DUMPSARENA

Certified Implementation Specialist - Vulnerability Response

ServiceNow CIS-VR

Version Demo

Total Demo Questions: 9

Total Premium Questions: 95

Buy Premium PDF

https://dumpsarena.co

sales@dumpsarena.co

sales@dumpsarena.co
dumpsarena.co

Topic Break Down

Topic	No. of Questions
Topic 1, Vulnerability Response Overview	27
Topic 2, Vulnerability Response Implementation	19
Topic 3, Vulnerability Response Administration	41
Topic 4, Vulnerability Response Reporting	8
Total	95

QUESTION NO: 1

What is the purpose of a Vulnerability Exception expiration date?

A. To define when the exception must be reviewed or renewed

B. To automatically delete the related Vulnerable Items

C. To set the scanner import schedule

D. To calculate the CVSS score

ANSWER: A

Explanation:

The expiration date defines when an approved Vulnerability Exception must be reviewed or is no longer valid. Exceptions represent a temporary, documented decision to defer normal remediation or accept risk for a defined scope. An expiration date prevents that decision from remaining in effect indefinitely without reassessment.

When an exception approaches expiration, stakeholders can review whether remediation is now possible, whether compensating controls remain effective, or whether a new risk decision is required. See the ServiceNow Vulnerability Exceptions documentation.

QUESTION NO: 2

Which module is used to adjust the frequency in which CVEs are updated?

A. NVD Auto-update

B. Update

C. CVE Auto-update

D. On-demand update

ANSWER: A

Explanation:

The **NVD Auto-update** module is used to configure how often ServiceNow retrieves and refreshes vulnerability intelligence from the National Vulnerability Database (NVD), including CVE information. In Vulnerability Response, NVD data supplies the standardized CVE records and associated vulnerability details used when processing and correlating vulnerability findings. The module provides the administrative configuration for the scheduled NVD import, so an administrator can set the update cadence to meet the organization's operational and security-data freshness requirements. Adjusting this schedule controls the frequency at which the platform checks for and imports available NVD updates rather than requiring a manual update each time.

Keeping the NVD import schedule appropriately configured helps ensure that newly published CVEs and changes to existing CVE content are available to Vulnerability Response workflows in a timely manner. ServiceNow documents the NVD and CWE import capability in its Vulnerability Response product documentation: NVD and CWE data import. Additional Vulnerability Response documentation is available from the Vulnerability Response product documentation.

QUESTION NO: 3

A Vulnerability Group contains several Vulnerable Items. What happens to the individual Vulnerable Items when the group is used to coordinate remediation?

A. They remain separate records associated with the group

B. They are merged into one Vulnerable Item

C. They are converted to Configuration Items

D. They are automatically closed

ANSWER: A

Explanation:

The individual Vulnerable Items remain separate records. A Vulnerability Group provides a way to organize related items and manage a coordinated remediation effort, but it does not merge or replace the underlying records.

Each Vulnerable Item continues to preserve its relationship to the affected CI and vulnerability, allowing the organization to retain asset-specific remediation status and verification information. See the ServiceNow Vulnerability Groups documentation.

QUESTION NO: 4

Which of the following best describes the Vulnerable item State Approval Workflow?

A. It is read-only, you can only change the Assignment Group members for the approval

B. It exists in the Security Operations Common scope so it can be modified by any Security Operations Admin

C. It can only be modified by System Administrators

D. It runs against the [sn_vul_change_approval] table

ANSWER: C

Explanation:

The Vulnerable Item State Approval Workflow can only be modified by System Administrators. This workflow is a protected, platform-level component used by Vulnerability Response to govern approval-driven vulnerable-item state transitions. Restricting its modification to the system administrator role helps preserve the integrity of the approval process, ensuring that state changes remain subject to the organization's intended controls and are not altered inadvertently by users who administer Security Operations features alone. In practice, Vulnerability Response administrators can manage vulnerability-response configuration and operational records within their delegated permissions, while changes to this workflow require the elevated access associated with a System Administrator. This distinction is important when planning workflow governance: teams should treat modifications as controlled platform configuration changes, test them appropriately, and limit access to personnel responsible for instance-wide administration. ServiceNow describes Vulnerability Response as a Security Operations capability for prioritizing and remediating vulnerabilities, with its behavior governed by platform configuration and role-based access controls. See the ServiceNow Vulnerability Response product overview and the ServiceNow access control documentation for related platform governance concepts.

QUESTION NO: 5

The three levels of users you will likely encounter that will need access to data displayed in the Vulnerability Response dashboard are: (Choose three.)

A. Security Analysts

B. Customers

C. CIO/CISO

D. Fulfillers

ANSWER: A B C

Explanation:

Security Analysts, Customers, and CIO/CISO represent the principal audiences for Vulnerability Response dashboard information because each consumes vulnerability data at a different operational or strategic level. Security Analysts need detailed, actionable visibility into vulnerable items, affected configuration items, risk context, exceptions, and remediation progress so they can investigate, prioritize, and coordinate vulnerability work. Customers need visibility into the vulnerabilities affecting the services, applications, assets, or business outcomes for which they are responsible. This supports accountability, informed risk decisions, and collaboration on remediation priorities. CIO/CISO leaders require aggregated and trend-oriented dashboard data to understand the organization's overall exposure, evaluate remediation performance, monitor risk posture, and communicate security status to executive stakeholders. ServiceNow Vulnerability Response is designed to normalize vulnerability findings, prioritize remediation using contextual information, and provide reporting appropriate to both operational teams and leadership. Role-based access controls should be applied so each audience can view the records and metrics necessary for its responsibilities while protecting sensitive vulnerability information. See the ServiceNow Vulnerability Response product overview and the ServiceNow Vulnerability Response documentation.

QUESTION NO: 6

Managers should have access to which role-based data access and visualizations? (Choose three.)

A. Aggregations for priority and workload

B. Time period views

C. Up-to-the-minute views

D. Drill-down to granularity

ANSWER: A B D

Explanation:

Managers need visualizations that support oversight, prioritization, and decisions across teams rather than only the immediate operational state of individual vulnerability records. **Aggregations for priority and workload** give a manager a consolidated picture of the volume and severity of assigned vulnerability work, enabling them to assess backlog, team capacity, remediation ownership, and where attention should be focused. **Time period views** enable managers to evaluate trends and performance over reporting intervals, such as whether vulnerability exposure or remediation progress is improving over weeks or months. This historical and comparative perspective is essential for planning, measuring progress against targets, and communicating risk posture to stakeholders. **Drill-down to granularity** complements aggregated reporting by allowing a manager to move from an overall metric into the underlying groups, assignments, vulnerable items, or records that account for the result. Managers can therefore validate dashboard findings and take informed action without losing the high-level view. These capabilities align with Vulnerability Response's use of dashboards, reporting, prioritization, and remediation workflows to manage vulnerability risk at scale. See the ServiceNow Vulnerability Response product overview and the ServiceNow Vulnerability Response documentation.

QUESTION NO: 7

After closing the Vulnerable Item (VI), it is recommended to:

A. Update the values in the Vulnerability Score Indicator (VSI) based on the criticality of the Vulnerability.

B. The VI remains active and in place until the Scanner rescans and closes the VI.

C. Mark the CI as exempt from the Vulnerability if the vulnerability was remediated.

D. Compare the Vulnerability with subsequent scans.

ANSWER: D

Explanation:

Compare the Vulnerability with subsequent scans. A Vulnerable Item represents a specific vulnerability detected on a configuration item, and its status should continue to be validated against incoming scanner data after remediation and closure. Subsequent scan imports provide the evidence that the vulnerable condition is no longer detected on the affected asset and help ensure that the closure remains appropriate over time. This is particularly important because a vulnerability can reappear after configuration changes, software changes, incomplete remediation, or changes in scanner coverage. Vulnerability Response uses integrations with vulnerability scanners to ingest findings and correlate them with vulnerable items, enabling organizations to maintain an accurate remediation posture rather than treating closure as a permanent assertion. Comparing later scan results also supports auditability: the organization can demonstrate that remediation was not only performed but subsequently verified through its normal vulnerability-detection process. ServiceNow describes Vulnerability Response as a process for prioritizing, managing, and remediating vulnerability findings, including findings received from scanner integrations. See the ServiceNow Vulnerability Response documentation and the Vulnerability Response integrations documentation.

QUESTION NO: 8

Which information should be reviewed before assigning remediation work for a Vulnerable Item? (Choose three.)

A. Affected Configuration Item

B. CI or service ownership information

C. Remediation target

D. User color theme

E. Number of dashboard favorites

ANSWER: A B C

Explanation:

The affected CI, the CI or service ownership information, and the remediation target should be reviewed before assigning remediation work. The affected CI identifies the asset requiring action, while ownership information helps route the work to the appropriate team or user. The remediation target indicates the expected completion timeframe and supports prioritization of work that is approaching or past its target.

The color theme selected by the user and the number of dashboard favorites do not determine remediation ownership or urgency. Vulnerability Response assignment should be based on operational and business context. See ServiceNow Vulnerability Response and the ServiceNow product documentation portal.

QUESTION NO: 9

Which of the following are benefits of using Vulnerability Groups? (Choose three.)

A. Coordinate remediation for related Vulnerable Items

B. Assign remediation ownership at an aggregate level

C. Track the progress of a related remediation effort

D. Replace the affected CI records in the CMDB

ANSWER: A B C

Explanation:

Vulnerability Groups enable remediation teams to manage related Vulnerable Items as a coordinated set of work. They provide an aggregate view of affected items, support assignment of the remediation effort to an appropriate group, and help teams track progress without managing every affected item independently.

A Vulnerability Group does not replace the individual Vulnerable Items. Each Vulnerable Item remains the record for a specific vulnerability affecting a specific CI and retains its own asset context and lifecycle information. See the ServiceNow Vulnerability Groups documentation.