HISHAM ABOEL-NASR

CyberSecurity SOC Analyst

@ h.anb@outlook.com
Madison, WI https://my-soc-portfolio-v1.netlify.app/en in https://www.linkedin.com/in/hisham-aboel-nasr-0x00/

EXPERIENCE

CyberSecurity SOC Analyst

BlueSifr

SEP 2025 – Ongoing Madison, WI

- Monitor real-time alerts and analyze logs from firewalls, EDR, and network devices to detect suspicious activity
- Investigate and respond to security incidents following IR and escalation procedures

IT Engineer

AVASO TECHNOLOGY SOLUTIONS

MARCH 2025 – ongoing Madison, WI

- Troubleshoot employee issues with laptops or phones
- Perform Imaging and Refreshing for the devices, making sure that they are up-to-date with software installed and ready for work environment.

PC and Network Technician

AXIOM TECHNOLOGY

August 2024 – Augest 2025 Madison, WI

- install, upgrade, support and troubleshoot XP, Windows 7, Windows 8.1, Windows 10 and Microsoft Office 2010, Cisco Jabber, another authorized desktop application.
- Maintain ticket updates for all reported incidents.

PROJECTS

Wazuh, TheHive and Shuffle

NOV 2024

Wazuh detects threats and sends alerts to Shuffle (SOAR). Shuffle then enriches the data and automatically creates and triages a Case in TheHive

Lima Charlie EDR

Jun 2023

Crafted a detection & response (D&R) rule on Lime Charlie to detect and alert an attack that I made from kali Linux Using sliver C2 server.

Practical Projects for SOC Analyst Roles

Oct 2023 – Ongoing

I have more Projects on my Website at the header

CERTIFICATIONS

Security Plus (SY0-701)

Comptia

Certified Defensive Security Analyst

hackthebox

SKILLS

Python | Bash | Powershell

Triage and Alert Handling
Yara & Sigma Rules | NIST Frameworks
SIEM (Splunk ,ELK ,Wazuh) | IDs/IPs
Penetration testing | Digital Forensics
Vulnerability assessment
Network analysis (Wireshark,Suricata,Zeek)
Firewalls/ACLs | Real-time Monitoring
Incident Response | Endpoint Analysis
Security Incident Reporting
Microsoft-Entra (Azure)
Compliance: GDPR, HIPAA, PCI-DSS
Threat Hunting | Malware Analysis
Log Analysis/Log Management | SOAR

Critical thinking | Problem solving
Strong communication skills
Team Work and collaboration
Adaptability | Attention to detail

EDUCATION

B.S. in Telecommunication and Electronics Engineering

FUTURE UNIVERSITY IN EGYPT

Fall 2015– June 2020

Cybersecurity Intern

TREND MICRO

Jun 2021 — Aug 2021

- Penetration testing and Web testing security.