INFOSECTRAIN

Exploring

SOC Career Pathways

(Security Operations Center)

2025

1. Entry-Level Roles

Job Title	Description	Skills Needed
SOC Analyst L1 (Tier 1)	Monitors alerts, triages events, and escalates incidents for further investigation.	Basic networking, SIEM tools, log analysis.
Security Monitoring Analyst	Focuses on real-time monitoring of security events and generating reports.	Knowledge of monitoring tools, basic IT skills.
Incident Response Technician	Provides first-level response during security incidents and escalates critical issues.	Understanding of incident handling and playbooks.

2. Mid-Level Roles

Job Title	Description	Skills Needed
SOC Analyst L2 (Tier 2)	Investigates escalated incidents, performs root cause analysis, & takes response actions.	Threat analysis, incident handling, advanced SIEM skills.
Threat Intelligence Analyst	Collects and analyzes threat data to anticipate and mitigate cyber risks.	Knowledge of IoCs, threat intelligence platforms.
Forensic Analyst	Conducts digital forensics investigations to uncover evidence during incidents or breaches.	Experience with forensic tools (FTK, EnCase).
Vulnerability Analyst	Identifies and prioritizes system vulnerabilities to help prevent attacks.	Vulnerability scanning tools (Nessus, Qualys).
Incident Response Analyst	Handles active incidents, coordinates containment efforts, and drafts post-incident reports.	Strong incident response experience.

3. Advanced Roles

Job Title	Description	Skills Needed
SOC Analyst L3 (Tier 3)	Performs advanced threat hunting, malware analysis, and develops detection rules.	Expert SIEM usage, malware analysis, threat hunting.
Threat Hunter	Proactively identifies undetected threats using behavioral analytics and anomaly detection techniques.	MITRE ATT&CK framework, anomaly detection.
Malware Analyst	Specializes in reverse-engineering malware to understand its behavior and develop countermeasures.	Reverse engineering, tools like Ghidra, IDA Pro.
SOC Team Lead	Manages and guides the SOC team while ensuring operational efficiency.	Leadership, SOC workflow expertise.

4. Management and Leadership Roles

Job Title	Description	Skills Needed
SOC Manager	Oversees SOC operations, manages teams, and ensures alignment with organizational goals.	Strategic planning, team leadership, incident oversight.
Incident Response Manager	Leads and coordinates response to major incidents, ensuring effective containment and recovery.	Crisis management, communication, incident strategy.
Cybersecurity Operations Director	Responsible for overall security operations and strategy, including SOC and threat management programs.	Executive leadership, strategic security planning.

5. Specialized Roles

Job Title	Description	Skills Needed
SIEM Engineer	Configures and maintains SIEM platforms, develops correlation rules, and tunes alerts.	SIEM architecture, scripting (Python, Regex).
Automation/SOAR Engineer	Implements security orchestration and automation workflows to enhance SOC efficiency.	SOAR tools (Splunk Phantom, Demisto), Python.
Cloud Security Analyst	Focuses on securing cloud environments and monitoring cloud-specific threats.	AWS/Azure/GCP security, cloud monitoring tools.
Red Team Analyst	Simulates attacks to identify weaknesses in SOC defenses.	Ethical hacking, penetration testing skills.
Blue Team Specialist	Defends against attacks by improving detection and response capabilities.	Defensive strategies, SIEM/EDR usage.

6. Emerging Roles

Job Title	Description	Skills Needed
AI/ML Security Specialist	Leverages AI/ML to improve threat detection and incident response capabilities.	Data science, AI/ML tools, cybersecurity expertise.
IoT Security Analyst	Secures Internet of Things (IoT) devices and identifies vulnerabilities in connected systems.	IoT protocols, device security knowledge.
Cyber Threat Researcher	Focuses on researching new attack vectors, TTPs, and creating innovative defensive techniques.	Research skills, threat intelligence expertise.