Data Center Security with Virtual Reality

Outline

Lesson 1: DC Security Threats

- Describe security threats and potential impacts on the network
- Understand the security challenges faced by the DC staff on a daily basis
- Explain why Cisco Validated Designs lead to a more secure infrastructure
- Describe security threats in the storage network
- Explain Zero Trust Networking

Lesson 2: Protecting the Management Network

- Discuss options for in band and out of band management
- Describe role-based access control
- Explain the role of TACACS and Identity Services Engine (ISE) for device administration control

Lesson 3: Firewalling the Data Center

- Positioning the Firewall Within Data Center Networks
- Cisco Firepower Portfolio
- Describe advanced policy configuration and Firepower system configuration options
- Configure policies to find and stop Ransomware
- Configure Correlation events, white rules, traffic profiles, and create respective events and remediate them
- Understand network and host based AMP on a server
- Configure and analyze host based AMP on a server
- Firewall Virtualization
- Design for Threat Mitigation
- Threat Mitigation Integration with other Cisco products

Lesson 4: Umbrella Integration

- Umbrella and Available Features Overview
- Destination Lists
- Content Categories
- Application Settings

- Tenant Controls
- Security Settings
- Integrations
- Selective Decryption Lists
- DNS Policies
- Firewall Policies
- Virtual Appliance
- Core Reports
- Management Reports
- Integrating Umbrella within Cisco SecureX

Lesson 5: Stealthwatch in the Data Center

- Explain what Cisco Stealthwatch is and how it works.
- Describe the goals of using Cisco Stealthwatch in the proactive and operational modes.
- Define basic concepts of investigation and detection of potential security issues using the Cisco Stealthwatch System.
- Complete workflows to identify indicators of compromise in your network.
- Describe alarm types and alarm notification within Cisco Stealthwatch.
- Explain the utility of maps in the Cisco Stealthwatch System.
- Describe how the Cisco Stealthwatch System contributes to successful incident handling

Lesson 6: Utilizing Tetration in the Data Center

- Enable pervasive visibility of traffic across datacenter infrastructure
- Uses long term data retention for forensics and analysis
- Create communication and dependencies for all applications within the datacenter
- Empower the company to utilize a whitelist policy model
- Identify behavior deviation in real time
- Perform forensics operations