Current Technologies
Computer Learning Centers

+1 (219) 764-3800
6210 Central Ave, Portage IN
sales@ctclc.com
www.ctclc.com

Cisco Partner
Platinum Learning

WHERE GREAT TRAINING HAPPENS EVERYDAY!

Conducting Threat Hunting and Defending using Cisco Technologies for CyberOps (CBRTHD)

Conducting Threat Hunting and Defending using Cisco Technologies for CyberOps (CBRTHD)

The Conducting Threat Hunting and Defending using Cisco Technologies for Cybersecurity (CBRTHD) training 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 training, 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 training, you will learn the core concepts, methods, and processes used in threat hunting investigations. This training 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 training 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. This training also earns you 40 Continuing Education (CE) credits toward recertification.

How you'll benefit

This class will help you:

- Learn how to perform 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
- Gain leading-edge career skills focused on cybersecurity
- Prepare for the 300-220 CBRTHD v1.0 exam
- Earn 40 CE credits toward recertification

Why Attend with Current Technologies CLC

- Our Instructors are in the top 10% rated by Cisco
- Our Lab has a dedicated 1 Gig Fiber Connection for our Labs
- Our Labs run up to Date Code for all our courses

Course Duration
5 days

Course Price
$4,300.00 or 44 CLCs

Methods of Delivery
- Instructor Led
- Virtual ILT
- On-Site

Who Should Attend

The primary audience for this course is as follows:

- Security Operations Center staff
- SOC Tier 2 Analysts
- Threat Hunters
- Cyber Threat Analysts
- Threat Managers

- Risk Managements

Prerequisites

There are no prerequisites for this training. However, the knowledge and skills you are recommended to have before attending this training are:

- General knowledge of networks and network security

OUTLINE

Module 1: Threat Hunting Theory

Module 2: Threat Hunting Concepts, Frameworks, and Threat Models

Module 3: Threat Hunting Process Fundamentals

Module 4: Threat Hunting Methodologies and Procedures

Module 5: Network-Based Threat Hunting

Module 6: Endpoint-Based Threat Hunting

Module 7: Endpoint-Based Threat Detection Development

Module 8: Threat Hunting with Cisco Tools

Module 9: Threat Hunting Investigation Summary: A Practical Approach

Module 10: Aftermath of a Threat Hunt

LAB OUTLINE

- Lab 1: Categorize Threats with MITRE ATTACK Tactics and Techniques
- Lab 2: Compare Techniques Used by Different APTs with MITRE ATTACK Navigator
- Lab 3: Model Threats Using MITRE ATTACK and D3FEND
- Lab 4: Prioritize Threat Hunting Using the MITRE ATTACK Framework and Cyber Kill Chain
- Lab 5: Determine the Priority Level of Attacks Using MITRE CAPEC
- Lab 6: Explore the TaHiTI Methodology
- Lab 7: Perform Threat Analysis Searches Using OSINT
- Lab 8: Attribute Threats to Adversary Groups and Software with MITRE ATTACK
- Lab 9: Emulate Adversaries with MITRE Caldera
- Lab 10: Find Evidence of Compromise Using Native Windows Tools
- Lab 11: Hunt for Suspicious Activities Using Open-Source Tools and SIEM
- Lab 12: Capturing of Network Traffic
- Lab 13: Extraction of IOC from Network Packets
- Lab 14: Usage of ELK Stack for Hunting Large Volumes of Network Data
- Lab 15: Analyzing Windows Event Logs and Mapping Them with MITRE Matrix

- Lab 16: Endpoint Data Acquisition
- Lab 17: Inspect Endpoints with PowerShell
- Lab 18: Perform Memory Forensics with Velociraptor
- Lab 19: Detect Malicious Processes on Endpoints
- Lab 20: Identify Suspicious Files Using Threat Analysis
- Lab 21: Conduct Threat Hunting Using Cisco Secure Firewall, Cisco Secure Network Analytics, and Splunk
- Lab 22: Conduct Threat Hunt Using Cisco XDR Control Center and Investigate
- Lab 23: Initiate, Conduct, and Conclude a Threat Hunt