Symantec Endpoint Protection 14: Differences course

COURSE DESCRIPTION

The *Symantec Endpoint Protection 14: Differences* course is designed for the network, IT security, and systems administration professionals in a Security Operations position who have experience with SEP 12 and need to understand the new features, how to upgrade to and manage SEP 14.

Delivery Method
Instructor-led/elibrary

Duration
One-day

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

- Know what's new and how to use the new security features
- Complete a fresh Install and upgrade from prior versions
- Understand and plan for changed features

Who Should Attend
Network, IT security, and systems administration professionals in a Security Operations position who are tasked with configuring optimum security settings for endpoints protected by Symantec Endpoint Protection 14

Prerequisites
You must have a working knowledge of Symantec Endpoint Protection 12, advanced computer terminology, including TCP/IP networking terms, Internet terms, and an administrator-level knowledge of Microsoft Windows operating systems.

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

COURSE OUTLINE

Introduction

- Course environment
- Lab environment

What's New?

Symantec Endpoint Protection Manager Server new features

- New cloud look
- Customizable replication schedule
- Subnet mask for explicit Group Update Providers
- In-product notifications
- Default computer mode client installation
- New programmable REST APIs – increased automation

Symantec Endpoint Protection Client new features (Mac clients)

- Device control
- Auto-upgrade from the manager

Symantec Endpoint Protection Client new features (Windows clients)

- Intelligent Threat Cloud Service
  - Standard client
  - Embedded or VDI client
  - Dark (offline) network
- Zero-day protection – Generic Exploit Mitigation

DRAFT

- Advanced Machine Learning
- New emulator improves scan performance
- Additional support for windows drive/folder variables in scans
- Ability to disable SONAR from scanning network drives
- Application Control driver leverage Windows 10 Device Guard to lock down device

Changed features

- Insight Lookup shares settings with Download Insight
- Password never expires option disabled by default
- Virus scan logic moved to AP user mode

Removed or unsupported features

- Any versions of Windows XP/ Server 2003/XP based Windows Embedded OSes
- Mac OS X 10.8
- SEP 11.x manager definition updates
- Import SEP 11.x clients
- Migrate Symantec Endpoint Protection Manager 11.x/12.0 to 14.
- vShield-enabled Shared Insight Cache and Security Virtual appliance.
- Network Access Control

Installing, Upgrading or Migrating

New clients

- Intelligent threat cloud service
- Selecting and installing the right client

Supported Upgrade Path

- Direct upgrade from version 12.x

SEP 11 migration best practice

- Installing new Symantec Endpoint Protection Manager on supported platform
- Upgrade client directly to SEP 14

Enhance Security

Generic Exploit Mitigation

- What is GEM?
- Benefits of GEM
- GEM Policy & Settings/Application Coverage
- Reporting on GEM detections

Advanced Machine Learning

- What is Advanced Machines Learning? (Detection and block zero-day malware before they execute)
- Benefits of AML
- Reporting on AML detections