Security Analyst Roadmap

A structured roadmap for **Security Analysis** (from beginner to advanced) should cover foundational cybersecurity concepts, tools, methodologies, and advanced threat-hunting techniques. Since you're also diving into **malware development and analysis**, this roadmap will incorporate **reverse engineering** and **malware forensics** to align with your **SOC role**.

Beginner Level (0-6 Months)

1. Cybersecurity Fundamentals

- Learn about **CIA Triad** (Confidentiality, Integrity, Availability).
- Understand basic security concepts: **authentication, authorization, encryption, hashing**.
- Study **OWASP Top 10** vulnerabilities (SQL Injection, XSS, etc.).
- Explore **Common Attack Vectors** (phishing, malware, DoS, insider threats).

2. Networking & Protocols

- Understand **OSI Model, TCP/IP, HTTP/S, DNS, ARP, ICMP**.
- Learn how to use **Wireshark** to analyze network packets.
- Understand **VPNs, Proxies, Firewalls, IDS/IPS** (Snort, Suricata).

3. Linux & Windows Security

- Learn **Linux command line (bash, cronjobs, log analysis: `/var/log` files)**.
- Windows security essentials: **Event Viewer, PowerShell, Group Policy, Sysmon**.
- **Active Directory Basics**: Authentication, Kerberos, NTLM, LDAP.

4. Security Tools & SIEM Basics

- Learn **SIEM (Security Information & Event Management)**:
  - ELK Stack (Elasticsearch, Logstash, Kibana).
  - Splunk (Logs, Alerts, Dashboards).
  - Microsoft Sentinel (for Azure environments).
- Master **basic log analysis** for incident detection.

Intermediate Level (6-12 Months)

5. Threat Intelligence & Malware Analysis

- Learn **Indicators of Compromise (IoCs)**.
- Understand **Cyber Kill Chain & MITRE ATT&CK Framework**.
- Begin **Static & Dynamic Malware Analysis** using:
  - **Static Analysis**: Strings, PE structure, dependencies.
  - **Dynamic Analysis**: Running malware in a controlled environment (Cuckoo Sandbox, Remnux).

6. Reverse Engineering & Exploit Development

- Learn **x86/x64 Assembly Language**.
- Understand **Windows Internals (Processes, Threads, Handles, Memory Layout)**.
- Reverse malware using **IDA Pro, Ghidra, Radare2**.
- Analyze memory dumps with **Volatility**.

7. Web & Application Security

- Deep dive into **SQL Injection, XSS, CSRF, SSRF, IDOR, RCE**.
- Learn **Burp Suite, ZAP Proxy, Postman** for API security testing.
- Practice **bug bounty hunting** (HackerOne, Bugcrowd, Open Bug Bounty).

8. Digital Forensics & Incident Response (DFIR)

- Memory Forensics (Volatility, Rekall).
- Disk Forensics (Autopsy, FTK Imager).
- Network Forensics (Wireshark, Zeek).

Advanced Level (12-24 Months)

9. Advanced Threat Hunting & SOC Operations

- Master **TTPs (Tactics, Techniques, Procedures)** from APT groups.
- Conduct **Threat Hunting** with YARA & Sigma rules.
- Create custom **Splunk SPL queries & SIEM alerts**.

10. Advanced Malware Development & Evasion Techniques

- Develop **custom malware** (C/C++, Python, Assembly).
- Learn **Shellcode Injection, Process Hollowing, DLL Injection**.
- Use **Metasploit, Cobalt Strike, Empire, Sliver** for Red Team tactics.
- Study **Bypassing AV/EDR** techniques (packing, encryption, obfuscation).

11. Red Team vs Blue Team Simulations

- Understand **Red Team (offensive)** vs. **Blue Team (defensive)** methodologies.
- Conduct **Purple Team exercises** for practical experience.
- Use **MITRE CALDERA** for automated attack emulation.

12. Cloud Security & DevSecOps

- Learn **AWS Security (IAM, KMS, Security Groups, GuardDuty)**.
- Understand **Azure Security (Sentinel, Defender, Key Vault, RBAC)**.
- Implement **CI/CD Security (Code Scanning, SAST, DAST, IAC Security)**.

Certifications (Optional but Helpful)

Beginner

 CompTIA Security+ – General security basics
 CCNA CyberOps – Network security & monitoring

Intermediate

 Certified SOC Analyst (CSA) – SOC operations
 GIAC GCFA (Forensic Analyst) – Incident response

Advanced

 OSCP (Offensive Security Certified Professional) – Ethical hacking & exploitation
 GREM (GIAC Reverse Engineering Malware) – Malware & reverse engineering
 CISSP (Certified Information Systems Security Professional) – Advanced security management

---

Practical Hands-On Labs

- **TryHackMe** & **Hack The Box** for practical security challenges.
- **Malware Analysis Labs** (FireEye FLARE VM, Remnux, Any.Run).
- **Blue Team Labs Online** for SOC & SIEM training.

This roadmap aligns well with **your SOC role and malware analysis learning** while gradually progressing into **advanced security operations, threat hunting, and malware forensics**.

Would you like me to refine this further based on your immediate learning goals?