CIS-SIR Q&As

Certified Implementation Specialist - Security Incident Response

Pass ServiceNow CIS-SIR Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.leads4pass.com/cis-sir.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by ServiceNow Official Exam Center

- **Instant Download** After Purchase
- **100% Money Back** Guarantee
- **365 Days** Free Update
- **800,000+** Satisfied Customers

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

What is the fastest way for security incident administrators to remove unwanted widgets from the Security Incident Catalog?

A. Clicking the X on the top right corner

B. Talking to the system administrator

C. Can\\'t be removed

D. Through the Catalog Definition record

Correct Answer: D

QUESTION 3

Which of the following process definitions are not provided baseline?

A. NIST Open

B. SAN Stateful

C. NIST Stateful

D. SANS Open

Correct Answer: A

QUESTION 4

Which improvement opportunity can be found baseline which can contribute towards process maturity and strengthen costumer\\'s overall security posture?

A. Post-Incident Review

B. Fast Eradication

C. Incident Containment

D. Incident Analysis

Correct Answer: D

QUESTION 5

What plugin must be activated to see the New Security Analyst UI?

A. Security Analyst UI Plugin

B. Security Incident Response UI plugin

C. Security Operations UI plugin

D. Security Agent UI Plugin

Correct Answer: D

QUESTION 6

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 7

What is the purpose of Calculator Groups as opposed to Calculators?

A. To provide metadata about the calculators

B. To allow the agent to select which calculator they want to execute

C. To set the condition for all calculators to run

D. To ensure one at maximum will run per group

Correct Answer: C

Reference: https://docs.servicenow.com/bundle/paris-security- management/page/product/security-incident-response/reference/setup-assistant- reference.html

QUESTION 8

When the Security Phishing Email record is created what types of observables are stored in the record? (Choose three.)

A. URLs, domains, or IP addresses appearing in the body

B. Who reported the phishing attempt

C. State of the phishing email

D. IP addresses from the header

E. Hashes and/or file names found in the EML attachment

F. Type of Ingestion Rule used to identify this email as a phishing attempt

Correct Answer: ADE

Reference: https://docs.servicenow.com/bundle/paris-security- management/page/product/security-incident-response/concept/sighting-searches-on- phishing-attacks.html

QUESTION 9

The severity field of the security incident is influenced by what?

A. The cost of the response to the security breach

B. The impact, urgency and priority of the incident

C. The time taken to resolve the security incident

D. The business value of the affected asset

Correct Answer: D

QUESTION 10

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