VMware - Security Operations for the Software-Defined Data Center

Code:	EDU-SOSDDC1
Length:	5 days
URL:	View Online

Overview:

Virtualization presents new opportunities for securing your data and systems. Virtualizing your data center often brings new challenges, requiring your IT staff to assume new, and sometimes unfamiliar, roles and responsibilities.

In the VMware Security Operations for the Software-Defined Data course, we teach you how to use the VMware Software-Defined Data Center product portfolio and tools to better manage administrator access, harden your VMware vSphere® environment, and secure data at rest and in motion. We also discuss compliance and automation to help you ensure that your deployments align with your security policies.

Overview:

Virtualization presents new opportunities for securing your data and systems. Virtualizing your data center often brings new challenges, requiring your IT staff to assume new, and sometimes unfamiliar, roles and responsibilities.

In the VMware Security Operations for the Software-Defined Data course, we teach you how to use the VMware Software-Defined Data Center product portfolio and tools to better manage administrator access, harden your VMware vSphere® environment, and secure data at rest and in motion. We also discuss compliance and automation to help you ensure that your deployments align with your security policies.

Objectives:
By the end of the course, you should be able to meet the following objectives:

- Describe the concepts involved in securing a software-defined data center (SDDC) and protecting the data in the data center
- Manage vSphere administrator access to hosts and the VMware vCenter Server™ system based on identified job roles and requirements
- Implement best-practice security of vSphere components based on organizational security policies
- Configure data protection for data at rest and data in motion
- Manage protection for virtual machines, endpoints, and networks
- Use microsegmentation to protect and manage multitier applications and network data
- Perform activity monitoring and logging, and explore relevant logs to meet compliance requirements
- Use VMware NSX® security groups, policies, and tags to automate deployment and security processes

- Use automation to respond to security-related events

Intended Audience:

- Experienced system administrators
- Cloud administrators
- System integrators
- Operational developers

Prerequisites:
Completion of one of the following:

- VMware vSphere: Install, Configure, Manage [V5.5 or V6]
- VMware vSphere: Fast Track
- Equivalent knowledge
- Experience working at the command prompt and with scripting tools like Windows PowerShell is highly recommended.
- An understanding of corporate or enterprise network implementations.

Outline:
1.Course Introduction

- Introductions and course logistics
- Course outline
- Course objectives

2.Security Concepts

- Key IT security principles for the SDDC
- Differences between securing traditional infrastructures and virtual infrastructures
- Identity and access management concepts for the SDDC
- Methods to secure your virtual infrastructure components
- Guest operating system access security
- Hardening concepts and how they apply to virtual infrastructure components

3.vSphere Security Identity and Access Management

- Role-based access control concepts
- Configuring role-based access control for VMware ESXi™ and vCenter Server
- Configuring vSphere single sign-on for administrative access
- Password hardening options
- Configuring ESXi local user management and integration with Active Directory (AD)
- ESXi security profiles and access to services

4.vSphere Hardening

- ESXi host hardening

- Implementing lockdown mode on ESXi hosts
- Configuring ESXi host-based firewall settings
- vCenter Server hardening
- Tools to reduce infrastructure vulnerabilities
- Implementing hardening best practices based on the vSphere Hardening Guide

5.Data Protection

- Data encryption technology
- Data-at-rest encryption options
- Datastore security options
- Configuring vSphere security certificate management using VMware Certificate Authority and VMware Endpoint Certificate Services
- Using the Certificate Automation Tool to manage vSphere certificates
- Establishing and using an IPsec VPN
- Using the VMware Endpoint Certificate Store

6.Network Security

- Managing network data in an SDDC
- Security policies and settings of vSphere switches
- Configuring vSphere advanced security features for distributed switches
- Using the VMware NSX distributed firewall and distributed router to implement microsegmentation
- Protecting and managing north-south traffic with VMware NSX® Edge™ services gateway and physical firewalls
- Managing access to the vSphere management network
- Using VMware NSX® Virtual Switch™ features to implement network security
- Designing clusters and racks to minimize vulnerabilities
- Limiting access to vSphere management networks
- Hardening network infrastructure components

7.Virtual Machine and Application Protection

- Securing virtual machine guest operating systems
- Using VMware NSX with Service Composer for Endpoint Protection
- Using distributed firewalls and microsegmentation to isolate and protect virtual machines
- Using VMware NSX identity-based firewalls to control network traffic based on AD user IDs
- Additional VMware NSX functionality using integration with third-party solutions

8.Data Center Security Compliance

- Using VMware vRealize® Log Insight™ to identify and analyze security-related log entries
- Implementing a distributed logging environment
- VMware vRealize® Configuration Manager™ compliance checkers

- VMware Realize® Operations Manager™ compliance monitoring
- vRealize Configuration Manager and vRealize Operations Manager integration
- Performing network flow monitoring to analyze network traffic

9.Automating Data Center Security

- Using VMware functions and tools to enforce consistent organizational security policies during infrastructure deployment
- Automating responses to security events
- Implementing security automation with security groups, security policies, and security tags
- Automatically applying security settings to newly provisioned virtual machines based on VMware NSX security policies

Course Details

Schedule (as of 4)

Date	Location