

# DUMPSBOSS.

## Certified Implementation Specialist - Security Incident Response Exam

ServiceNow CIS-SIR

Version Demo

Total Demo Questions: 10

Total Premium Questions: 60

Buy Premium PDF

<https://dumpsboss.co>

[support@dumpsboss.co](mailto:support@dumpsboss.co)

support@dumpsboss.co  
dumpsboss.co

## QUESTION NO: 1

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

**ANSWER: A D E**

### Explanation:

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

## QUESTION NO: 2

Which of the following are potential benefits for utilizing Security Incident assignment automation?

(Choose two.)

- A. Decreased Time to Containment
- B. Increased Mean Time to Remediation
- C. Decreased Time to Ingestion
- D. Increased resolution process consistency

**ANSWER: B D**

## QUESTION NO: 3

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

**ANSWER: D**

## QUESTION NO: 4

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

**ANSWER: A B C**

## QUESTION NO: 5

There are several methods in which security incidents can be raised, which broadly fit into one of these categories:

\_\_\_\_\_. (Choose two.)

- A. Integrations
- B. Manually created
- C. Automatically created
- D. Email parsing

**ANSWER: B C**

### Explanation:

Reference: <https://docs.servicenow.com/bundle/paris-security-management/page/product/security-incident-response/concept/si-creation.html>

## QUESTION NO: 6

To configure Security Incident Escalations, you need the following role(s): \_\_\_\_\_.

- A. sn\_si.admin
- B. sn\_si.admin or sn\_si.manager
- C. sn\_si.admin or sn\_si.ciso
- D. sn\_si.manager or sn\_si.analyst

**ANSWER: A**

**Explanation:**

Reference: <https://docs.servicenow.com/bundle/paris-security-management/page/product/security-incident-response/task/escalate-security-incident.html>

## QUESTION NO: 7

What factor, if any, limits the ability to close SIR records?

- A. Opened related INC records
- B. Best practice dictates that SIR records should be set to 'Resolved' never to 'Closed'
- C. Nothing, SIR records could be closed at any time
- D. All post-incident review questioners have to be completed first

**ANSWER: A**

## QUESTION NO: 8

What are two of the audiences identified that will need reports and insight into Security Incident

Response reports? (Choose two.)

- A. Analysts
- B. Vulnerability Managers
- C. Chief Information Security Officer (CISO)
- D. Problem Managers

**ANSWER: A B**

**Explanation:**

Reference: <https://www.servicenow.com/content/dam/servicenow-assets/public/en-us/doc-type/resource-center/data-sheet/ds-security-operations.pdf>

## QUESTION NO: 9

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

- A. Type
- B. Source
- C. Classification
- D. Description

**ANSWER: C**

**Explanation:**

Reference: [https://docs.servicenow.com/bundle/paris-security-management/page/product/security-incident-response/concept/c\\_ScIncdUseAlrts.html](https://docs.servicenow.com/bundle/paris-security-management/page/product/security-incident-response/concept/c_ScIncdUseAlrts.html)

## QUESTION NO: 10

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

**ANSWER: D**