SECUREIT CONSULT

www.secureitconsult.com

TREND MICRO Authorized Training Center

Trend Micro™ VISION ONE™ XDR TRAINING FOR CERTIFIED PROFESSIONALS

Course Description

This is a three-day, instructor-led training course. Participants will learn how to use the features in Trend Micro Vision One for extended detection response (XDR) activities.

This course describes some of the concepts related to extended detection and response. Lessons in the course detail how to connect Trend Micro and third-party products to Trend Micro Vision One, how to install XDR sensors on devices in the infrastructure, how to navigate and interpret workbenches, how to incorporate third party threat intelligence, how to search for information within the Trend Micro Vision One data lake, and how to automate responses using Security Playbooks.

This course is taught by Trend Micro-certified trainers and incorporates a variety of hands-on lab exercises, allowing participants to put the lesson content into action.

Key Information	
Course Title:	Trend Micro Vision One XDR Training for Certified Professional
Product ID:	TRNN1040 or TRNM0003
Course Length:	Three Days
Level:	Professional
Delivery Language:	English

COURSE OBJECTIVES:

After completing this course, participants will be able to:

- Describe the benefits of an XDR solution
- Connect Trend Micro products to Trend Micro Vision One
- Collect telemetry from endpoints, email, the web, and the network
- Integrate third-party products with Trend Micro Vision One
- Interpret and navigate within Workbenches
- Use the Search tools to locate information in the data lake
- Create Playbooks to streamline response activities Participants are required to bring a laptop

computer with a recommended screen resolution of at least 1980 x 1080 or above and a display size of 15" or above.

Certifications and Related Examinations

Upon completion of this course, participants may choose to complete the certification exam to obtain designation as a Trend Micro Certified Professional for Vision One XDR

Target audience

This course is geared to members of an organization's security operations teams that are responsible for detecting, investigating, prioritizing, and responding to threats who are new to, or have limited knowledge of, Trend Micro Vision One.

This course is also beneficial to administrators responsible for performing initial setup operations such as connecting products to Trend Micro Vision One and enabling XDR sensors on devices.

Course Prerequisites

Prerequisites to attend this course include:

- A working knowledge of Trend Micro endpoint and network protection solutions and services
- An understanding of basic networking concepts and principles will be helpful

Participants must also have successfully completed the Trend Micro Vision One Fundamentals e-learning course on the Trend Micro Education Portal. Participants are required to bring a laptop computer with a recommended screen resolution of at least 1980 x 1080 or above and a display size of 15" or above.

Certifications and Related Examinations:

Upon completion of this course, participants may complete the certification examination, in order to validate their Trend Micro Certified
Professional for Deep Security certification for another 2 years.

Detailed Course Outline:

Topics Covered:

XDR Concepts

- Collecting telemetry
- Data correlation
- MITRE ATT&CK

Trend Micro Vision One

- How Trend Micro Vision One fits into the Trend Micro One platform
- Trend Micro Vision One core capabilities
- Trend Micro Vision One features for XDR
- Trend Micro Vision One apps

Sharing Threat Intelligence

- Curated and custom intelligence reports
- Suspicious object management
- Sandbox analysis

Connecting Trend Micro Products

- Collecting security events
- Connecting Trend Micro Apex One™ as a Service
- Connecting Deep Security™ Software
- Connecting Trend Micro Cloud One™ – Endpoint & Workload Security
- Connecting Cloud App Security
- Connecting the Service Gateway
- Connecting Web Security™
- Connecting Deep Discovery™ Inspector
- Connecting TippingPoint™ SMS

Enabling XDR Sensors

- Installing Endpoint Basecamp
- Creating Endpoint Groups and Security Policies
- Enabling endpoint sensors
- Enabling email sensors
- Enabling network sensors
- Enabling web sensors

Integrating with Third-Party Products

- Integration Purposes

Using the XDR Apps

- XDR Apps
- Viewing raw security event and activity data
- Filtering security event and activity data
- Workbenches
- Workbench actions
- Execution profiles
- Network analytics
- Automating responses
- Targeted attack detection
- Response management
- Managed XDR service

Searching the Data Lake

- Simple and complex search syntax
- Search tips
- Watchlists

Responding to Incidents Using Security Playbooks

- Playbook templates
- Playbook triggers
- Playbook conditions
- Playbook action