Free Questions for CIS-SIR by braindumpscollection

Shared by Dickson on 06-06-2022

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

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.

Options:

A- TLP:GREEN

B- TLP:AMBER

C- TLP:RED

D- TLP:WHITE

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.

Answer:

B

Question 2

Question Type: MultipleChoice

A Post Incident Review can contain which of the following? (Choose three.)

Options:

A- Post incident Question:naires

B- An audit trail

C- Attachments associated with the security incident

D- Key incident fields

E- Performance Analytics reports

Answer:

A, B, D

Question 3

Question Type: MultipleChoice

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

Options:

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

Answer:

B

Question 4

Question Type: MultipleChoice

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

Options:

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

Answer:

D

Question 5

Question Type: MultipleChoice

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

Options:

A- admin

B- sn_si.admin

C- rest_api_explorer

D- security_admin

Answer:

A, C

Question 6

Question Type: **MultipleChoice**

What field is used to distinguish Security events from other IT events?

Options:

A- Type

B- Source

C- Classification

D- Description

Answer:

C

Question 7

Question Type: MultipleChoice

Which of the following fields is used to identify an Event that is to be used for Security purposes?

Options:

A- IT

B- Classification

C- Security

D- CI

Answer:

B

Question 8

Question Type: MultipleChoice

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

Options:

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

Answer:

A

Question 9

Question Type: MultipleChoice

David is on the Network team and has been assigned a security incident response task. What role does he need to be able to view and work the task?

Options:

A- Security Analyst

B- Security Basic

C- External

D- Read

Answer:

A

Question 10

Question Type: MultipleChoice

Which of the following tag classifications are provided baseline? (Choose three.)

Options:

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

Answer:

A, C, G

Question 11

Question Type: **MultipleChoice**

Which of the following process definitions are not provided baseline?

Options:

A- NIST Open

B- SAN Stateful

C- NIST Stateful

D- SANS Open

Answer:

A