

ServiceNow Vulnerability Response Implementation

Varighed: 2 Days Kursus Kode: SNVRI Leveringsmetode: Virtuel deltagelse

Beskrivelse:

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

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.

Målgruppe:

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

Agenda:

- | | |
|--|--|
| ■ During this two-day interactive training course participants learn how to run a successful customer Vulnerability Response Implementation. | ■ Configure Vulnerability Groups |
| ■ Participants will: | ■ Configure Criticality Calculator Groups |
| ■ Prepare to Implement Vulnerability Response | ■ Perform Vulnerability Remediation Task Assignments |
| ■ Configure NVD Auto-Updates | ■ Design a Severe Vulnerability Workflow |
| ■ Perform a full Qualys Integration | ■ Work with Vulnerability Dashboards and Reports |
| ■ Preview Rapid7 and Tenable Integrations | ■ 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. |

Forudsætninger:

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

Indhold:

| | | |
|--|---|--|
| 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 |

Flere Informationer:

For yderligere informationer eller booking af kursus, kontakt os på tlf.nr.: 44 88 18 00

training@globalknowledge.dk

www.globalknowledge.com/da-dk/

Global Knowledge, Stamholmen 110, 2650 Hvidovre