Understanding Cisco Cybersecurity Operations Fundamentals (CPLL-CCNACBR)

Duration: 180 Days

The Understanding Cisco Cybersecurity Operations Fundamentals (CCNACBR) Learning Path provides an understanding of the network infrastructure devices, operations, and vulnerabilities of the TCP/IP protocol suite, and basic information security concepts, common network application operations and attacks, the Windows and Linux operating systems, and the types of data that are used to investigate security incidents. After completing this Learning Path, you will have the basic knowledge required to perform the job role of an associate-level cybersecurity analyst in a threat-centric security operations center (SOC).

This Learning Path prepares you for the 200-201 CCNACBR v1.2 exam. If passed, you earn the Cisco Certified Network Professional (CCNA) Cybersecurity certification and the role of a junior or entry-level cybersecurity operations analyst in a SOC.

Skills You'll Learn:

- Gain an understanding and follow established security procedures for response to alerts converted to incidents
- Learn about different models for incident investigations and response
- Discover how to identify common attack vectors, malicious activities, and suspicious behaviors

Learning Path Objectives:

1. Cybersecurity Foundations: Establish core security operations knowledge, including SOC roles, types, and metrics; security principles and risk management; access control models; cloud security and shared responsibility; and cryptography fundamentals.
2. Endpoint Systems: Build the operating system literacy required for security analysis, covering Windows and Linux architecture, file systems, permissions, processes, and the command-line interfaces (cmd.exe, PowerShell, Bash) used in security tasks.
3. Network Controls: Examine network protocols and their security implications, plus the controls that protect infrastructure, including ACLs, NAT/PAT, WAFs, IDS/IPS, and endpoint security solutions (host firewalls, AV/AM, EPP/EDR, MDM).
4. Threat Landscape: Develop the ability to identify and analyze adversaries through threat actor profiling, the Cyber Kill Chain, the MITRE ATT&CK Framework, social engineering (generative-AI-enhanced attacks), network attack fundamentals, and advanced/emerging threats.

5. Security Analytics: Focus on the data and analysis techniques central to monitoring and investigation, including NSM data types, log data sources, NetFlow, web application attacks, advanced log analysis, and packet capture and forensics.
6. Security Operations Platforms: Cover the technologies that power modern SOCs, including malware analysis and threat intelligence, SIEM architecture and best practices, SOAR automation use cases, and the Cisco XDR platform for unified detection and response.
7. Incident Response: Complete the Learning Path with incident response planning (NIST SP 800-61 Rev 2/Rev 3, NIST CSF 2.0, CMMC), CSIRT roles and operations, security monitoring playbooks, and threat hunting methodologies (HMM, the Cyber Threat Hunting Cycle, STRIDE/PASTA).