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

Course Duration: 40 Hours **Course code: CBRTHD**

1. Course Overview

The Conducting Threat Hunting and Defending using Cisco Technologies for CyberOps (CBRTHD) training is a 5-day Cisco threat hunting course that 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. 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.

2. What you'll learn?

After completing 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

Phone: +91-999-911-1686 **Mail Us:** info@ssdntech.com

- Describe the process of threat hunting from a practical perspective
- Describe the process of threat hunt reporting

3. Target Audience

Anyone involved in the hunting of threats within a network.

4. Pre-Requisites

Attendees should meet the following prerequisites:

- General knowledge of networks
- Cisco CCNP Security certification

Recommended prerequisites:

- CCNA - Implementing and Administering Cisco Solutions
- CBROPS - Understanding Cisco Cybersecurity Operations Fundamentals
- CBRCOR - Performing CyberOps Using Cisco Security Technologies

5. Course content

Threat Hunting Theory

- Threat Hunting Concepts
- Threat Hunting Types
- Conventional Threat Detection vs Threat Hunting

Threat Hunting Concepts, Frameworks and Threat Models

- Cybersecurity Concepts
- Common Threat Hunting Platforms
- Threat Hunting Frameworks
- Threat Modeling
- Case Study: Use the PASTA Threat Model

Threat Hunting Process Fundamentals

- Threat Hunting Approaches
- Threat Hunting Tactics and Threat Intelligence
- Defining Threat Hunt Scope and Boundaries
- Planning the Threat Hunt Process

Threat Hunting Methodologies and Procedures

- Investigative Thinking
- Identify Common Anolmalies
- Analyze Device and System Logs
- Determine the Best Threat Hunt Methods
- Automate the Threat Hunting Process

Network-Based Threat Hunting

- Operational Security Considerations
- Performing Network Data Analysis and Detection Development
- Performing Threat Hunting in the Cloud

Endpoint-Based Threat Hunting

- Threat Hunting for Endpoint-Based Threats
- Acquiring Data from Endpoint
- Performing Host-Based Analysis

Endpoint-Based Threat Detection Development

- Analyze Endpoint Memory
- Examining Systems Memory Using Forensics
- Developing Endpoint Detection Methods
- Uncovering New Threats, Indicators and Building TTPs

Threat Hunting with Cisco Tools

- Threat Hunting with Cisco Tools
- Cisco XDR Components

Threat Hunting Investigation Summary: A Practical Approach

- Conducting a Threat Hunt

Reporting the Aftermath of a Threat Hunt Investigation

- Measure the Success of a Threat Hunt
- Report Your Findings
- Threat Hunting Outcomes