

ServiceNow Security Operations (SecOps) Fundamentals

Duration: 2 Days **Course Code: SNSOF**

Overview:

Learn about the Security Incident Response, Vulnerability Response, and Threat Intelligence applications. This two-day course covers the foundational topics of the ServiceNow Security Operation suite. The Security Operations Suite includes the Security Incident Response, Vulnerability Response, and Threat Intelligence applications. The Security Operations Suite provides the tools needed to manage the identification of threats and vulnerabilities within your organization as well as specific tools to assist in the management of Security Incidents.

Virtual Learning

This interactive training can be taken from any location, your office or home and is delivered by a trainer. This training does not have any delegates in the class with the instructor, since all delegates are virtually connected. Virtual delegates do not travel to this course, Global Knowledge will send you all the information needed before the start of the course and you can test the logins.

Target Audience:

This course is designed for Security Operations administrators, ServiceNow administrators, and consultants who need to configure and administer ServiceNow Security Management. Additional training in ServiceNow administration, scripting, integration, and development would be helpful.

Objectives:

- A combination of lecture content and lab work helps attendees achieve the following:
 - Discuss the Current State of Security
 - Explain the Security Operations Maturity levels
 - Describe Security Incident Response Components and Configuration
 - Demonstrate the Baseline Security Incident Response Lifecycle
 - Identify Security Incident Response Workflow-Based Responses
 - Configure Vulnerability Assessment and Management Response tools
- Explore the ServiceNow Threat Intelligence application
- Employ Threat Sources and Explore Attack Modes and Methods
- Define Observables, Indicators of Compromise (IOC) and IoC Look Ups
- Discuss Security Operations Common Functionality
- Use Security Operations Integrations
- Demonstrate how to view and analyze Security Operations data

Prerequisites:

Students should have attended the ServiceNow Fundamentals course. In addition, students should be familiar with the ServiceNow user interface, know how to manage lists, and know how to configure users, roles, and groups.

- SNF - ServiceNow Fundamentals
- SNPI - ServiceNow Platform Implementation

Follow-on-Courses:

- SNSIRI - ServiceNow Security Incident Response (SIR) Implementation

Content:

DAY ONE	Lab 2.2 Explore Vulnerable Items and Vulnerability Groups	Module 4: Threat Intelligence
Module 1: Security Operations Overview	2.3 Vulnerability Management	4.1 Threat Intelligence Definition
1.1 Current State of Security and Security Operations Maturity Levels	Lab 2.3 Vulnerability Groups (for Grouping Vulnerable Items)	4.2 Threat Intelligence Terminology
1.2 Introducing ServiceNow Security Operations	2.4 Configuration Compliance	4.3 Threat Intelligence Toolsets
1.3 Essential Platform and Security Administration Concepts	Lab 2.4 Vulnerability Remediation	Lab 4.3.1 Review and Update an Existing Attack Mode or Method
Lab 1.3 Security Operations User Administration	DAY TWO	Lab 4.3.2 Working with Indicators of Compromise (IOC) Lookups
1.4 Security Operations Common Functionality	Module 3: Security Incident Response	Lab 4.3.3 Automated Lookups in Security Incidents
Lab 1.4.1 Security Operations Common Functionality	3.1 Security Incident Response Overview	4.4 Trusted Security Circles
Lab 1.4.2 Email Parser	3.2 Security Incident Response Components and Configuration	Module 5: Security Operations Integrations
Module 2: Vulnerability Response	Lab 3.2 Security Incident Response Configuration	5.1 Work with Security Operations
2.1 Vulnerability Response Overview	3.3 Baseline Security Incident Response Lifecycle	Lab 5.1 Navigating Security Operations Integrations
Lab 2.1 Explore the Vulnerability Response Application	Lab 3.3 Creating Security Incidents	Module 6: Data Visualization
2.2 Vulnerability Classification and Assignment	3.4 Security Incident Response Workflow-Based Responses	6.1 Understand Security Operations Monitoring and Reporting

Further Information:

For More information, or to book your course, please call us on Head Office Tel.: +974 40316639

training@globalknowledge.qa

www.globalknowledge.com/en-qa/

Global Knowledge, Qatar Financial Center, Burj Doha, Level 21, P.O.Box 27110, West Bay, Doha, Qatar