Conducting Threat Hunting and Defending using Cisco Technologies for CyberOps

Duration: 5 Days **Course Code: CBRTHD** **Version: 1.1**

Overview:

The Conducting Threat Hunting and Defending using Cisco Technologies for Cybersecurity (CBRTHD) course 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.
The Conducting Threat Hunting and Defending using Cisco Technologies for Cybersecurity (CBRTHD) course 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.

Target Audience:

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

Objectives:

- **By the end of this course, you should be able to:**
- 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

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

- CCNA - Implementing and Administering Cisco Solutions
- CBROPS - Understanding Cisco Cybersecurity Operations Fundamentals

Testing and Certification

- 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.

- CBRCOR - Performing CyberOps Using Cisco Security Technologies

Content:

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 ATTACK Tactics and Techniques
- Compare Techniques Used by Different APTs with MITRE ATTACK Navigator
- Model Threats Using MITRE ATTACK and D3FEND
- Prioritize Threat Hunting Using the MITRE ATTACK Framework and Cyber Kill Chain
- Determine the Priority Level of Attacks Using MITRE CAPEC
- Explore the TaHiTI Methodology
- Perform Threat Analysis Searches Using OSINT
- Attribute Threats to Adversary Groups and Software with MITRE ATTACK
- Emulate Adversaries with MITRE Caldera
- Find Evidence of Compromise Using Native Windows Tools
- Hunt for Suspicious Activities Using Open-Source Tools and SIEM
- Capturing of Network Traffic
- Extraction of IOC from Network Packets
- Usage of ELK Stack for Hunting Large Volumes of Network Data
- Analyzing Windows Event Logs and Mapping Them with MITRE Matrix
- Endpoint Data Acquisition
- Inspect Endpoints with PowerShell
- Perform Memory Forensics with Velociraptor
- Detect Malicious Processes on Endpoints
- Identify Suspicious Files Using Threat Analysis
- Conduct Threat Hunting Using Cisco Secure Firewall, Cisco Secure Network Analytics, and Splunk
- Conduct Threat Hunt Using Cisco XDR Control Center and Investigate
- Initiate, Conduct, and Conclude a Threat Hunt

Further Information:

For More information, or to book your course, please call us on 00 20 (0) 2 2269 1982 or 16142

training@globalknowledge.com.eg

www.globalknowledge.com/en-eg/

Global Knowledge, 16 Moustafa Refaat St. Block 1137, Sheraton Buildings, Heliopolis, Cairo