C)VSE™

mile2®
CYBER SECURITY CERTIFICATIONS

Certified Virtualization Security Engineer

KEY DATA

Course Name: Certified Virtualization Security Engineer

Duration: 4 Days

Language: English

Format
Instructor Led Training
Instructor Led Online Training

Prerequisites:
Network+ Certification or Equivalent Knowledge
Two Years' Experience with Microsoft or Linux Servers
Basic Virtualization/Cloud Knowledge
Certified Virtualization Engineer or equivalent knowledge

Student Materials:
Student Workbook – 400+ Pages
Student Lab Guide – 200+ Pages

Certification Exams:
Certified Virtualization Security Engineer

CEUs: 32

WHO SHOULD ATTEND?

Virtualization and Cloud Administrators and Engineers, Virtualization and Cloud Security Engineers, System Administrators and Engineers

COURSE OVERVIEW

This fast paced, deep dive, hands-on course provides not only the foundation needed for highly secure deployment of VMware vSphere, it also provides a complete understanding of the CIA triad as it relates to virtualization. This course will cover everything from design, configuration, best practices, performance monitoring, and just about everything in between! We endeavor to provide an understanding of what can and cannot be performed to secure your virtualized datacenter!

COURSE OBJECTIVES

- The Datacenter is under attack and mistakes made in implementing the virtual platform can lead to a major attack. It has happened before and will again.
- Every day we read about new methods of attacking Infrastructure as a Service such as Amazon, now learn how a properly designed virtual layer can aid in mitigating some of these attacks.
- Learn how Confidentiality can be improved with some awesome features implemented in vSphere.
- Learn how Integrity can be maintained with a proper design and implementation of VMware vSphere.
- Learn now Availability is designed into the VMware vSphere architecture and how you can improve and maintain this.
- Spend some time performing a few hacks, and a lot of time implementing a secure architecture with hands on labs
- **Much of your time will be hands on!**

Career

Foundational

C)VSE™

All combos Include:

- Online Video
- Electronic Book (Workbook/Lab guide*)
  *in technical classes only
- Exam Prep Questions
- Exam

ias™ INFORMATION ASSURANCE SERVICES · pt™ PENETRATION TESTING · dr™ DISASTER RECOVERY · gs™ GENERAL SECURITY · sc™ SECURE CODING · vbp™ VIRTUALIZATION BEST PRACTICES · ws™ WIRELESS SECURITY · cf™ COMPUTER FORENSICS

ACCREDITATIONS

mile2 is **ACCREDITED** by the **NSA CNSS 4011-4016**
Is **MAPPED** to NIST/Homeland Security NICCS's Cyber Security Workforce Framework
is **APPROVED** on the **FBI Cyber Security Certification Requirement list (Tier 1-3)**

UPON COMPLETION

Students will:

- Have learned the pros, cons, best practices, and skills of virtualization.
- Be able to design, secure, deploy, and manage virtual machines.
- Be ready to sit for the C)VSE exam.

EXAM INFORMATION

The **Certified Virtualization Security Engineer** exam is taken online through Mile2's Assessment and Certification System ("MACS"), which is accessible on your mile2.com account. The exam will take 2 hours and consist of 100 multiple choice questions. The cost is $400 USD and must be purchased from Mile2.com.

OUTLINE

Course Introduction
Module 1 – Virtualization and Cloud Overview
Module 2 – vSphere Monitoring and Performance (Availability Constraints)
Module 3 – vSphere Native Security
Module 4 – vSphere Security Risks
Module 5 – Designing for Security
Module 6 – Hardening vSphere
Module 7 – Managing Risk and Compliance
Module 8 – Third Party Mitigation Solutions

COURSE DETAILS

Course Introduction

Chapter 1 – Virtualization and Cloud Overview

1. Overview of Virtualization
2. Overview of Cloud Technologies
3. Design
    a. Functional Requirements
    b. Security Implications
    c. Examples

Chapter 2 – vSphere Monitoring and Performance (Availability Constraints)

1. Configuring ESXi resources for best performance (HOL)
    a. Understanding the resources such as CPU, Memory and Disk
2. Configuring the VM for best performance (HOL)
3. Monitoring the vSphere and vCloud Infrastructure (HOL)
    a. vCenter Performance Tab (HOL)
    b. esxtop (HOL)
4. Configuring Alarms (HOL)
5. Using Resource Pools properly (HOL)
6. Troubleshooting performance issues
7. vSphere Logs (HOL)

Chapter 3 – vSphere Native Security

1. ESXi Native Controls
    a. Active Directory Integration (HOL)
    b. Managing the Firewall (HOL)
    c. Logging
    d. Lock Down Mode
    e. Acceptance Level
    f. Secure Boot Support
    g. VMKernel Preventative Controls
    h. File System Structure
    i. Hardening SSH (HOL)
    j. MOB
    k. Authentication Proxy
2. vCenter Native Controls
    a. Encrypted vMotion
    b. Managed Object Browser
    c. NFC SSL
    d. Audit Quality Logging
3. VM Native Controls
    a. Security out of the Box
    b. Secure Boot Support
    c. Advanced Settings
    d. VM Encryption
    e. VM Sandboxing

Chapter 4 – vSphere Security Risks

4. Introduction to Risk
    a. How virtualization differs
5. Known Risks
    a. ESXi Host
    b. vCenter
    c. vNetwork
    d. vStorage
    e. Others

Chapter 5 – Designing for Security

1. Designing the Network
    a. vNetwork Native Controls
    b. Recommendations for Design

2. Storage Implications
    a. vStorage Native Controls
    b. Recommendations for Design
3. Implications for Management Access

Chapter 6 – Hardening vSphere

1. Introduction to the Hardening Guide
2. Hardening the ESXi Host
    a. vNetwork
    b. vStorage
    c. Availability
3. Hardening vCenter
4. Hardening Virtual Machines
    a. Advanced Settings
    b. Easy PowerCLI

Chapter 7 – Managing Risk and Compliance

1. Overview of Compliance
2. vRealize Operations Manager
3. PowerCLI supporting risk management
4. Free Compliance Checking Tools

Chapter 8 – Third Party Mitigation Solutions

1. Catbird
2. Cisco Adaptive Security Virtual Appliance
3. Firefly Host – Juniper Networks Product
4. HyTrust
5. Sophos Endpoint Antivirus – Cloud
6. Reflex VMC
7. TrendMicro Deep Security
8. WatchGuard