VCEplus.com

CIS-SIR.VCEplus.premium.exam.60q

Number: CIS-SIR
Passing Score: 800
Time Limit: 120 min
File Version: 1.0

Website: https://vceplus.com - https://vceplus.co
VCE to PDF Converter: https://vceplus.com/vce-to-pdf/
Facebook: https://www.facebook.com/VCE.For.All.VN/
Twitter : https://twitter.com/VCE_Plus

CIS-SIR

Certified Implementation Specialist – Security Incident Response

Version 1.0

VCEplus.com

CEplus.com

Exam A

QUESTION 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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Reference: https://docs.servicenow.com/bundle/paris-security-management/page/product/security-incident-response/reference/setup-assistant-reference.html

QUESTION 3 The following term is used to describe any observable occurrence: _____.

A. Incident
B. Log
C. Ticket
D. Alert
E. Event

Correct Answer: E
Section: (none)
Explanation

Explanation/Reference:

QUESTION 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

Correct Answer: D

CEplus.com

Section: (none)
Explanation
Explanation/Reference:

QUESTION 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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Reference: https://docs.servicenow.com/bundle/paris-security-management/page/product/security-incident-response/reference/setup-assistant-reference.html

QUESTION 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

Correct Answer: AB
Section: (none)
Explanation

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

QUESTION 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

Correct Answer: BCD
Section: (none)
Explanation

Explanation/Reference:
Reference: https://docs.servicenow.com/bundle/paris-security-management/page/product/security-incident-response/concept/sir-new-ui-add-playbook.html

QUESTION 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

CEplus.com

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Reference: https://docs.servicenow.com/bundle/quebec-security-management/page/product/security-operations-common/concept/get-running-processes-capability.html

QUESTION 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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Reference: https://docs.servicenow.com/bundle/quebec-security-management/page/product/security-incident-response/reference/installed-with-sir.html

QUESTION 12
There are several methods in which security incidents can be raised, which broadly fit into one of these categories: _____. (Choose two.)

A. Integrations

CEplus.com

B. Manually created
C. Automatically created
D. Email parsing

Correct Answer: BC
Section: (none)
Explanation

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

QUESTION 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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 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

Correct Answer: A
Section: (none)
Explanation

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

QUESTION 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

Correct Answer: BD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 17 A flow consists of one or more actions and a what?

A. Change formatter
B. Catalog Designer
C. NIST Ready State
D. Trigger

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Reference: https://docs.servicenow.com/bundle/quebec-servicenow-platform/page/administer/flow-designer/concept/flows.html

QUESTION 18 Flow Triggers can be based on what? (Choose three.)

A. Record changes
B. Schedules
C. Subflows
D. Record inserts
E. Record views

Correct Answer: ABC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

CEplus.com

QUESTION 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

Correct Answer: ABC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 21 What does
a flow require?

A. Security orchestration flows
B. Runbooks
C. CAB orders
D. A trigger

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

CEplus.com

QUESTION 22
Knowledge articles that describe steps an analyst needs to follow to complete Security incident tasks might be associated to those tasks through which of the following?

A. Work Instruction Playbook
B. Flow
C. Workflow
D. Runbook
E. Flow Designer

Correct Answer: D
Section: (none)
Explanation

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

QUESTION 23
Which of the following process definitions allow only single-step progress through the process defined without allowing step skipping?

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

Correct Answer: B
Section: (none)
Explanation

CEplus.com

Explanation/Reference:
QUESTION 24 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
Section: (none)
Explanation

Explanation/Reference:
Reference: https://docs.servicenow.com/bundle/paris-security-management/page/product/security-incident-response/concept/urp-about.html

QUESTION 25 What parts of the Security Incident Response lifecycle is responsible for limiting the impact of a security incident?

A. Post Incident Activity
B. Detection & Analysis
C. Preparation and Identification
D. Containment, Eradication, and Recovery

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Reference: https://searchsecurity.techtarget.com/definition/incident-response

QUESTION 26 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
Section: (none)
Explanation

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

QUESTION 27 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

Correct Answer: A
Section: (none)

CEplus.com

Explanation

Explanation/Reference:

QUESTION 28 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

Correct Answer: ADE
Section: (none)
Explanation

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

QUESTION 29 What plugin must be activated to see the New
Security Analyst UI?

A. Security Analyst UI Plugin
B. Security Incident Response UI plugin
C. Security Operations UI plugin
D. Security Agent UI Plugin

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 30 The benefits of improved Security Incident Response are
expressed _____.

A. as desirable outcomes with clear, measurable Key Performance Indicators
B. differently depending upon 3 stages: Process Improvement, Process Design, and Post Go-Live
C. as a series of states with consistent, clear metrics
D. as a value on a scale of 1-10 based on specific outcomes

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 31
This type of integration workflow helps retrieve a list of active network connections from a host or endpoint, so it can be used to enrich incidents during investigation.

A. Security Incident Response – Get Running Services
B. Security Incident Response – Get Network Statistics
C. Security Operations Integration – Sightings Search

CEplus.com

D. Security Operations Integration – Block Request

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Reference: https://docs.servicenow.com/bundle/quebec-security-management/page/product/security-incident-response/concept/cj-sir-capfmw-about.html

QUESTION 32 Joe is on the SIR Team and needs to be able to configure Territories and Skills.

What role does he need?

A. Security Basic
B. Manager
C. Security Analyst
D. Security Admin

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Reference: https://docs.servicenow.com/bundle/quebec-security-management/page/product/security-incident-response/reference/installed-with-sir.html

QUESTION 33 Why should discussions focus with the end in mind?

A. To understand desired outcomes
B. To understand current posture
C. To understand customer's process
D. To understand required tools

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 34 Which of the following State Flows are provided for Security Incidents? (Choose three.)

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

Correct Answer: ACD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 35
Chief factors when configuring auto-assignment of Security Incidents are _____.
A. Agent group membership, Agent location and time zone

CEplus.com

B. Security incident priority, CI Location and agent time zone
C. Agent skills, System Schedules and agent location
D. Agent location, Agent skills and agent time zone

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Reference: https://docs.servicenow.com/bundle/paris-security-management/page/product/security-incident-response/task/t_ConfigureSIM.html

QUESTION 36 Which ServiceNow automation capability extends Flow Designer to integrate business processes with other systems?

A. Workflow
B. Orchestration
C. Subflows
D. Integration Hub

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Reference: https://docs.servicenow.com/bundle/quebec-servicenow-platform/page/administer/flow-designer/concept/flow-designer.html

QUESTION 37 In order to see the Actions in Flow Designer for Security Incident, what plugin must be activated?

A. Performance Analytics for Security Incident Response
B. Security Spoke
C. Security Operations Spoke
D. Security Incident Spoke

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Reference: https://docs.servicenow.com/bundle/paris-security-management/page/product/security-incident-response-orchestration/concept/sir-flows-and-templates.html

QUESTION 38 How do you select which process definition to use?

A. By selecting the desired process within the Process Definition module
B. By selecting the desired process within the Process Selection module
C. By setting the process definition record to Active
D. By setting the Script Include record to Active

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Reference: https://docs.servicenow.com/bundle/paris-security-management/page/product/security-incident-response/reference/setup-assistant-reference.html

QUESTION 39
What role(s) are required to add new items to the Security Incident Catalog?

CEplus.com

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
Section: (none)
Explanation

Explanation/Reference:
Reference: https://docs.servicenow.com/bundle/orlando-it-service-management/page/product/service-catalog-management/task/t_DefineACatalogItem.html

QUESTION 40 What is calculated as an arithmetic mean taking into consideration different values in the CI, Security Incident, and User records?

A. Priority
B. Business Impact
C. Severity
D. Risk Score

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 41 What is the name of the Inbound Action that validates whether an inbound email should be processed as a phishing email for URP v2?

CEplus.com

A. User Reporting Phishing (for Forwarded emails)
B. Scan email for threats
C. User Reporting Phishing (for New emails)
D. Create Phishing Email

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 42 When a record is created in the Security Incident Phishing Email table what is triggered to create a Security Incident?

A. Ingestion Rule
B. Transform flow
C. Transform workflow
D. Duplication Rule

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Reference: https://docs.servicenow.com/bundle/paris-security-management/page/product/security-incident-response/concept/urp-about.html

QUESTION 43

CEplus.com

If a desired pre-built integration cannot be found in the platform, what should be your next step to find a certified integration?

A. Build your own through the REST API Explorer
B. Ask for assistance in the community page
C. Download one from ServiceNow Share
D. Look for one in the ServiceNow Store

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 44 Incident severity is influenced by the business value of the affected asset.

Which of the following are asset types that can be affected by an incident? (Choose two.)

A. Business Service
B. Configuration Item
C. Calculator Group
D. Severity Calculator

Correct Answer: AB
Section: (none)
Explanation

Explanation/Reference:

CEplus.com

QUESTION 45 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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 46 Why is it important that the Platform (System) Administrator and the Security Incident administrator role be separated? (Choose three.)

A. Access to security incident data may need to be restricted
B. Allow SIR Teams to control assignment of security roles
C. Clear separation of duty
D. Reduce the number of incidents assigned to the Platform Admin
E. Preserve the security image in the company

Correct Answer: BCD
Section: (none)
Explanation

CEplus.com

Explanation/Reference:

QUESTION 47 Using the KB articles for Playbooks tasks also gives you which of these advantages?

A. Automated activities to run scans and enrich Security Incidents with real time data
B. Automated activities to resolve security Incidents through patching
C. Improved visibility to threats and vulnerabilities
D. Enhanced ability to create and present concise, descriptive tasks

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 48 The EmailUserReportedPhishing script include processes inbound emails and creates a record in which table?

A. ar_sn_si_phishing_email
B. sn_si_incident
C. sn_si_phishing_email_header
D. sn_si_phishing_email

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 49 A flow consists of _____. (Choose two.)

A. Scripts
B. Actions
C. Processes
D. Actors
E. Triggers

Correct Answer: BE
Section: (none)
Explanation

Explanation/Reference:
Reference: https://docs.servicenow.com/bundle/paris-servicenow-platform/page/administer/flow-designer/concept/flows.html

QUESTION 50 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

CEplus.com

Section: (none)
Explanation

Explanation/Reference:

QUESTION 51 Which of the following tag classifications are provided baseline?
(Choose three.)

A. Traffic Light Protocol
B. Block from Sharing
C. IoC Type
D. Severity
E. Cyber Kill Chain Step
F. Escalation Level
G.Enrichment whitelist/blacklist

Correct Answer: ACG
Section: (none)
Explanation

Explanation/Reference:
Reference: https://docs.servicenow.com/bundle/paris-security-management/page/product/security-operations-common/task/create-class-group-and-tags.html

QUESTION 52 David is on the Network team and has been assigned a security incident response task.

What role does he need to be able to view and work the task?

A. Security Analyst
B. Security Basic
C. External
D. Read

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 53 When a service desk agent uses the Create Security Incident UI action from a regular incident, what occurs?

A. The incident is marked resolved with an automatic security resolution code
B. A security incident is raised on their behalf but only a notification is displayed
C. A security incident is raised on their behalf and displayed to the service desk agent
D. The service desk agent is redirected to the Security Incident Catalog to complete the record producer

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 54 Which of the following fields is used to identify an Event that is to be used for Security purposes?

CEplus.com

A. IT
B. Classification
C. Security
D. CI

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Reference: https://docs.servicenow.com/bundle/paris-it-operations-management/page/product/event-management/task/t_EMManageEvent.html

QUESTION 55 What field is used to distinguish Security events from other IT events?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Reference: https://docs.servicenow.com/bundle/paris-security-management/page/product/security-incident-response/concept/c_ScIncdUseAlrts.html

QUESTION 56 What specific role is required in order to use the REST API Explorer?

CEplus.com

A. admin
B. sn_si.admin
C. rest_api_explorer
D. security_admin

Correct Answer: AC
Section: (none)
Explanation

Explanation/Reference:
Reference: https://developer.servicenow.com/dev.do#!/learn/learning-plans/orlando/technology_partner_program/app_store_learnv2_rest_orlando_introduction_to_the_rest_api_explorer

QUESTION 57 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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 58

CEplus.com

Which one of the following reasons best describes why roles for Security Incident Response (SIR) begin with "sn_si"?
A. Because SIR is a scoped application, roles and script includes will begin with the sn_si prefix
B. Because the Security Incident Response application uses a Secure Identity token
C. Because ServiceNow checks the instance for a Secure Identity when logging on to this scoped applicationD. Because ServiceNow tracks license use against the Security Incident Response Application

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 59 A Post Incident Review can contain which of the following?
(Choose three.)

A. Post incident questionnaires
B. An audit trail
C. Attachments associated with the security incident
D. Key incident fields
E. Performance Analytics reports

Correct Answer: ABD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 60 Security tag used when a piece of information requires support to be effectively acted upon, yet carries risks to privacy, reputation, or operations if shared outside of the organizations involved.

A. TLP:GREEN
B. TLP:AMBER
C. TLP:RED
D. TLP:WHITE

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

www.vceplus.com - Free Questions & Answers - Online Courses - Convert VCE to PDF - VCEplus.com

CEplus.com

Color	When should it be used?	How may it be shared?
TLP:RED Not for disclosure, restricted to participants only	Sources may use TLP:RED when information cannot be effectively acted upon by additional parties, and could lead to impacts on a party's privacy, reputation, or operations if misused.	Recipients may not share TLP:RED information with any parties outside of the specific exchange, meeting, or conversation in which it was originally disclosed. In the context of a meeting, for example, TLP:RED information is limited to those present at the meeting. In most circumstances, TLP:RED should be exchanged verbally or in person.
TLP:AMBER Limited disclosure, restricted to participants' organizations	Sources may use TLP:AMBER when information requires support to be effectively acted upon, yet carries risks to privacy, reputation, or operations if shared outside of the organizations involved.	Recipients may only share TLP:AMBER information with members of their own organization, and with clients or customers who need to know the information to protect themselves or prevent further harm. Sources are at liberty to specify additional intended limits of the sharing: these must be adhered to
TLP:GREEN Limited disclosure, restricted to the community	Sources may use TLP:GREEN when information is useful for the awareness of all participating organizations as well as with peers within the broader community or sector.	Recipients may share TLP:GREEN information with peers and partner organizations within their sector or community, but not via publicly accessible channels. Information in this category can be circulated widely within a particular community. TLP:GREEN information may not be released outside of the community.
TLP:WHITE Disclosure is not limited	Sources may use TLP:WHITE when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules.	TLP:WHITE information may be distributed without restriction.

CEplus.com

www.vceplus.com - Free Questions & Answers - Online Courses - Convert VCE to PDF - VCEplus.com