# 3-Month SOC Analyst Hands-On Roadmap

This roadmap provides a clear 3-month plan to gain practical SOC Analyst experience. It combines guided labs, SIEM practice, and real-world investigations. Recommended pace: **10–12 hours per week**.

## Month 1 – Foundations & Core SOC Labs

• **Week 1:** LetsDefend – SOC Analyst Path → Complete Intro to SOC, Phishing Email Analysis, Alert Triage, Log Analysis modules.
• **Week 2:** TryHackMe – SOC Level 1 Path → Rooms: Intro to SOC, Splunk Basics, Windows Event Logs, Network Traffic Analysis.
• **Week 3:** Blue Team Labs Online → Solve 3 beginner Investigations (log triage, phishing, brute force).
• **Week 4:** RangeForce Community Edition → SOC Fundamentals modules (SIEM basics, detection).

**Goal:** Finish at least 8 guided investigations and document screenshots/notes.

## Month 2 – SIEM Skills & Threat Hunting

• **Week 1:** Splunk Free/Trial → Install Splunk, ingest sample logs, create dashboard detecting failed logins.
• **Week 2:** Splunk Boss of the SOC (BOTS) → Complete beginner challenge, practice SPL queries, write incident report.
• **Week 3:** CyberDefenders → Challenges: Brute Force, Phishing, Malware Traffic.
• **Week 4:** Elastic Security (ELK) → Set up Elastic SIEM or use cloud trial. Run detection queries on sample dataset.

**Goal:** Build a Splunk dashboard and complete at least 3 CyberDefenders cases with documented reports.

## Month 3 – Realistic Incidents & Home SOC Setup

• **Week 1:** LetsDefend – Malware Analysis Basics → Analyze malicious document or phishing attack and create IOC report.
• **Week 2:** Hack The Box – SOC Labs (Beginner Tier) → Investigate live incidents using SIEM/EDR environment.
• **Week 3:** DetectionLab or Security Onion → Deploy Windows + Splunk/ELK + Kali in VM. Simulate attacks and detect them.
• **Week 4:** Portfolio Polish & Job Prep → Organize case studies, dashboards, and lab documentation into GitHub/Notion. Draft a SOC-focused resume.

**Goal:** Complete at least 15 investigations, create Splunk/Elastic dashboards, and showcase a functioning home SOC lab (optional).

**Final Outcome:**
• A portfolio of 15+ completed investigations and case studies.
• Splunk/Elastic dashboards demonstrating SIEM skills.
• Optional home SOC lab setup for interviews.
• Ready to apply for SOC Analyst (Tier 1) or SOC Intern roles.