■■ SOC Analyst 3-Month Daily Roadmap (5 Hrs/Day)

■ Month 1 – Foundations (Networking, Linux, Security Basics)
■ Goal: Build strong IT + cybersecurity fundamentals.

Week 1 – Networking Basics
Day 1–2: Learn OSI model, TCP/IP, ports & protocols (HTTP, DNS, SMTP, FTP, SSH)
Day 3: Study firewalls, VPNs, IDS/IPS basics
Day 4: Packet analysis intro with Wireshark (capture HTTP/HTTPS traffic)
Day 5: Networking lab (ping, traceroute, netstat, nmap basics)
Day 6: Review & practice (quiz + flashcards)
Day 7: Write a 1-page summary of what you learned (portfolio start)

Week 2 – Linux & Windows Basics
Day 8–9: Linux commands (file system, grep, find, ps, chmod, networking tools)
Day 10: User management & permissions
Day 11: Windows basics (Event Viewer, PowerShell, Task Manager, registry)
Day 12: Practice lab: set up Ubuntu + Windows VM
Day 13: Simulate login attempts, check logs in Linux & Windows
Day 14: Document commands + screenshots in portfolio

Week 3 – Cybersecurity Fundamentals (Security+)
Day 15: CIA triad, threats, malware types
Day 16: Phishing, ransomware, DDoS, SQL injection basics
Day 17: Authentication methods (MFA, Kerberos, SAML, OAuth)
Day 18: Risk management (vulnerabilities, exploits, mitigation)
Day 19: Incident response lifecycle (NIST framework)
Day 20: Review with flashcards (Quizlet/Anki)
Day 21: Lab: Simulate brute-force login, detect in logs

Week 4 – Intro to SOC & Tools
Day 22: What is a SOC? Roles (Tier 1–3 analysts)
Day 23: SIEM introduction (Splunk, ELK, QRadar)
Day 24: Install Splunk free edition, add test logs
Day 25: Splunk queries (SPL basics)
Day 26: SIEM use cases (failed logins, suspicious IPs)
Day 27: TryHackMe “SOC Fundamentals” module
Day 28: Document findings in portfolio

■ Month 2 – SOC Skills & Hands-On Practice
■ Goal: Learn SOC workflows + SIEM tools + detection skills.

Week 5 – SIEM & Log Analysis
Day 29: Splunk hands-on (indexing logs, search queries)
Day 30: Detect brute force attempts with Splunk
Day 31: Install ELK Stack (Elasticsearch, Kibana, Logstash)
Day 32: Practice queries in Kibana
Day 33: Compare Splunk vs ELK usage
Day 34: Blue Team Labs (basic log challenges)
Day 35: Document a SOC investigation case

Week 6 – Threats & Detection
Day 36: Malware types (worms, trojans, spyware)

Day 37: Common attacker techniques (MITRE ATT&CK; basics)
Day 38: Hands-on: detect port scan logs with SIEM
Day 39: Detect phishing attempts with SIEM (email logs)
Day 40: Detect privilege escalation attempts
Day 41: TryHackMe “SOC Level 1 – Threat Intelligence”
Day 42: Write report: “How I detected suspicious activity with Splunk”

Week 7 – Incident Response
Day 43: Phases of incident response (Preparation → Detection → Containment → Eradication → Recovery → Lessons)
Day 44: Hands-on: Investigate brute force → block IP → report
Day 45: Case study: WannaCry ransomware attack
Day 46: TryHackMe “Blue Team Fundamentals”
Day 47: Write mock incident report (Tier 1 SOC report style)
Day 48: Review & quizzes
Day 49: Portfolio update (include reports + screenshots)

Week 8 – Real SOC Workflows
Day 50: Learn ticketing systems (Jira, ServiceNow basics)
Day 51: Escalation process (Tier 1 → Tier 2 → Tier 3)
Day 52: Detect insider threats with SIEM logs
Day 53: Threat intelligence feeds (AlienVault OTX, AbuseIPDB)
Day 54: TryHackMe “Security Operations” module
Day 55: Blue Team Labs (phishing + malware detection)
Day 56: Review & create SOC analyst cheat sheet

■ Month 3 – Advanced Practice & Job Prep
■ Goal: Master SOC workflows, build portfolio, prepare for interviews.

Week 9 – Threat Hunting Basics
Day 57: Intro to threat hunting vs monitoring
Day 58: MITRE ATT&CK; framework deep dive
Day 59: Use ATT&CK; to map detection techniques in Splunk
Day 60: Detect persistence techniques (scheduled tasks, registry changes)
Day 61: Detect lateral movement attempts (SMB, RDP logs)
Day 62: TryHackMe “Threat Hunting” room
Day 63: Portfolio update

Week 10 – Forensics & Malware Basics
Day 64: Digital forensics basics (disk, memory, network)
Day 65: Tools (Autopsy, Volatility framework basics)
Day 66: Simple memory analysis lab (detect malicious process)
Day 67: Malware sandbox basics (Any.Run demo)
Day 68: TryHackMe “Intro to Malware Analysis”
Day 69: Document findings in portfolio
Day 70: Review

Week 11 – Mock SOC Environment
Day 71: Set up SIEM + simulated attacks (Metasploitable VM)
Day 72: Detect brute force → investigate logs
Day 73: Detect phishing email attack
Day 74: Detect data exfiltration attempt
Day 75: Create incident reports for all 3 cases
Day 76: TryHackMe “Blue Team SOC Level 1 Final”
Day 77: Portfolio update

Week 12 – Job Preparation & Applications
Day 78: Build SOC Analyst resume (highlight labs + skills)
Day 79: Create LinkedIn profile (connect with cybersecurity pros)
Day 80: Write SOC-specific GitHub/blog posts
Day 81: Practice SOC interview questions (technical + scenario-based)
Day 82: Apply for entry-level SOC Analyst jobs
Day 83: Mock interview with a friend/mentor
Day 84: Final review of tools (Splunk, ELK, Wireshark, TryHackMe reports)
Day 85–90: Continue applications + practice while waiting for responses