Symantec Endpoint Detection and Response 4.5
Administration

Description
The Symantec Endpoint Detection and Response 4.5 Administration course is designed for the IT security professional in a Security Operations role. This course covers how to detect, investigate, remediate, and recover from an incident using Symantec Endpoint Detection and Response, as well as the prerequisite SEDR configurations and considerations to perform endpoint detection and response.

Delivery Method
Instructor-led

Duration
2 day

Objectives
By the completion of this course, you will be able to:

- Configure SEDR to perform endpoint detection and response
- Identify evidence of suspicious and malicious activity
- Search for indicators of compromise
- Block, isolate, and remove threats in the environment
- Collect forensic information

Who Should Attend?
The Endpoint Detection and Response 4.5 Administration course is intended for students who wish to perform Incident Response activities with Symantec Endpoint Detection and Response.

Prerequisites
This course assumes that students are familiar with Symantec Endpoint Detection & Response and Symantec Endpoint Protection.

Hands-On
This course includes practical hands-on exercises that enable you to test your new skills and begin to use those skills in a working environment.

Outline

Module 1: The Evolving Threat Landscape
- Challenges of endpoint detection and response in the environment
- How Symantec Endpoint Detection and Response meets those challenges
- Symantec Endpoint Detection and Response Components
- Symantec Endpoint Detection and Response Management Console
- Symantec Endpoint Detection and Response User Accounts and Roles

Module 2: Detecting Threats in the Environment
- Understanding Suspicious & Malicious Activity
- Prerequisite configuration or considerations
- Identifying evidence of suspicious/malicious activity with SEDR

Module 3: Investigating Threats in the Environment
- Understanding Indicators of Compromise
- Searching for Indicators of Compromise
- Analyzing Endpoint Activity Recorder Data
- Additional Investigation Tools

Module 4: Responding to Threats in the Environment
- Isolating Threats in The Environment
- Blocking Threats in The Environment
- Removing Threats in The Environment
- Tuning the Environment

Module 5: Reporting on Threats in the Environment
- Notifications and Reporting
- Collecting forensic data for further investigation of security incidents
- Using SEDR to create a Post Incident Report

Symantec™
A Division of Broadcom

For product information and a complete list of distributors, visit our website at: broadcom.com