

[Module 1:Course Introduction](#)

- Introductions and course logistics
- Course objectives

[Module 2:Security Basics](#)

- Define information security related concepts
- Explain different types of firewalls and their use cases
- Describe the operation of Intrusion Detection and Intrusion Prevention Systems

[Module 3:VMware Intrinsic Security](#)

- Define VMware intrinsic security strategy
- Describe VMware intrinsic security portfolio
- Explain how NSX-T Data Center aligns in the intrinsic security strategy

[Module 4:Implementing Zero-Trust Security](#)

- Define Zero-Trust Security
- Describe the five pillars of a Zero-Trust Architecture
- Define NSX segmentation and its use cases
- Describe the steps needed to enforce Zero-Trust with NSX segmentation

[Module 5: User and Role Management](#)

- Integrate NSX-T Data Center and VMware Identity Manager™
- Integrate NSX-T Data Center and LDAP
- Describe the native users and roles in NSX-T Data Center
- Create and assign custom user roles

[Module 6:Distributed Firewall](#)

- Configure Distributed Firewall rules and policies
- Describe the Distributed Firewall architecture
- Troubleshoot common problems related to Distributed Firewall
- Configure time-based policies
- Configure Identity Firewall rules

[Module 7:Gateway Security](#)

- Configure gateway firewall rules and policies
- Describe the architecture of the gateway firewall
- Identify and troubleshoot common gateway firewall issues
- Configure URL analysis and identify common configuration issues

[Module 8:Operating Internal Firewalls](#)

- Use vRealize Log Insight, vRealize Network Insight, and NSX Intelligence to operate NSX firewalls
- Explain NSX Intelligence visualization and recommendation capabilities
- Explain security best practices related to grouping, tagging, and rule configuration

[Module 9: Network Introspection](#)

- Explain network introspection
- Describe the architecture and workflows of North-South and East-West service insertion
- Troubleshoot North-South and East-West service insertion

[Module 10: Endpoint Protection](#)

- Explain Endpoint Protection
- Describe the architecture and workflows of endpoint protection
- Troubleshoot endpoint protection

[Module 11: Advanced Threat Prevention](#)

- Describe the MITRE ATT&CK Framework
- Explain the different phases of a cyber attack
- Describe how NSX security solutions can be used to protect against cyber attacks
- Configure and troubleshoot Distributed IDS/IPS
- Describe the capabilities of Network Detection and Response