

## ServiceNow Security Operations (SecOps) Fundamentals

Duration: 365 Days    Course Code: SNSOF    Delivery Method: Elearning (Self-paced)

### 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.

#### e-Learning

Interactive self-paced content that provides flexibility in terms of pace, place and time to suit individuals and organisations. These resources also consist of online books, educational podcasts and vodcasts, and video-based learning.

### 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

#### Module 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

#### Module 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

### DAY TWO

#### Module 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

#### Module 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

#### Module 5: Security Operations Integrations

##### 5.1 Work with Security Operations

##### Lab 5.1 Navigating Security Operations Integrations

#### Module 6: Data Visualization

##### 6.1 Understand Security Operations Monitoring and Reporting

---

## Further Information:

For More information, or to book your course, please call us on 00 20 (0) 2 2269 1982 or 16142

[training@globalknowledge.com.eg](mailto:training@globalknowledge.com.eg)

[www.globalknowledge.com/en-eg/](http://www.globalknowledge.com/en-eg/)

Global Knowledge, 16 Moustafa Refaat St. Block 1137, Sheraton Buildings, Heliopolis, Cairo