CBRTHD

Conducting Threat Hunting and Defending using Cisco Technologies for Cybersecurity

40 horas | Profissional | Cisco

Cisco Continuing Education Credits

40 CE Credits

INTRODUÇÃO

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 training 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

OBJETIVO DO CURSO

• Define threat hunting and identify core concepts used to conduct threat hunting investigations
• Examine threat hunting investigation concepts, frameworks, and threat models
• Define cyber threat hunting process fundamentals
• Define threat hunting methodologies and procedures
• Describe network-based threat hunting
• Identify and review endpoint-based threat hunting
• Identify and review endpoint memory-based threats and develop endpoint-based threat detection
• Define threat hunting methods, processes, and Cisco tools that can be utilized for threat hunting
• Describe the process of threat hunting from a practical perspective
• Describe the process of threat hunt reporting

PÚBLICO-ALVO

Security Operations Center staff, SOC Tier 2 Analysts, Threat Hunters, Cyber Threat Analysts, Threat Managers, Risk Management professionals

PRÉ-REQUISITOS

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
These skills can be found in the following Cisco Learning Offerings:
• Implementing and Administering Cisco Solutions (CCNA)
• Understanding Cisco Cybersecurity Operations Fundamentals (CBROPS)
• Performing CyberOps Using Cisco Security Technologies (CBRCOR)

CONTEÚDO PROGRAMÁTICO

Course Outline

Threat Hunting Theory

Threat Hunting Concepts, Frameworks, and Threat Models

Threat Hunting Process Fundamentals

Threat Hunting Methodologies and Procedures

Network-Based Threat Hunting

Endpoint-Based Threat Hunting

Endpoint-Based Threat Detection Development

Threat Hunting with Cisco Tools

Threat Hunting Investigation Summary: A Practical Approach

Aftermath of a Threat Hunt

Lab Outline

Categorize Threats with MITRE ATT&CK

Compare Techniques with MITRE Navigator

Model Threats Using MITRE ATT&CK and D3FEND

Explore TaHiTI Methodology

Perform Threat Analysis Using OSINT

Emulate Adversaries with MITRE Caldera

Hunt for Suspicious Activities Using SIEM

Extract IOC from Network Packets

Analyze Windows Event Logs

Perform Memory Forensics with Velociraptor

Detect Malicious Processes

Conduct Threat Hunting Using Cisco Secure Firewall and XDR