VMware NSX – Security Ninja Program

NSX Security Solutions Implementation Workshop

VMWARE NSX – SECURITY NINJA PROGRAM

LIVE ONLINE

Brought to you by
VMware & 27 Virtual

27 ViRTUAL

CONTACT

For more information, please contact your VMware Customer Sales Executive or the 27 Virtual team

With the proven success of the software-defined approach to an application-centric data center organizations are realizing the attack surface has been moved to their virtualized workloads and beyond. The result – is that the attack surface is now much larger than ever before. Those virtualized workloads include traditional Virtual Machines as well as Containers and now Cloud Native Applications. The attack surface extends beyond the virtual and containerized workloads in the data center it also extends to physical servers and appliances

During this course, participants learn through presentations, discussions, and hands-on labs how to implement NSX-based Security features to secure both Virtual and Physical workloads through the Virtualized Data Center Edge (North–South) as well as within the Virtualized Data Center (East–West). All concepts covered will be reinforced through purpose-built lab exercises.

This class is designed to be delivered as a Live Online Instructor-led event. During the workshop, the topics are delivered through open discussions, whiteboarding, and live demonstrations. Attendees Perform Hand-On Labs to reinforce all topics discussed.

Course objectives

By the end of this course, participants would have met the following objectives:

- Understand the taxonomy of an attack
- Review knowledge base resources available for attack mitigation
- Follow the OSI approach to Infrastructure Security
- Implement NSX Micro-Segmentation for a Virtualized and Physical workload
- Implement Layer 7 App-ID Context-Aware Firewall Policies
- Implement User Identity-Based Firewall rules for control in a VDI environment
- Configure Distributed IDS / IPS in a VMware NSX deployment
- Dive deep into the provided analytics of NSX Intelligence
- Implement VMware NSX NDR (NSX Network Threat Detection and Response)
- Implement NSX Advanced Threat Prevention

WONDERING IF YOU SHOULD ATTEND

This technical workshop is designed for:

- Solution Architects
- Technical Managers
- Security Analyst
- Security Administrators
- Cloud Architects
- Data Center Engineers
- vSphere Administrators
- VCP certification is preferred but not required (All would benefit from attending

Brought to you by
VMware and 27 Virtual.

27 ViRTUAL

CONTACT

For more information, please contact your VMware Customer Executive or the 27 Virtual.

Please bring a laptop and if possible, a second screen (tablet, portable monitor, or smartphone).

NSX Security Workshop Agenda (All times are in CDT)

DAY 1	
09:00	Introduction to NSX-T Vision and Strategy
10:00	NSX Architecture and Components
10:30	BREAK
10:45	NSX Architecture and Components Cont'd
11:15	Lab – Configure NSX Manager Cluster
11:45	NSX Architecture and Components Cont'd
12:30	LUNCH
13:30	Lab – NSX Manager Initial Configuration
14:15	NSX Application Platform – Overview & Architecture
15:15	Lab: NAPP Deployment
15:30	BREAK
15:45	Lab: NAPP Deployment (Cont'd)
16:30	Data Center Traffic Visibility and Security Planning
17:15	END OF DAY
DAY 2	
09:00	Day -1 Review
09:30	Lab: Planning workload Security with NSX Intelligence
10:00	Securing East/West Traffic in the Data Center
10:45	BREAK
11:00	Lab: Distributed Firewall
11:45	Implementing Context-Aware Firewall
12:30	LUNCH
13:30	Lab – L7 Firewalling
14:15	Securing Virtual Desktop Deployments
14:45	Lab: Securing Virtual Desktops

vmware®

15:15	BREAK
15:30	Securing Physical Servers
16:15	Lab: Securing Physical Servers with NSX
17:00	END OF DAY
DAY 3	
09:00	Day 2 Review
09:30	Managing Security for North-South Traffic & Non-NSX Managed Networks
10:45	BREAK
11:00	Lab: Implementing NSX Gateway Firewall
11:30	Lab: Implementing Advanced North/South Protection
12:15	LUNCH
13:15	Exploring the MITRE ATT&CK Knowledge Base
14:15	Lab: Leveraging the MITRE ATT&CK
15:30	BREAK
15:45	Distributed IDS IPS – Implementing Intrusion Detection and Prevention
16:45	Lab: Distributed IDPS
17:30	End of Day
DAY 4	
09:00	Day 3 Review
09:30	Implementing Advanced Threat Prevention
10:30	BREAK
10:45	Implementing Advanced Threat Prevention (cont'd)
11:15	Lab: NSX Advanced Threat Prevention
12:30	LUNCH
13:30	Lab: NSX Advanced Threat Prevention (Cont'd)
14:00	Network Traffic Analysis
14:45	Lab: Network Detection and Response
15:30	BREAK

15:45	Securing Container Workloads
16:30	Lab: Securing Container Workload
17:00	End of Day

Day 5	
09:00	Day 4 Review
09:30	NSX Federation
10:15	Lab: Securing Federated Workloads
10:45	BREAK
11:00	Lab: NSX Security Implementation Use Cases
12:30	LUNCH
13:30	Lab: NSX Security Implementation Use Cases (cont'd)
17:00	End of Day