



# CIS-SIR<sup>Q&As</sup>

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

Which of the following process definitions are not provided baseline?

- A. NIST Open
- B. SAN Stateful
- C. NIST Stateful
- D. SANS Open

Correct Answer: A

---

### QUESTION 2

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 3

What role(s) are required to add new items to the Security Incident Catalog?

- A. requires the sn\_si.admin role
- B. requires the sn\_si.catalog role
- C. requires both sn\_si.write and catalog\_admin roles
- D. requires the admin role

Correct Answer: D

Reference: [https://docs.servicenow.com/bundle/orlando-it-service-management/page/product/service-catalog-management/task/t\\_DefineACatalogItem.html](https://docs.servicenow.com/bundle/orlando-it-service-management/page/product/service-catalog-management/task/t_DefineACatalogItem.html)

---

### QUESTION 4



Select the one capability that restricts connections from one CI to other devices.

- A. Isolate Host
- B. Sightings Search
- C. Block Action
- D. Get Running Processes
- E. Get Network Statistics
- F. Publish Watchlist

Correct Answer: A

Reference: <https://docs.servicenow.com/bundle/paris-security-management/page/product/security-incident-response/task/perform-addtl-tasks-on-si.html>

---

#### QUESTION 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

Correct Answer: BC

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

[CIS-SIR PDF Dumps](#)

[CIS-SIR VCE Dumps](#)

[CIS-SIR Study Guide](#)