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.

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:

- **After you complete this course you will be able to:**
- 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:

Attendees should meet the following 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.
- SNSAF - ServiceNow Administration Fundamentals
- SNPI - ServiceNow Platform Implementation

Follow-on-Courses:

- SNSIRI - ServiceNow Security Incident Response (SIR) Implementation

Content:

Security Operations Overview

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

Vulnerability Response

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

Security Incident Response

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

Threat Intelligence

- Threat Intelligence Definition
- Threat Intelligence Terminology
- Threat Intelligence Toolsets
- Trusted Security Circles
- 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

Security Operations Integrations

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

Data Visualization

- Understand Security Operations Monitoring and Reporting

Further Information:

For More information, or to book your course, please call us on Head Office 01189 123456 / Northern Office 0113 242 5931

info@globalknowledge.co.uk

www.globalknowledge.com/en-gb/

Global Knowledge, Mulberry Business Park, Fishponds Road, Wokingham Berkshire RG41 2GY UK