Practice Exam Questions

servicenow

Certified Implementation Specialist - Security Incident Response

EXAMKILLER

Help Pass Your Exam At First Try

Total Question: 60 QAs

Question No: 1
What makes a playbook appear for a Security Incident if using Flow Designer?
A. Actions defined to create tasks
B. Trigger set to conditions that match the security incident
C. Runbook property set to true
D. Service Criticality set to High
Answer: B

Question No: 2
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
Answer: C

Question No: 3
The following term is used to describe any observable occurrence: _____.
A. Incident
B. Log
C. Ticket
D. Alert
E. Event
Answer: E

Question No: 4
The severity field of the security incident is influenced by what?
A. The cost of the response to the security breach
B. The impact, urgency and priority of the incident
C. The time taken to resolve the security incident
D. The business value of the affected asset
Answer: D

Question No: 5
The Risk Score is calculated by combining all the weights using _____.
A. an arithmetic mean
B. addition
C. the Risk Score script include
D. a geometric mean
Answer: A

Question No: 6
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

Question No: 7
What three steps enable you to include a new playbook in the Selected Playbook choice list? (Choose three.)
A. Add the TLP: GREEN tag to the playbooks that you want to include in the Selected Playbook choice list
B. Navigate to the sys_hub_flow.list table
C. Search for the new playbook you have created using Flow Designer
D. Add the sir_playbook tag to the playbooks that you want to include in the Selected Playbook choice list
E. Navigate to the sys_playbook_flow.list table
Answer: B,C,D

Question No: 8
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

Question No: 9
What is the fastest way for security incident administrators to remove unwanted widgets from the Security Incident Catalog?
A. Clicking the X on the top right corner
B. Talking to the system administrator
C. Can't be removed
D. Through the Catalog Definition record
Answer: D

Question No: 10
Select the one capability that retrieves a list of running processes on a CI from a host or endpoint.
A. Get Network Statistics
B. Isolate Host
C. Get Running Processes
D. Publish Watchlist
E. Block Action
F. Sightings Search

Answer: C

Question No: 11
Which Table would be commonly used for Security Incident Response?
A. sysapproval_approver
B. sec_ops_incident
C. cmdb_rel_ci
D. sn_si_incident
Answer: D

Question No: 12
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

Question No: 13
What is the first step when creating a security Playbook?
A. Set the Response Task's state
B. Create a Flow
C. Create a Runbook
D. Create a Knowledge Article
Answer: B

Question No: 14
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

Question No: 15
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: 16
What is the key to a successful implementation?
A. Sell customer the most expensive package
B. Implementing everything that we offer
C. Understanding the customer's goals and objectives
D. Building custom integrations
Answer: C

Question No: 17
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

Question No: 18
Flow Triggers can be based on what? (Choose three.)
A. Record changes
B. Schedules
C. Subflows
D. Record inserts
E. Record views
Answer: A,B,C

Question No: 19
Which one of the following users is automatically added to the Request Assessments list?
A. Any user that adds a worknote to the ticket
B. The analyst assigned to the ticket
C. Any user who has Response Tasks on the incident
D. The Affected User on the incident
Answer: C

Question No: 20
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: 21
What does a flow require?