

# VMware Security Operations for the Software-Defined Data Center

## Course 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.

This five-day course teaches you how to use the VMware software-defined data center (SDDC) product portfolio and tools to better manage administrator access, harden your VMware vSphere® environment, and secure data at rest and in motion. This course also discusses end-user computing (EUC) security, as well as compliance and automation to help you ensure that your deployments align with your security policies.

## Course Objectives

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

- Describe the concepts involved in securing an 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 security best practices of vSphere components based on organizational security policies
- Configure data protection for data at rest and data in motion
- Manage protection for server and desktop-class virtual machines, endpoints, and networks
- Use microsegmentation to protect and manage multitier applications and network data
- Describe VMware AirWatch® functionality to protect mobile computing and EUC deployments
- 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

## Target Audience

Experienced system administrators, cloud administrators, system integrators, operational developers

## Prerequisites

This class requires completion of one of the following courses:

- [VMware vSphere 6.x: Install, Configure, Manage](#)
- [VMware vSphere 6.x: Fast Track](#)
- An understanding of corporate or enterprise network implementations

Experience working at the command prompt and with scripting tools like Windows PowerShell is highly recommended.

## Certifications

No certifications are tied to this course.

## Course Delivery Options

- Classroom
- Live Online
- [Onsite](#)

## Product Alignment

- Compute: VMware ESXI™, vSphere, and vCenter Server
- EUC: VMware Horizon® View™
- Network: VMware NSX
- VMware vRealize® Operations™
- VMware vRealize® Log Insight™
- VMware vRealize® Automation™
- VMware AirWatch

## Course Modules

### 1 Course Introduction

- Introductions and course logistics
- 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
- EUC and mobile computing risks
- 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 for vSphere and View
- Configuring role-based access control for ESXi, vCenter Server, and View
- Configuring vSphere single sign-on for administrative access
- Password hardening options
- Configuring ESXi local user management and integration with Active Directory
- 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 for server and desktop virtual machines
- View endpoint protection best practices
- Datastore security options

- View PCoIP encryption
- VMware Operating System Optimization Tool for desktop and server virtual machines
- Introducing VMware AirWatch for mobile and desktop security
- VMware AirWatch and VMware NSX integration
- 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, Mobility, and Application Protection

- Securing virtual machine guest operating systems
- Mobile device security with VMware AirWatch
- Using VMware NSX with Service Composer for Endpoint Protection
- Using distributed firewalls and microsegmentation to isolate and protect virtual machines



VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 [www.vmware.com](http://www.vmware.com)

© 2016 VMware, Inc. All rights reserved. The product or workshop materials is protected by U.S. and international copyright and intellectual property laws. VMware products are covered by one or more patents listed at <http://www.vmware.com/download/patents.html>. VMware is a registered trademark or trademark of VMware, Inc. in the United States and/or other jurisdictions. All other marks and names mentioned herein may be trademarks of their respective companies.

VMware warrants that it will perform these workshop services in a reasonable manner using generally accepted industry standards and practices. THE EXPRESS WARRANTY SET FORTH IS IN LIEU OF ALL OTHER WARRANTIES, EXPRESS, IMPLIED, STATUTORY OR OTHERWISE INCLUDING IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE WITH RESPECT TO THE SERVICES AND DELIVERABLES PROVIDED BY VMWARE, OR AS TO THE RESULTS WHICH MAY BE OBTAINED THEREFROM. VMWARE WILL NOT BE LIABLE FOR ANY THIRD-PARTY SERVICES OR PRODUCTS IDENTIFIED OR REFERRED TO CUSTOMER. All materials provided in this workshop are copyrighted by VMware ("Workshop Materials"). VMware grants the customer of this workshop a license to use and make reasonable copies of any Workshop Materials strictly for the purpose of facilitating such company's internal understanding, utilization and operation of its licensed VMware product(s). Except as set forth expressly in the sentence above, there is no transfer of any intellectual property rights or any other license granted under the terms of this workshop. If you are located in the United States, the VMware contracting entity for the service will be VMware, Inc., and if outside of the United States, the VMware contracting entity will be VMware International Limited.

- Using VMware NSX identity-based firewalls to control network traffic based on Active Directory user IDs
- Additional VMware NSX functionality using integration with third-party solutions

## 8 Data Center Monitoring and Compliance

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

## 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

## Contact

If you have additional questions or need help registering for this course, click [here](#).



VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 [www.vmware.com](http://www.vmware.com)  
© 2016 VMware, Inc. All rights reserved. The product or workshop materials is protected by U.S. and international copyright and intellectual property laws. VMware products are covered by one or more patents listed at <http://www.vmware.com/download/patents.html>. VMware is a registered trademark or trademark of VMware, Inc. in the United States and/or other jurisdictions. All other marks and names mentioned herein may be trademarks of their respective companies.

VMware warrants that it will perform these workshop services in a reasonable manner using generally accepted industry standards and practices. THE EXPRESS WARRANTY SET FORTH IS IN LIEU OF ALL OTHER WARRANTIES, EXPRESS, IMPLIED, STATUTORY OR OTHERWISE INCLUDING IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE WITH RESPECT TO THE SERVICES AND DELIVERABLES PROVIDED BY VMWARE, OR AS TO THE RESULTS WHICH MAY BE OBTAINED THEREFROM. VMWARE WILL NOT BE LIABLE FOR ANY THIRD-PARTY SERVICES OR PRODUCTS IDENTIFIED OR REFERRED TO CUSTOMER. All materials provided in this workshop are copyrighted by VMware ("Workshop Materials"). VMware grants the customer of this workshop a license to use and make reasonable copies of any Workshop Materials strictly for the purpose of facilitating such company's internal understanding, utilization and operation of its licensed VMware product(s). Except as set forth expressly in the sentence above, there is no transfer of any intellectual property rights or any other license granted under the terms of this workshop. If you are located in the United States, the VMware contracting entity for the service will be VMware, Inc., and if outside of the United States, the VMware contracting entity will be VMware International Limited.