Vendor: ServiceNow

Exam Code:CIS-SIR

Exam Name: Certified Implementation Specialist - Security Incident Response

Version: Demo

QUESTION 1

Flow Triggers can be based on what? (Choose three.)

A. Record changes

B. Schedules

C. Subflows

D. Record inserts

E. Record views

Correct Answer: ABC

QUESTION 2

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

Correct Answer: ABC

QUESTION 3

Chief factors when configuring auto-assignment of Security Incidents are.

A. Agent group membership, Agent location and time zone

B. Security incident priority, CI Location and agent time zone

C. Agent skills, System Schedules and agent location

D. Agent location, Agent skills and agent time zone

Correct Answer: D

Reference: https://docs.servicenow.com/bundle/paris-security- management/page/product/security-incident-response/task/t_ConfigureSIM.html

---

QUESTION 4

Which one of the following reasons best describes why roles for Security Incident Response (SIR) begin with "sn_si"?

A. Because SIR is a scoped application, roles and script includes will begin with the sn_si prefix

B. Because the Security Incident Response application uses a Secure Identity token

C. Because ServiceNow checks the instance for a Secure Identity when logging on to this scoped application

D. Because ServiceNow tracks license use against the Security Incident Response Application

Correct Answer: B

QUESTION 5

Joe is on the SIR Team and needs to be able to configure Territories and Skills. What role does he need?

A. Security Basic

B. Manager

C. Security Analyst

D. Security Admin

Correct Answer: D

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

---

QUESTION 6

What is the first step when creating a security Playbook?

A. Set the Response Task\\'s state

B. Create a Flow

C. Create a Runbook

D. Create a Knowledge Article

Correct Answer: B

QUESTION 7

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

Correct Answer: A

QUESTION 8

What parts of the Security Incident Response lifecycle is responsible for limiting the impact of a security incident?

A. Post Incident Activity

B. Detection and Analysis

C. Preparation and Identification

D. Containment, Eradication, and Recovery

Correct Answer: D

Reference: https://searchsecurity.techtarget.com/definition/incident-response

---

QUESTION 9

A flow consists of one or more actions and a what?

A. Change formatter

B. Catalog Designer

C. NIST Ready State

D. Trigger

Correct Answer: D

Reference: https://docs.servicenow.com/bundle/quebec-servicenow- platform/page/administer/flow-designer/concept/flows.html

---

QUESTION 10

Which of the following process definitions allow only single-step progress through the process defined without allowing step skipping?

A. SANS Stateful

B. NIST Stateful

C. SANS Open

D. NIST Open

Correct Answer: B

QUESTION 11

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

Correct Answer: D

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

---

QUESTION 12

Which one of the following users is automatically added to the Request Assessments list?

A. Any user that adds a worknote to the ticket

B. The analyst assigned to the ticket

C. Any user who has Response Tasks on the incident

D. The Affected User on the incident

Correct Answer: C