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.passapply.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

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

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

QUESTION 3

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 4

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 5

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 6

What specific role is required in order to use the REST API Explorer?

A. admin

B. sn_si.admin

C. rest_api_explorer

D. security_admin

Correct Answer: AC

Reference: https://developer.servicenow.com/dev.do#!/learn/learning-plans/orlando/technology_partner_program/app_store_learnv2_rest_orlando_introduction_to_the_rest_a pi_explorer

QUESTION 7

What does a flow require?

A. Security orchestration flows

B. Runbooks

C. CAB orders

D. A trigger

Correct Answer: D

QUESTION 8

Which of the following is an action provided by the Security Incident Response application?

A. Create Outage state V1

B. Create Record on Security Incident state V1

C. Create Response Task set Incident state V1

D. Look Up Record on Security Incident state V1

Correct Answer: D

QUESTION 9

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 10

Security tag used when a piece of information requires support to be effectively acted upon, yet carries risks to privacy, reputation, or operations if shared outside of the organizations involved.

A. TLP:GREEN

B. TLP:AMBER

C. TLP:RED

D. TLP:WHITE

Correct Answer: B

Color	When should it be used?	How may it be shared?
TLP:RED Not for disclosure, restricted to participants only	Sources may use TLP:RED when information cannot be effectively acted upon by additional parties, and could lead to impacts on a party's privacy, reputation, or operations if misused.	Recipients may not share TLP:RED information with any parties outside of the specific exchange, meeting, or conversation in which it was originally disclosed. In the context of a meeting, for example, TLP:RED information is limited to those present at the meeting. In most circumstances, TLP:RED should be exchanged verbally or in person.
TLP:AMBER Limited disclosure, restricted to participants' organizations	Sources may use TLP:AMBER when information requires support to be effectively acted upon, yet carries risks to privacy, reputation, or operations if shared outside of the organizations involved.	Recipients may only share TLP:AMBER information with members of their own organization, and with clients or customers who need to know the information to protect themselves or prevent further harm. Sources are at liberty to specify additional intended limits of the sharing: these must be adhered to
TLP:GREEN Limited disclosure, restricted to the community	Sources may use TLP:GREEN when information is useful for the awareness of all participating organizations as well as with peers within the broader community or sector.	Recipients may share TLP:GREEN information with peers and partner organizations within their sector or community, but not via publicly accessible channels. Information in this category can be circulated widely within a particular community. TLP:GREEN information may not be released outside of the community.
TLP:WHITE Disclosure is not limited	Sources may use TLP:WHITE when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules.	TLP:WHITE information may be distributed without restriction.

Table