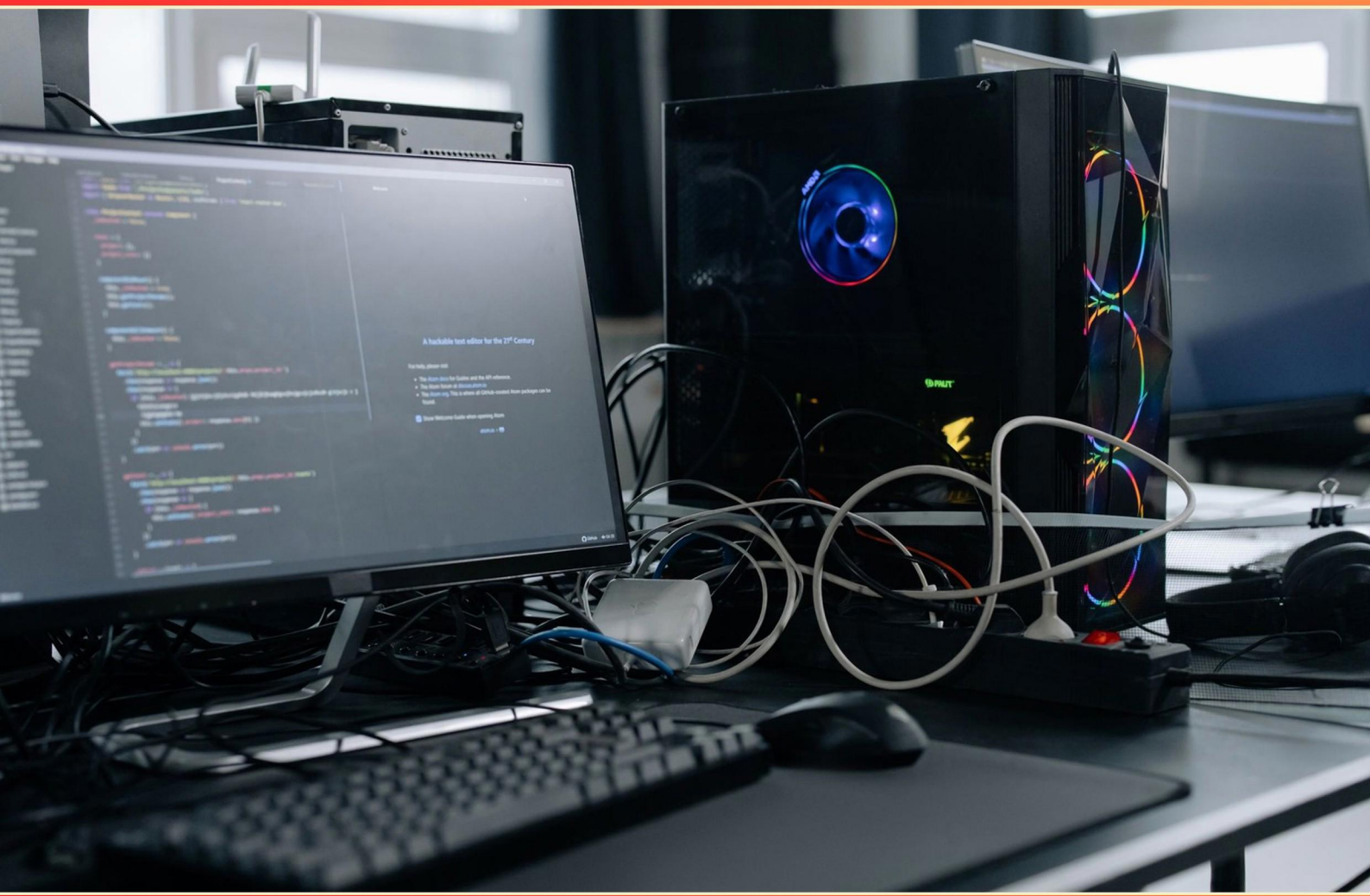
SERVICENOW CIS VULNERABILITY RESPONSE PRACTICE TEST (SAMPLE)

STUDY GUIDE



SAMPLE STUDY GUIDE WITH LIMITED QUESTIONS

VISIT US ONLINE FOR THE FULL VERSION STUDY GUIDE

https://servicenowcisvulnresponse.examzify.com

Table of Contents

Introduction

Preparing for a certification exam can feel overwhelming, but with the right tools, it becomes an opportunity to build confidence, sharpen your skills, and move one step closer to your goals. At Examzify, we believe that effective exam preparation isn't just about memorization, it's about understanding the material, identifying knowledge gaps, and building the test-taking strategies that lead to success.

This guide was designed to help you do exactly that.

Whether you're preparing for a licensing exam, professional certification, or entry-level qualification, this book offers structured practice to reinforce key concepts. You'll find a wide range of multiple-choice questions, each followed by clear explanations to help you understand not just the right answer, but why it's correct.

The content in this guide is based on real-world exam objectives and aligned with the types of questions and topics commonly found on official tests. It's ideal for learners who want to:

- Practice answering questions under realistic conditions,
- Improve accuracy and speed,
- Review explanations to strengthen weak areas, and
- Approach the exam with greater confidence.

We recommend using this book not as a stand-alone study tool, but alongside other resources like flashcards, textbooks, or hands-on training. For best results, we recommend working through each question, reflecting on the explanation provided, and revisiting the topics that challenge you most.

Remember: successful test preparation isn't about getting every question right the first time, it's about learning from your mistakes and improving over time. Stay focused, trust the process, and know that every page you turn brings you closer to success.

Let's begin.

How to Use This Guide

This guide is designed to help you study more effectively and approach your exam with confidence. Whether you're reviewing for the first time or doing a final refresh, here's how to get the most out of your Examzify study guide:

1. Start with a Diagnostic Review

Skim through the questions to get a sense of what you know and what you need to focus on. Your goal is to identify knowledge gaps early.

2. Study in Short, Focused Sessions

Break your study time into manageable blocks (e.g. 30 – 45 minutes). Review a handful of questions, reflect on the explanations.

3. Learn from the Explanations

After answering a question, always read the explanation, even if you got it right. It reinforces key points, corrects misunderstandings, and teaches subtle distinctions between similar answers.

4. Track Your Progress

Use bookmarks or notes (if reading digitally) to mark difficult questions. Revisit these regularly and track improvements over time.

5. Simulate the Real Exam

Once you're comfortable, try taking a full set of questions without pausing. Set a timer and simulate test-day conditions to build confidence and time management skills.

6. Repeat and Review

Don't just study once, repetition builds retention. Re-attempt questions after a few days and revisit explanations to reinforce learning. Pair this guide with other Examzify tools like flashcards, and digital practice tests to strengthen your preparation across formats.

There's no single right way to study, but consistent, thoughtful effort always wins. Use this guide flexibly, adapt the tips above to fit your pace and learning style. You've got this!

Questions

1. What is the role of the 'sn_vul.vr_import_admin' in Vulnerability Response?

A. Administer vulnerabilities

B. Import remediation items

C. Configure vulnerability settings

D. Read vulnerability reports

2. Where can you define Filter Groups?

A. Vulnerability Response > Vulnerability Scanning > Filter Groups

B. Security Operations > Groups > Filter Groups

C. Vulnerability Management > Scanning > Filter Definitions

D. ServiceNow > Configuration > Filter Groups

3. What does the workflow 'Vulnerability Response - Scan Vulnerable Item' create after being triggered?

A. A resolution report for the vulnerable item

B. A scan record for the vulnerable item

C. An alert for the system administrator

D. A deployment schedule for the remediation

4. How does the 'Business Impact' classification influence vulnerability prioritization?

A. It determines the urgency of the resolution

B. It determines the criticality of vulnerabilities based on service importance

C. It evaluates historical data on vulnerabilities

D. It allows for user-defined customization of priorities

5. Which framework can be integrated optionally with Configuration Compliance for continuous monitoring?

A. GRC (Governance, Risk, and Compliance)

B. ITIL Framework

C. COBIT

D. ISO 27001

6. Which system property activates the creation of a vulnerability-centric group?

A. sn_vul.auto_create_group

B. sn_vul.allow_vul_group_creation

C. sn_vul.autocreate_vul_centric_group

D. sn_vul.group_creation_enabled

7. Which application in ServiceNow uses results from third-party Secure Configuration Assessment scanners?

A. Incident Management

B. Configuration Compliance

C. Security Incident Response

D. Change Management

8. Which of the following best describes a proactive approach to vulnerability management?

A. Waiting for incidents to occur before addressing them

B. Regularly scanning and assessing system vulnerabilities

C. Training employees only after a breach

D. Documenting vulnerabilities after they are resolved

9. Why is Configuration Management important in the context of Vulnerability Response?

A. It collects user feedback on incidents

B. It helps know what to protect and the overall business impact of a compromise

C. It prioritizes incident responses

D. It enhances customer service delivery

10. Which of the following functions does the sn_vul.vr_import_admin role perform?

A. It allows reading solution records

B. It manages user roles in security operations

C. It runs scheduled jobs for integrations

D. It creates and updates vulnerability reports

Answers

1. B
2. B
3. B
4. B
5. A
6. C
7. B
8. B
9. B
10. C

Explanations

1. What is the role of the 'sn_vul.vr_import_admin' in Vulnerability Response?

A. Administer vulnerabilities

B. Import remediation items

C. Configure vulnerability settings

D. Read vulnerability reports

The role of 'sn_vul.vr_import_admin' within Vulnerability Response is specifically focused on importing remediation items. This role allows users to integrate and upload necessary data related to vulnerabilities, such as fixes and patches, into the ServiceNow platform. This is crucial for ensuring that the system has the most current information to facilitate the remediation of vulnerabilities in a timely manner. Importing remediation items effectively supports the overall vulnerability management process by allowing organizations to assess and address security issues proactively. In contrast, other options focus on different aspects of vulnerability management. Administering vulnerabilities involves more comprehensive oversight and management tasks, configuring settings pertains to adjusting the system configurations for vulnerabilities, and reading vulnerability reports is more about data assessment rather than data input. Therefore, the import function is key to ensuring that remediation items are available for the Vulnerability Response team to act upon.

2. Where can you define Filter Groups?

A. Vulnerability Response > Vulnerability Scanning > Filter Groups

B. Security Operations > Groups > Filter Groups

C. Vulnerability Management > Scanning > Filter Definitions

D. ServiceNow > Configuration > Filter Groups

Defining Filter Groups is a key function related to managing and organizing vulnerabilities within the Security Operations module. In ServiceNow, Filter Groups are utilized to categorize and manage different sets of records based on specific criteria, allowing teams to focus on relevant vulnerabilities. The option indicating Security Operations > Groups > Filter Groups is correct because this path leads directly to the area where administrators can create and manage Filter Groups applicable to the Security Operations suite, which includes vulnerability management. Here, users can define and configure different filters to segment vulnerabilities based on their attributes, making it easier to prioritize and assign response activities. The other options may refer to different paths in ServiceNow but do not lead to the proper section for defining Filter Groups as it pertains to Security Operations. This understanding of the correct navigation is important for effective management of vulnerabilities in the ServiceNow platform, helping ensure that security teams can efficiently handle existing and emerging threats.

3. What does the workflow 'Vulnerability Response - Scan Vulnerable Item' create after being triggered?

A. A resolution report for the vulnerable item

B. A scan record for the vulnerable item

C. An alert for the system administrator

D. A deployment schedule for the remediation

The workflow 'Vulnerability Response - Scan Vulnerable Item' is designed to initiate the scanning process for vulnerable items within the system. When this workflow is triggered, it creates a scan record for the vulnerable item, which is critical for tracking the status of the vulnerability, its assessment, and subsequent responses. This scan record serves as a formal documentation of the vulnerability scan, helping stakeholders understand what vulnerabilities exist, where they are located, and what steps might need to be taken to address them. Creating a scan record allows for a structured approach to vulnerability management, ensuring that all relevant data is captured for analysis and reporting. This facilitates better decision-making regarding remediation efforts and helps maintain accountability throughout the vulnerability response life cycle.

4. How does the 'Business Impact' classification influence vulnerability prioritization?

A. It determines the urgency of the resolution

B. It determines the criticality of vulnerabilities based on service importance

C. It evaluates historical data on vulnerabilities

D. It allows for user-defined customization of priorities

The 'Business Impact' classification plays a crucial role in vulnerability prioritization by determining the criticality of vulnerabilities based on the importance of the services they affect. This classification allows organizations to assess which vulnerabilities could have a more significant adverse impact on business operations, financial performance, or reputation. When vulnerabilities are evaluated with respect to the critical services they correspond to, it helps in directing resources and efforts towards addressing the most impactful issues first. By understanding the business context and the impact that a particular vulnerability may have, organizations can prioritize their remediation efforts effectively, ensuring that the most pressing risks are mitigated in alignment with their operational priorities. This strategic approach enhances the overall security posture and minimizes potential disruptions to essential services, ultimately supporting business continuity. Other options do touch upon various aspects of vulnerability management, such as urgency of resolution, historical data evaluation, and customization of priorities, but they do not directly address how the classification of business impact specifically shapes the prioritization of vulnerabilities in accordance with their significance to the organization's operations.

5. Which framework can be integrated optionally with Configuration Compliance for continuous monitoring?

A. GRC (Governance, Risk, and Compliance)

B. ITIL Framework

C. COBIT

D. ISO 27001

The Governance, Risk, and Compliance (GRC) framework can be integrated optionally with Configuration Compliance for continuous monitoring due to its comprehensive approach to managing an organization's governance, risk management, and compliance with regulations and policies. This integration allows for a seamless flow of information between the two systems, enhancing an organization's ability to assess its compliance posture continuously. GRC enables organizations to align their IT and business objectives, ensuring that risks are managed effectively while meeting compliance requirements. When integrated with Configuration Compliance, GRC can leverage the data collected from continuous monitoring processes to provide insights, report on compliance status, and facilitate risk assessments, thereby improving overall governance effectiveness. Other frameworks, like ITIL or COBIT, focus on best practices related to IT service management and governance, but they do not provide the same emphasis on compliance and risk management as GRC does. Similarly, ISO 27001 is a standard for information security management but does not enhance configuration compliance in the context of ongoing risk and governance in the same way GRC does. Therefore, the GRC framework stands out as the most suitable option for integration with Configuration Compliance for continuous monitoring.

6. Which system property activates the creation of a vulnerability-centric group?

A. sn_vul.auto_create_group

B. sn_vul.allow_vul_group_creation

C. sn_vul.autocreate_vul_centric_group

D. sn_vul.group_creation_enabled

The system property that activates the creation of a vulnerability-centric group is indeed associated with its caption to ensure a vulnerability-focused approach in managing security incidents. In this case, the correct choice is the one that directly references the auto-creation of a group specifically tailored to vulnerabilities. The naming convention indicates that this property is designed to automate the grouping of vulnerabilities, integrating them into a cohesive management strategy for improved response and remediation. This is critical in environments dealing with numerous vulnerabilities, as it allows for a streamlined process in addressing and managing security threats more effectively. While other options may seem plausible at first, they don't specifically denote the focused functionality associated with vulnerability-centric groupings. Thus, understanding the specific context and naming helps in recognizing why this property is precisely the right one for facilitating the desired automated response capabilities related to vulnerabilities.

7. Which application in ServiceNow uses results from third-party Secure Configuration Assessment scanners?

A. Incident Management

B. Configuration Compliance

C. Security Incident Response

D. Change Management

The correct choice is Configuration Compliance because this application in ServiceNow is specifically designed to evaluate the security posture of the organization's configurations against established standards and best practices. It makes use of data gathered from third-party Secure Configuration Assessment scanners to identify deviations or vulnerabilities in the configuration of systems and applications. The integration of these scanner results allows Configuration Compliance to provide comprehensive assessments that can help organizations monitor compliance with security policies and frameworks. This functionality is critical for organizations striving to maintain a secure environment by ensuring that their configurations adhere to necessary security guidelines. In contrast, Incident Management focuses on restoring service after an incident, Security Incident Response deals with managing security breaches or attacks, and Change Management is concerned with managing changes to IT services. While these applications might benefit from security data in broader terms, they do not utilize secure configuration assessment scanner results specifically for compliance and assessment purposes as Configuration Compliance does.

8. Which of the following best describes a proactive approach to vulnerability management?

A. Waiting for incidents to occur before addressing them

B. Regularly scanning and assessing system vulnerabilities

C. Training employees only after a breach

D. Documenting vulnerabilities after they are resolved

A proactive approach to vulnerability management involves actively identifying and mitigating vulnerabilities before they can be exploited. Regularly scanning and assessing system vulnerabilities is a cornerstone of this strategy, as it enables organizations to discover weaknesses in their systems, applications, and networks on an ongoing basis. By conducting frequent scans and assessments, organizations can stay ahead of potential threats and take necessary actions to remediate vulnerabilities before they become a problem. This approach contrasts significantly with other options, where waiting for incidents to occur or addressing vulnerabilities only after a breach indicates a reactive or after-the-fact approach. Similarly, training employees only after a breach fails to prepare them for future risks, and documenting vulnerabilities post-resolution does not contribute to preventing vulnerabilities in the first place. Therefore, the practice of regularly scanning and assessing vulnerabilities is essential for maintaining robust security and resilience against threats.

9. Why is Configuration Management important in the context of Vulnerability Response?

A. It collects user feedback on incidents

B. It helps know what to protect and the overall business impact of a compromise

C. It prioritizes incident responses

D. It enhances customer service delivery

Configuration Management plays a pivotal role in Vulnerability Response because it provides an understanding of the assets within an organization and their interrelationships. This knowledge is crucial for identifying what needs to be protected, especially against potential vulnerabilities. By maintaining an accurate and up-to-date configuration management database (CMDB), organizations can assess the business impact of a compromise more effectively. This means that if a vulnerability is identified, the organization can quickly determine which systems are at risk, how critical those systems are to business operations, and what the potential consequences of a breach would be. This comprehensive awareness shapes the overall strategy for addressing vulnerabilities, ultimately leading to more effective risk management and mitigation efforts. Other aspects, such as user feedback, incident prioritization, or customer service delivery, while important in their own right, do not directly contribute to the foundational understanding of what vulnerabilities might exist or how they impact the organization's assets in the same way that Configuration Management does.

10. Which of the following functions does the sn_vul.vr_import_admin role perform?

A. It allows reading solution records

B. It manages user roles in security operations

C. It runs scheduled jobs for integrations

D. It creates and updates vulnerability reports

The function of the sn_vul.vr_import_admin role is primarily associated with running scheduled jobs for integrations. This role is designed to oversee the importation of vulnerability data into the ServiceNow platform, which involves setting up and managing integrations that pull in data from various sources. Scheduled jobs are critical in automation, ensuring that vulnerability data is regularly and accurately updated without requiring manual intervention. The role facilitates the seamless integration of vulnerability information, making it easier for security operations teams to stay current with the latest vulnerabilities that may impact their environments. By efficiently managing these scheduled jobs, the role helps organizations maintain a robust vulnerability management process. Other options regarding reading solution records, managing user roles, or creating and updating vulnerability reports pertain to different aspects of vulnerability response, but they do not directly reflect the core function of the sn_vul.vr_import_admin role. Only the ability to run scheduled jobs for integrations aligns with the responsibilities and duties assigned to this specific role.

Next Steps

Congratulations on reaching the final section of this guide. You've taken a meaningful step toward passing your certification exam and advancing your career.

As you continue preparing, remember that consistent practice, review, and self-reflection are key to success. Make time to revisit difficult topics, simulate exam conditions, and track your progress along the way.

If you need help, have suggestions, or want to share feedback, we'd love to hear from you. Reach out to our team at hello@examzify.com.

Or visit your dedicated course page for more study tools and resources:

https://servicenowcisvulnresponse.examzify.com

We wish you the very best on your exam journey. You've got this!