



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

ID CBRTHD Price on request Duration 5 days

#### Who should attend

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

#### 1 Nisk Managements

This course is part of the following Certifications
Cisco Certified Cybersecurity Professional (CCCP)

#### **Prerequisites**

The knowledge and skills you are expected to have before attending this training are:

- General knowledge of networks
- Cisco CCNP Security certification

These skills can be found in the following Cisco Learning Offerings:

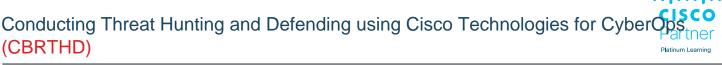
- Implementing and Administering Cisco Solutions (CCNA)
- Understanding Cisco Cybersecurity Operations Fundamentals (CBROPS)
- Performing CyberOps Using Cisco Security Technologies (CBRCOR)
- !

#### **Course Objectives**

- 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

## Conducting Threat Hunting and Defending using Cisco Technologies for Cyber Platinum Learning



### **Training Centres worldwide**





#### Fast Lane Institute for Knowledge Transfer (Switzerland) AG

Husacherstrasse 3 CH-8304 Wallisellen Tel. +41 44 832 50 80

info@flane.ch, https://www.flane.ch