Instructor Led Training Course Catalog

Enterprise Security Group

July 2024

Table of Contents

Endpoint Security

Symantec Endpoint Security delivers the most complete, integrated endpoint security platform on the planet. As an on-premises, hybrid, or cloud-based solution, the single-agent Symantec platform protects all your traditional and mobile endpoint devices, and uses artificial intelligence (AI) to optimize security decisions. A unified cloud-based management system simplifies protecting, detecting and responding to all the advanced threats targeting your endpoints.

- **Keep your business running.** Compromised endpoints are highly disruptive to business. Innovative attack prevention and attack surface reduction delivers the strongest security across the entire attack life cycle (e.g., stealthy malware, credential theft, fileless, and “living off the land” attacks).
- **Prevent the worst-case scenario.** Full blown breaches are CISOs' worst nightmare. Deliver detection and remediation of persistent threats with sophisticated attack analytics and prevention of AD credential theft.
- **Manage smarter. Work less.** Intelligent automation and AI-guided policy management enhance administrator productivity; Symantec experts fortify SOC teams to meet customer needs without hiring additional headcount.
- **Manage everything in one place** Integrated Cyber Defense Manager (ICDm) is a single cloud management console that strengthens overall endpoint security posture.
- **Endpoint security delivered your way.** With a single agent, protection across traditional and mobile devices, and onprem, cloud or hybrid management.

Symantec Data Center Security Server Advanced 6.x Planning, Implementation, and Administration R1

Course Code: 000210

Course Description

The Symantec Data Center Security Server Advanced 6.x Planning, Implementation, and Administration R1 course is an introduction to implementing and managing a Data Center Security: Server Advanced deployment. The architecture and individual components of the SDCS:SA solution are detailed and explained. Agent installation and configuration are taught along with deployment and management of SDCS:SA agents and policies across the enterprise. The course also covers SDCS:SA Policy creation/modification in detail.

Delivery Method

Instructor-Led

Duration

Three Days

Course Objectives

- Describe the major components of Data Center Security: Server Advanced and how they communicate.
- Install the management server, consoles, and agent.
- Define, manage, and create assets, policies, events and configurations.
- Understand policy creation and editing in depth.

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.

Prerequisites

- You should have working knowledge of TCP/IP protocols and communications concepts.
- You must have experience with the Windows and UNIX operating systems in general.
- A basic understanding of key security disciplines (firewalls, intrusion detection/prevention, policy management, vulnerability assessment, antivirus protection and so on) is required.

Certification

250-426 Administration of Symantec Data Center Security Server Advanced 6.7

Course Outline

Module 1: Introduction to Security Risks and Risk

- Security Risks
- Security Risk Management
- Managing and Protecting Systems
- Corporate Security Policies and Security
- Assessments
- Host-Based Computer Security Issues

Module 2: SDCS: Server Advanced Overview

- Component Overview
- How Does SDCS:SA Work?
- Policy Types and Platforms
- Management Console Overview
- Agent User Interface Overview

Module 3: Installation and Deployment

- Planning the Installation
- Deployment Planning
- Server Installation
- Installing the Server Management Console
- Installing a Windows Agent ▪ Installing a Unix Agent

Module 4: Configuring Agents

- Assets Defined
- Agent Architecture
- Viewing Agents and Assets
- Managing Agents
- Managing Agents on Assets by Command Line

Module 5: Policy Overview

- Prevention Policy Overview
- Detection Policy Overview
- Policy Workspace
- Implementing Policies with SDCS:SA
- SDCS:SA Use Cases

Module 6: Windows Prevention Policies

- Windows Prevention Policy Structure
- Editing Windows Prevention Policy
- Advanced Policy Settings: Global Policy Options
- Advanced Policy Settings: Sandboxes
- Resource Lists
- Custom Sandboxes

Module 7: UNIX and Legacy Prevention Policies

- Unix and Legacy Prevention Policies
- Global Policy Options
- Daemon and Service Options
- Interactive Program Options
- Resource Lists
- Sandbox Options
- Custom Sandboxes
- Trusted Users, Groups, and Applications
- Profile Lists
- Predefined Prevention Policies

Module 8: Advanced Prevention

- Profile Applications
- Customize Predefined Prevention Policies
- Custom Sandbox
- Prepare for IPS Policy Deployment
- Create New Policies

Module 9: Detection Policies

- Detection Policy Details
- Predefined Detection Policies

Module 10: Event Management

- Defining Events
- Viewing Events
- Event Handling and Bulk Logging ▪ Creating Alerts

Module 11: Agent Management and Troubleshooting

- Configurations Defined
- Creating and Editing Configurations
- Bulk Logging Details
- Analyzing Event Log Files and Bulk Loading
- Troubleshooting Agents Using Logs and Configuration Files
- Using Agent Diagnostic Policies
- Using Agent Command-line Interface

Module 12: System Management

- Database Management
- Managing Users and Roles
- Server Management
- Server Logs

Symantec Data Center Security Server Advanced 6.x Diagnostics and Troubleshooting

Course Code: 000212

Course Description

The *Symantec Data Center Server Advanced 6.x Diagnostics and Troubleshooting R1* course is designed for the IT security management professional tasked with troubleshooting Data Center Security Server Advanced (SDCSSA). Students learn how to troubleshoot the SDCSSA server, UMC, and agent core components. You also learn how to identify services, examine configuration files, interpret log files and use that information for diagnosis and troubleshooting.

Delivery Method

Instructor-Led

Duration

Two Days

Course Objectives

- Identify the process flow between all DCSSA components
- Troubleshoot and change Management server and
- Unified Management Console (UMC) configurations
- Solve agent issues with special emphasis placed on communication, certificate issues, and agents or agent status not displaying in UMC.
- Tune and troubleshoot policies on Windows and Linux/Unix agents.
- Research and solve Server and Agent installation and upgrade issues

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.

Prerequisites

- You must have attended the Symantec Data Security Sever Advanced 6.x Administration R1 course or have one year of day-to-day experience maintaining an SDCSSA environment, which includes basic troubleshooting.
- Broadcom also recommends that you visit Symantec eLibrary and take the fifteen-minute introductory to Symantec Diagnostic and Troubleshooting Methodology course.

Certification

250-426 Administration of Symantec Data Center

Security Server Advanced 6.7

Course Outline

Module 1: Examining the SDCSSA Architecture and Components

- Describing the SDCSSA architecture
- Describing each component's role
- Describing how components interact when performing common tasks
- Isolating SDCSSA components to troubleshoot

Module 2: Troubleshooting the Management Server

- Identify Management server core components and their roles
- Examine services and dependencies
- Identify and examine logs
- Identify and examine configuration, communication, and certificate issues
- Diagnose and troubleshoot management server changes

Module 3: Troubleshooting Management and UMC Consoles

- Identify core components
- Examine services and dependencies
- Research authentication issues
- Identify, examine, and troubleshoot configuration, communication, and certificate issues
- Examine the applying policy process

Module 4: Troubleshooting Agents

- Identifying Windows agent components
- Troubleshooting Windows agents
- Identifying Linux agent components
- Troubleshooting Linux agents

Module 5: Troubleshooting Prevention and Detection Policies

- Examine Prevention policy components
- Examine policy logs (local)
- Troubleshooting Prevention policies
- Examine Detection policy components
- Troubleshoot Detection policies
- Manage events
- Tune policies

Module 6: Troubleshooting Installations and Upgrades

- Locate installation and upgrade information
- Troubleshoot Management server installation and upgrades
- Troubleshoot Management Console installation and upgrades
- Troubleshoot Windows, Linux, and Unix Agent installation and upgrades

Symantec Endpoint Detection and Response 4.x Planning, Implementation and Administration R1.1

Course Code: 000265

Course Description

The *Symantec Endpoint Detection and Response 4.x Planning, Implementation, and Administration* course is designed for the IT security and systems administration professional in a Security Operations role. This course covers how to investigate, remediate, and recover from a security incident using Symantec Endpoint Detection and Response, as well as the prerequisite sizing and architecture configurations for implementing Symantec Endpoint Detection and Response On-Prem.

Delivery Method

Instructor-Led

Duration

Three Days

Course Objectives

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

- Plan and implement a Symantec Endpoint Detection and Response deployment
- 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 ▪ Manage System Settings

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.

Prerequisites

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

Additional Courses Available

Students interested in Administration of Symantec Endpoint Detection and Response utilizing the cloud management interface available as part of Symantec Endpoint Security Complete should take the following course:

- Symantec Endpoint Security Complete Administration R1.x

Course Outline

Module 1: Introduction

- The Evolving Threat Landscape
- Challenges of Endpoint Detection and Response in the environment
- How Symantec Endpoint Detection and Response meets objectives
- Components of Symantec Endpoint Detection and
- Response
- Shared Technologies
- Symantec Endpoint Detection and Response Add-Ons and Integrations

Module 2: Architecture and Sizing

- Architecture and Sizing Overview
- Architecture
- Sizing

Module 3: Implementation

- System Requirements
- Installing and Bootstrapping
- Setup Wizard
- Management Console Overview
- Managing Certificates
- User Accounts and Roles
- Symantec Endpoint Protection Integration

Module 4: Detecting Threats

- Understanding Suspicious & Malicious Activity
- Prerequisite configuration or considerations
- Identifying evidence of suspicious/malicious activity with Symantec EDR

Module 5: Investigating Threats

- General Stages of an Advanced Attack
- Understanding Indicators of Compromise
- Searching for Indicators of Compromise
- Analyzing Endpoint Activity Recorder Data
- Additional Investigation Tools

Module 6: Responding to Threats

- Cybersecurity Framework
- Isolating Threats in The Environment
- Blocking Threats in The Environment
- Removing Threats in The Environment
- Tuning the Environment

Module 7: Reporting on Threats

- Recovery Overview
- Notifications and Reporting
- Collecting forensic data for further investigation of security incidents
- Using Symantec EDR to create a Post Incident Report

Module 8: Managing System Settings

- Managing Certificates
- Importing and Exporting Incident Rules State
- Event and Incident Forwarding
- Splunk Integration

Symantec Endpoint Protection 14.x Administration R1

Course Code: 000229

Course Description

The *Symantec Endpoint Protection 14.x Administration R1* 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 and with configuring optimum security settings for endpoints protected by Endpoint Protection.

Delivery Method

Instructor-Led

Duration

Five Days

Course Objectives

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

- Describe how the Endpoint Protection Manager (SEPM) communicates with clients and make appropriate changes as necessary.
- Design and create 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).
- Configure Group Update Providers.
- Create location aware updates. ▪ Secure endpoints against network and file-based threats
- Control endpoint integrity and compliance ▪ Enforce an adaptive security posture

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.

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.

Additional Courses Available

Students interested in Administration of Symantec endpoints utilizing the cloud management interface available, as part of Symantec Endpoint Security Complete should take the following course:

- Symantec Endpoint Security Complete Administration R1

Certification

250-428: Administration of Symantec Endpoint

Protection 14

Course Outline

Module 1: Managing Console Access and Delegating Authority

- Creating Administrator Accounts
- Managing Administrator Accounts
- Configuring Directory Server Authentication for an Administrator Account

Module 2: Managing Client-to-Server Communication

- Analyzing Client-to-SEPM Communication
- Restoring Communication Between Clients and SEPM
- Verifying Clients are Online with the SEPM

Module 3: Managing Client Architecture and Active Directory Integration

- Describing the Interaction Between Sites, Domains, and Groups
- Managing Groups, Locations, and Shared Policies
- Importing Active Directory Organizational Units (OUs)
- Controlling Access to Client User Interface Settings

Module 4: Managing Clients and Responding to Threats

- Introducing the Clients View
- Monitoring SEP Clients Using the Clients View
- Responding to Incidents Using the Clients View

Module 5: Monitoring the Environment and Responding to Threats

- Monitoring Critical Log Data Using the Summary page
- Identifying New Incidents Using the Logs Page
- Monitoring Actions Sent to Clients Using the Command Status View
- Configuring Notifications

Module 6: Creating Incident and Health Status Reports

- Monitoring Critical Data Using the Reports Page
- Identifying New Incidents Using Quick Reports and Filters
- Configuring Scheduled Reports

Module 7: Introducing Content Updates Using LiveUpdate

- Describing the LiveUpdate Ecosystem
- Configuring LiveUpdate
- Troubleshooting LiveUpdate
- Examining the Need for an Internal LiveUpdate
- Administrator Server
- Configuring an Internal LiveUpdate Administrator Server

Module 8: Analyzing the SEPM Content Delivery System

- Describing Content Updates
- Configuring LiveUpdate on the SEPM
- Monitoring a LiveUpdate Session
- Managing Content on the SEPM
- Monitoring Content Distribution for Clients

Module 9: Managing Group Update Providers

- Introducing Group Update Providers
- Adding Group Update Providers
- Adding Multiple Group Update Providers and
- Configuring Explicit Group Update Providers
- Identifying and Monitoring Group Update Providers

Module 10: Manually Downloading Certified and Rapid Release Definitions

- Downloading Certified SEPM Definitions from
- Symantec Security Response
- Downloading Certified Windows Client Definitions from Symantec Security Response
- Downloading Rapid Release Definitions from
- Symantec Security Response
- Downloading Certified and Rapid Release
- Definitions from Symantec Security Response for
- Mac and Linux Clients
- Locating Statically Named Definitions

Module 11: Protecting Against Network Attacks and Enforcing Corporate Policies using the Firewall Policy

- Preventing Network Attacks
- Examining Firewall Policy Elements
- Creating Custom Firewall Rules
- Enforcing a Corporate Security Policy with Firewall Rules
- Configuring Advanced Firewall Features

Module 12: Blocking Network Threats with Intrusion Prevention

- Introducing Intrusion Prevention Technologies
- Configuring the Intrusion Prevention Policy
- Managing Custom Signatures
- Monitoring Intrusion Prevention Events

Module 13: Protecting Against MemoryBased Attacks

- Memory Exploit Mitigation
- Configuring the Memory Exploit Mitigation Policy
- Preventing Defense Evasion

Module 14: Preventing Attacks with SEP Layered Security

- Virus and Spyware Protection
- File Reputation
- Insight Lookup
- Emulator and Machine Learning Engine
- Download Insight
- Auto-Protect Scans
- SONAR
- Administrator-defined Scans

Module 15: Securing Windows Clients

- Platform and Virus and Spyware Protection Policy Overview
- Tailoring scans to meet an environment's needs
- Ensuring real-time protection for clients
- Detecting and remediating risks in downloaded files
- Identifying zero-day and unknown threats
- Preventing email from downloading malware
- Configuring advanced options
- Monitoring virus and spyware activity

Module 16: Securing Linux Clients

- Navigating the Linux Client
- Configuring Virus and Spyware Settings for Linux Clients
- Monitoring Linux Clients
- SEP for Linux Logs

Module 17: Securing Mac Clients

- Touring SEP for Mac Client
- Securing Mac Clients
- Monitoring Mac Clients
- SEP Logs on Mac Clients

Module 18: Providing Granular Control with Host Integrity

- Introducing Host Integrity
- Host Integrity Concepts
- Configuring Host Integrity
- Troubleshooting Host Integrity ▪ Monitoring Host Integrity

Module 19: Controlling Application and File Access

- Application Control Overview ▪ Application Control Concepts
- Configuring Application Control
- Monitor Application Control Events

Module 20: Restricting Device Access for Windows and Mac Clients

- Introducing Device Control
- Windows Device Control Concepts
- Mac Device Control Concepts
- Configuring Device Control
- Monitoring Device Control Events

Module 21: Hardening Clients with System Lockdown

- Describing System Lockdown
- Creating and Managing the File Fingerprint List
- System Lockdown use cases

Module 22: Customizing Protection Based on User Location

- Creating Locations
- Adding Policies to Locations
- Monitoring Location Awareness

Module 23: Managing Security Exceptions

- Describing Security Exceptions
- Describing Automatic Exclusions
- Managing Exceptions
- Monitoring Security Exceptions

Symantec Endpoint Protection 14.2 Maintain and Troubleshoot

Course Code: 000101

Course Description

The Symantec Endpoint Protection 14.2 Maintain and Troubleshoot course is designed for the IT security management professional tasked with troubleshooting Symantec Endpoint Protection 14.2. Students learn how to troubleshoot installations, monitor and troubleshoot the SEPM, client-to-SEPM communication, content distribution, client deployments, and protection technologies. The class also covers how to follow Symantec best practices for remediating a virus outbreak, automating functionality with REST APIs, and integrating Symantec Endpoint Protection with 3rd party applications.

Delivery Method

Instructor-led

Duration

Three days

Course Objectives

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

- Monitor, maintain, and troubleshoot a Symantec Endpoint Protection environment.
- Upgrade the Symantec Endpoint Protection environment.
- Use best practices when troubleshooting and remediating a virus outbreak.
- Automate functionality with Rest APIs and integrate Symantec Endpoint Protection with 3rd party applications.

Prerequisites

This course assumes that students have attended Symantec Endpoint Protection 14.2 Configure and Protect or have relevant experience maintaining a SEP environment, including basic troubleshooting.

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

Introduction

- Course overview
- The classroom lab environment

Module 1: Troubleshooting Techniques and Tools

- Use a systematic approach for problem solving.
- Describe Symantec and third-party troubleshooting tools and how they are used.
- Know which SEPM and SEP client logs to research when troubleshooting specific issues.
- Use the Symantec Knowledge Base and interact with Symantec Technical Support.

Module 2: Troubleshooting the Console

- Describe the components that make up the Symantec Endpoint Protection Manager.
- Describe SEPM services and their roles.
- Troubleshoot problems related to the SEPM services that prevent you from logging onto the console.
- Describe the database configuration and connection methods.
- Configure email to enable an administrator to reset passwords and know where to check administrator permissions.

Module 3: Installation and Migration Issues

- Troubleshoot and resolve a failed Symantec Endpoint Protection Manager installation.
- Troubleshoot and resolve a failed Symantec Endpoint Protection for Windows client install.
- Troubleshoot and resolve a failed Symantec Endpoint Protection for Mac client install.
- Troubleshoot and resolve a failed Symantec Endpoint Protection for Linux client install.

Module 4: Client Communication Issues

- Identify the interactions between the client and the SEPM.
- Identify heartbeat process.
- Locate and configure debug logs for client communication issues.
- Describe communications issues from the client perspective.
- Identify Linux and Mac communication issues.

Module 5: Content Distribution Issues

- Troubleshoot and resolve LiveUpdate issues on the SEPM and client.
- Troubleshoot and resolve issues between a client and management server.
- Troubleshoot and resolve issues from clients who retrieve updates from a Group Update Provider.

Module 6: Extending the SEP infrastructure

- Describe how data is transferred during replication and know which replication logs are affected.
- Automate functionality with Rest APIs.
- Integrate Symantec Endpoint Protection with third party applications.

Module 7: Responding to a Security Incident

- Identify and examine useful SEPM reports for incent response
- Learn the best approach for handling a virus outbreak
- Identify and submit false positives to Broadcom

Module 8: Performance Issues

- Assess SEP performance using sizing and scalability recommendations
- Optimize performance for the SEPM
- Optimize performance for the SEP client
- Utilities and other resources
- Case studies

Symantec Endpoint Security Complete Administration R1.4

Course Code: 000264

Course Description

The *Symantec Endpoint Security Complete Administration R1.4* 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 a SESC endpoint security environment. The course focuses on SES Complete cloud-based management using the ICDm management console.

Delivery Method

Instructor-Led

Duration

Five Days

Course Objectives

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

- Describe the benefits of using a multi-layered cloudbased environment for endpoint security.
- Secure endpoints against network, file based, and emerging threats.
- Control endpoint integrity and compliance.
- Respond to security threats using SESC monitoring and reporting.
- Enforce adaptive security compliance.
- Protect Active Directory
- Use SESC in a Hybrid Environment / Migrate to the Cloud

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.

Prerequisites

This course assumes that students have a basic understanding of advanced computer terminology, an administrator-level knowledge of Microsoft Windows operating systems, and have viewed the “Symantec Endpoint Security Complete – Basic Administration” eLearning content prior to attending this course.

Certification

250-580: Symantec Endpoint Security Complete Administration R2

Course Outline

Module 1: Introduction to Endpoint Security Complete

- Introduction
- SES Complete Architecture
- SES Complete Cloud-Based Management
- SES Complete in a Hybrid Environment
- SES Complete Device Group Management
- SES Complete Client Deployment ▪ SES Device Management

Module 2: Configuring SES Complete Security Controls

- Policy Overview
- Threat Overview and the MITRE ATT&CK Framework
- Preventing Initial Access
- Preventing Execution
- Preventing Persistence
- Preventing Privilege Escalation
- Preventing Defense Evasion
- Preventing Discovery
- Blocking Command & Control
- Blocking Exfiltration
- Blocking the Impact Phase
- Managing Content Updates
- Policy Versioning and History

Module 3: Responding to Threats with ICDm

- The ICDm Home Page
- Searching SES Data
- Using SES Reports
- Configuring Alerts
- Managing Mitigation
- Acting on Events

Module 4: Endpoint Detection and Response

- Introduction to EDR
- Detecting Threats
- Investigating Threats
- Responding to Threats

Module 5: Attack Surface Reduction

- Reduce the Attack Surface with Adaptive Protection
- Reduce the Attack Surface with Application Control
- Reduce the Attack Surface with Custom Application Behavior
- Reduce the Attack Surface with Host Integrity

Module 6: Mobile and Modern Device Security

- Definition of Modern and Mobile Devices
- Modern and Mobile Threats
- Introducing Network Integrity
- Network Integrity Policy Configuration
- Network Integrity for Windows 10 Modern Devices
- Network Integrity for Mobile Devices ▪ Exploring Generated Alerts

Module 7: Threat Defense for Active Directory

- Active Directory Security Challenges
- Introducing Threat Defense for Active Directory
- TDAD Configuration
- Threat Scenarios and Remediation

Module 8: Working with a Hybrid Environment

- Reasons for Moving to the Cloud
- SES / SEP Hybrid Architecture
- Moving to Hybrid Managed
- Policies and Device Management from the Cloud
- Migrating to the Cloud

Information Security

Information security controls are vital to protecting an organization’s sensitive data from falling into the wrong hands, as well as its reputation and bottom line. Symantec Information Security delivers a world-class data access and protection platform that provides our customers with visibility and control of their information everywhere it goes and mitigates the risk of data breaches, account takeover fraud, lateral movement attacks, and shadow IT.

Learn more by taking the courses in this section.

Symantec CloudSOC R3 Administration

Course Code: 000270

Course Description

The *Symantec CloudSOC R3 Administration* course provides an overview of the CloudSOC service, covering initial setup, deployment options and service configuration. The courseware introduces each topic with an accompanying workflow and is designed for IT professionals wishing to develop the knowledge and skills to manage the Symantec CloudSOC (CASB) solution.

Delivery Method

Instructor-Led

Duration

Two Days

Course Objectives

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

- Describe the major functions of CloudSOC.
- Import Firewall and/or Proxy information to provide granular information on the current behaviors of end users.
- Configure CloudSOC to monitor data at rest and in motion.
- Create policies to monitor and control what is uploaded and with whom data is shared.
- Describe important integration points with other products within the Symantec portfolio.

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.

Prerequisites

This course assumes that students have a basic understanding of information security concepts.

Certification

- 250-443: Symantec CloudSOC Administration R2 Technical Specialist

Course Outline

Module 1: Introduction to Symantec CloudSOC

- Benefits and Challenges of Cloud Applications
- Problems CloudSOC Solves
- CloudSOC tools, information sources, and traffic flows

Module 2: Configuring the Symantec CloudSOC Portal

- Basic Navigation
- Managing Users, Groups, and Access Profiles
- Administrative Actions in the Settings Menu
- Auditing administrative actions
- Configuring Two-Factor Authentication

Module 3: Identifying and Addressing Potential Risks in Cloud Applications

- Cloud applications and their risks
- The Cloud Application Discovery and Safe Adoption Lifecycle
- The Cloud Application Adoption Workflow
- The CloudSOC Business Readiness Rating
- Importing firewall/proxy logs
- Using Audit data to inform policy in ProxySG

Module 4: Identifying How Data is Used and Shared in Cloud Applications

- Risk of shadow IT and shadow data
- Risk of malware and advanced threats
- Configuring CloudSOC to collect cloud-application log data
- Understanding how CloudSOC monitors data in motion
- Configuring CloudSOC to monitor data in motion

Module 5: Identifying and Remediating Risky Behavior in Cloud Applications

- Identifying and remediating risky behavior in cloud applications: overview
- Understanding and configuring detectors
- Reviewing anomalous or unauthorized user activity
- Creating ThreatScore-based policies

Module 6: Protecting Data in Cloud Applications

- Understanding the CloudSOC data protection workflow
- Using CloudSOC to control data exposure
- Integrating CloudSOC with Information Centric Encryption (ICE)
- Integrating CloudSOC with Symantec DLP

Module 7: Understanding Reporting Options in CloudSOC and Third-Party Solutions

- Overview of default CloudSOC reporting
- Integrating CloudSOC with SIEM solutions

Symantec Data Loss Prevention 16.x Administration

Course Code: 000236

Course Description

The *Symantec Data Loss Prevention 16.x Administration* course is designed to provide you with the fundamental knowledge to configure and administer the Symantec Data Loss Prevention Enforce platform. The hands-on labs include exercises for configuring the Enforce server, detection servers, and DLP agents; creating policies; detecting and responding to incidents; performing incident reporting; and administering users and roles. You are introduced to the following Symantec Data Loss Prevention components: Network Monitor, Network Prevent, Network Discover, Network Protect, Endpoint Prevent, and Endpoint Discover. In addition, the course includes some introductory discussion of the integration with Symantec CloudSOC CASB.

NOTE: This course is delivered on a Microsoft Windows platform.

Delivery Method

Instructor-Led

Duration

Five Days

Course Objectives

By the end of this course, you will be able to configure and use Symantec Data Loss Prevention 16.x.

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.

Prerequisites

- Working knowledge of Windows server-class operating systems and commands
- Networking and Network Security concepts
- Technical users responsible for creating and maintaining policies and incident responses

Course Outline

Module 1: Data Loss Prevention Landscape

- Data loss risk management
- Data Loss Prevention landscape
- Data Loss Prevention use cases

Module 2: Overview of Symantec Data Loss Prevention

- Symantec Data Loss Prevention Suite
- Symantec Data Loss Prevention architecture

Module 3: Identifying and Describing Confidential Data

- Identifying confidential data
- Configuring Symantec Data Loss Prevention to recognize confidential data
- Described Content Matching (DCM)
- User Risk-Based Detection
- Exact matching (EDM and EMDI)
- Indexed Document Matching (IDM)
- Vector Machine Learning (VML)
- Sensitive Image Recognition
- Custom file type detection
- Using policy templates
- **Hands-On Labs**: Tour the Enforce console, create policy groups, configure policies for Personally Identifiable Information (PII) detection, configure a policy for PCI compliance, configure a policy to protect confidential documents, configure a policy to protect source code, configure a policy for Form Recognition, use a template to add a DLP policy, export policies for use at a Disaster Recovery (DR) site, configure Optical Character Recognition (OCR)

Module 4: Locating Confidential Data Stored on Premises and in the Cloud

- Determining where to search for confidential data
- Locating confidential data on corporate repositories
- Locating confidential data in the Cloud
- Locating confidential data on endpoint computers
- **Hands-On Labs**: Run a Content Enumeration Scan, run a high-speed Discover scan, scan a Windows target, scan endpoint computers for confidential data

Module 5: Understanding How Confidential Data is Being Used

- Monitoring confidential data moving across the network
- Monitoring confidential data being used in the Cloud
- Monitoring confidential data being used on endpoint computers
- **Hands-On Labs**: Update the DLP Agent using
- LiveUpdate, Configure Network Prevent for Email to monitor SMTP messages, use Network Prevent for Email to monitor SMTP messages, monitor Endpoint activity

Module 6: Educating Users to Adopt Data Protection Practices

- Implementing corporate training on data protection policies
- Providing notifications of user policy violations
- **Hands-On Labs**: Configure the Active Directory lookup plugin, create custom attributes, configure email notifications, configure onscreen notifications

Module 7: Preventing Unauthorized Exposure of Confidential Data

- Using response rules to prevent the exposure of confidential data
- Protecting confidential data in motion
- Protecting confidential data in use
- Protecting confidential data at rest
- **Hands-On Labs**: Configure SMTP blocking, test Optical Character Recognition (OCR) and the “HIPAA and HITECH (including PHI)” policy, configure endpoint blocking, configure endpoint User Cancel, scan and quarantine files on a server file share target, scan and quarantine files on an endpoint target

Module 8: Remediating Data Loss Incidents and Tracking Risk Reduction

- Reviewing risk management frameworks
- Using incident reporting options to identify and assess risk
- Creating tools that support the organization's risk reduction process
- Communicating risk to stakeholders
- Understanding advanced reporting options and analytics
- **Hands-On Labs**: Define incident statuses and status groups, configure Smart Responses, configure roles and users, reassign users' default roles, create work queues, test workflow, use reports to track risk exposure and reduction

Module 9: Enhancing Data Loss Prevention with Integrations

- Symantec DLP integration mechanisms
- Symantec DLP integrations with other Symantec products
- Symantec DLP + Microsoft Purview Information Protection (MPIP)
- **Hands-On Labs**: Use the incident "flag for deletion" function, create a Web report, schedule and send reports

Module 10: Course Review

- Review of Symantec Data Loss products and architecture
- Review of the stages in a Data Loss Prevention implementation

Symantec Data Loss Prevention 16.x Differences

Course Code: 000240

Course Description

The *Symantec Data Loss Prevention 16.0 Differences* course is designed for experienced Data Loss Prevention (DLP) administrators and users who are already familiar with Symantec DLP and want to learn latest the features introduced in Symantec DLP 16.0. The course covers endpoint, detection, storage, reporting, and API features in the 16.0 release. These features include enhanced support for LiveUpdate (for upgrading DLP Agents), the new Linux DLP Agent, thirdparty certificates for Endpoint Servers and DLP Agents, User Risk-Based Detection (powered by an integration with Symantec Information Centric Analytics), Structured

Data Matching, High-Speed File-System Scanning (for Network Discover), and Incident Reporting enhancements.

Delivery Method

Instructor-Led

Duration

Two days

This includes a half-day of instructor lecture and two days of access to a Symantec DLP 16.0 practice environment.

Course Objectives

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

- Understand Symantec DLP 16.0 endpoint, detection, storage, reporting, and API features
- Understand how to important Symantec DLP 16.0 features such as User Risk-Based Detection, Structured Data Matching, and High-Speed File-System Scanning

Practice Environment

Students in this course are provided access to a Symantec DLP 16.0 practice environment (sandbox) in which to explore and experiment with the latest version of the product.

Prerequisites

- Strong knowledge of Symantec DLP
- Experience using Symantec DLP

Additional Courses Available

- Symantec Data Loss Prevention 16.0 Differences (eLearning)
- Symantec Data Loss Prevention 15.x Administration
- Symantec Data Loss Prevention 15.5 Planning and Implementation
- Symantec Data Loss Prevention 15.5 Policy Authoring and Incident Remediating

Course Outline

Module 1: Symantec DLP 16.0 Endpoint Features

- LiveUpdate Enhancements for DLP Agent Updates
- Linux DLP Agent
- General Endpoint Updates
- Windows DLP Agent Support for Microsoft Information Protection Classification of Microsoft Outlook Emails
- Mac DLP Agent Print Coverage
- Translatable Strings for Endpoint Messages
- Endpoint IPv6 Support
- Custom Certificates for Endpoint Servers and DLP Agents

Module 2: Symantec DLP 16.0 Detection Features

- Improved Data Identifier Engine
- Structured Data Matching
- Boolean Compact Policy (BCP) Tree
- User Risk-Based Detection

Module 3: Symantec DLP 16.0 Storage, Reporting, & API Features

- High-Speed File-System Scans
- Incident List Enhancements
- Incident Masking
- Enforce REST APIs

Network Security

End users are everywhere and need quick access to data and cloud applications around the clock. Organizations must stop inbound and outbound threats that target their end users, information, and key infrastructure. Today’s web protection must account for this reality while balancing security, performance, complexity, and cost. Our Network Security portfolio includes the solutions customers need to do just that, whether in the cloud, on-premises, or both.

Symantec ProxySG 7.3 Administration with Secure Web Gateway

Course Code: 000012

Description

The ProxySG 7.3 Administration with Secure Web Gateway course provides a detailed exploration of the Symantec Secure Web Gateway family of network protection products. It is primarily focused on the ProxySG and its role in providing security and web filtering services, but also includes integrations with Management Center, Reporter, Web Isolation, Content Analysis, and Cloud solutions.

Delivery Method

Instructor-Led

Duration

Three Days

Objectives

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

- Describe the major functions of the ProxySG as a secure web gateway
- Understand how network security and administrative tasks are enhanced by integrating the ProxySG with the other members of the Symantec Secure Web Gateway family

Prerequisites

This course assumes that students have a basic understanding of networking concepts, such as local area networks (LANs), the Internet, security, and IP protocols.

Labs

The modules are accompanied by recorded lab demonstrations that illustrate the topics covered in the modules

Course Outline

Module 1: Introduction to the Symantec Secure Web Gateway

- Overview of the Symantec Secure Web Gateway family of products
- Introduction to the ProxySG, including key features, SGOS, the Global Intelligence Network, and management consoles

Module 2: Intercept traffic and apply policy

- Proxy services
- Writing policies in the Visual Policy Manager

Module 3: Apply security and web usage policy to encrypted traffic

- Key components of SSL encryption
- Managing SSL traffic with the ProxySG
- Integrating the SSL Visibility Appliance

Module 4: Provide security and web usage policies based on role or group

- Authentication on the ProxySG
- Authentication realms, credentials, and modes

Module 5: Enforce corporate guidelines for acceptable Internet browsing behavior

- Determine appropriate use guidelines
- Write appropriate use policies

Module 6: Protect the endpoint from malicious activity

- Writing security policies using threat risk levels
- Ensuring safe downloads

Module 7: Centrally manage, monitor, and report on security activity

- Using Management Center to manage ProxySGs
- Using the SG Admin Console
- Generating reports in Reporter

Module 8: Maintaining the ProxySG, Management Center, and Reporter for optimal performance

- Monitoring the ProxySG within Management Center
- Using built-in health checks on devices

Module 9: Prevent malware and phishing threats while allowing broad web access

- Symantec Web Isolation fundamentals
- Isolation options for protecting privileged users and defending against phishing attacks
- Authentication in explicit and transparent proxy modes

Module 10: Enhance security by adding virus scanning and sandboxing with Content Analysis

- Virus scanning and sandboxing with Content Analysis
- Scanning best practices

Module 11: Expand security capabilities with cloud integrations

- Integrating Web Security Service
- Integrating CloudSOC Audit

Module 12: Course review

Symantec Web Isolation Planning, Implementation and Administration R2

Course Code: 000195

Course Description

The *Symantec Web Isolation Planning, Implementation, and Administration R2* course provides a detailed introduction to Symantec's two cloud-based isolation services: High Risk Isolation (HRI) and the Web Isolation dedicated tenant. The course includes implementation of the key protection scenarios with both Web Security Service and the ProxySG, as well as a description of the functions available in the Web Isolation management console.

Delivery Method

Instructor-Led

Duration

One Day

Course Objectives

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

- Describe the major Web Isolation functions and capabilities
- Write policies to selectively isolate risky and uncategorized websites, allow privileged users greater access, and defend against phishing and ransomware attacks
- View reports and monitor solution performance

Hands-On

This course includes pre-recorded demonstrations that illustrate the concepts discussed in the lessons

Prerequisites

- Basic understanding of networking concepts
- Basic understanding of network security concepts
- Basic understanding of the use of proxy servers

Course Outline

Module 1 Introduction to Symantec Web Isolation

- The need for a web isolation solution
- Symantec Web isolation—Protection without detection
- High Risk Isolation web traffic protection
- Web Isolation dedicated tenant web traffic protection

Module 2: Implementing Web Isolation

- Implementing Isolation with Web Security Service
- Implementing Isolation with the ProxySG

Module 3: Administering the Web Isolation dedicated tenant

- Web isolation management console overview
- Removing active content from webpages
- Isolating links embedded in email to defend against phishing attacks
- Enabling safe file download protections
- Working with applications remotely

Module 4: Viewing reports, monitoring performance, and troubleshooting

- Viewing reports
- Monitoring performance
- Troubleshooting tools

Module 5: Integrating Web Isolation with DLP, CloudSOC Mirror Gateway, and Email Security.cloud

- Integrating Web Isolation with DLP
- Integrating Web Isolation with CloudSOC Mirror Gateway
- Integrating Web Isolation with Symantec Email Security.cloud
- Integrating Web Isolation with third-party providers

Module 6: Course review

- Symantec Web Isolation course review

Symantec Web Protection – Cloud SWG Planning, Implementation and Administration R1

Course Code: 000208

Course Description

The Symantec Web Protection - Cloud SWG Planning, Implementation, and Administration course is intended for IT professionals who will be planning, installing, configuring or administering the Symantec Cloud Secure Web Gateway.

Delivery Method

Instructor-Led

Duration

Two Days

Course Objectives

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

- Describe the architecture, components and process flow of Cloud SWG
- Identify installation, configuration and administration of the core features and products of Cloud SWG.
- Identify the key elements for planning a Cloud SWG deployment

Labs

- Lab Login and Cloud SWG Portal Introduction
- Install and Explore the WSS Agent
- Create a Bypass List
- Create a Custom PAC File for Remote Locations
- Implement Web and Cloud Access Protection Integration
- Install Auth Connector
- Create and Deploy Policies to Limit Social Media Use
- Create a Source Geography based Policy to Ensure Save Internet Usage
- Create a Customized Response Page
- Block Sites Based on Risk Level
- Improved Administration with Cloud SWG Reporting Tools

Prerequisites

- Working knowledge of cloud based solutions
- Knowledge of internet traffic protocols
- Basic understanding of principles of authentication

Additional Courses Available

- Web Protection Cloud SWG – Diagnostics and Troubleshooting
- Web Protection Edge SWG – Planning, Implementation, and Administration
- Web Protection Edge SWG – Diagnostics and Troubleshooting

Certification

Exam 250-554: Administration of Symantec Web Security Service – R1.2

Course Outline

Module 1: Cloud Delivered Security

- What is Cloud Delivered Security
- What are the Key Considerations for Having Cloud Delivered Security
- What are the Key Features Needed for Cloud Delivered Security

Module 2: Cloud SWG Connection Architecture and Functionality

- Cloud SWG Infrastructure
- Cloud SWG Connection Architecture
- Cloud SWG Features
- Cloud SWG Additional Products

Module 3: Getting Started with Cloud SWG

- Initial Registration
- User Administration
- Licensing
- Data Privacy Settings

Module 4: Enable Remote Users to Securely Access the Internet

- Remote Users and Solutions
- WSS Agent Access Method
- Web and Cloud Access Protection Access Method
- Cloud Connect Defense (CCD) Access

Module 5: Provide Safe and Proper Web Usage Based on User Identity

- Authentication and Cloud SWG
- Auth Connector SAML
- Remote Authentication Methods with Auth Connector
- Authentication with WSS Agent and Web and Cloud
- Access Protection Access Methods

Module 6: Create a more Effective Work Environment for Employee Web Usage

- Configure Content Filtering Rules to Determine Internet Usage
- Setting Global Content Filtering Policy Rules
- Creating Custom Response Pages
- Universal Policy Enforcement

Module 7: Providing Web Protection Against Malware

- Cloud SWG Threat Protection
- Malware Analysis and Cloud SWG
- Threat Protection Policies ▪ Creating Threat Protection Policy Rules

Module 8: Enable Encrypted Traffic Inspection

- Encrypted Traffic
- SSL Configuration
- Configuring SSL Exceptions
- Topic Title

Module 9: Enable Corporate Users to Securely Access the Internet

- Firewall/VPN (IPsec) Access Method
- FQDN-IKEv2 Firewall Access Method
- TransProxy (Explicit Proxy Over IPsec) Access Method
- Proxy Forwarding Access Method

Module 10: Identify Web Usage and Security Statistics with Reports

- Reports Overview
- Pre-defined Reports
- Simple Reporting
- Custom Reporting
- Forensic Reporting
- Managing and Using Reports

Module 11: Enable Mobile Users to Securely Access the Internet

- About Mobile Device Security
- Authentication for Mobile Users
- SEP-Mobile Solution
- Android Mobile Access Enrolment Process

Module 12: Planning Cloud SWG Deployments

- Assessment of Needs
- Design – Access Methods and Authentication
- Design – Policy, Reporting and Threat Protection
- Design Evaluation

Symantec Web Protection – Cloud SWG Diagnostics and Troubleshooting R1

Course Code: 000214

Course Description

The Symantec Cloud Secure Web Gateway Diagnostics and Troubleshooting course is intended for IT professionals who will be diagnosing and troubleshooting the Symantec Cloud Secure Web Gateway.

Delivery Method

Instructor-Led and Virtual Academy

Duration

Two Days

Course Objectives

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

- Describe the architecture, components and process flow of Cloud SWG
- Identify the steps to diagnose, troubleshoot and resolve a broad range of issues with Cloud SWG to include Access Methods, Authentication Means, Web and File Access, as well as Performance Issues

Hands-on Labs

- Setup FQDN Firewall Lab
- Break Tenant Lab
- Setup Fail Over Lab
- Explicit Over IPsec Lab
- Setup Agents Lab
- Troubleshooting Agents Lab
- Install Auth Connector Lab
- Configure Auth Connector as SAML IdP Lab
- Troubleshooting Auth Connector as SAML IdP Lab
- Configure Captive Portal Lab
- Reporting Lab
- SymDiag Lab

Prerequisites

- Working knowledge of cloud based solutions
- Knowledge of internet traffic protocols
- Basic understanding of principles of authentication

Additional Courses Available

- Web Protection Cloud SWG – Planning, Implementation, and Administration
- Web Protection Edge SWG – Planning, Implementation, and Administration
- Web Protection Edge SWG – Diagnostics and Troubleshooting R1

Course Outline

Module 1: Cloud SWG Architecture, Components, Architecture and Integrations

- Understand the Troubleshooting Methodology
- Know the core components
- Comprehend the Architecture and Process flow ▪ Basic understanding of:
- Cloud Firewall Service
- Data Loss Prevention Integration
- CloudSOC Integration
- Web Isolation Integration

Module 2: Cloud SWG Corporate Access Methods

- Define problems with Corporate Access Methods
- Diagnose and Solve problems with Corporate Access Methods
- Results with Corporate Access Methods

Module 3:Cloud SWG Remote Access Methods

- Define problems with Remote Access Methods
- Diagnose and Solve problems with Remote Access Methods
- Results with Remote Access Methods

Module 4: Website and File Access Issues

- Define problems with Authentication Means
- Diagnose and Solve problems with Authentication Means
- Results with Authentication Means

Module 5: Provide Safe and Proper Web Usage Based on User Identity

- Define Website and File Access Issues
- Diagnose and Solve Website and File Access Issues
- Results with Website and File Access Issues

Module 6: Cloud SWG Performance Issues

- Component, Architecture and Process Flow of WSS Internet Performance Issues
- Define problems with Cloud SWG Internet Performance Issues
- Diagnose Problems with Cloud SWG Internet Performance Issues
- Solving Problems with Cloud SWG Internet Performance Issues
- Results of Internet Performance Issues with Cloud SWG

Module 7: Key Points of Diagnostics and Troubleshooting

- Examining Cloud SWG Architecture, Components, and Integrations – Key Points
- Corporate Access Methods Module – Key Points
- Remote Access Methods Module – Key Points
- Authentication Means Module – Key Points
- Troubleshooting Website and File Access Issues – Key Points
- Troubleshooting Performance Issues – Key Points

Symantec Web Protection – Edge SWG Planning, Implementation and Administration R1

Course Code: 000209

Course Description

The *Symantec Web Protection—Edge SWG Planning, Implementation, and Administration* course provides a detailed introduction to the features that comprise Edge SWG, which is the on-premise component of Symantec Web Protection. These applications include ProxySG, Management Center, Reporter, Content Analysis, and High Risk Isolation.

Delivery Method

Instructor-Led

Duration

Four days

Course Objectives

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

- Describe the major Edge SWG functions and capabilities
- Write policies to defend enterprise networks against malware attacks and to enforce acceptable Internet browsing behavior
- Understand how the various applications work together to secure enterprise networks
- View reports and monitor solution performance

Hands-On

This course includes practical hands-on exercises that enable students to test their understanding of the concepts presented in the lessons.

Prerequisites

- Basic understanding of networking concepts
- Basic understanding of network security concepts
- Basic understanding of the use of proxy servers

Additional Courses Available

- Web Protection Cloud SWG – Planning, Implementation, and Administration
- Web Protection Cloud SWG – Diagnostics and Troubleshooting R1
- Web Protection Edge SWG – Diagnostics and Troubleshooting R1

Course Outline

Module 1: Introduction to Symantec Edge SWG

- ▪ Overview of Web Protection Suite
- Overview of Edge SWG components

Module 2: Intercepting web traffic and applying policy

- How the ProxySG intercepts traffic
- Writing policy on the ProxySG
- Layer and rule evaluation order in the VPM

Module 3: Applying security and web usage policy to encrypted traffic

- Introduction to TLS
- Managing HTTPS traffic on the ProxySG

Module 4: Providing security and web usage policies based on role or group

- Authentication basics on the ProxySG
- Using IWA authentication on the ProxySG
- Authentication modes in explicit and transparent modes
- Connecting to the Windows domain directly using IWA direct
- Connecting to the Windows domain using IWA BCAAA
- Using roles and groups in policy

Module 5: Enforcing corporate guidelines for acceptable Internet browsing behavior

- Create strong corporate guidelines for acceptable Internet use
- Use website categorization to enforce acceptable use guidelines
- Provide the ProxySG with categorization databases to be referenced in policy
- Set the Request URL Category object in policy to enforce acceptable use guidelines
- Inform users when web access is denied or restricted due to policy

Module 6: Protecting the endpoint from malicious activity

- WebPulse technical details
- Introduction to Intelligence Services
- Using Intelligence Services data feeds in policy
- Ensuring safe downloads

Module 7: Centrally managing devices with Management Center

- How Management Center centralizes and simplifies device management
- Configuring the ProxySG with the ProxySG Admin Console
- Creating and distributing VPM policies
- Creating and managing jobs
- Use reports to analyze web browsing activity

Module 8: Reporting for Edge SWG features

- How Reporter delivers centralized web reporting
- Configuring access logging on the ProxySG
- Using the Reporter Admin Console to configure log processing on Reporter

Module 9: Enhancing security with virus scanning

- Introduction to Content Analysis
- Exploring the Content Analysis management console
- Configuring communication with the ProxySG over ICAP
- Configuring malware scanning options

Module 10: Using malware analysis to analyze potentially malicious files

- Introduction to malware analysis
- Preparing the use malware analysis
- Performing malware analysis

Module 11: Providing security for risky and unknown websites with High Risk Isolation

- Introduction to High Risk Isolation
- Configuring HRI
- Overview of Symantec Web Isolation

Module 12: Monitoring Edge SWG features

- Monitoring devices from within Management Center
- Monitor and maintain the Content Analysis
- Troubleshooting tips

Module 13: Understanding SGOS architecture and caching on the Edge SWG

- SGOS architecture
- Caching on the Edge SWG
- Using HTTP compression

Module 14: Using built-in diagnostic tools on the Edge SWG

- Exploring sysinfo files
- Using policy tracing and policy coverage
- Using packet captures
- Sending service information to Symantec

Module 15: Expanding security with cloud integrations

- Introduction to Cloud SWG
- Using Universal Policy Enforcement
- Integrating CloudSOC with Symantec Web Protection

Module 16: Course review

- Symantec Web Protection--Edge SWG Planning, Implementation, and Administration course review

Appendix A: Using Content Policy Language (CPL)

- Basic CPL concepts
- Intermediate CPL concepts
- Using CPL best practices

Appendix B: Introduction to Hypertext Transport Protocol (HTTP)

- Basic HTTP concepts

Symantec Web Protection – Edge SWG Diagnostics and Troubleshooting R1

Course Code: 000234

Course Description

The *Symantec Web Protection—Edge SWG Diagnostics and Troubleshooting R1* course provides a structured approach to diagnosing and solving common troubleshooting issues related to Edge SWG deployments. The course will emphasize building competency in the use of the powerful diagnostic tools available on the Edge SWG.

Delivery Method

Instructor-Led

Duration

One Day

Course Objectives

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

- Describe the troubleshooting methodology as recommended by Symantec.
- Diagnose and solve a variety of issues using tools such as sysinfo files, packet captures, and policy traces.
- Be able to provide various diagnostic files to Symantec Support when requested.

Hands-On

This course includes both analysis of pre-existing diagnostic files (such as sysinfo, packet capture, policy traces) as well as practical hands-on exercises that enable students to test their understanding of the concepts presented in the lessons.

Prerequisites

It’s expected that students will have taken the Symantec Web Protection - Edge SWG Planning, Implementation, and Administration R1 course.

Course Outline

Module 1: Edge SWG Diagnostics and Troubleshooting Overview

- Symantec troubleshooting methodology
- Symantec Edge SWG component review
- Key diagnostic tools review

Module 2: Diagnosing Common Issues on the Edge SWG

- Diagnosing CPU usage issues
- Diagnosing memory usage issues
- Diagnosing issues with external dependencies

Module 3: Troubleshooting Authentication Issues on the Edge SWG

- Overview of authentication on the Edge SWG
- Defining issues related to authentication
- Diagnosing issues related to authentication
- Solving issues related to authentication
- Result—Communicating result or contacting Symantec support

Module 4: Troubleshooting Encrypted Traffic Management Issues on the Edge SWG

- Review of SSL interception on the Edge SWG
- Defining issues related to SSL interception
- Diagnosing issues related to SSL interception
- Solving issues related to SSL interception
- Result—Communicating result or contacting Symantec support

Module 5: Troubleshooting DNS Issues on the Edge SWG

- Overview of DNS service on the Edge SWG
- Defining issues related to DNS lookups
- Diagnosing issues related to DNS lookups
- Solving issues related to DNS lookups
- Result—Communicating result or contacting Symantec support

Module 6: Troubleshooting Policy Issues on the Edge SWG

- Review of policy operations on the Edge SWG
- Defining policy issues on the Edge SWG
- Diagnosing policy issues on the Edge SWG
- Solving policy issues on the Edge SWG
- Result—Communicating result or contacting Symantec support

Carbon Black

Carbon Black Endpoint empowers security teams to simplify operations and accelerate workflows across their endpoints, workloads and containers to drive better security outcomes with fewer tools to manage. Top security professionals choose Carbon Black for endpoint protection because it provides granular control over and context about their environment in an easy-to-use console that doesn't require significant upkeep so they can focus on accelerating their business.

Carbon Black App Control secures critical systems, prevents unwanted changes and ensures continuous compliance with regulatory mandates. Employing a Positive Security Model, which enables a default/deny security posture, Carbon Black App Control continuously protects against cyber-threats that evade traditional security defences. App Control does not rely on a library or "list" of files to maintain, which can easily become outdated. Instead, it employs multiple approval methods, including IT & Cloud Driven Trust, Trusted Publishers, Custom Rules and validated External Sources

Carbon Black Enterprise EDR empowers security teams with customizable defences, deep visibility and accelerated threat detection and response capabilities. From a single agent and console, it empowers teams to prioritize high quality data by detecting and responding to threats in real time, stopping active attacks and repairing damage quickly.

Carbon Black XDR elevates your cybersecurity defences and makes it harder for attackers to hide and ransomware to thrive. With extensive visibility across endpoints, workloads, users, and networks, Carbon Black XDR levels up EDR to deliver a comprehensive protection strategy with one intuitive console. It enables organizations to find real threats in minutes, not days, through faster detection and response and automated telemetry correlation. Carbon Black's unique approach ensures a proactive stance against sophisticated threats and enhanced security across an organization's digital environment.

Carbon Black Workload is a cloud-native security solution that enables security teams to detect, prevent, and respond to advanced threats. It combines deep visibility and workload hardening with industry-leading prevention, detection, and response capabilities to protect workloads running in on premises and cloud environments. CB Workload collects detailed workload telemetry in a single console and enables security, infrastructure and cloud teams to automatically secure new and existing workloads at every point in the security lifecycle, while simplifying operations and consolidating the IT and security stack.

VMware Carbon Black App Control Administrator

Course Code: 000274

Course Description

This one-day course teaches you how to use the VMware Carbon Black® App ControlTM product and leverage the capabilities to configure and maintain the system according to their organization's security posture and organizational policies. This course provides an in-depth, technical understanding of the Carbon Black App Control product through comprehensive coursework and hands-on scenario based labs.

Delivery Method

Instructor-Led

Duration

One Day

Course Objectives

Upon completion of this course, you will be able to:

- Describe the components and capabilities of application control
- Manage and configure the Carbon Black App Control server based on organizational requirements
- Create policies to control enforcement levels and agent functionality
- Implement rules to support the organization's security posture
- Use the Carbon Black App Control tools to understand agent and server data

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.

Prerequisites

There are no prerequisites for this course.

Course Outline

Module 1: Course Introduction

- Introductions and course logistics
- Course Objectives

Module 2: Login Accounts and Groups

- User accounts
- User roles

Module 3: Policies

- Modes and Enforcement Levels
- Rule sets

Module 4: Notifiers

- Agent side display notification use

Module 5: Computer Details

- Related views

Module 6: Override

- Use Case and functionality

Module 7: Software Approvals

- Methods and use cases

Module 8: Custom Rules

- Rule type and use cases

Module 9: Tools

- Meters and Alerts

Module 10: Events

- Agent and server events
- View agent information

Module 11: Baseline Drift

- Changes in a baseline

VMware Carbon Black App Control Advanced Administrator

Course Code: 000275

Course Description

This one-day course teaches you how to configure and scope the rules within VMware Carbon Black® App ControlTM product to maintain the system according to your organization's security posture and organizational policies. Additionally, this course covers troubleshooting both the server and the agent for Carbon Black App Control and how to identify issues that impact normal operations. This course provides an in-depth, technical understanding of the Carbon Black App Control product through comprehensive coursework and hands-on scenario-based labs.

Delivery Method

Instructor-Led

Duration

One Day

Course Objectives

Upon completion of this course, you will be able to:

- Manage and configure the Carbon Black App Control sever based on organizational requirements
- Implement rules to support business processes and automatic approvals
- Identify scenarios and use cases for Custom rules and Event rules
- Describe common troubleshooting scenarios for the Carbon Black App Control server
- Describe common troubleshooting scenarios for the Carbon Black App Control Windows agent

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.

Prerequisites

This course requires completion of one following course

- VMware Carbon Black App Control Administration

Course Outline

Module 1: Course Introduction

- Introductions and course logistics
- Course objectives

Module 2: Custom Rules Basics

- Execute / Write action rules
- Precedence
- Paths

Module 3: Custom Rules Best Practices

- Rule Triad
- Rule multiplication

Module 4: Rule Types

- Custom rule type overview

Module 5: Optimizing Custom Rules

- Evaluating events

Module 6: Event Rules

- Creating and editing
- Testing before implementing

Module 7: Troubleshooting Considerations

- Server versus agent issues

Module 8: Server Capabilities

- Tools, logs, common issues, scenarios

Module 9: Agent Capabilities

- Tools, logs, common issues, scenarios

VMware Carbon Black EDR Administrator

Course Code: 000282

Course Description

This one-day course teaches you how to use the VMware Carbon Black® EDR™ product and leverage the capabilities to configure and maintain the system according to your organization's security posture and policies. This course provides an in-depth, technical understanding of the Carbon Black EDR product through comprehensive coursework and hands-on scenario-based labs.

Delivery Method

Instructor-Led

Duration

One Day

Course Objectives

- Upon completion of this course, you will be able to:
- Describe the components and capabilities of the
- Carbon Black EDR server
- Identify the architecture and data flows for Carbon Black EDR communication
- Describe the Carbon Black EDR server installation process
- Manage and configure the Carbon Black EDR sever based on organizational requirements
- Perform searches across process and binary information
- Implement threat intelligence feeds and create watchlists for automated notifications
- Describe the different response capabilities available from the Carbon Black EDR server
- Use investigations to correlate data between multiple processes

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.

Prerequisites

There are no prerequisites for this course.

Course Outline

Module 1: Course Introduction

- Introductions and course logistics

Module 2: Planning and Architecture

- Hardware and software requirements
- Architecture
- Data flows
- Server installation review
- Installing sensors

Module 3: Server Installation & Administration

- Configuration and settings
- Carbon Black EDR users and groups

Module 4: Process Search and Analysis

- Filtering options
- Creating searches
- Process analysis and events

Module 5: Binary Search and Banning Binaries

- Filtering options
- Creating Searches
- Hash banning

Module 6: Search best practices

- Search operators
- Advanced queries

Module 7: Threat Intelligence

- Enabling alliance feeds
- Threat reports details
- Use and functionality

Module 8: Watchlists

- Use and Functionality

Module 9: Alerts / Investigations/ Response

- Creating Watchlists Using the HUD
- Alerts workflow
- Using network isolation
- Using live response

VMware Carbon Black Advanced Administrator

Course Code: 000283

Course Description

This one-day course teaches you how to use the advanced features of the VMware Carbon Black® EDR™ product. This usage includes gaining access to the Linux server for management and troubleshooting in addition to configuring integrations and using the API. This course provides an in-depth, technical understanding of the Carbon Black EDR product through comprehensive coursework and hands-on scenario-based labs. This class focuses exclusively on advanced technical topics related to the technical back-end configuration and maintenance.

Delivery Method

Instructor-Led

Duration

One Day

Course Objectives

Upon completion of this course, you will be able to:

- Describe the components and capabilities of the Carbon Black EDR server
- Identify the architecture and data flows for Carbon Black EDR communication
- Identify the architecture for a cluster configuration and Carbon Black EDR cluster communication Describe the Carbon Black EDR server data types and data locations
- Use the API to interact with the Carbon Black EDR server without using the UI
- Create custom threat feeds for use in the Carbon Black EDR server
- Perform the integration with a syslog server Use different server-side scripts for troubleshooting
- Troubleshoot sensor-side configurations and communication

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.

Prerequisites

This course requires completion of the following course:

- VMware Carbon Black EDR Administration

Course Outline

Module 1: Module 1: Course Introduction

- Introductions and course logistics
- Course objectives

Module 2: Architecture

- Data flows and channels
- Sizing considerations
- Communication channels and ports

Module 3: Server Datastores

- SOLR database
- Storage configurations and data aging
- Partition states
- Postgres
- Modulestore

Module 4: EDR API

- CBAPI overview
- Viewing API calls in the browser
- Utilizing the API to access data

Module 5: Threat Intelligence Feeds

- Feed structure
- Report indicator types
- Custom threat feed creation and addition

Module 6: Syslog Integration

- SIEM support
- Configuration

Module 7: Troubleshooting

- Server-side scripts
- Server logs
- Sensor operations

VMware Carbon Black EDR Advanced Analyst

Course Code: 000273

Course Description

This one-day course teaches you how to use the VMware Carbon Black® EDR™ product during incident response. Using the SANS PICERL framework, you will configure the server and perform an investigation on a possible incident. This course provides guidance on using Carbon Black EDR capabilities throughout an incident with an in-depth, hands-on, scenario-based lab.

Delivery Method

Instructor-Led

Duration

One Day

Course Objectives

Upon completion of this course, you will be able to:

- Utilize Carbon Black EDR throughout an incident
- Implement a baseline configuration for Carbon Black EDR
- Determine if an alert is a true or false positive • Fully scope out an attack from moment of compromise
- Describe Carbon Black EDR capabilities available to respond to an incident
- Create addition detection controls to increase security

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.

Prerequisites

This course requires completion of the following course:

- VMware Carbon Black EDR Administrator

Course Outline

Module 1: Course Introduction

- Introductions and course logistics
- Course Objectives

Module 2: VMware Carbon Black EDR & Incident Response

- Framework identification and process

Module 3: Preparation

- Implement the Carbon Black EDR instance according to organizational requirements

Module 4: Identification

- Use initial detection mechanisms
- Process alerts
- Proactive threat hunting
- Incident determination

Module 5: Containment

- Incident scoping
- Artifact collection
- Investigation

Module 6: Eradication

- Hash banning
- Removing artifacts
- Continuous monitoring

Module 7: Recovery

- Rebuilding endpoints
- Getting to a more secure state

Module 8: Lessons Learned

- Tuning Carbon Black EDR
- Incident close out

VMware Carbon Black EDR Install, Configure, Manage v7.x

Course Code: 000279

Course Description

This three-day, hands-on training course provides you with the knowledge, skills, and tools to achieve competency in installing, configuring, and managing the VMware Carbon Black® EDR™ environment. This course introduces you to product features, capabilities, and workflows for managing endpoint security. Hands on labs enable learners to reinforce topics by performing operations and tasks within the product in a training environment.

Delivery Method

Instructor-Led

Duration

Three Days

Course Objectives

Upon completion of this course, you will be able to:

- Describe the architecture of a Carbon Black EDR implementation
- Perform the installation, upgrade, and configuration of the Carbon Black EDR server
- Describe the purpose and use of multiple datastores in the server
- Perform live queries across endpoints to gather additional data
- Perform effective searches across the dataset to find security artifacts related to the endpoints
- Manage Threat Intelligence Feeds and Watchlists
- Describe connectors in Carbon Black EDR
- Troubleshoot server and sensor problems
- Analyze data found in the Heads-Up Display
- Manage investigations to group and summarize security incidents and artifacts
- Perform the different response capabilities available to users in Carbon Black EDR
- Use the Carbon Black EDR API to automate tasks

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.

Prerequisites

There are no prerequisites for this course

Course Outline

Module 1: Course Introduction

- Introductions and course logistics
- Course objectives

Module 2: Planning and Architecture

- Describe the architecture and components of Carbon Black EDR
- Explain single and cluster server requirements
- Identify the communication requirements for Carbon Black EDR

Module 3: Server Installation, Upgrade, and Administration

- Install the Carbon Black EDR server
- Describe the options during the installation process
- Install a Carbon Black EDR sensor
- Confirm data ingestion in the Carbon Black EDR server
- Identify built-in administration tools
- Manage sensor groups
- Manage users and teams

Module 4: Exploring Server Datastores

- Describe the datastores used in Carbon Black EDR
- Interact with the available datastores

Module 5: Performing Live Query

- Describe live query capabilities
- Perform queries across endpoints

Module 6: Searching and Best Practices

- Describe the capabilities and data available in the process search
- Perform process searches to find specific endpoint activity
- Describe the capabilities and data available in the binary search
- Perform binary searches to find application data
- Describe the query syntax and advanced use cases
- Perform advanced queries across the dataset

Module 7: Threat Intelligence Feeds and Watchlists

- Define Threat Intelligence Feeds
- Manage the available Threat Intelligence Feeds
- Describe the use of Watchlists
- Manage Watchlists in the environment

Module 8: Connectors in VMware Carbon Black EDR

- Configure connectors in Carbon Black EDR
- Troubleshoot connectors

Module 9: Troubleshooting VMware Carbon Black EDR

- Identify the available troubleshooting scripts in the Carbon Black EDR server
- Run troubleshooting scripts to identify problems
- Generate a sensor log bundle
- Identify the location of sensor registry keys

Module 10: Head-Up Display Page Overview

- Identify panels relating to endpoint data
- Analyze endpoint data provided by the panels
- Identify panels relating to operations data
- Analyze operations data provided by the panels
- Identify panels relating to server data
- Analyze server data provided by the panels
- Define alert generation in Carbon Black EDR
- Manage alerts

Module 11: Performing Investigations

- Describe investigations
- Explore data used in an investigation
- Manage investigations
- Manage investigation events
- Describe hash banning
- Manage banned hashes

Module 12: Performing Investigations

- Describe isolation in Carbon Black EDR
- Manage isolating endpoints
- Describe live response capabilities
- Manage live response sessions

Module 13: Overview of Postman and the VMware Carbon Black EDR API

- Explain the use of the API
- Differentiate the APIs available for Carbon Black EDR
- Explain the purpose of API tokens
- Create an API token
- Explain the API URL
- Create a valid API request
- Import a collection to Postman
- Initiate an API request from Postman
- Perform operations manually using Postman
- Analyze the use cases for Postman
- Show basic automation tasks using the API and curl
- Compare the usage of curl with Postman

VMware Carbon Black Cloud Endpoint Standard

Course Code: 000277

Course Description

This one-day course teaches you how to use the VMware Carbon Black Cloud Endpoint™ Standard product and leverage the capabilities to configure and maintain the system according to your organization's security posture and policies. This course provides an in-depth, technical understanding of the product through comprehensive coursework and hands-on scenario based labs.

Delivery Method

Instructor-Led

Duration

One Day

Course Objectives

Upon completion of this course, you will be able to:

- Describe the components and capabilities of VMware Carbon Black Cloud Endpoint Standard
- Identify the architecture and data flows for Carbon Black Cloud Endpoint Standard communication
- Perform searches across endpoint data to discover suspicious behavior
- Manage the Carbon Black Cloud Endpoint Standard rules based on organizational requirements
- Configure rules to address common threats
- Evaluate the impact of rules on endpoints
- Process and respond to alerts
- Describe the different response capabilities available from VMware Carbon Black Cloud™

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.

Prerequisites

This course requires completion of the following course:

- VMware Carbon Black Cloud Fundamentals

Course Outline

Module 1: Course Introduction

- Introductions and course logistics
- Course objectives

Module 2: Data Flows and Communication

- Hardware and software requirements
- Architecture ▪ Data flows

Module 3: Searching Data

- Creating searches
- Analyzing events
- Search operators
- Advanced queries

Module 4: Policy Components

- Rules
- Local scanner
- Sensor capabilities

Module 5: Prevention Capabilities Using Rules

- Rule types
- Rule creation
- Reputation priority
- Configuring rules
- Evaluating rule impact

Module 6: Processing Alerts

- Alert triage
- Alert actions

Module 7: Response Capabilities

- Using quarantine
- Using live response
- Hash banning

VMware Carbon Black Cloud Audit and Remediation

Course Code: 000276

Course Description

This one-day course teaches you how to use the VMware Carbon Black® Cloud Audit and Remediation™ product to build queries for IT hygiene, incident response, and vulnerability assessment to support your organization's security posture and policies. This course provides an in-depth, technical understanding of the product through comprehensive coursework and hands-on scenario-based labs.

Delivery Method

Instructor-Led

Duration

One Day

Course Objectives

Upon completion of this course, you will be able to

- Describe the components and capabilities of VMware Carbon Black Cloud Audit and Remediation
- Identify the architecture and data flows for Carbon Black Cloud Audit and Remediation communication
- Describe the use case and functionality of recommended queries
- Achieve a basic knowledge of SQL
- Describe the elements of a SQL query
- Evaluate the filtering options for queries
- Perform basic SQL queries on endpoints
- Describe the different response capabilities available from VMware Carbon Black Cloud

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.

Prerequisites

This course requires completion of the following course:

- VMware Carbon Black Cloud Fundamental

Course Outline

Module 1: Course Introduction

- Introductions and course logistics
- Course Objectives

Module 2: Data Flows and Communication

- Hardware and software requirements
- Architecture
- Data flows

Module 3: Query Basics

- Osquery
- Available tables
- Query scope
- Running versus scheduling

Module 4: Recommended Queries

- Use cases
- Inspecting the SQL query

Module 5: SQL Basics

- Components
- Tables
- Select statements
- Where clause
- Creating basic queries

Module 6: Filtering Results

- Where clause
- Exporting and filtering

Module 7: Basic SQL Queries

- Query creation
- Running queries
- Viewing results

Module 8: Advanced Search Capabilities

- Advanced SQL options
- Threat hunting

Module 9: Response Capabilities

- Using live response

VMware Carbon Black Cloud Enterprise EDR

Course Code: 000278

Course Description

This one-day course teaches you how to use the VMware Carbon Black® Cloud Enterprise EDR™ product and leverage its capabilities to configure and maintain the system according to your organization's security posture and policies. This course provides an in-depth, technical understanding of the product through comprehensive coursework and hands-on scenario-based labs.

Delivery Method

Instructor-Led

Duration

One Day

Course Objectives

Upon completion of this course, you will be able to:

- Describe the components and capabilities of VMware Carbon Black Cloud Enterprise EDR
- Identify the architecture and data flows for VMware Carbon Black Cloud Enterprise EDR communication
- Perform searches across endpoint data to discover suspicious behavior
- Manage watchlists to augment the functionality of VMware Carbon Black Cloud Enterprise EDR
- Create custom watchlists to detect suspicious activity in your environment
- Describe the process for responding to alerts in VMware Carbon Black Cloud Enterprise EDR
- Discover malicious activity within VMware Carbon Black Cloud Enterprise EDR
- Describe the different response capabilities available from VMware Carbon Black Cloud

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.

Prerequisites

This course requires completion of the following course:

- VMware Carbon Black Cloud Fundamentals

Course Outline

Module 1: Course Introduction

- Introductions and course logistics
- Course Objectives

Module 2: Data Flows and Communication

- Hardware and software requirements
- Architecture
- Data flows

Module 3: Searching Data

- Creating searches
- Search operators
- Analyzing processes
- Analyzing binaries
- Advanced queries

Module 4: Managing Watchlists

- Subscribing
- Alerting
- Custom watchlists

Module 5: Alert Processing

- Alert creation
- Analyzing alert data
- Alert actions

Module 6: Threat Hunting in Enterprise EDR

- Cognitive Attack Loop
- Malicious behaviors

Module 7: Response Capabilities

- Using quarantine
- Using live response

VMware Carbon Black Cloud Plan and Deploy

Course Code: 000281

Course Description

This two-day hands-on training course provides you with the knowledge, skills, and tools to achieve competency in planning and deploying VMware Carbon Black Cloud™ in your environment. This course explains the VMware Carbon Black Cloud components, managing users and roles in VMware Carbon Black Cloud, configuring policies to support sensor deployment and management, and presents methods for deploying sensors across endpoints and workloads.

Delivery Method

Instructor-Led

Duration

Two Days

Course Objectives

Upon completion of this course, you will be able to:

- Describe the VMware Carbon Black Cloud platform
- Manage VMware Carbon Black Cloud roles and users
- Identify VMware Carbon Black Cloud sensor requirements
- Configure VMware Carbon Black Cloud sensor policies and workload protection
- Install VMware Carbon Black Cloud sensors on endpoints
- Manage VMware Carbon Black Cloud sensors
- Identify a properly registered sensor installation

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

Prerequisites

There are no prerequisites for this course.

Course Outline

Module 1: Course Introduction

- Introductions and course logistics
- Course objectives

Module 2: Introduction to VMware Carbon Black Cloud

- Describe the VMware Carbon Black Cloud platform
- List the VMware Carbon Black Cloud operating environment requirements
- Identify files that are suspicious or potential threats according to VMware Carbon Black Cloud
- List the events collected by VMware Carbon Black Cloud
- Describe data flows on VMware Carbon Black Cloud

Module 3: Managing VMware Carbon Black Cloud Roles and Users

- Describe the use of roles within VMware Carbon Black Cloud
- Detail RBAC capabilities within VMware Carbon Black Cloud
- Explain how to create and edit a custom role in VMware Carbon Black Cloud
- Describe enterprise and MSSP roles within the VMware Carbon Black Cloud
- Describe how to manage new console users
- Explain how to edit a user
- Detail the effect of a user role on a console user
- Describe authentication mechanisms
- Explain how to enable two-factor authentication

Module 4: VMware Carbon Black Cloud Sensor Requirements

- Describe VMware Carbon Black Cloud sensor resource usage
- List the supported operating systems for VMware Carbon Black Cloud sensors
- Explain sensor usage within VMware Carbon Black Cloud

Module 5: Preparing for Deployment

- Identify configuration settings for endpoints in Sensor Policy settings
- Create and edit policies within VMware Carbon Black Cloud
- Describe the methods to assign sensors to a policy
- Identify best practices for operationalizing VMware Carbon Black Cloud

Module 6: Installing Sensors

- Identify the features and limitations of activation codes
- Describe how to send an installation request
- Explain how to successfully complete an attended installation
- List the differences between activation codes and company codes
- Describe how to generate a new company code
- List the differences between attended and unattended sensor installation methods
- Identify the correct deployment strategy for a given scenario
- Describe how to capture sensor installation logs for troubleshooting sensor installations
- List common installation errors

Module 7: Deploying Workloads

- Recognize the deployment process for VMware Carbon Black Cloud Workload
- Identify eligible workloads in a vSphere environment configured with Workload Protection
- Recognize how to enable the VMware Carbon Black Cloud sensor on a VM Workload

Module 8: Managing Sensors

- Explain the differences in sensor status
- Describe sensor update capabilities
- Explain sensor actions
- Manage vSphere workloads

Module 9: Post-Deployment Validation

- Validate sensor details within the console
- Test sensor functionality from within the console
- Validate sensor functionality on the endpoint

VMware Carbon Black Cloud Advanced Operations and Troubleshooting

Course Code: 000280

Course Description

This two-day, hands-on training course provides you with the advanced knowledge, skills, and tools to achieve competency in performing advanced operations and troubleshooting of VMware Carbon Black Cloud. This course will go into integrating VMware Carbon Black Cloud with other third-party components and utilizing the API and the SDK to automate operations within the product and your security stack. This course will also enable you to troubleshoot common problems during sensor installation, operations, and within the VMware Carbon Black Cloud console with hands-on lab problems.

Delivery Method

Instructor-Led

Duration

Two Days

Course Objectives

Upon completion of this course, you will be able to:

- Describe and determine use cases for integrating with VMware Carbon Black Cloud
- Configure, automate, and troubleshoot the VMware Carbon Black Cloud Syslog Integration
- Use VMware Carbon Black Cloud APIs to pull data with Postman
- Install and use the VMware Carbon Black Cloud Python SDK
- Automate operations using the VMware Carbon Black Cloud SDK and APIs
- Identify and troubleshoot VMware Carbon Black Cloud sensor installations
- Gather troubleshooting data within the browser to remediate or escalate problems
- Identify and resolve sensor usage, networking, and performance problems with the VMware Carbon Black Cloud sensor

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.

Prerequisites

Before taking this course, learners should have completed:

- VMware Carbon Black Cloud Plan and Deploy

Learners should also have the following understanding or knowledge:

- Managing and working with various Linux and Windows operating systems
- Working experience of security operation

Course Outline

Module 1: Course Introduction

- Introductions and course logistics
- Course objectives

Module 2: VMware Carbon Black Cloud Integrations

- Describe the integration capabilities with VMware Carbon Black Cloud
- Determine integration use cases for VMware Carbon Black Cloud
- Identify required components for integrating VMware Carbon Black Cloud
- Differentiate VMware Carbon Black Cloud integration vendors

Module 3: VMware Carbon Black Cloud Syslog Integration

- Describe the function of the Syslog Connector
- Generate API and SIEM keys from the Cloud console
- Validate a successful Syslog integration
- Describe how to automate the Syslog Connector
- Troubleshoot problems with the Syslog integration

Module 4: Using Postman

- Explain the concept and purpose of an API
- Interpret common REST API Status codes
- Recognize the difference between platform and product APIs
- Using the Postman Client to initiate API calls
- Create a custom access level and respective API key
- Create a valid API request

Module 5: Using the VMware Carbon Black Cloud Python SDK

- Install the VMware Carbon Black Cloud Python SDK
- Describe the different authentication methods
- Evaluate the best authentication method for a given task

Module 6: Automating Operations

- Automate basic Incident Response tasks using the VMware Carbon Black Cloud SDK and API
- Automate basic watchlist interactions using the VMware carbon Black Cloud SDK and API

Module 7: Sensor Installation Troubleshooting

- Describe sensor install log collection process
- Identify sensor install log parameters
- Create a detailed sensor install log
- Locate sensor install logs on an endpoint
- Interpret sensor install success from an install log
- Determine likely cause for install failure using sensor logs
- Propose resolution steps for a given sensor install failure

Module 8: VMware Carbon Black Cloud Console Troubleshooting

- Identify sensor bypass status reasons
- Simplify console data exports using search
- Describe differences in Audit Log detail levels
- Locate built-in browser tools
- Gather console diagnostics logs from a browser
- Review console diagnostics logs

Module 9: Sensor Operations Troubleshooting

- Identify available types of diagnostic logs
- Gather appropriate diagnostic logs for a given issue
- Identify steps for resolving software interoperability problems
- Identify steps for resolving resource problems
- Identify steps for resolving network problems

Broadcom Education Contact details

Americas

Americas.Education@Broadcom.com

EMEA

EMEA.Education@Broadcom.com

APJ

APJ.Education@Broadcom.com

Broadcom Inc.

Corporate Headquarters

1320 Ridder Park Drive

San Jose, California, 95131

United States

https://www.broadcom.com/