3-Month SOC Analyst Hands-On Roadmap

This 3-month intensive plan helps you gain practical SOC Analyst experience with guided labs, SIEM practice, and a portfolio of real investigations. Estimated time: 10–12 hours/week.

Month 1 – Foundations & Core SOC Labs

Week	Platform & Focus	Key Tasks	Portfolio Output
1	LetsDefend – SOC Analyst Path	Complete: Intro to SOC, Phishing Email Analysis, Alert Triage, Log Analysis	Screenshots & notes from Investigation modules
2	TryHackMe – SOC Level 1 Path	Rooms: Intro to SOC, Splunk Basics, Windows Event Logs, Network Traffic Analysis	Splunk dashboard screenshots
3	Blue Team Labs Online	Solve 3 beginner Investigations (log triage, phishing, brute force)	Write-ups
4	RangeForce Community Edition	SOC Fundamentals modules (SIEM basics, detection)	Completion badge

Month 2 – SIEM Skills & Threat Hunting

Week	Platform & Focus	Key Tasks	Portfolio Output
1	Splunk Free/Trial	Install Splunk, ingest sample logs. Create dashboards for failed logins.	Splunk dashboard screenshots
2	Splunk Boss of the SOC (BOTS)	Complete beginner BOTS challenge. Practice SPL queries.	SPL queries + PDF report
3	CyberDefenders	Challenges: Brute Force, Phishing, Malware Traffic	Case write-ups
4	Elastic Security (ELK)	Set up Elastic SIEM or use cloud trial. Run detection queries on sample dataset.	Saved Kibana queries + dashboards

Month 3 – Realistic Incidents & Home SOC Setup

Week	Platform & Focus	Key Tasks	Portfolio Output
1	LetsDefend – Malware Analysis Basics	Analyze a malicious document or phishing attack.	SOC report
2	Hack The Box – SOC Labs (Beginner Tier)	Investigate live incidents using SIEM/EDR tools.	Investigation report
3	DetectionLab or Security Onion (VM)	Deploy VM lab + Splunk/ELK + Kali in VMware. Simulate attacks, detect them.	Network diagram + detection screenshots
4	Portfolio Polish & Job Prep	Organize all case studies, dashboards, and lab documentation.	Publish portfolio into GitHub/Notion

Outcome after 3 Months: A portfolio of 15+ completed investigations, Splunk/Elastic dashboards, and optionally your own SOC Lab demo — ready for SOC Analyst job applications.