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.pass4itsure.com/cis-sir.html

100% Passing Guarantee
100% Money Back Assurance

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

QUESTION 1

The Risk Score is calculated by combining all the weights using.

A. an arithmetic mean

B. addition

C. the Risk Score script include

D. a geometric mean

Correct Answer: A

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

QUESTION 2

When a service desk agent uses the Create Security Incident UI action from a regular incident, what occurs?

A. The incident is marked resolved with an automatic security resolution code

B. A security incident is raised on their behalf but only a notification is displayed

C. A security incident is raised on their behalf and displayed to the service desk agent

D. The service desk agent is redirected to the Security Incident Catalog to complete the record producer

Correct Answer: A

QUESTION 3

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

QUESTION 4

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 5

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 6

If the customer\\'s email server currently has an account setup to report suspicious emails, then what happens next?

A. an integration added to Exchange keeps the ServiceNow platform in sync

B. the ServiceNow platform ensures that parsing and analysis takes place on their mail server

C. the customer\\'s systems are already handling suspicious emails

D. the customer should set up a rule to forward these mails onto the ServiceNow platform

Correct Answer: D

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

QUESTION 7

What is calculated as an arithmetic mean taking into consideration different values in the CI, Security Incident, and User records?

A. Priority

B. Business Impact

C. Severity

D. Risk Score

Correct Answer: B

QUESTION 8

This type of integration workflow helps retrieve a list of active network connections from a host or endpoint, so it can be used to enrich incidents during investigation.

A. Security Incident Response ?Get Running Services

B. Security Incident Response ?Get Network Statistics

C. Security Operations Integration ?Sightings Search

D. Security Operations Integration ?Block Request

Correct Answer: B

Reference: https://docs.servicenow.com/bundle/quebec-security- management/page/product/security-incident-response/concept/cj-sir-capfmw-about.html

QUESTION 9

The benefits of improved Security Incident Response are expressed.

A. as desirable outcomes with clear, measurable Key Performance Indicators

B. differently depending upon 3 stages: Process Improvement, Process Design, and Post Go-Live

C. as a series of states with consistent, clear metrics

D. as a value on a scale of 1-10 based on specific outcomes

Correct Answer: C

QUESTION 10

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

Correct Answer: ACG

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