ALPHV Ransomware Case Study
2026

- Mapped observed TTPs to MITRE ATT&CK and reconstructed the attack chain from Sysmon, Windows Event Logs and Wireshark PCAP captures to identify foothold and lateral movement indicators.
- Drafted an incident response playbook covering containment, eradication and escalation for ransomware incidents.

### DMZ Security Gate Prototype
2026

- Applied security engineering and network architecture principles (DMZ, network partitioning, access control) on an Arduino IoT gateway to test perimeter defenses and attack surface; documented test cases and findings.

### Phishing URL Detection System
2025

- Built a Python/TensorFlow model to classify malicious links; engineered feature-extraction pipelines and tuned detection thresholds for deployment and evaluation.

### AI-Based Deepfake Detection for Bank Security
2025

- Developed CNN transfer-learning models in Python to detect deepfake videos for banking security; evaluated model performance and false-positive tradeoffs.

## Volunteer

### Volunteer Event Coordinator
May 2026 – May 2026

*Doha International Book Fair (35th Edition)*

- Coordinated volunteers and visitors for event operations.

## Certificates

**Implementing End-to-End Security Controls for Cloud and AI Workloads** 2026
Microsoft

**Certificate of Completion Intro to Splunk** May 2026
Splunk

**Deloitte Cybersecurity Job Simulation Certificate** Mar 2026
Deloitte

**International Battle of Hackers (IBOH)** Sep 2024
Asia Pacific University of Technology and Innovation (APU)

**Certificate Elite Security Operations Center (SOC)** Aug 2024
Tecforte

**CCNAv7 Switching, Routing, and Wireless Essentials Certificate** Aug 2024
Cisco Networking Academy

**CCNAv7 Introduction to Networks Certificate** Sep 2023
Cisco Networking Academy

## Languages

Arabic (Native), English (Fluent)