ATMIC NETWORKS
YOUR GUIDE TO GLOBAL CERTIFIATION

"Please note that these files may not be up to date. However, the questions will help you understand the exam format and typical question patterns."

www.atmicnetworks .com

Warning: Keep connected with our support team for latest updates

Question: 1

Select the three components of a Fitter Condition: Choose 3 answers

A. Field
B. Sum
C. Operator
D. Value

Answer: B

Question: 2

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

Answer: D

Question: 3

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

Answer: D

Question: 4

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

Answer: A

Question: 5

ServiceNow Vulnerability Response tables typically start with which prefix?

A. snvr_
B. snvuln_
C. vul_
D. sn_vul_

Answer: D

Question: 6

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?

Answer: C

Question: 7

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

Question: 8

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)

Answer: D

Question: 9

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

Answer: C

Question: 10

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

A. L
B. XL
C. XXL
D. Ultra

Answer: B

Question: 11

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

Answer: A

Question: 12

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. Ul Pages. Business Rules, Vulnerability Scanners

Answer: B

Question: 13

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

Answer: D

Question: 14

What is the ID associated with the Vulnerability Response plugln?

A. com.snc.threat.intelllgence
B. com.snc.vulnerability
C. com.snc.threat.feeds
D. com.snc.securityjncident

Answer: C

Question: 15

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

A. Tenable
B. MITRE
C. NIST
D. Qualys

Answer: B

Question: 16

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)

Answer: A

Question: 17

Which of the following provides a list of software weaknesses?

A. Third Party Entries
B. NVD
C. CWE
D. Vulnerable Items

Answer: B

Question: 18

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

Answer: D

Question: 19

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

Answer: A

Question: 20

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

Answer: C

Question: 21

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

Answer: A

Question: 22

sn_vul.itsm_popup is the properly 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

Answer: A

Question: 23

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

Answer: D

Question: 24

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

Answer: C

Question: 25

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

Answer: A

Question: 26

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

Answer: B

Question: 27

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

Answer: A

Question: 28

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

A. Conditions
B. Favorites
C. Filte Group
D. Filters

Answer: B

Question: 29

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

Answer: C

Question: 30

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: A

Question: 31

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

Answer: D

Question: 32

Which Vulnerability maturity level provides advanced owner assignment?

A. Enterprise risk trending
B. Automated prioritization
C. Manual operations
D. Improved remediation

Answer: B

Question: 33

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

Answer: C

Question: 34

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

Answer: A

Question: 35

What do Vulnerability Exceptions require?

A. An Approval by default
B. An Exception Workflow
C. A GRC integration
D. A Filter Group

Answer: A

Question: 36

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

Answer: C

Question: 37

Approvals within the Vulnerability Application are created based on:

A. The sys_approval and the 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. Ths sys_approval table

Answer: D

Question: 38

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

Answer: B

Question: 39

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

Answer: C

Question: 40

What option can be used to close out a Vulnerable item Record or initiate the Exception Process?

A. Complete
B. Update
C. Close/Defer
D. Save

Answer: D

Question: 41

What must Vulnerability Exceptions be supplied by default?

A. A reason for the exception
B. Integrations with GRC to handle the exception
C. Requirement Actions for the exception
D. A manual approval authority for the exception

Answer: A

Question: 42

Which of the following best describes a Vulnerability Group?

A. Groups Vis using a Filter against Vulnerable Item Fields
B. A Filter defining a sub-set of Cls to be treated as a group
C. The User Group assigned to resolving the Vulnerable Item
D. Must have a corresponding filter group

Answer: D

Question: 43

In order to more easily manage large sets of Vulnerable Items, you would want to create:

A. Vulnerability Groups
B. Script Includes
C. Filter Groups
D. Vulnerability Sets

Answer: B

Question: 44

Which of the following is the property that controls whether Vulnerability Groups are created by default based on Vulnerabilities in the system?

A. sn_vul.autocreate_vul_centric_group
B. sn_vul.autocreate_groups
C. sn_vul.autocreate_vul_grouping
D. sn_vul.create_default_vul_groups

Answer: C

Question: 45

What system property allows for the auto creation of Vulnerability Groups based on the Vulnerable Item's Vulnerability?

A. sn_vul.autocreate_vul_filter_group
B. sn_vul.autocreate_vul_approval_group
C. sn_vul.autocreate_vul_group_item
D. sn_vul.autocreate_vul_centric_group

Answer: A

Question: 46

Where in the platform can you create Filter Groups?

A. Vulnerability > Administration > Filter Groups
B. Vulnerability > Groups > Filter Groups
C. Security Operations > Administration > Filter Groups
D. Security Operations > Groups > Filter Groups

Answer: D

Question: 47

Which of the following can NOT be used for building Vulnerability Groups?

A. Vulnerability
B. Filter Groups
C. Condition Builder
D. Advanced Scripts

Answer: B

Question: 48

Filter groups can be used In Vulnerability Response to group what type of vulnerability records?

A. Vulnerability groups
B. Third Party Entries
C. Vulnerable Items
D. Vulnerable Software

Answer: C

Question: 49

If fixing a Vulnerable Item outweighs the benefits, the correct course of action is:

A. Mark the CI inactive in the CMDB and notify the CI owner
B. Record the accepted risk and Close/Defer the Vulnerable Item
C. Deprioritize the Vulnerable item Records (VIT) to push them further down the list so it can be ignored
D. Add the CI to the Vulnerability Scanners exclusions Related List

Answer: A

Question: 50

A common Integration point with Vulnerability is:

A. Workflow Mappings
B. Risk Indicators within GRC
C. Service Catalog
D. Knowledge Base

Answer: A

Question: 51

Which of the following is a common Integration point between Vulnerability and GRC?

A. Security Incident Response
B. Change
C. Problem
D. Risk Indicators

Answer: D

Question: 52

What is the ServiceNow application used for process automation?

A. Knowledge Base
B. Workflows
C. SLAs
D. Service Catalog

Answer: B

Question: 53

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 Adminstrators
D. It runs against the [sn_vul_change_approval] table

Answer: C

Question: 54

To ensure that Vulnerabilities are processed correctly, you can define a Service Level Agreement (SLA) for Vulnerability Response. To achieve this you would:

A. Create a custom workflow to monitor the time between States
B. Log in as a system admin, and using the globally scoped baseline SLA Modules
C. Have the role of Vulnerability admin, but only in the Vulnerability Scope
D. Make sure you have at least the sn_vul.vulnerability_write role and using the baseline SLA Application Modules

Answer: B

Question: 55

What role Is required to view the Vulnerability Overview Dashboard?

A. sn_vul.vulnerability.read
B. sn_vul.manager
C. sn_vul.ciso
D. sn_vul.vulnerability.wnte

Answer: A

Question: 56

Managers should have access to which role-based data access and visualizations? Choose 3 answers

A. Aggregations for priority and workload
B. Time period views
C. Up-to-the-minute views
D. Drill-down to granularity

Answer: D

Question: 57

To get useful reporting regarding the most vulnerable CI's, which statement applies?

A. You must purchase a separate PA module.
B. Your CI population must be huge.
C. You must have good KPi's defined.
D. Your CMDB must be up to date and useful.

Answer: B

Question: 58

What type of data would the CIO/CISO want on the dashboard?

A. Aggregations for priority and workload
B. Drill-down to granularity
C. Single, clear indicators of organizational health
D. Up to the minute views

Answer: A

Question: 59

The three levels of users you will likely encounter that will need access to data displayed in the Vulnerability Response dashboard are: Choose 3 answers

A. Security Analysts
B. Customers
C. CIO/CISO
D. Fulfillers

Answer: A

Question: 60

What is the best way to develop a complete list of Vulnerability Reports?

A. Recommend that the client purchase the full Performance Analytics package.
B. Ask the CISO.
C. Work with the customer to identify the things that will be most useful to them.
D. Use the standard out of the box reports only.

Answer: B