EndExam

QUESTION & ANSWER

Accurate study guides, High passing rate!

We offer free update service for one year!

http://www.endexam.com

Exam : **CIS-SIR**

Title : Certified Implementation Specialist -Security Incident Response Exam

Version : DEMO

1.What does a flow require?
A. Security orchestration flows
B. Runbooks
C. CAB orders
D. A trigger
Answer: D

2.A flow consists of one or more actions and a what?
A. Change formatter
B. Catalog Designer
C. NIST Ready State
D. Trigger
Answer: D
Explanation:
Reference:
https://docs.servicenow.com/bundle/quebec-servicenow-platform/page/administer/flow-designer/concept/flows.html

3.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
Answer: A
Explanation:
Reference:
https://docs.servicenow.com/bundle/paris-security-management/page/product/security-incident-response/task/perform-addtl-tasks-on-si.html

4.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

5.A pre-planned response process contains which sequence of events?

A. Organize, Analyze, Prioritize, Contain
B. Organize, Detect, Prioritize, Contain
C. Organize, Prepare, Prioritize, Contain
D. Organize, Verify, Prioritize, Contain
Answer: A