skillsoft global knowledge™

SERVICENOW SECURITY INCIDENT RESPONSE (SIR) IMPLEMENTATION

Course Code: 821284

Learn the domain knowledge, technical aspects, and various processes needed to effectively manage a Security Incident Response implementation (SIRI).

This two-day course covers the domain knowledge, common implementation technical aspects, and various processes needed to effectively manage a Security Incident Response implementation (SIRI).

Attendees will learn and practice various tactical skills and strategies that will better prepare them to implement Security Incident Response (SIR). Through lectures, group discussion, hands-on labs and simulations, participants build on existing knowledge and skills by applying implementation best practices.

What You'll Learn

Course topics include:

- Security Incident Response Overview
- Create Security Incidents
- Security Incident and Threat Intelligence Integrations
- Security Incident Response Management
- Risk Calculations and Post Incident Response
- Security Incident Automation
- Data Visualization
- Family Delta Module
- Capstone Project

Who Needs to Attend

This course is suitable for anyone who will be working on a ServiceNow implementation of the Security Incident Response applications. Examples, include:

- Technical Consultants and Administrators – who will be configuring, developing or supporting the Security Incident Response applications
- Project/Program/Engagement Managers – who will be leading implementation of Security Incident Response applications in ServiceNow
- Operations Managers – who have oversight of work which will be facilitated

using Security Incident Response applications in ServiceNow

SERVICENOW SECURITY INCIDENT RESPONSE (SIR) IMPLEMENTATION

Course Code: 821284

CLASSROOM LIVE	$2,850 CAD	2 Day

Classroom Live Outline

Module 1: Security Incident Response Overview: Identify the goals of Security Incident Response (SIR), Discuss the importance of understanding customers and their goals, and discuss how Security Incident Response meets customer expectations.

Module 2: Create Security Incidents: Determine how to create Security Incident Response incidents: Setup Assistant, Using the Service Catalog, Manual Creation, and Via Email Parsing.

Module 3: Security Incident and Threat Intelligence Integrations: Discuss different integration capabilities, Describe the Three Key Security Incident Response Integrations: Custom, Platform, Store & Share.

Module 4: Security Incident Response Management: Describe the Security Incident Response Management process and components: Assignment Options, Escalation Paths, Security Tags, Process Definitions and Selection.

Module 5: Risk Calculations Post Incident Response: Identify Calculators and Risk Scores, Be able to post Incident Reviews.

Module 6: Security Incident Automation: Discuss the Security Incident Response Automation processes available on the ServiceNow Platform: Workflows, Flow Designer, and Playbooks.

Module 7: Data Visualization: Explain the different Security Incident Response Dashboards and Reports available in the ServiceNow platform: Data Visualization, Dashboards and Reporting, Performance Analytics.

Module 8 Security Incident Response Family Release DELTA: Learn about the new, enhanced, and/or deprecated features of the current Security Incident Response

family release.

Module 9 Capstone Project: There is a final take-home Capstone project where participants provision a Developer instance and complete directed tasks to reinforce the concepts learned in class.

SERVICENOW SECURITY INCIDENT RESPONSE (SIR) IMPLEMENTATION

Course Code: 821284

VIRTUAL CLASSROOM LIVE	$2,850 CAD	2 Day

Virtual Classroom Live Outline

Module 1: Security Incident Response Overview: Identify the goals of Security Incident Response (SIR), Discuss the importance of understanding customers and their goals, and discuss how Security Incident Response meets customer expectations.

Module 2: Create Security Incidents: Determine how to create Security Incident Response incidents: Setup Assistant, Using the Service Catalog, Manual Creation, and Via Email Parsing.

Module 3: Security Incident and Threat Intelligence Integrations: Discuss different integration capabilities, Describe the Three Key Security Incident Response Integrations: Custom, Platform, Store & Share.

Module 4: Security Incident Response Management: Describe the Security Incident Response Management process and components: Assignment Options, Escalation Paths, Security Tags, Process Definitions and Selection.

Module 5: Risk Calculations Post Incident Response: Identify Calculators and Risk Scores, Be able to post Incident Reviews.

Module 6: Security Incident Automation: Discuss the Security Incident Response Automation processes available on the ServiceNow Platform: Workflows, Flow Designer, and Playbooks.

Module 7: Data Visualization: Explain the different Security Incident Response Dashboards and Reports available in the ServiceNow platform: Data Visualization, Dashboards and Reporting, Performance Analytics.

Module 8 Security Incident Response Family Release DELTA: Learn about the new, enhanced, and/or deprecated features of the current Security Incident Response

family release.

Module 9 Capstone Project: There is a final take-home Capstone project where participants provision a Developer instance and complete directed tasks to reinforce the concepts learned in class.

Aug 27 - 28, 2025 | 9:00 AM - 5:00 PM CDT

Sep 29 - 30, 2025 | 9:00 AM - 5:00 PM CDT

Nov 13 - 14, 2025 | 9:00 AM - 5:00 PM CST

SERVICENOW SECURITY INCIDENT RESPONSE (SIR) IMPLEMENTATION

Course Code: 821284

ON-DEMAND	$0 CAD

On-Demand Outline

Introduction

Module1: Security Incident Response Overview and Data Visualization

- Introducing Security Incident Response
- Security Incident Response Maturity Matrix
- Security Incident Lifecycle
- Data Visualization
- Understanding the Customer's Goals and Meeting Customer Expectations
- Security Incident Personas and Roles
- SIRI Knowledge Check Module 1 (Tokyo)
- Module 1: Key Takeaways

Module 2: Security Incident Creation and Threat Intelligence

- Explore How to Create Security Incidents
- How to Create Security Incidents using the Service Catalog
- How to Create Security Incidents via Email Parsing
- Major Security Incident Response
- Understanding Threat Intelligence
- MITRE-ATT&CK Framework
- SIRI Knowledge Check Module 2 (Tokyo)
- Module 2: Key Takeways

Module 3: Security Incident and Threat Intelligence Integrations

- Integrations - Questions to Ask
- ServiceNow Store and Share
- Managing Pre-Built Integrations
- Capability Framework Gold Standard
- Microsoft Defender - Endpoint Management

- Data Loss Prevention
- Malware Information Sharing Platform
- Creating a Custom Integration
- SIRI Knowledge Check Module 3 (Tokyo)
- Module 3: Key Takeaways

Module 4: Security Incident Response Management

- Analyst Workspace
- Standard Automated Assignment Options and Escalation Paths
- Major Security Incident Management
- Security Tags
- Process Definitions and Selection & Lab 4.4 Security Incident Process Selection
- SIRI Knowledge Check Module 4 (Tokyo)
- Module 4: Key Takeaways

Module 5: Risk Calculations and Post Incident Response

- Security Incident Calculator Groups and Risks Scores
- Post Incident Reviews & Lab 5.2 Post Incident Reviews
- SIRI Knowledge Check Module 5 (Tokyo)
- Module 4: Key Takeaways

Module 6: Automation and Standard Processes

- Automate Security Incident Response Overview
- Security Incident Automation using Flows and Workflows
- Playbook Automation (Knowledge Articles and Runbooks)
- Use Case: User Reported Phishing v2
- SIRI Knowledge Check Module 6 (Tokyo)
- Module 6: Key Takeaways

Take Home Capstone Project

Summary and Conclusion

Certified Implementation Specialist – Security Incident Response Voucher Info

On-Demand Labs

- Lab 1.1 Initial Application Setup
- Lab 1.1 Initial Application Setup - Recap
- Lab 2.1 Manual Creation of Security Incidents
- Lab 2.2 Major Security Incident Response
- Lab 2.4 Build Smarter Security with MITRE ATT&CK
- Lab 3.1 ServiceNow Store and Share
- Lab 3.3 Custom Security Incident Integration
- Lab 4.3 Configuring Security Tags
- Lab 5.2 Post Incident Reviews

SERVICENOW SECURITY INCIDENT RESPONSE (SIR) IMPLEMENTATION

Course Code: 821284

PRIVATE GROUP TRAINING	2 Day

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

Date created: 7/31/2025 1:31:51 AM