# **Module 1: Network & Cybersecurity Fundamentals**

**1. Basic IT Knowledge:**

**Operating Systems:**

* + Basic functionalities of Windows, Linux.

**IT Infrastructure:**

* + Familiarity with servers, databases, firewalls, routers, switches

**2. Networking Concepts:**

**Introduction to Networking:**

* + What is a network?
  + Benefits of networking
  + Types of networks (LAN, MAN, WAN)
  + Network topologies (bus, star, ring, mesh, hybrid)

**Network Components:**

* + Nodes (computers, servers, printers, etc.)
  + Network devices (hubs, switches, routers, modems)
  + Network media (wired, wireless)

**Network Protocols:**

* + Definition of protocols
  + TCP/IP protocol suite
  + OSI model (overview)
  + Common network protocols (HTTP, FTP, SMTP, DNS)

**Network Addressing:**

* + IP addresses (IPv4, IPv6)
  + Subnetting
  + DHCP
  + DNS

**Network Security:**

* + Threats to network security
  + Security measures (firewalls, encryption, antivirus)

**Network Troubleshooting:**

* + Common network problems
  + Troubleshooting techniques
  + Network diagnostic tools

**Additional Topics (Optional):**

* + Cloud computing and networking
  + Network virtualization
  + Network performance metrics

**3. Cybersecurity Fundamentals:**

**Introduction to Cybersecurity:**

* + Definition and significance
  + Key terms and concepts (threat, vulnerability, risk)

**Common Cyber Threats:**

* + Types of malwares (virus, worm, Trojan, ransomware)
  + Phishing attacks
  + Insider threats

**4. Security Principles:**

**CIA Triad:**

* + Confidentiality, Integrity, Availability

**Security Models and Frameworks:**

* + Principles of least privilege, defense in depth
  + Common security frameworks (NIST, ISO/IEC 27001)

**Security Policies and Procedures:**

* + Importance and implementation
  + Regular policy reviews and updates

**5. Understanding Threats and Vulnerabilities:**

**Types of Cyber Threats:**

* + Detailed exploration of malware, phishing, insider threats

**Common Vulnerabilities:**

* + Unpatched software
  + Misconfigurations

**Threat Modeling and Vulnerability Assessment:**

* + Basics and methodologies

# **Module 2: Advanced Cybersecurity and SOC Analyst Skills**

**6. Logs and Event Data:**

**Introduction to Logs:**

* + Importance in cybersecurity
  + Types of logs (system, application, security)

**Log Analysis**

* + Basic techniques and tools
  + Identifying anomalies and patterns

**7. Incident Response Basics**

**Understanding Security Incidents**

* + Definition and types of incidents

**Incident Response Process**

* + Steps: Preparation, Identification, Containment, Eradication, Recovery, Lessons Learned
  + Importance of an incident response plan

**8. Introduction to SIEM**

**What is SIEM?**

* + Definition and purpose
  + Role in a SOC

**Basic Functions of SIEM**

* + Log collection
  + Correlation and alerting

**9. Security Tools**

**Overview of Security Tools**

* + Antivirus, firewalls, IDS/IPS, EDR
  + Basic functionalities and use cases

**Staying Updated with Tools**

* + Importance of learning the latest tools and technologies

**10. Soft Skills for SOC Analysts**

**Communication Skills**

* + Importance in teamwork and incident handling

**Critical Thinking and Problem-Solving**

* + Applying logical approaches to troubleshooting

**Continuous Learning and Adaptability**

* + Keeping up with evolving cyber threats

**11. Certifications and Training**

**Relevant Certifications**

* + CompTIA Security+, CEH, CISSP

**Hands-On Training**

* + Importance of labs and practical exercises

**Learning Resources**

* + Books, online courses, forums