PassQueen
a.k.a dumpsqueen.com

Certified Implementation Specialist - Security Incident Response Exam

ServiceNow CIS-SIR

Version Demo

Total Demo Questions: 8

Total Premium Questions: 87

Buy Premium PDF

https://passqueen.com

support@passqueen.com

Topic Break Down

Topic	No. of Questions
Topic 1, Security Incident Response Overview	12
Topic 2, Security Incident Response Configuration	38
Topic 3, Security Incident Response Process	20
Topic 4, Security Incident Response Integrations	17
Total	87

QUESTION NO: 1

Which of the following are potential benefits for utilizing Security Incident assignment automation?

(Choose two.)

A. Decreased Time to Containment

B. Increased Mean Time to Remediation

C. Decreased Time to Ingestion

D. Increased resolution process consistency

ANSWER: A D

Explanation:

Decreased Time to Containment is a key benefit of Security Incident assignment automation because incoming incidents can be routed immediately to the appropriate assignment group or responder based on defined conditions, such as incident category, affected service, severity, or other record attributes. Reducing the manual triage and handoff time helps the organization begin investigation and containment sooner, which limits the potential scope and business impact of an incident.

Increased resolution process consistency is also a benefit because automated assignment applies the same routing logic every time the specified criteria are met. This creates a repeatable process for directing work to teams with the required ownership and expertise, rather than relying on an individual to select a group manually. Consistent routing improves accountability, supports predictable response workflows, and helps teams meet operational targets. ServiceNow Security Operations is designed to orchestrate and streamline security response processes, including assigning and managing security incidents. See ServiceNow Security Operations and ServiceNow Security Incident Response.

QUESTION NO: 2

Why is it important that the Platform (System) Administrator and the Security Incident administrator role be separated? (Choose three.)

A. Access to security incident data may need to be restricted

B. Allow SIR Teams to control assignment of security roles

C. Clear separation of duty

D. Reduce the number of incidents assigned to the Platform Admin

E. Preserve the security image in the company

ANSWER: A B C

Explanation:

Separating the Platform (System) Administrator role from the Security Incident administrator role supports the sensitive nature of Security Incident Response operations. **Access to security incident data may need to be restricted** because incident records can contain confidential evidence, affected-user information, indicators of compromise, investigation notes, and other information that should be available only to authorized security personnel. A distinct Security Incident administrator role enables more deliberate access governance for the SIR application and its operational data.

Allow SIR Teams to control assignment of security roles is also important because the security organization can administer its own SIR-specific access model and ensure that analysts, responders, and security managers receive the permissions appropriate to their responsibilities. This reduces dependency on broad platform-administration access for normal security-team administration.

Clear separation of duty provides accountability and limits the concentration of administrative power. Platform administrators can manage the underlying ServiceNow platform, while Security Incident administrators manage the security-

response application and its authorized users. This separation supports least-privilege practices and auditable governance for sensitive security operations. ServiceNow documents Security Incident Response roles and their responsibilities in its Security Incident Response roles documentation; see also ServiceNow's Security Operations overview.

QUESTION NO: 3

If a desired pre-built integration cannot be found in the platform, what should be your next step to find a certified integration?

A. Build your own through the REST API Explorer

B. Ask for assistance in the community page

C. Download one from ServiceNow Share

D. Look for one in the ServiceNow Store

ANSWER: D

Explanation:

Look for one in the ServiceNow Store is correct because the Store is ServiceNow's central marketplace for applications, integrations, spokes, and other extensions that can be installed on a ServiceNow instance. When an integration is not already available as a pre-built capability in the product, the Store is the appropriate next place to search for an integration provided by ServiceNow or a partner. Store listings identify the publisher, describe compatibility and installation requirements, and provide supporting documentation, helping an implementation team evaluate whether an integration meets its Security Incident Response use case and organizational requirements. Searching the Store also supports a governed approach to integrations: teams can assess an existing packaged solution before committing effort to custom development. For Security Incident Response implementations, this can be particularly useful when connecting security tools, threat-intelligence sources, or external workflow platforms. ServiceNow's documentation describes the Store as the location for discovering and obtaining ServiceNow applications and integrations, while the Store itself provides searchable listings and publisher information. Review the listing details and any prerequisites before installation, and follow the organization's normal change, security, and application-governance processes. See the ServiceNow Store and ServiceNow's Store overview for more information.

QUESTION NO: 4

Which two Flow Designer components can be configured after a flow trigger? (Choose two.)

A. Actions

B. Flow logic

C. Triggers

D. Application menus

ANSWER: A B

Explanation:

Actions and **Flow logic** can be configured after a trigger. Actions perform work, such as creating a response task, updating a Security Incident, or sending a notification. Flow logic controls how that work proceeds by providing constructs such as conditions, waits, loops, and branches.

A trigger starts the flow and is configured as the entry point rather than as a subsequent component. See the ServiceNow Flow Designer documentation.

QUESTION NO: 5

Which Flow Designer element contains the event or conditions that determine when a flow starts?

A. Trigger

B. Action

C. Data pill

D. Spoke

ANSWER: A

Explanation:

Trigger is correct because the trigger defines when Flow Designer starts a flow. A trigger can be based on a record event, such as a Security Incident being created or updated, or on another supported trigger type such as a schedule.

After the trigger conditions are met, Flow Designer runs the configured actions and flow logic. See the ServiceNow Flow Designer trigger documentation.

QUESTION NO: 6

There are several methods in which security incidents can be raised, which broadly fit into one of these categories: _____. (Choose two.)

A. Integrations

B. Manually created

C. Automatically created

D. Email parsing

ANSWER: B C

Explanation:

ServiceNow Security Incident Response groups the ways a security incident record is opened into the broad categories **Manually created** and **Automatically created**. A manually created incident is one entered directly by a user, typically by a security analyst or another authorized fulfiller, when they identify an event requiring investigation and response. This supports analyst-led intake, triage, and the capture of incident details from sources that are not already connected to the platform.

An automatically created incident is generated through configured automation, such as inbound security tooling, integrations, event processing, or other rules that create a Security Incident Response record when specified conditions are met. This category enables organizations to turn detected security events into actionable incident records without requiring a person to create each record individually. The broad classification is based on whether a person directly creates the incident or whether the platform creates it through an automated process; individual technical intake methods are implementations within those high-level categories. See ServiceNow's Security Incident Response incident creation documentation and the Security Incident Response product documentation.

QUESTION NO: 7

Which Flow Designer logic should be used when an action must run only when specified conditions are met?

A. For Each

B. If

C. Wait for Duration

D. Flow Trigger

ANSWER: B

Explanation:

If is correct because it evaluates a condition and runs the actions placed in the applicable branch only when the configured criteria are satisfied. In a Security Incident Response flow, an If condition can determine whether an incident requires escalation, enrichment, assignment to a specialized team, or a containment action.

Using conditional logic helps ensure that flows execute only the actions relevant to the incident context. See the Flow Designer documentation.

QUESTION NO: 8

What is the name of the Inbound Action that validates whether an inbound email should be processed as a phishing email for URP v2?

A. User Reporting Phishing (for Forwarded emails)

B. Scan email for threats

C. User Reporting Phishing (for New emails)

D. Create Phishing Email

ANSWER: A

Explanation:

User Reporting Phishing (for Forwarded emails) is the inbound email action used by User Reported Phishing version 2 to validate that an incoming message is a user-submitted phishing report before it enters the phishing-report processing flow. In a forwarding-based reporting workflow, users send a suspicious message to the organization's configured reporting mailbox. ServiceNow receives that message as an inbound email and this action evaluates the incoming report in the context of URP v2, ensuring that it is handled as a reported phishing email. Once the message qualifies, the URP process can preserve the relevant email information and initiate the Security Incident Response workflow used to investigate, triage, and remediate the report. This validation step is important because a reporting mailbox can receive general mail as well as forwarded suspicious messages, and only messages meeting the URP forwarding criteria should be routed into the phishing workflow. ServiceNow's Security Incident Response documentation describes User Reported Phishing as the capability for users to report potentially malicious emails and for security teams to investigate them through a managed response process. See the ServiceNow User Reported Phishing documentation and the ServiceNow inbound email actions documentation.