SOC ANALYST ROADMAP

A SOC role is often the doorway into cybersecurity.

Phase 1 — Build the Foundation (0–2 Months)

Learn Core IT & Networking

You cannot defend what you don't understand.

Focus on:

- IP addresses
- DNS
- VPNs
- Firewalls
- TCP/UDP
- HTTP/HTTPS
- Active Directory basics
- Linux + Windows fundamentals

Goal:

Be able to explain:

- How devices communicate

- What “normal” traffic looks like
- What suspicious behavior might look like

Recommended Beginner Certs

- CompTIA A+ (optional if brand new to IT)
- CompTIA Network+
- CompTIA Security+

Security+ is the best starting point for SOC.

Phase 2 — Understand Security Fundamentals (2–4 Months)

Learn:

- CIA Triad
- Authentication & authorization
- Least privilege
- Zero Trust
- Common attack types:
    - phishing
    - malware
    - ransomware
    - brute force
    - privilege escalation

Learn Security Tools

High level understanding of:

- SIEM
- EDR/XDR
- IDS/IPS
- Vulnerability scanners
- Email security tools

Important Concepts

- Logs
- Alerts
- Indicators of compromise (IOCs)
- Incident response lifecycle
- MITRE ATT&CK framework

Phase 3 — Learn SOC Operations (4–6 Months)

Learn What SOC Analysts Actually Do

Daily responsibilities:

- Monitor alerts
- Investigate suspicious activity
- Escalate incidents
- Write incident notes
- Review logs
- Triage phishing emails
- Validate false positives
- Follow playbooks/runbooks

Learn SIEM Platforms

Popular examples:

- Splunk
- Microsoft Sentinel
- IBM QRadar

Practice:

- Searching logs
- Creating detections
- Investigating failed logins
- Identifying suspicious PowerShell commands

Phase 4 — Hands-On Labs (Critical)

This is where students become employable.

Build a Home Lab

Use:

- VirtualBox or VMware
- Windows VM
- Linux VM
- Kali Linux

Practice:

- Reading logs
- Simulating attacks
- Using Wireshark
- Basic incident investigations

Platforms for Practice

- TryHackMe
- Hack The Box
- LetsDefend
- Blue Team Labs Online

LetsDefend is especially good for SOC simulation practice.

Phase 5 — Build Resume Experience (6–9 Months)

Projects Matter

Examples:

- Built a home SOC lab
- Investigated phishing simulations

- Configured Splunk dashboards
- Created incident response reports
- Monitored Windows event logs
- Performed malware traffic analysis with Wireshark

Learn Basic Scripting

Very helpful:

- Python
- PowerShell
- Bash

(Not to become a developer but to automate simple tasks and understand attacker behavior)

Phase 6 — Apply for Entry-Level Roles

Common Titles

- SOC Analyst I
- Cybersecurity Analyst
- Security Monitoring Analyst
- Incident Response Analyst
- Blue Team Analyst

Skills Employers Want

- Communication
- Documentation
- Critical thinking
- Curiosity
- Calmness under pressure

Technical skills can be taught.
Strong analytical thinking and consistency matter a lot.

Interested in becoming a SOC Analyst or starting your cybersecurity journey? I help students understand the roadmap, build the right skills, and create a realistic path into the industry through mentorship, guidance, and hands-on learning. To get started or learn more, reach out to me at CloudConfidenceHQ@gmail.com.