How to be A Soc Analyst

Skills
Certificates
Experience
Beyond..

Muhammad Eissa

What skills do I need ?

- Analytical mindset is a Must.
- Network Knowledge / experience.
- System Knowledge (windows & Linux).
- Security Knowledge / experience.
- SIEM Knowledge / experience.
- Ethical Hacienda knowledge / experience.
- Imagination for simulation.
- Programming / Scripting.
- Communication skills.
- IT Operation is a must have skill.

What will I do ?

- A lot of monitoring, monitoring and monitoring
- Investigation over and over.
- Reports making and tuning.
- Keep an eye for suspicious activity (not just monitoring).
- Have your tools always ready for the investigation such as Virustotal,anyrun, ibm xforce, shodan, many many more.
- Shifts 24/7 working.
- Document incidents and investigations.
- responsible for reviewing alerts, the evaluation of its urgency and relevancy.
-

What Certificate do I need ?

- Qualification are the major but certificates endures them.
- CCNA. Network Understanding is must
- Security+ & CCNA Security. Network Security is must
- MCSA for Windows Server Administration. System understating is must
- CCNA Cyber OPS.
- SANS GCIH.
- CEH. Attucks understanding and how to defend them is must.

What are SOC Roles ?

- Tire 1 or level 1 SOC Analyst.
- Tire 2 or level 2 SOC Analyst.
- Tire 3 or level 3 SOC Analyst. (Expert Level Focused)
- SIEM Admin.
- SOC Manager.

Summary

- This Video include my personal opinion for SOC candidates based on my experience.
- The conditions are different from environment to another.
- Hope you all the success and bright future in your career.