DUMPSARENA

Certified Implementation Specialist - Security Incident Response Exam

ServiceNow CIS-SIR

Version Demo

Total Demo Questions: 10

Total Premium Questions: 60

Buy Premium PDF

https://dumpsarena.co

sales@dumpsarena.co

sales@dumpsarena.co
dumpsarena.co

QUESTION NO: 1

Which of the following process definitions are not provided baseline?

A. NIST Open

B. SAN Stateful

C. NIST Stateful

D. SANS Open

ANSWER: A

QUESTION NO: 2

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:

Reference: https://docs.servicenow.com/bundle/paris-security-management/page/product/ security-incident-response/concept/si-creation.html

QUESTION NO: 3

What three steps enable you to include a new playbook in the Selected Playbook choice list? (Choose three.)

A. Add the TLP: GREEN tag to the playbooks that you want to include in the Selected Playbook choice list

B. Navigate to the sys_hub_flow.list table

C. Search for the new playbook you have created using Flow Designer

D. Add the sir_playbook tag to the playbooks that you want to include in the Selected Playbook choice list

E. Navigate to the sys_playbook_flow.list table

ANSWER: B C D

Explanation:

Reference: https://docs.servicenow.com/bundle/paris-security-management/page/product/ security-incident-response/concept/sir-new-ui-add-playbook.html

QUESTION NO: 4

Knowledge articles that describe steps an analyst needs to follow to complete Security incident tasks might be associated to those tasks through which of the following?

A. Work Instruction Playbook

B. Flow

C. Workflow

D. Runbook

E. Flow Designer

ANSWER: D

Explanation:

Reference: https://docs.servicenow.com/bundle/paris-security-management/page/product/ security-incident-response/task/perform-addtl-tasks-on-si.html

QUESTION NO: 5

Which Table would be commonly used for Security Incident Response?

A. sysapproval_approver

B. sec_ops_incident

C. cmdb_rel_ci

D. sn_si_incident

ANSWER: D

Explanation:

Reference: https://docs.servicenow.com/bundle/quebec-security-management/page/product/ security-incident-response/reference/installed-with-sir.html

QUESTION NO: 6

A pre-planned response process contains which sequence of events?

A. Organize, Analyze, Prioritize, Contain

B. Organize, Detect, Prioritize, Contain

C. Organize, Prepare, Prioritize, Contain

D. Organize, Verify, Prioritize, Contain

ANSWER: A

QUESTION NO: 7

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: B C D

QUESTION NO: 8

Using the KB articles for Playbooks tasks also gives you which of these advantages?

A. Automated activities to run scans and enrich Security Incidents with real time data

B. Automated activities to resolve security Incidents through patching

C. Improved visibility to threats and vulnerabilities

D. Enhanced ability to create and present concise, descriptive tasks

ANSWER: C

QUESTION NO: 9

Which of the following tag classifications are provided baseline? (Choose three.)

A. Traffic Light Protocol

B. Block from Sharing

C. IoC Type

D. Severity

E. Cyber Kill Chain Step

F. Escalation Level

G. Enrichment whitelist/blacklist

ANSWER: A C G

Explanation:

Reference: https://docs.servicenow.com/bundle/paris-security-management/page/product/ security-operations-common/task/create-class-group-and-tags.html

QUESTION NO: 10

For Customers who don't use 3rd-party systems, what ways can security incidents be created?

(Choose three.)

A. Security Service Catalog

B. Security Incident Form

C. Inbound Email Parsing Rules

D. Leveraging an Integration

E. Alert Management

ANSWER: A B C