SERVICENOW SECURITY OPERATIONS (SECOPS) FUNDAMENTALS

Course Code: 821285

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.

What You'll Learn

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

Who Needs to Attend

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.

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.

skillsoft
global
knowledge™

SERVICENOW SECURITY OPERATIONS (SECOPS) FUNDAMENTALS

Course Code: 821285

CLASSROOM LIVE	$2,850 CAD	2 Day

Classroom Live Outline

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

SERVICENOW SECURITY OPERATIONS (SECOPS) FUNDAMENTALS

Course Code: 821285

VIRTUAL CLASSROOM LIVE	$2,850 CAD	2 Day

Virtual Classroom Live Outline

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

May 15 - 16, 2025 | 9:00 AM - 5:00 PM CDT

Jun 26 - 27, 2025 | 9:00 AM - 5:00 PM CDT skillsoft global knowledge™

SERVICENOW SECURITY OPERATIONS (SECOPS) FUNDAMENTALS

Course Code: 821285

ON-DEMAND	$0 CAD

On-Demand Outline

SOF Module 1: Security Operations Overview

- Module 1.1: Current State of Security and Security Operations Maturity levels
- Module 1.2: Introducing ServiceNow Security Operations
- Module 1.3: Essential Platform and Security Administration Concepts
- Module Summary

SOF Module 2: Security Operations Common Functionality

- Module 2.1: Security Operations Common Functionality
- Module 2.2: Workflow, Orchestration and Data Enrichment
- Module 2.3: Understanding Email Processing
- Module 2 Summary

SOF Module 3: Vulnerability Response

- Module 3.1: Vulnerability Response Overview - Part 1 of 3
- Module 3.1: Vulnerability Response Overview - Part 2 of 3
- Module 3.1: Vulnerability Response Overview - Part 3 of 3
- Module 3.2: Infrastructure Vulnerability Response - Part 1 of 3
- Module 3.2: Infrastructure Vulnerability Response - Part 2 of 3
- Module 3.2: Infrastructure Vulnerability Response - Part 3 of 3
- Module 3.3: Application Vulnerability Response
- Module 3.4: Container Vulnerability Response
- Module 3.5: Configuration Compliance
- Module 3 Summary

SOF Module 4: Security Incident Response

- Module 4.1: Security Incident Response Overview
- Module 4.2: Security Incident Response Components and Configuration
- Module 4.3: Security Incident Response Workflow-Based Responses

- Module 4 Summary

SOF Module 5: Threat Intelligence

- Module 5.1: Threat Intelligence Definition
- Module 5.2: Threat Intelligence Terminology - Part 1 of 2
- Module 5.2: Threat Intelligence Terminology - Part 2 of 2
- Module 5.3: Threat Intelligence Toolsets and Integrations
- Module 5 Summary

On-Demand Labs

- Lab 1.3: Security Operations User Administration
- Lab 2.2: Security Operations Common Functions
- Lab 2.3: Security Operations Email Parser
- Lab 3.1: Explore the Vulnerability Response Application
- Lab 3.1.2: Explore Vulnerability Entries
- Lab 3.2: Explore Vulnerable Items and Solutions
- Lab 3.2.2: Watch Topics and Remediation Efforts
- Lab 3.2.3: Vulnerability Remediation
- Lab 4.2 Creating Security Incidents
- Lab 4.2.2 Security Incident Response Configuration
- Labs 5.3.1 and 5.3.2
- Lab 5.3.3 Automated Lookups in Security Incidents

SERVICENOW SECURITY OPERATIONS (SECOPS) FUNDAMENTALS

Course Code: 821285

PRIVATE GROUP TRAINING	2 Day

Visit us at www.globalknowledge.com or call us at 1-866-716-6688.

Date created: 5/9/2025 2:09:26 AM

Copyright © 2025 Global Knowledge Training LLC. All Rights Reserved.