

## ServiceNow Vulnerability Response Implementation

Durée: 2 Jours    Réf de cours: SNVRI    Méthodes d'apprentissage: Intra-entreprise & sur-mesure

### Résumé:

Learn the details of Vulnerability Response in ServiceNow.

This two-day course covers Vulnerability Response essentials such as why customers need Vulnerability Response, what Vulnerability Response is, and how to properly implement Vulnerability Response.

Participants will learn the common technical aspects of a Vulnerability Response implementation as well as experience various processes to effectively manage a Vulnerability Response implementation. Additionally, participants will learn tactical skills and strategies that will better prepare them to implement Vulnerability Response in a scalable, repeatable, and efficient manner.

Topics:

- Vulnerability Response Overview
- Getting Data into Vulnerability Response
- Tools to Manage Vulnerability Response Data
- Automating Vulnerability Response
- Vulnerability Response Data Visualization
- Vulnerability Response Delta for the Paris Release
- Capstone Project for Vulnerability Response Implementation

### Company Events

These events can be delivered exclusively for your company at our locations or yours, specifically for your delegates and your needs. The Company Events can be tailored or standard course deliveries.

### Public visé:

This course is suitable for anyone who will be working on a ServiceNow implementation of the Vulnerability Response applications. Examples, include: Process Owners – who will be champions for their process domain Technical Consultants and Administrators – who will be configuring, developing or supporting the Vulnerability Response applications Project/Program/Engagement Managers – who will be leading implementation of Vulnerability Response applications in ServiceNow Operations Managers – who have oversight of work which will be facilitated using Vulnerability Response applications in ServiceNow

### Objectifs pédagogiques:

- During this two-day interactive training course participants learn how to run a successful customer Vulnerability Response Implementation.
- Participants will:
  - Prepare to Implement Vulnerability Response
  - Configure NVD Auto-Updates
  - Perform a full Qualys Integration
  - Preview Rapid7 and Tenable Integrations
- Configure Vulnerability Groups
- Configure Criticality Calculator Groups
- Perform Vulnerability Remediation Task Assignments
- Design a Severe Vulnerability Workflow
- Work with Vulnerability Dashboards and Reports
- These objectives are achieved through a combination of demos, lecture, and group discussions. Lab exercises woven throughout the class walk you through how to effectively implement Vulnerability Response.

### Pré-requis:

- SNF - ServiceNow Fundamentals
- SNPI - ServiceNow Platform Implementation
- SNSOF - ServiceNow Security Operations (SecOps) Fundamentals
- ILFN4 - ITIL® 4 Foundation - Examen inclus

## Contenu:

Module 1 Vulnerability Response Overview	-Lab 2.1 Configure NVD Auto-Update	Module 4: Labs
Module 1: Objectives	-Lab 2.2 Full Qualys Integration and Store Preview	-Lab 4.1 Configure Vulnerability Exception Workflow
-Define ServiceNow Security Operations	Module 3 Tools to Manage Vulnerability Response	Module 5 Vulnerability Response Data Visualization
-Discuss Vulnerability Response	Module 3: Objectives	Module 5: Objectives
-Examine Vulnerability Response within the ServiceNow Platform	-Configure Vulnerability Groups for Easier Management	-Demonstrate Data Visualization through Dashboards and Reporting
Module 1: Labs	-Employ Tasking for Vulnerability Remediation	-Discuss Performance Analytics
-Lab 1.2 Exploring Vulnerability Response	Module 3: Labs	Module 5: Labs
-Lab 1.3 Preparing to Implement Vulnerability Response	-Lab 3.1 Configure Vulnerability Groups	-Lab 5.1 Dashboards and Reports
Module 2 Getting Data Into Vulnerability Response	-Lab 3.2 Configure Vulnerability Calculator Groups	Module 6 Vulnerability Response Paris Delta
Module 2: Objectives	-Lab 3.3 Vulnerability Remediation Task Assignment	Module 6: Objectives
-Definition of Vulnerabilities and Vulnerable Items	Module 4 Automating Vulnerability Response	-Discuss the new features in the Paris release
-Integrate Vulnerability Response with Vulnerability Scanners and Other Data Sources	Module 4: Objectives	-Define the changed features in the Paris release
-Scanner Integration and CMDB Reconciliation	-Demonstrate how to handle Vulnerability Exceptions	Module 7 Vulnerability Response Implementation Capstone Project
Module 2: Labs	-Construct Workflows for Process Automation	In order to reinforce the various topics presented in the Vulnerability Response Implementation course, the final course component is a take-home five task capstone project

## 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.
- Suivi d'exécution : Une feuille d'émargement par demi-journée de présence est signée par tous les participants et le formateur.
- En fin de formation, le participant est invité à s'auto-évaluer sur l'atteinte des objectifs énoncés, et à répondre à un questionnaire de satisfaction qui sera ensuite étudié par nos équipes pédagogiques en vue de maintenir et d'améliorer la qualité de nos prestations.