[May-2022 CIS-SIR Dumps are Available for Instant Access from ExamcollectionPass [Q36-Q55

[May-2022] CIS-SIR Dumps are Available for Instant Access from ExamcollectionPass
Study resources for the Valid CIS-SIR Braindumps!

Understanding useful and specialized parts of ServiceNow Certified Implementation Specialist - Security Incident Response Exam

The accompanying will be examined in **SERVICENOW CIS-SIR exam dumps**:

  - Miter ATT&CK Framework- Explore How to Create Security Incidents- Understanding Threat Intelligence **NEW QUESTION 36**

The Risk Score is calculated by combining all the weights using.

* an arithmetic mean
* addition
* the Risk Score script include
* a geometric mean

NEW QUESTION 37

Which ServiceNow automation capability extends Flow Designer to integrate business processes with other systems?
* Workflow
* Orchestration
* Subflows
* Integration Hub

NEW QUESTION 38

Which one of the following users is automatically added to the Request Assessments list?
* Any user that adds a worknote to the ticket
* The analyst assigned to the ticket
* Any user who has Response Tasks on the incident
* The Affected User on the incident

NEW QUESTION 39

In order to see the Actions in Flow Designer for Security Incident, what plugin must be activated?
* Performance Analytics for Security Incident Response
* Security Spoke
* Security Operations Spoke
* Security Incident Spoke

NEW QUESTION 40

What three steps enable you to include a new playbook in the Selected Playbook choice list? (Choose three.)
* Add the TLP: GREEN tag to the playbooks that you want to include in the Selected Playbook choice list
* Navigate to the sys_hub_flow.list table
* Search for the new playbook you have created using Flow Designer
* Add the sir_playbook tag to the playbooks that you want to include in the Selected Playbook choice list
* Navigate to the sys_playbook_flow.list table

NEW QUESTION 41

The benefits of improved Security Incident Response are expressed _____.
* as desirable outcomes with clear, measurable Key Performance Indicators
* differently depending upon 3 stages: Process Improvement, Process Design, and Post Go-Live
* as a series of states with consistent, clear metrics
* as a value on a scale of 1-10 based on specific outcomes

NEW QUESTION 42

Select the one capability that retrieves a list of running processes on a CI from a host or endpoint.
* Get Network Statistics
* Isolate Host
* Get Running Processes
* Publish Watchlist
* Block Action
* Sightings Search
Explanation/Reference: https://docs.servicenow.com/bundle/quebec-security-management/page/product/security-operations-common/concept/get-running-processes-capability.html

NEW QUESTION 43

The Risk Score is calculated by combining all the weights using _____.
* an arithmetic mean
* addition
* the Risk Score script include
* a geometric mean
Explanation/Reference: https://docs.servicenow.com/bundle/paris-security-management/page/product/security-incident-response/reference/setup-assistant-reference.html

NEW QUESTION 44

Chief factors when configuring auto-assignment of Security Incidents are.
* Agent group membership, Agent location and time zone
* Security incident priority, CI Location and agent time zone
* Agent skills, System Schedules and agent location
* Agent location, Agent skills and agent time zone

NEW QUESTION 45

If the customer’s email server currently has an account setup to report suspicious emails, then what happens next?
* an integration added to Exchange keeps the ServiceNow platform in sync
* the ServiceNow platform ensures that parsing and analysis takes place on their mail server
* the customer’s systems are already handling suspicious emails
* the customer should set up a rule to forward these mails onto the ServiceNow platform
Explanation/Reference: https://docs.servicenow.com/bundle/paris-security-management/page/product/security-incident-response/concept/urp-about.html

NEW QUESTION 46

What is calculated as an arithmetic mean taking into consideration different values in the CI, Security Incident, and User records?
* Priority
* Business Impact
* Severity
* Risk Score

NEW QUESTION 47

What is the fastest way for security incident administrators to remove unwanted widgets from the Security Incident Catalog?
* Clicking the X on the top right corner
* Talking to the system administrator
* Can’t be removed
* Through the Catalog Definition record

NEW QUESTION 48

What plugin must be activated to see the New Security Analyst UI?
* Security Analyst UI Plugin
* Security Incident Response UI plugin

* Security Operations UI plugin
* Security Agent UI Plugin

NEW QUESTION 49

What parts of the Security Incident Response lifecycle is responsible for limiting the impact of a security incident?
* Post Incident Activity
* Detection & Analysis
* Preparation and Identification
* Containment, Eradication, and Recovery
Explanation/Reference: https://searchsecurity.techtarget.com/definition/incident-response

NEW QUESTION 50

There are several methods in which security incidents can be raised, which broadly fit into one of these categories:. (Choose two.)
* Integrations
* Manually created
* Automatically created
* Email parsing

NEW QUESTION 51

Joe is on the SIR Team and needs to be able to configure Territories and Skills.

What role does he need?
* Security Basic
* Manager
* Security Analyst
* Security Admin
Explanation/Reference: https://docs.servicenow.com/bundle/quebec-security-management/page/product/security-
incident-response/reference/installed-with-sir.html

NEW QUESTION 52

What is the key to a successful implementation?
* Sell customer the most expensive package
* Implementing everything that we offer
* Understanding the customer’s goals and objectives
* Building custom integrations

NEW QUESTION 53

Which Table would be commonly used for Security Incident Response?
* sysapproval_approver
* sec_ops_incident
* cmdb_rel_ci
* sn_si_incident

NEW QUESTION 54

Flow Triggers can be based on what? (Choose three.)
* Record changes
* Schedules
* Subflows
* Record inserts
* Record views

NEW QUESTION 55

Why is it important that the Platform (System) Administrator and the Security Incident administrator role be separated? (Choose three.)
* Access to security incident data may need to be restricted
* Allow SIR Teams to control assignment of security roles
* Clear separation of duty
* Reduce the number of incidents assigned to the Platform Admin
* Preserve the security image in the company

Understanding useful and specialized parts of ServiceNow Certified Implementation Specialist - Security Incident Response Exam
The accompanying will be examined in **SERVICENOW CIS-SIR exam dumps**:
        - Process Definitions and Selection- Standard Automated Assignment Options- Definition of Escalation Paths- Security Tags
Updated CIS-SIR Tests Engine pdf - All Free Dumps Guaranteed:
https://www.examcollectionpass.com/ServiceNow/CIS-SIR-practice-exam-dumps.html]