# ServiceNow Security Incident Response (SIR) Implementation

**Durée: 365 Jours** **Réf de cours: SNSIRI** **Méthodes d'apprentissage: E-learning**

## Résumé:

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.

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.

## Public visé:

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 applicationsProject/Program/Engagement Managers  who will be leading implementation of Security Incident Response applications in ServiceNowOperations Managers  who have oversight of work which will be facilitated using Security Incident Response applications in ServiceNow

## Objectifs pédagogiques:

- 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

## Pré-requis:

- SNF - ServiceNow Fundamentals
- SNPI - ServiceNow Platform Implementation
- SNSOF - ServiceNow Security Operations (SecOps) Fundamentals

## Test et certification

ServiceNow requires the completion of prerequisite training course(s) in preparation for the Certified Implementation Specialist - Security Incident Response exam (CIS-SIR) . Information provided in the following ServiceNow training course(s) contain source material for the exam.

## Contenu:

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.