Conducting Threat Hunting and Defending using Cisco Technologies for Cybersecurity (CPLL-CBRTHD)

Duration: 180 Days

The Conducting Threat Hunting and Defending using Cisco Technologies for Cybersecurity (CBRTHD) Learning Path introduces and guides you to a proactive security search through networks, endpoints, and datasets to hunt for malicious, suspicious, and risky activities that may have evaded detection by existing tools. In this Learning Path, you will learn the core concepts, methods, and processes used in threat hunting investigations. Threat hunting involves going beyond what Security Operations Center (SOC) analysts already know or have been alerted to. Traditional cyber detection technologies will only identify malicious risks and behaviors. The art of threat hunting is about venturing into the unknown. In this Learning Path, you will learn the core concepts, methods, and processes used in threat hunting investigations. This Learning Path provides an environment for attack simulation and threat hunting skill development using a wide array of security products and platforms from Cisco and third-party vendors. You will perform genuine threat hunting exercises within simulated network environments.

This Learning Path prepares you for the 300-220 CBRTHD v1.0 exam. If passed, you earn the Cisco Certified Specialist – Threat Hunting and Defending certification and satisfy the concentration exam requirement for the Cisco Certified Network Professional (CCNP) Cybersecurity certification.

Skills You'll Learn:

- Conduct security searches across networks, endpoints, and datasets to identify hidden malicious activities that evade traditional detection tools
- Utilize MITRE ATT&CK, D3FEND, and the Cyber Kill Chain to model, prioritize, and attribute threats to specific adversary groups
- Perform network traffic analysis, endpoint data acquisition, and memory forensics using tools like PowerShell and Velociraptor
- Gain an understanding of threat hunting using Cisco-specific technologies, including Cisco Secure Firewall, Cisco XDR, and Cisco Secure Network Analytics
- Execute the end-to-end threat hunting lifecycle, from adversary emulation and OSINT research to professional reporting and aftermath analysis

Learning Path Objectives:

1. Threat Hunting Foundations: Explore threat hunting cybersecurity practices and core concepts for conducting threat hunting investigations.

2. Network and Endpoint Threat Hunting: Examine topics and examples of threat hunting in networks and cloud environments.
3. Implementing, Analyzing, and Reporting the Threat Hunt: Follow a complete threat hunt from start to finish, identify the key phases of a threat hunt exercise, and identify potential threat hunt findings and outcomes.