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

QUESTION 1

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 2

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

QUESTION 3

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 4

If a desired pre-built integration cannot be found in the platform, what should be your next step to find a certified integration?

A. Build your own through the REST API Explorer

B. Ask for assistance in the community page

C. Download one from ServiceNow Share

D. Look for one in the ServiceNow Store

Correct Answer: D

QUESTION 5

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