EXAMTOPICS

- Expert Verified, Online, **Free**.

Custom View Settings

Topic 1 - Exam A

Question #1 *Topic 1*

Select the three components of a Filter Condition: (Choose three.)

A. Field

B. Sum

C. Operator

D. Value

Question #2 *Topic 1*

SLAs are used to ensure VUL are processed in a timely matter. Which field is used to determine the expected timeframe for remediating a VIT?

A. Updated

B. Remediation status

C. Remediation target

D. Closed

Question #3 *Topic 1*

What is the minimum role required to create and change Service Level Agreements for Vulnerability Response groups?

A. sla_manager

B. admin

C. sn_vul.vulnerability_write

D. sn_vul.admin

Question #4 *Topic 1*

Changes made within a named Update Set in a different application scope:

A. Will be captured

B. Will throw errors

C. Will not be captured

D. Will be partially captured

Question #5 *Topic 1*

ServiceNow Vulnerability Response tables typically start with which prefix?

A. snvr_

B. snvuln_

C. vul_

D. sn_vul_

Question #6 *Topic 1*

In regard to the Security Operations Process, which of the following statements defines the “Identify” phase?

A. What processes and assets need protection?

B. What techniques can identify incidents?

C. What safeguards are available?

D. What techniques can restore capabilities?

E. What techniques can contain impacts of incidents?

Question #7 *Topic 1*

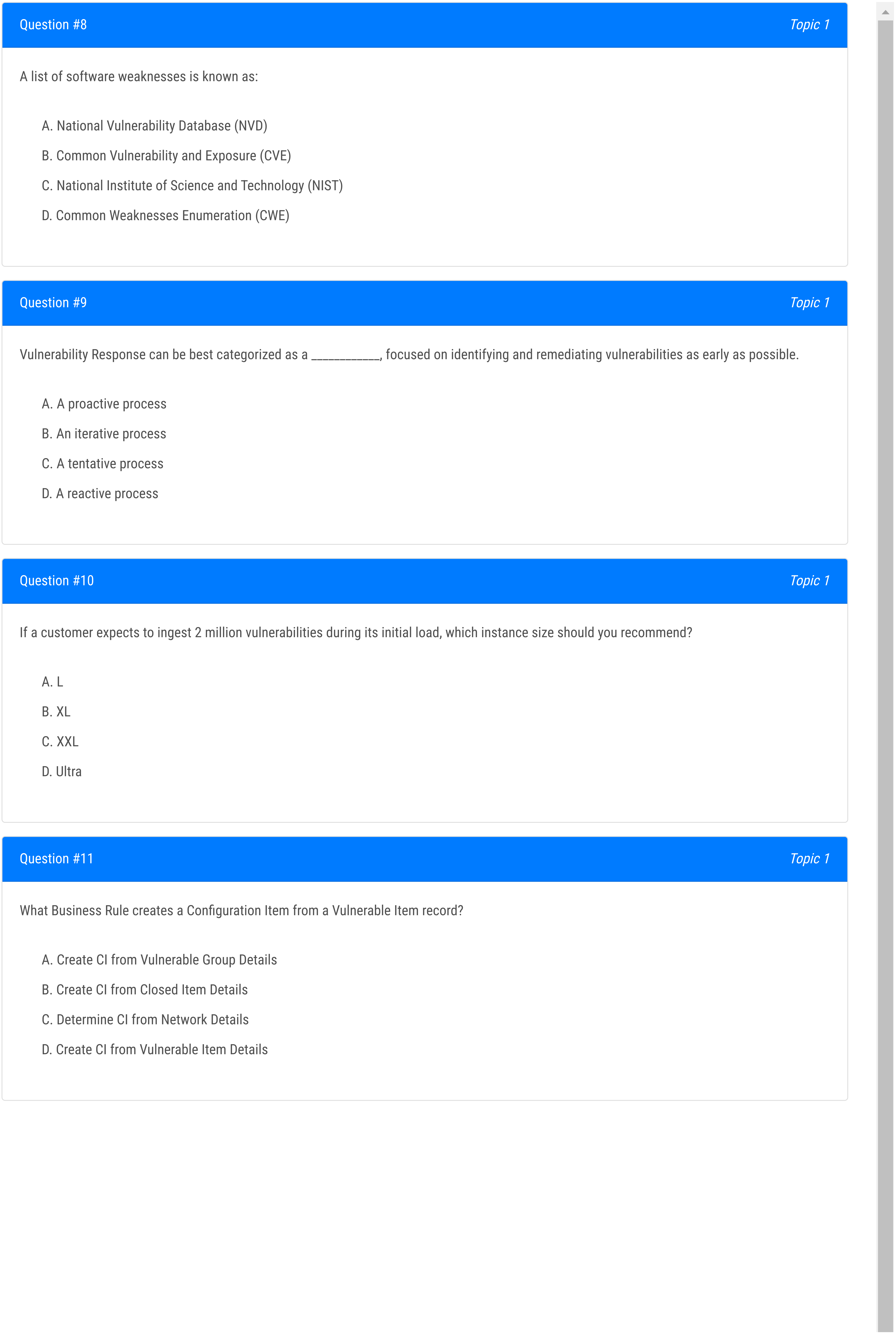
Which module is used to adjust the frequency in which CVEs are updated?

A. NVD Auto-update

B. Update

C. CVE Auto-update

D. On-demand update



Question #8 *Topic 1*

A list of software weaknesses is known as:

A. National Vulnerability Database (NVD)

B. Common Vulnerability and Exposure (CVE)

C. National Institute of Science and Technology (NIST)

D. Common Weaknesses Enumeration (CWE)

Question #9 *Topic 1*

Vulnerability Response can be best categorized as a ____________, focused on identifying and remediating vulnerabilities as early as possible.

A. A proactive process

B. An iterative process

C. A tentative process

D. A reactive process

Question #10 *Topic 1*

If a customer expects to ingest 2 million vulnerabilities during its initial load, which instance size should you recommend?

A. L

B. XL

C. XXL

D. Ultra

Question #11 *Topic 1*

What Business Rule creates a Configuration Item from a Vulnerable Item record?

A. Create CI from Vulnerable Group Details

B. Create CI from Closed Item Details

C. Determine CI from Network Details

D. Create CI from Vulnerable Item Details

Question #12 *Topic 1*

The components installed with Vulnerability Response include:

A. Tables, Scheduled Jobs, Security Operations Common

B. Business Rules, Roles, Workflows

C. Properties, Client Scripts, Wizards

D. UI Pages, Business Rules, Vulnerability Scanners

Question #13 *Topic 1*

What is the purpose of Scoped Applications?

A. Suppliers can only charge for applications when they are scoped

B. Scoped applications are scalable, Global applications are not

C. Scoping encapsulates and protects data and functionality

D. An application needs to be scoped in order to be deployed as a plugin

Question #14 *Topic 1*

What is the ID associated with the Vulnerability Response plugin?

A. com.snc.threat.intelligence

B. com.snc.vulnerability

C. com.snc.threat.feeds

D. com.snc.security_incident

Question #15 *Topic 1*

Where can you find information related to the Common Vulnerabilities and Exposures (CVE)?

A. Tenable

B. MITRE

C. NIST

D. Qualys

Question #16 *Topic 1*

Which one of the following record types can be considered the intersection of Vulnerability source information and CMDB CI records?

A. Vulnerability

B. Vulnerability Task

C. CMDB_CI_Vuln

D. Vulnerable Item (VI)

Question #17 *Topic 1*

Which of the following provides a list of software weaknesses?

A. Third Party Entries

B. NVD

C. CWE

D. Vulnerable Items

Question #18 *Topic 1*

Filter Groups provide a way to:

A. Decouple the use of the grouping from the definition of the grouping

B. Build criteria once

C. Reuse criteria in a variety of places

D. All of the above

Question #19 *Topic 1*

Which module within the Vulnerability Response application could be used to get information from the National Vulnerability Database (NVD) at any moment?

A. On-Demand Update

B. NVD Auto-Update

C. Vulnerable Software

D. NVD Patch

Question #20 *Topic 1*

Which statement about patching is most correct?

A. Mature organizations abandon patching

B. Patch management and Vulnerability Response are interchangeable terms

C. Patching is one of many responses to a Vulnerability

D. As long as you are patching actively, Vulnerability Response isn't necessary

Question #21 *Topic 1*

The Vulnerability Admin role (sn_vul.admin) can modify Vulnerability Application Properties and can be delegated to the following role(s):

A. ServiceNow Security Operations Admin (sn_sec.admin)

B. Security Admin (security.admin)

C. Vulnerability Response Admin (sn_vul_resp.admin)

D. All of the above

E. None of the above

Question #22 *Topic 1*

sn_vul.itsm_popup is the property that is set to True or False based on the customer desire for a popup when creating a Problem or Change record from a Vulnerability or VI record.

A. True

B. False

Question #23 *Topic 1*

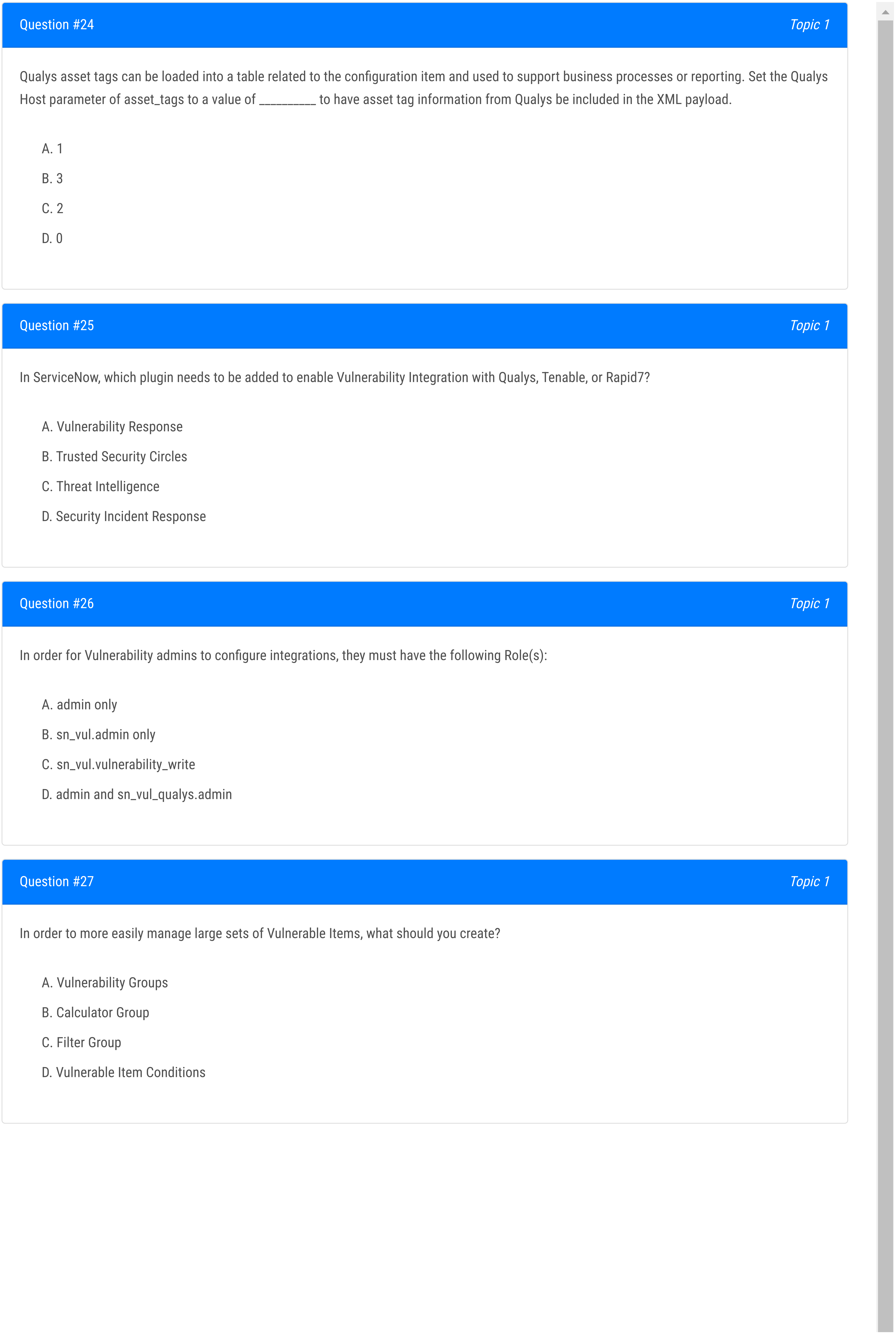
Items in the ServiceNow Store are built and supported by:

A. An Implementation Partner

B. The company that created the Application

C. ServiceNow Professional Services

D. ServiceNow Technical Support



Question #24 *Topic 1*

Qualys asset tags can be loaded into a table related to the configuration item and used to support business processes or reporting. Set the Qualys Host parameter of asset_tags to a value of __________ to have asset tag information from Qualys be included in the XML payload.

A. 1

B. 3

C. 2

D. 0

Question #25 *Topic 1*

In ServiceNow, which plugin needs to be added to enable Vulnerability Integration with Qualys, Tenable, or Rapid7?

A. Vulnerability Response

B. Trusted Security Circles

C. Threat Intelligence

D. Security Incident Response

Question #26 *Topic 1*

In order for Vulnerability admins to configure integrations, they must have the following Role(s):

A. admin only

B. sn_vul.admin only

C. sn_vul.vulnerability_write

D. admin and sn_vul_qualys.admin

Question #27 *Topic 1*

In order to more easily manage large sets of Vulnerable Items, what should you create?

A. Vulnerability Groups

B. Calculator Group

C. Filter Group

D. Vulnerable Item Conditions

Question #28 *Topic 1*

This functionality provides a simple way to build criteria once, which can be reused in other platform areas.

A. Conditions

B. Favorites

C. Filter Group

D. Filters

Question #29 *Topic 1*

To facilitate the remediation of a Vulnerable Item what type of item is most commonly used?

A. Create a Problem

B. Create a Security Incident

C. Create a KB article

D. Create a Change

Question #30 *Topic 1*

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

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

Question #31 *Topic 1*

Vulnerability Response is a scoped application; which prefix is attached to all items related to the application?

A. cmn_vul

B. vul

C. sn_vul

D. x_vul

Question #32 *Topic 1*

Which Vulnerability maturity level provides advanced owner assignment?

A. Enterprise risk trending

B. Automated prioritization

C. Manual operations

D. Improved remediation

Question #33 *Topic 1*

Which application provides the opportunity to align security events with organizational controls, automatically appraising other business functions of potential impact?

A. Performance Analytics

B. Event Management

C. Governance, Risk, and Compliance

D. Service Mapping

Question #34 *Topic 1*

Ignoring a Vulnerable Item:

A. Permanently removes the item from the list of Active Vulnerable Items

B. Move the item to the Slushbucket

C. Has no impact on the list of Active Vulnerable Items

D. Temporarily removes the item from the list of Active Vulnerable Items

Question #35 *Topic 1*

What do Vulnerability Exceptions require?

A. An Approval by default

B. An Exception Workflow

C. A GRC integration

D. A Filter Group

Question #36 *Topic 1*

Best Practices dictate that when creating a Change task from a Vulnerable Item, which of the following fields should be used for assigning the Assigned To field on the Change task?

A. Assigned To on Vulnerable Item

B. Managed By on CMDB_CI

C. Assigned To on CMDB_CI Record

D. Best Practice does not dictate a specific field

Question #37 *Topic 1*

Approvals within the Vulnerability Application are created based on:

A. The sys_approval and the sn_vul_vulnerable_item tables

B. The sn_vul_vulnerable_item and sn_vul_vulnerability tables

C. The sn_vul_change_approval table

D. The sys_approval table

Question #38 *Topic 1*

Some customers may have a clearly-defined, well-documented vulnerability exception process and some may even provide a diagram illustrating that process.
What is the main advantage of having this documentation when translating it into a Flow or Workflow?

A. Perfect opportunity for process improvement

B. Understand their internal process

C. Build the Flow/Workflow directly into the platform

D. No advantage

Question #39 *Topic 1*

When an approval is rejected for a Vulnerable Item exception, what happens to the State field for that record?

A. It reverts to 'Analysis'

B. It is set to 'New'

C. It is set to 'In Review'

D. It will be set back to its previous value