Security Operations (SecOps) Fundamentals

1: Security Operations Overview

- 1.1 Current State of Security and Security Operations Maturity Levels
- 1.2 Introducing ServiceNow Security Operations
- 1.3 Essential Platform and Security Administration Concepts
- Lab 1.3 Security Operations User Administration
- 1.4 Security Operations Common Functionality
- Lab 1.4.1 Security Operations Common Functionality
- Lab 1.4.2 Email Parser

2: Vulnerability Response

- 2.1 Vulnerability Response Overview
- Lab 2.1 Explore the Vulnerability Response Application
- 2.2 Vulnerability Classification and Assignment
- Lab 2.2 Explore Vulnerable Items and Vulnerability Groups
- 2.3 Vulnerability Management
- Lab 2.3 Vulnerability Groups (for Grouping Vulnerable Items)
- 2.4 Configuration Compliance
- Lab 2.4 Vulnerability Remediation

3: Security Incident Response

- 3.1 Security Incident Response Overview
- 3.2 Security Incident Response Components and Configuration
- Lab 3.2 Security Incident Response Configuration
- 3.3 Baseline Security Incident Response Lifecycle
- Lab 3.3 Creating Security Incidents
- 3.4 Security Incident Response Workflow-Based Responses

4: Threat Intelligence

- 4.1 Threat Intelligence Definition
- 4.2 Threat Intelligence Terminology
- 4.3 Threat Intelligence Toolsets
- Lab 4.3.1 Review and Update an Existing Attack Mode or Method
- Lab 4.3.2 Working with Indicators of Compromise (IOC) Lookups
- Lab 4.3.3 Automated Lookups in Security Incidents
- 4.4 Trusted Security Circles

5: Security Operations Integrations

- 5.1 Work with Security Operations
- Lab 5.1 Navigating Security Operations Integrations

6: Data Visualization

- 6.1 Understand Security Operations Monitoring and Reporting