MOHAMED SABER

SOC level 1

01225084795

mosaberpro2206165@gmail.com

LinkedIn

SUMMARY

1. Understanding Incident Response: Gain a clear understanding of what incident response entails, including the phases of preparation, detection, analysis, containment, eradication, recovery, and post-incident activities.
2. Building a Strong Foundation: Develop a solid foundation in computer science, networking, and cybersecurity fundamentals. This includes understanding how systems work, common security threats and vulnerabilities, and basic defensive techniques.

EDUCATION

2023 – 2024

pts and ejpt

Alexandria university

Cyber security
2022 – 2026

SKILLS

- PTS
- Python3
- c++
- c#
- linux
- Dart
- Flutter
- Java
- JFrame
- SQL

CERTIFICATIONS

- ECIR
- EJPT
- Flutter
- Linux admin

PROFESSIONAL EXPERIENCE

Flutter development

- Monitoring and Analysis: Security Analysts are responsible for monitoring security alerts and events generated by various security systems such as Intrusion Detection Systems (IDS), Security Information and Event Management (SIEM) systems, and firewalls. They analyze these alerts to determine their significance and potential impact on the organization's security.
- Incident Detection and Response: Security Analysts play a key role in detecting and responding to security incidents. They investigate suspicious activities, assess the scope and severity of incidents, and take appropriate actions to contain and mitigate security breaches.

SOC LEV 1

1. **Learn the Basics: Start by building a strong foundation in computer science, networking, and cybersecurity fundamentals. Understand how computers work, how data is transmitted over networks, and common security principles and concepts.**
2. **Gain Technical Skills: Develop practical skills in areas such as operating systems (e.g., Linux, Windows), networking protocols, web technologies (e.g., HTML, HTTP), scripting languages (e.g., Python, Bash), and cybersecurity tools (e.g., Nmap, Metasploit, Wireshark).**
3. **Learn about Penetration Testing: Familiarize yourself with the methodologies, techniques, and tools used in penetration testing. Understand the phases of a penetration test, including reconnaissance, enumeration, vulnerability scanning, exploitation, and post-exploitation.**
4. **Practice Ethical Hacking: Set up a lab environment where you can safely practice hacking techniques and tools. Experiment with different attack scenarios and learn how to exploit common vulnerabilities such as SQL injection, cross-site scripting (XSS), and buffer overflows.**
5.