Endpoint Protection 14.2 Manage and Administer

COURSE DESCRIPTION

The Symantec Endpoint Protection 14.2: Manage and Administer course is designed for the network, IT security, and systems administration professional in a Security Operations position tasked with the day-to-day operation of the SEPM on-premise management console.

Delivery Method

Instructor-led and Virtual Academy

Duration

Two days

Course Objectives

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

- Describe how the Symantec Endpoint Protection Manager (SEPM) communicates with clients and make appropriate changes as necessary.
- Design and create Symantec Endpoint Protection group structures to meet the needs of your organization.
- Respond to threats using SEPM monitoring and reporting.
- Analyze the content delivery system (LiveUpdate).
- Reduce bandwidth consumption using the best method to deliver content updates to clients.
- Configure Group Update Providers.
- Create location aware content updates.
- Use Rapid Release definitions to remediate a virus outbreak.

Who Should Attend

The SEP 14.2 Manage and Administer course is intended for students who are charged with managing and monitoring Symantec Endpoint Protection endpoints.

Prerequisites

This course assumes that students have a basic understanding of advanced computer terminology, including TCP/IP networking and Internet terms, and an administrator-level knowledge of Microsoft Windows operating systems.

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.

COURSE OUTLINE

Module 1: Managing Console Access and Delegating Authority

- Create SEP administrator accounts and delegate administrative tasks to Limited administrators.

Module 2: Managing Client-to Server Communication

- Analyze client-to-SEPM communication, restore communication between clients and the SEPM, and verify that clients are online with the SEPM.

© 2019 Symantec Corporation. All Rights Reserved. Symantec, the Symantec Logo and the Checkmark Logo are trademarks or registered trademarks of Symantec Corporation or its affiliates in the U.S. and other countries. Other names may be trademarks of their respective owners.

Module 3: Managing Client Architecture and Active Directory Integration

- Describe the interaction between sites, domains, and groups and how to manage groups, locations, and policy inheritance. You also learn how to import Active Directory Organizational Units and control access to client user interface settings.

Module 4: Managing Clients and Responding to Threats

- Identify and verify the protection status for all computers and monitor for health status and anomalies. You also learn how to respond to threats.

Module 5: Monitoring the Environment and Responding to Threats

- Monitor critical log data, identify new incidents, and proactively respond to threats.

Module 6: Creating Incident and Health Status Reports

- Create reports that reflect your environment's security status and health.

Module 7: Introducing Content Updates Using LiveUpdate

- Describe the content delivery system (LiveUpdate) and learn how to reduce bandwidth consumption using the best method to deliver content updates to clients.

Module 8: Analyzing the SEPM Content Delivery System

- Analyze the content delivery system and learn to configure and manage content distribution for clients.

Module 9: Managing Group Update Providers

- Configure and monitor Group Update Providers. Examine the Group Update Provider health and status.

Module 10: Managing Certified and Rapid Release Definitions

- Use Rapid Release definitions to remediate a virus outbreak.

Module 11: Configuring Location Aware Content Updates

- Examine, configure, and monitor location aware content update updates.

© 2019 Symantec Corporation. All Rights Reserved. Symantec, the Symantec Logo and the Checkmark Logo are trademarks or registered trademarks of Symantec Corporation or its affiliates in the U.S. and other countries. Other names may be trademarks of their respective owners.