Hisham Aboel-Nasr

h.anb@outlook.com | +1-6083344485

OBJECTIVE

Highly motivated Junior SOC Analyst proficient in threat monitoring, incident detection, and log analysis, seeking to contribute to a real-time security operations team.

WORK EXPERIENCE

BLUESIFR | Soc Analyst

2025 SEP - till now | 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.

AVASO TECHNOLOGY SOLUTIONS | IT Engineer

2025 March - till now | Madison,WI

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

AXIOM TECHNOLOGY

PC and Network Technician job

2024 August - 2025 Augest | 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.

CERTIFICATIONS

COMPTIA | Comptia Security+ (SY0-701)

Jun 2024 | Madison,WI , US

CDSA | Certified Defensive Security Analyst From HackTheBox

NOV 2025 | Madison,WI , US

EDUCATION AND INTERNSHIPS

FUTURE UNIVERSITY IN EGYPT

Telecommunication and Electronics Engineering

Grad. June 2020 | Bachelor degree

TREND MICRO

| Cybersecurity Intern

Jun 2021 – Aug 2021 | Cairo, Egypt

- Penetration testing and Web testing security

PROJECTS

WAZUH , THEHIVE AND SHUFFLE

NOV 2024 | Madison, WI, USA

Alert pop up -> mimikatz usage detected and the soc analyst got an email for the attack details.

LIMA CHARLIE EDR

Jun 2023 | Online

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

PRACTICAL PROJECTS FOR SOC ANALYST ROLES

Oct 2023 | Madison,WI , US

- I have more Projects in my Website ,down below you will find my website

SKILLS

PROGRAMMING

• Python • JavaScript • Bash • Powershell

CYBERSECURITY

• SIEM (Splunk ,ELK ,Wazuh) • Phishing Campaigns • Penetration testing • Vulnerability assessment • Network analysis (Wireshark,Suricata,Zeek) • Web application security and testing • Real-time Monitoring • Firewall Configuration • Digital Forensics • Incident Response • Endpoint Analysis • IDs/IPs (snort) • Yara & Sigma Rules • Security Incident Reporting

IT

• Linux • Windows • Network Configuration •Technical Support
• Active Directory • System Administration • MS Office • Hardware • Service-Now (Ticketing system) • Microsoft-Entra (Azure)

SOFT SKILLS

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

LINKS

LinkedIn: Hesham-AboelNasr-linkedIn
My-Website: https://my-soc-portfolio-v1.netlify.app/en