1. Course Details:

Course Code : SECR-004
Course Title : Security Operations for the Software-Defined Data Center
Course Duration : 5 Days

2. 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.
- 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.

3. Learning Outcomes:

- 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 micro segmentation 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

4. Course Contents:

Introduction

- Introductions and course logistics
- Course objectives

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

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

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

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

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 micro segmentation
- 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

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 micro segmentation to isolate and protect virtual machines
- 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

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

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

5. Attendance Reports:

- Send daily attendance reports to trainingdep
- Send full attendance report to training dep. by the end of thecourse
- Attend 100 % from the course days also providedaily
- Issue attendance certificate for participant who attend minimum 80% from the course duration

6. Pre/Post Reports:

- Pre- assessment before starting training.
- Post assessment after finish training
- Full report for the deferent between Pre-& Post assessment

7. Who Should Attend?

- Cloud administrators
- System integrators
- Operational developers