

Certified Virtualization Security Engineer (C)VSE)

Modality: Virtual Classroom

Duration: 4 Days

About this course:

This hands-on course is giving the essential fundamental understanding required for the profoundly secure VMware vSphere deployment. It additionally offers intensive information on the triad of CIA identified with virtualization. This quick-paced course covers all zones from best practices to execution monitoring, structure to set up, and everything in between identified with these angles. It is our objective to outfit the participant with a total comprehension of how their virtualized data center can be made sure about and through what implies. This course is preliminary for understudies who might want to sit for the exam of CVSE.

The compensation for a Virtualization Security Engineer is \$110,000 annually.

Course Objective:

Upon the finish of this course, understudies will have the option to:

- Comprehend that when the Datacenter is enduring an onslaught and errors are made in executing the virtual stage, it could prompt a significant assault. It has occurred previously and will once more.
- Figure out how an appropriately planned virtual layer can aid in mitigating assaults.
- Figure out how secrecy can be improved with certain highlights applied in vSphere.
- Figure out how integrity can be kept up with an appropriate plan and execution of VMware vSphere.
- Figure out how accessibility is planned into the VMware vSphere design and how you can enhance and look after this.
- Invest some energy playing out a couple of hacks, and a ton of time executing safe engineering with hands-on labs.
- Virtualization and Cloud Overview
- vSphere Monitoring and Performance (Availability Constraints)
- vSphere Native Security
- vSphere Security Risks
- Designing for Security
- Hardening vSphere
- Managing Risk and Compliance
- Third-Party Mitigation Solutions & Scanning
- Advanced Management of Desktop Pools

Audience:

This course is designed for:

- Cloud and Virtualization Administrators and Engineers.
- Security Engineers of Virtualization and Cloud.
- System Engineers and Administrators.

Prerequisites:

Experience of two years with Linux or MS Servers Simple Virtualization or Cloud understanding
Certified Virtualization Engineer or equal information

Network+ Certification or Equivalent Knowledge

Suggested prerequisites courses:

Virtualization Technologies Introduction

CompTIA Network+ (Exam N10-006) (CompTIA Net)

Course Outline:

- **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 & Scanning
- **Module 14** - Advanced Management of Desktop Pools