ServiceNow Security Incident Response (SIR) Implementation

Durée: 2 Jours **Réf de cours: SNSIRI** **Méthodes d'apprentissage: Virtual 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.

Virtual Learning

This interactive training can be taken from any location, your office or home and is delivered by a trainer. This training does not have any delegates in the class with the instructor, since all delegates are virtually connected. Virtual delegates do not travel to this course, Global Knowledge will send you all the information needed before the start of the course and you can test the logins.

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:

No prerequisite

- 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.

Autres moyens pédagogiques et de suivi:

• Compétence du formateur : Les experts qui animent la formation sont des spécialistes des matières abordées et ont au minimum cinq ans d'expérience d'animation. Nos équipes ont validé à la fois leurs connaissances techniques (certifications le cas échéant) ainsi que leur compétence pédagogique.

• Evaluation : Chaque participant, à l'issue de la formation, répond à un questionnaire d'évaluation qui est ensuite étudié par nos équipes pédagogiques en vue de maintenir et d'améliorer la qualité de nos prestations.

• Suivi d'exécution : Une feuille d'émargement par demi-journée de présence est signée par tous les participants et le formateur.