ROADMAP
to SOC analyst career path

Here is a clear roadmap for a SOC Analyst career path, outlining key stages from entry-level roles to advanced positions such as a SOC Manager. Each stage highlights necessary skills, certifications, and experience, providing a comprehensive guide for career progression in cybersecurity.

01
- Understand the role and responsibility of a SOC analyst

02
Get the right education:
- Degree
- Certifications
- Soft skills and analytics
- Basic IT and cybersecurity skills

03
Gain hands-on experience:
- Internships
- Home labs
- Capture the Flag challenges
- Open-source projects

04
Learn about various security tools:
- SIEM
- IDS/IPS
- EDR
- Firewall and network traffic analyzer

05
Stay updated on cybersecurity trends:
- Follow cybersecurity blogs, forums, and podcasts.
- Join cybersecurity communities (Reddit, LinkedIn, Discord).
- Keep up with the latest tools, frameworks, and attack techniques.

06
Apply for entry level SOC positions, such as:
- Junior SOC Analyst
- SOC Analyst I
- Security Analyst
- Incident Responder

07
- Gain experience, build strong skills, and broaden your scope.

08
Earn more relevant certifications:
- CISM, CISSP
- GSOC, GCIH, ITIL Foundation

09
- Gain experience on incident response, compliance, and crisis management

10
- Pursue leadership roles such as SOC team lead.

11
- Build a strong network and gain experience with SOC operations, leadership roles, and successful incident response.

12
- Apply for SOC manager position

13
Continue professional development:
- Attend conferences like Black Hat, DEFCON, and RSA to stay on top of trends and gain insights into leading security teams.
- Consider taking courses in leadership, management, and business strategy.
- As you gain more experience, begin coaching new analysts and other leaders to strengthen your leadership position in the cybersecurity community.