EXAMTOPICS

-Expert Verified, Online, **Free**.



CERTIFICATION TEST

-CertificationTest.net - Cheap & Quality Resources With Best Support

Question #1 *Topic 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

Suggested Answer: *B*
Official Answer: B

Community vote distribution
B (100%)

MarlyB Most Recent 1 year, 3 months ago
E-book: Add Playbook action allows users to add Playbooks to the Security Incident even if they do not match the trigger conditions, provided the selected Playbooks are not in running state.
upvoted 1 times

MrBravo 2 years ago
Vancouver p. 219: "For a Playbook to be invoked automatically, [...] trigger condition must be met [...] and then the playbook tab is rendered."
upvoted 1 times

MrBravo 2 years, 1 month ago
B is correct.
upvoted 1 times

Hadex12345 2 years, 2 months ago
Has anyone used this material and passed?yeah, 100%
upvoted 1 times

Hadex12345 2 years, 2 months ago
Has anyone used this material and passed?
upvoted 1 times

Sazeka 1 year, 12 months ago
yeah, 100%
upvoted 2 times

stophs 2 years, 8 months ago
b is correct
upvoted 1 times

Question #2 *Topic 1*

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

Suggested Answer: *C*

Official Answer: C

Community vote distribution

D (100%)

MarlyB Most Recent 1 year, 3 months ago

E-book: Calculator groups are used to group specific calculators together, for which only one (at maximum) will run.

upvoted 1 times

NokoNice 1 year, 8 months ago

Calculator groups are used to group specific calculators together, for which only one will run

upvoted 1 times

ademir_amaral 2 years, 2 months ago

D is correct!

upvoted 1 times

sings193 2 years, 2 months ago

D page 230

upvoted 1 times

kapshawn 2 years, 2 months ago

D is correct

upvoted 1 times

mlemartien 2 years, 6 months ago

Documentation is very clear about that

upvoted 1 times

mlemartien 2 years, 6 months ago

Answer should be D

upvoted 1 times

MrBravo 2 years, 7 months ago

D seems correct.

upvoted 1 times

stophs 3 years, 2 months ago

D is correct

upvoted 2 times

cristina_makeup 3 years, 5 months ago

I believe the correct answer should be D. According to the book: Calculator groups are used to group specific calculators together, for which only one at maximum will run

upvoted 4 times

Question #3 *Topic 1*

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

A. Incident

B. Log

C. Ticket

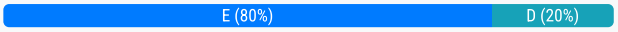
D. Alert

E. Event

Suggested Answer: *E*

Official Answer: E

Community vote distribution



MarlyB Most Recent 1 year, 3 months ago

E-book: Security Events --> Any observable occurrence in a system or network that is related to the security of that system or network.

upvoted 1 times

NokoNice 1 year, 8 months ago

an indication that something notable has occurred.

upvoted 1 times

MrBravo 2 years, 6 months ago

Should be E, my bad

upvoted 2 times

MrBravo 2 years, 6 months ago

"Event is anything that occurs and might cause something to occur"

upvoted 1 times

Question #4 *Topic 1*

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

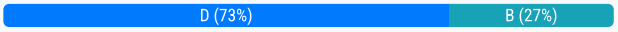
C. The time taken to resolve the security incident

D. The business value of the affected asset

Suggested Answer: *D*

Official Answer: D

Community vote distribution



NokoNice Most Recent 1 year, 8 months ago

D is Correct: Incident Severity is influenced by the business value of the affected asset

upvoted 1 times

mlemartien 2 years, 6 months ago

eBook says D

upvoted 2 times

MrBravo 2 years, 6 months ago

Vancouver p. 71: "Incident severity is influenced by the business value of the affected asset"

upvoted 2 times

Zbtinjo 2 years, 7 months ago

D is correct (eBook Page # 59).

upvoted 2 times

MrBravo 2 years, 7 months ago

D seems correct.

upvoted 1 times

sgawas 3 years ago

Answer is D because Severity is influenced with Business Value of Asset i.e. either Business Service or CI selected in Security Incident

upvoted 4 times

sephereth 3 years, 1 month ago

I am leaning towards B explanation: The severity of a security incident in ServiceNow is influenced by the impact of the incident, the size of your tech team, on-call schedules, high- and low-traffic times of day for your service, the frequency of incidents and other factors.

upvoted 1 times

Remo878 3 years, 2 months ago

The correct answer is B. The impact, urgency, and priority of the incident. These factors play a significant role in determining the severity level of a security incident. The severity field reflects the technical severity or criticality of the incident based on its potential impact, urgency for resolution, and the assigned priority. By considering the impact, urgency, and priority, organizations can assess the severity of an incident and allocate appropriate resources and response efforts accordingly. While the cost of the response to the security breach (option A), the time taken to resolve the security incident (option C), and the business value of the affected asset (option D) may be important considerations in incident response, they are not direct influences on the severity field in ServiceNow's Security Incident module. However, these factors can indirectly impact the assessment of impact, urgency, and priority, which, in turn, can contribute to determining the severity of the incident.

upvoted 2 times

stophs 3 years, 2 months ago

d is correctD is wrong, it should be B

upvoted 3 times

stophs 3 years, 2 months ago

Selected Answer: D

d is correct

upvoted 3 times

sephereth 3 years, 1 month ago

D is wrong, it should be B

upvoted 1 times

Question #5 *Topic 1*

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

Suggested Answer: *A*

Official Answer: A

Community vote distribution

A (100%)

MarlyB Most Recent 1 year, 3 months ago

E-book: The risk score is calculated as an arithmic mean, representing the risk based on CI Business Impact, Security Incident Business Impact, Security Incident Priority, Security Incident Severity and User Business Impact.

upvoted 1 times

MrBravo 2 years ago

Vancouver, p. 259: "The risk score is calculated as an arithmetic mean, representing the risk based on CI Business Impact, Security Incident Business Impact, Security Incident Priority, SI Severity and User Business Impact

upvoted 1 times

stophs 2 years, 8 months ago

a is correct https://docs.servicenow.com/bundle/tokyo-security-management/page/product/security-incident-response/reference/setup-assistant-reference.html#c_SeverityCalculators

upvoted 4 times

Question #6 *Topic 1*

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

Suggested Answer: *A, B*

Official Answer: AB

Community vote distribution

AC (100%)

solflower16 Highly Voted 2 years, 11 months ago

Answer should be: Analysts Chief Information Security Officer (CISO)

upvoted 5 times

MarlyB Most Recent 1 year, 3 months ago

The E-book gives 3 Reporting Audiences: - Analysts - Managers - CIO/CISO Since it is managers in general and not specifically Vulnerability Managers, I'm going for A & C.

upvoted 1 times

mlemartien 2 years ago

A & C are correct

upvoted 1 times

sgawas 2 years, 6 months ago

A & C is correct

upvoted 1 times

sephereth 2 years, 7 months ago

A and C is correct

upvoted 2 times

Question #7 *Topic 1*

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

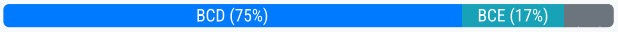
D. Add the sir_playbook tag to the playbooks that you want to include in the Selected Playbook choice list

E. Navigate to the sys_playbook_flow.list table

Suggested Answer: *B, C, D*

Official Answer: BCD

Community vote distribution



PMP_Azure Most Recent 11 months, 3 weeks ago

sys_hub_flow is for the entire Integration Hub whereas sir_playbook_flow is for playbooks which will appera in the list. So, the answer should be: C D E.

upvoted 1 times

MarlyB 1 year, 3 months ago

Not found in the E-book, but on http://servicenow.com/docs/bundle/yokohama-security-management/page/product/security-incident-response/concept/sir-new-ui-add-playbook.html After you have created a playbook using Flow Designer, follow these steps to include it in the Selected Playbook choice list: Navigate to sys_hub_flow 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.

upvoted 2 times

NokoNice 1 year, 8 months ago

1. Navigate to sys_hub_flow table. 2. Search for the new playbook you have created using Flow Designer. 3. Add the sir_playbook tag to the playbooks that you want to include in the Selected Playbook choice list.

upvoted 2 times

MrBravo 2 years, 6 months ago

After you have created a playbook using Flow Designer, follow these steps to include it in the Selected Playbook choice list: Navigate to sys_hub_flow 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. https://docs.servicenow.com/bundle/vancouver-security-management/page/product/security-incident-response/concept/sir-new-ui-add-playbook.html

upvoted 3 times

stophs 3 years, 2 months ago

bcd are correct

upvoted 4 times

Question #8 *Topic 1*

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

Suggested Answer: *D*
Official Answer: D

Community vote distribution
A (100%)

MarlyB Most Recent 1 year, 3 months ago
E-book: As mentioned before, ServiceNow added two further stages to the NIST/SANS Security Incident Response process: - Review - post-incident analysis - Prepare - priorities for action, drivers for change arising from the review etc. Both of these are learning and improvement opportunities that contribute towards process maturity and strengthen the overall security posture of the customer.
upvoted 1 times

mlemartien 2 years ago
Definitely A
upvoted 1 times

Sazeka 2 years, 4 months ago
Correct
upvoted 1 times

sephereth 2 years, 7 months ago
ebook p.238, both Review and Prepare are learning and improvement Opportunities that contribute towards process manturity and strengthen the overall security posture of the customer - Review: post-incident analysis, lessons indentified (and hopefully lessons learnt) - Prepare: priorities for action, drivers for change arisisng from the review, including implementing preventative measures to prevent a recurrence. both points indicate towards post-incident review (which includes analysis), so keyword should be "post-incident"
upvoted 3 times

Remo878 2 years, 8 months ago
Post incident analysis
upvoted 3 times

Question #9 *Topic 1*

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

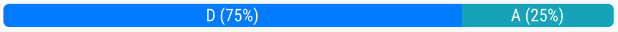
C. Can't be removed

D. Through the Catalog Definition record

Suggested Answer: *D*

Official Answer: D

Community vote distribution



sephereth Highly Voted 2 years, 1 month ago

Explanation: i've found this... To remove unwanted widgets from the Security Incident Catalog in ServiceNow, security incident administrators can follow these steps: Go to Security Incident > Catalog & Knowledge > Maintain Catalog Items. Select the widgets that you want to remove. Click the Deactivate button. The widgets will be deactivated and will no longer be displayed in the Security Incident Catalog. The other options are incorrect: A. Clicking the X on the top right corner will only delete the widget from the current view. It will not remove the widget from the catalog. B. Talking to the system administrator is not necessary. Security incident administrators can remove unwanted widgets themselves.

upvoted 5 times

MarlyB Most Recent 1 year, 3 months ago

Found this: https://support.servicenow.com/kb?id=kb_article_view&sysparm_article=KB0793438 The records are Catalog Items for the Security Incident Catalog. These were likely installed with Demo Data when you installed the "Security Incident Response" Plugin. These are there to provide sample security incident products and services within the customer-facing Security Incident Catalog view: https://docs.servicenow.com/csh?topicname=sir-landing-page.html&version=latest You can Deactivate these by following the steps below. NEXT STEPS: 1. Navigate to Security Incident > Catalog & Knowledge > Maintain Catalog Items 2. Select the ones you would like to Deactivate in the List View 3. Scroll down to the bottom of the List View and click the red "Deactivate" button

upvoted 1 times

6b9c31f 1 year, 3 months ago

By impersonating a Security Incident Admin I was able to remove it just by clicking on the X on the top of the widget. And the answer talks about widgets and not items. So I think it doesn't make sense to deactivate the catalog items

upvoted 1 times

6b9c31f 1 year, 3 months ago

By impersonating a Security Incident Admin I was able to remove it just by clicking on the X on the top of the widget

upvoted 1 times

Question #10 *Topic 1*

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

Suggested Answer: *C*

Official Answer: C

Community vote distribution

C (100%)

MarlyB Most Recent 1 year, 3 months ago

https://www.servicenow.com/docs/bundle/yokohama-security-management/page/product/security-operations-integrations/concept/secops-integration-get-running-processes-workflow.html The Security Operations - Get Running Processes flow is a high-level flow independent of integrations. It retrieves a list of running processes on a configuration item (CI) from a host. Use it to fulfill an integration, such as Carbon Black, or for a Windows-based security incident.

upvoted 1 times

NokoNice 1 year, 8 months ago

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

upvoted 1 times

sephereth 2 years, 1 month ago

The Get Running Processes capability retrieves a list of running processes on a CI from a host or endpoint in ServiceNow. This capability is useful for security incident response teams to identify malicious processes running on a host or endpoint and to take appropriate action.

upvoted 1 times

Question #11 *Topic 1*

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

Suggested Answer: *D*

Official Answer: D

Community vote distribution

D (100%)

MarlyB Most Recent 1 year, 3 months ago

E-book: Security Incident [sn_si_incident]

upvoted 1 times

NokoNice 1 year, 8 months ago

D is correct

upvoted 1 times

sephereth 2 years, 1 month ago

ebook p.32, Security Incident [sn_si_incident] extends from Service Order [sn_order] extends from Task [task], commonly used tables for reporting are, Security Incident [sn_si_incident], Security incident Audit Log [sn_si_audit_log] and Task [task]

upvoted 2 times

Question #12 *Topic 1*

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

Suggested Answer: *B, C*
Official Answer: BC

Community vote distribution
BC (100%)

MarlyB Most Recent 1 year, 3 months ago
Because A & D also fall under the 'Automatically' category.
upvoted 1 times

NokoNice 1 year, 8 months ago
Security incidents can be created manually using the form or automatically from security events received from integrated third-party alert monitoring tools such as Splunk.
upvoted 2 times

MrBravo 2 years, 6 months ago
Vancouver, p. 64.
upvoted 1 times

Question #13 *Topic 1*

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

Suggested Answer: *B*

Official Answer: B

Community vote distribution

B (100%)

sephereth Most Recent 2 years, 1 month ago

The steps involved in creating a security playbook in ServiceNow: 1. Create a Flow. 2. Create a Runbook. 3. Create a Response Task. 4. Create an Incident Response Task. 5. Create an Incident Response Plan.

upvoted 2 times

Question #14 *Topic 1*

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

Suggested Answer: *A*
Official Answer: A

Community vote distribution
A (100%)

NokoNice Most Recent 1 year, 8 months ago
https://www.servicenow.com/docs/bundle/xanadu-security-management/page/product/security-incident-response/task/escalate-security-incident.html
upvoted 1 times

MrBravo 2 years, 6 months ago
Vancouver p. 233
upvoted 1 times

sephereth 3 years, 1 month ago
The role sn_si.admin is required to configure Security Incident Escalations in ServiceNow because it provides the necessary permissions to create and manage security incident response groups and escalation policies.
upvoted 3 times

Question #15 *Topic 1*

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

Suggested Answer: *B, D*

Official Answer: BD

Community vote distribution

AD (100%)

Remo878 Highly Voted 2 years, 8 months ago

The potential benefits for utilizing Security Incident assignment automation are: A. Decreased Time to Containment D. Increased resolution process consistency

upvoted 6 times

sephereth Highly Voted 2 years, 7 months ago

ebook p197, explains the benefits of alternative approaches (auto-assignment) - shortening containment time (a) - improving resolution process consistency (d)This is correct.

upvoted 6 times

sephereth 2 years, 7 months ago

Selected Answer: AD

ebook p197, explains the benefits of alternative approaches (auto-assignment) - shortening containment time (a) - improving resolution process consistency (d)

upvoted 6 times

Sazeka 2 years, 4 months ago

This is correct.

upvoted 1 times

momoboukhriss Most Recent 1 year, 10 months ago

A and D correct

upvoted 1 times

sgawas 2 years, 6 months ago

A and D is right answer

upvoted 2 times

Question #16 *Topic 1*

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

Suggested Answer: *C*

Official Answer: C

Community vote distribution

C (100%)

MrBravo Most Recent 2 years ago

Lol, muist be C

upvoted 2 times

Question #17 *Topic 1*

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

A. Change formatter

B. Catalog Designer

C. NIST Ready State

D. Trigger

Suggested Answer: *D*

Official Answer: D

Community vote distribution

D (100%)

sephereth Most Recent 2 years, 1 month ago

the components of a flow are: Triggers - The event that starts the flow. Actions - The steps that the flow takes. Conditions - The criteria that must be met for the flow to continue. Branches - The paths that the flow can take based on conditions.

upvoted 1 times

Question #18 *Topic 1*

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

A. Record changes

B. Schedules

C. Subflows

D. Record inserts

E. Record views

Suggested Answer: *A, B, C*

Official Answer: ABC

Community vote distribution

ABD (100%)

stophs Highly Voted 2 years, 2 months ago

ABD ARE CORRECT Record Changes (A): A record change in a database can act as a trigger for a flow. For example, if the status of a security incident record changes from "New" to "In Progress", this could trigger a flow that notifies the assigned security analyst and provides them with relevant information about the incident. Schedules (B): A flow can also be triggered based on a predefined schedule. For instance, a flow could be configured to run a network scan for potential security vulnerabilities every night at midnight. In this case, the arrival of the scheduled time (midnight) would trigger the flow. Record Inserts (D): A record insert, or the creation of a new record in a database, can trigger a flow. For example, if a new user account is created in a system, this could trigger a flow that automatically sends a welcome email to the new user and assigns them to the appropriate user groups based on their role.

upvoted 7 times

sephereth Most Recent 2 years, 1 month ago

correct answer is A B and D

upvoted 1 times

Question #19 *Topic 1*

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

Suggested Answer: *C*

Official Answer: C

Community vote distribution

B (100%)

5650bdf Most Recent 1 year, 5 months ago

Answer is B

upvoted 1 times

NokoNice 1 year, 7 months ago

B is correct

upvoted 2 times

sgawas 2 years ago

Answer is B, all assigned users/analyst and person who added manually to list

upvoted 3 times

Remo878 2 years, 2 months ago

B. The analyst assigned to the ticket

upvoted 3 times

Question #20 *Topic 1*

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

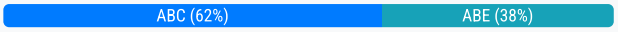
D. Leveraging an Integration

E. Alert Management

Suggested Answer: *A, B, C*

Official Answer: ABC

Community vote distribution



abrakadabrek Most Recent 1 year, 8 months ago

Alert Management typically integrates with monitoring or security system, so involves integration

upvoted 2 times

NokoNice 1 year, 8 months ago

https://www.servicenow.com/docs/de-DE/bundle/xanadu-security-management/page/product/security-incident-response/concept/si-creation.html

upvoted 3 times

sephereth 2 years, 1 month ago

abc is correct

upvoted 1 times

stophs 2 years, 2 months ago

ABC ARE CORRECT

upvoted 2 times

Question #21 *Topic 1*

What does a flow require?

A. Security orchestration flows

B. Runbooks

C. CAB orders

D. A trigger

Suggested Answer: *D*

Official Answer: D

Community vote distribution

D (100%)

sephereth Most Recent 2 years, 1 month ago

Components of a flow are: 1. Triggers - The event that starts the flow. 2. Actions - The steps that the flow takes. 3. Conditions - The criteria that must be met for the flow to continue. 4. Branches - The paths that the flow can take based on conditions.

upvoted 1 times

Question #22 *Topic 1*

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

Suggested Answer: *D*

Official Answer: D

Community vote distribution

D (100%)

Sazeka Most Recent 1 year, 10 months ago

The answer D is correct. Reported in the ebook page 294:

upvoted 1 times

sgawas 2 years ago

D is right answer as Run book allows to specify steps for working on task

upvoted 1 times

sephereth 2 years, 1 month ago

A ServiceNow runbook is an electronic or physical document that lists detailed procedures for handling every expected situation that an IT system may experience. Based on changes in system condition, incoming requests and other factors, system administrators determine which procedures to run and when to run them.

upvoted 1 times

Question #23 *Topic 1*

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

Suggested Answer: *B*

Official Answer: B

Community vote distribution



c396608 Most Recent 1 year, 5 months ago

Both NIST and SANS Stateful require sequential steps, but NIST Stateful treats Containment, Eradication, and recovery as a collective, thereby satisfying the question of a Single-step sequential process

upvoted 1 times

Sazeka 1 year, 10 months ago

B is correct. According to the Ebook page 218: The NIST Stateful process definition allows analysts to move from one step to the next in sequential order without skipping any step. On the other hand, the NIST Open process definition permits analyst to move freely from one state to the next.

upvoted 2 times

sephereth 2 years, 1 month ago

oob configuration has - NIST Stateful - NIST Open - SANS Open - Example *note, Stateful means step by step (can't skip to any statues), while Open allows skipping steps so in this case B is the right answer

upvoted 3 times

Question #24 *Topic 1*

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

Suggested Answer: *D*
Official Answer: D

Community vote distribution
D (100%)

Sazeka Most Recent 1 year, 10 months ago
The correct answer is D. According to the Ebook Security Incident Response (Tokyo) page 63: "If the customer currently has an email account on their email server where these emails are sent to, they MUST forward the email to the platform address specified here (ServiceNow) so that the parsing and transform maps can take place."
upvoted 1 times

sephereth 2 years, 1 month ago
ServiceNow can monitor a designated email account, and when an email arrives, it can be parsed and processed according to predefined rules. So, emails need to be forwarded to the ServiceNow platform for parsing.
upvoted 2 times

Question #25 *Topic 1*

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

Suggested Answer: *D*

Official Answer: D

Community vote distribution

D (100%)

NokoNice Most Recent 1 year, 8 months ago

Containment, Eradication, and Recovery

upvoted 1 times

Sazeka 1 year, 10 months ago

D correct, according to the Ebook of Security Incident Response (Tokyo) page 218

upvoted 1 times

sephereth 2 years, 1 month ago

ebook p.218, Containment is the process of isolating the affected systems to prevent further damage. Eradication is the process of removing the cause of the incident from the affected systems. Recovery is the process of restoring the affected systems to their normal state. ebook p.221, ...drastrically reducing time to containment and providing enhanced vsibility of sercurity incidents...

upvoted 3 times

Question #26 *Topic 1*

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

Suggested Answer: *A*

Official Answer: A

Community vote distribution

A (100%)

NokoNice Most Recent 1 year, 7 months ago

Isolate Host

upvoted 1 times

sephereth 2 years, 1 month ago

Explanation: ebook p.147, Isolate Host: Provides a way to Isolate an endpoint or a host assoicated with a security incident, Isolate host is executed against a configuration item (CI). Example: Carbon Black.

upvoted 3 times

Question #27 *Topic 1*

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'

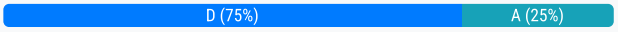
C. Nothing, SIR records could be closed at any time

D. All post-incident review questioners have to be completed first

Suggested Answer: *A*

Official Answer: A

Community vote distribution



NokoNice Most Recent 1 year, 8 months ago

All post-incident review questioners have to be completed first

upvoted 1 times

mrohv 1 year, 8 months ago

from my experience working in servicenow SIRs. i need to complete the post incident questionaire. i see some have answered A and D quoting Ebooks? where can i get those?

upvoted 1 times

MrBravo 2 years, 6 months ago

Vancouver p. 272

upvoted 1 times

MrBravo 2 years, 6 months ago

Security Incident cannot be closed until all questionnaries have been completed.

upvoted 1 times

Sazeka 2 years, 10 months ago

A is the right answer. According to the Ebook of Security Incident Response (Tokyo) page 240

upvoted 1 times

sgawas 3 years ago

Cannot close SIR until all the questionnaire answers by participants

upvoted 2 times

sephereth 3 years, 1 month ago

Selected Answer: A

Explanation: if there are opened related incident records, then the current SIR record cannot be closed

upvoted 1 times

sephereth 3 years, 1 month ago

Explanation: if there are opened related incident records, then the current SIR record cannot be closedSorry, thats correct, it's D. Explanation: ebook p.240, Security Incident cannot be closed until all questionnaries have been completed.

upvoted 1 times

sephereth 3 years, 1 month ago

Sorry, thats correct, it's D. Explanation: ebook p.240, Security Incident cannot be closed until all questionnaries have been completed.

upvoted 4 times

Question #28 *Topic 1*

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

Suggested Answer: *A, D, E*

Official Answer: ADE

Community vote distribution

ADE (100%)

MrBravo Most Recent 2 years ago

Vancouver p. 334 IP addresses from the header URLs, domains, or IP addresses appearing in the body Hashes found in the EML attachment File names foind in the EML attachment

upvoted 1 times

Sazeka 2 years, 4 months ago

According to the ebook of Security Incident Response (Tokyo) p.98, Observables stateful properties: E-Observed MD5 hashes (e) A- Observed IP address (a) D- Observed email addresses (d)

upvoted 2 times

sephereth 2 years, 7 months ago

Explanation: ebook p.98, Observables stateful properties: - Observed MD5 hashes (e) - Observed IP address (a) - Observed DNS names (a) - Observed email addresses (d)

upvoted 2 times

Question #29 *Topic 1*

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

Suggested Answer: *D*

Official Answer: D

Community vote distribution

B (100%)

NokoNice Most Recent 1 year, 8 months ago

Security Incident Response UI plugin

upvoted 1 times

Sazeka 1 year, 10 months ago

According to the ebook of Security Incident Response (Tokyo) page 295 : "to activate the new security Analyst UI, the request the security Incident Response UI Plugin (com.app_secops_ui) through Now support (HI) portal"

upvoted 1 times

podep95607 1 year, 10 months ago

B is correct

upvoted 1 times

sephereth 2 years, 1 month ago

Security Incident Response UI is the correct answer, A, C and D doesn't exist in the OOB instance store

upvoted 2 times

stophs 2 years, 2 months ago

BISCORRECT https://docs.servicenow.com/en-US/bundle/store-release-notes/page/release-notes/store/security-operations/store-secops-rn-sir-ui-1.html

upvoted 3 times

Question #30 *Topic 1*

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

Suggested Answer: *C*

Official Answer: C

Community vote distribution

A (100%)

Remo878 Most Recent 2 years, 2 months ago

A is right

upvoted 3 times

Question #31 *Topic 1*

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

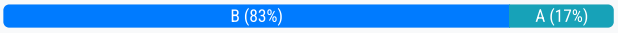
C. Security Operations Integration – Sightings Search

D. Security Operations Integration – Block Request

Suggested Answer: *B*

Official Answer: B

Community vote distribution



NokoNice Most Recent 1 year, 8 months ago

The Get Network Statistics capability retrieves a list of active network connections from a host or endpoint. It can be used for incident enrichment during investigations. This capability is triggered automatically when a configuration item is added to a security incident....https://www.servicenow.com/docs/bundle/xanadu-security-management/page/product/security-operations-common/concept/get-network-statistics-capability.html

upvoted 1 times

DukeCheckem 2 years, 2 months ago

See sephereths comment

upvoted 1 times

Sazeka 2 years, 4 months ago

A is correctMistyped, B is the correct answer

upvoted 1 times

Sazeka 2 years, 4 months ago

Selected Answer: A

A is correct

upvoted 1 times

Sazeka 2 years, 4 months ago

Mistyped, B is the correct answer

upvoted 1 times

sephereth 2 years, 7 months ago

Explanation: ebook p.147, Get Network Statistics: REtrieves a list of active netowkr connections from an endpoint or host, This capability is used for incident nerichment during investigations.Thanks correctAgreeeed

upvoted 3 times

sephereth 2 years, 7 months ago

Selected Answer: B

Explanation: ebook p.147, Get Network Statistics: REtrieves a list of active netowkr connections from an endpoint or host, This capability is used for incident nerichment during investigations.

upvoted 3 times

Sazeka 2 years, 4 months ago

Thanks correct

upvoted 1 times

MrBravo 2 years ago

Agreeeed

upvoted 1 times

Question #32 *Topic 1*

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

Suggested Answer: *D*
Official Answer: D

Community vote distribution
D (100%)

Sazeka Most Recent 1 year, 10 months ago
The correct answer is D According to the ebook of Security Incident Response (Tokyo) page 42
upvoted 1 times

sephereth 2 years, 1 month ago
ServiceNow Administrators implement the security requirements that relate to the business organization. Failed logins, password encryption, access control rules, and audit logs are also their responsibilities.
upvoted 1 times

Question #33 *Topic 1*

Why should discussions focus with the end in mind?

A. To understand desired outcomes

B. To understand current posture

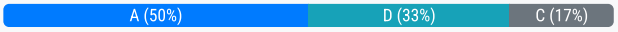
C. To understand customer's process

D. To understand required tools

Suggested Answer: *A*

Official Answer: A

Community vote distribution



Sazeka Most Recent 1 year, 10 months ago

A. To understand desired outcomes The book emphasizes the importance of starting with the end in mind to understand the desirable outcome. This helps in framing the discussion and leads to questions about the tools and processes that will be needed to achieve those outcomes. So, option A is the most appropriate answer in this context.

upvoted 3 times

Sazeka 1 year, 10 months ago

Sorry for the previous response, the answer is in the last sentence: According to the Ebook of Security Incident Response (Tokyo) page 35: Most discussions will tend to focus on process ("How do we do this?") but it helps to begin with the end in mind: "why is this needed? " to try and define the desirable outcome. FROM THERE, EXPECT TO DERIVE QUESTIONS ABOUT WHAT THE TOOLSETS (PRODUCT) WILL LOOK LIKE: WHAT DO PEOPLE SEE? HOW WILL IT BE PRESENTED? WHAT CAN MAKE PEOPLE PRODUCTIVE? Therefore the correct answer cannot be C but D.A. To understand desired outcomes The book emphasizes the importance of starting with the end in mind to understand the desirable outcome. This helps in framing the discussion and leads to questions about the tools and processes that will be needed to achieve those outcomes. So, option A is the most appropriate answer in this context.A. To understand desired outcomes The book emphasizes the importance of starting with the end in mind to understand the desirable outcome. This helps in framing the discussion and leads to questions about the tools and processes that will be needed to achieve those outcomes. So, option A is the most appropriate answer in this context.

upvoted 1 times

Sazeka 1 year, 10 months ago

A. To understand desired outcomes The book emphasizes the importance of starting with the end in mind to understand the desirable outcome. This helps in framing the discussion and leads to questions about the tools and processes that will be needed to achieve those outcomes. So, option A is the most appropriate answer in this context.A. To understand desired outcomes The book emphasizes the importance of starting with the end in mind to understand the desirable outcome. This helps in framing the discussion and leads to questions about the tools and processes that will be needed to achieve those outcomes. So, option A is the most appropriate answer in this context.

upvoted 1 times

Sazeka 1 year, 10 months ago

Sorry for the previous response, the answer is in the last sentence: According to the Ebook of Security Incident Response (Tokyo) page 35: Most discussions will tend to focus on process ("How do we do this?") but it helps to begin with the end in mind: "why is this needed? " to try and define the desirable outcome. FROM THERE, EXPECT TO DERIVE QUESTIONS ABOUT WHAT THE TOOLSETS (PRODUCT) WILL LOOK LIKE: WHAT DO PEOPLE SEE? HOW WILL IT BE PRESENTED? WHAT CAN MAKE PEOPLE PRODUCTIVE? Therefore the correct answer cannot be C but D.

upvoted 1 times

Sazeka 1 year, 10 months ago

The correct answer is C. According to the Ebook of Security Incident Response (Tokyo) page 35: Most discussions will tend to focus on process ("How do we do this?") but it helps to begin with the end in mind: "why is this needed? " to try and define the desirable outcomes.

upvoted 1 times

Question #34 *Topic 1*

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

Suggested Answer: *A, C, D*
Official Answer: ACD

Community vote distribution
ABC (89%) AB (11%)

stophs Highly Voted 2 years, 2 months ago
ABC ARE CORRECT D DONT EXISIT IN SNOW
upvoted 5 times

Haicare Most Recent 1 year, 4 months ago
ABC are correct
upvoted 1 times

NokoNice 1 year, 8 months ago
NIST Stateful, NIST Open and SANS Open
upvoted 1 times

sgawas 2 years ago
A, B, C
upvoted 1 times

sephereth 2 years, 1 month ago
Selected Answer: AB
Explanation: oob configuration has - NIST Stateful - NIST Open - SANS Open - Example
upvoted 1 times

sephereth 2 years, 1 month ago
Explanation: oob configuration has - NIST Stateful - NIST Open - SANS Open - Examplesorry i meant AB and C.....
upvoted 1 times

sephereth 2 years, 1 month ago
sorry i meant AB and C.....
upvoted 1 times

cristina_makeup 2 years, 5 months ago
According to the book the correct answer is NIST Stateful, NIST Open and SANS Open
upvoted 3 times

Question #35 *Topic 1*

Chief factors when configuring auto-assignment of Security Incidents are _____.

A. Agent group membership, Agent location and time zone

B. Security incident priority, CI Location and agent time zone

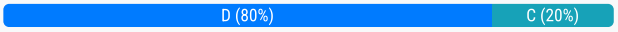
C. Agent skills, System Schedules and agent location

D. Agent location, Agent skills and agent time zone

Suggested Answer: *D*

Official Answer: D

Community vote distribution



NokoNice Most Recent 1 year, 7 months ago

Ignore my first answer; i meant to say D is correct Agent location, Agent skills, and agent time zone

upvoted 1 times

NokoNice 1 year, 8 months ago

Agent location, Agent skills and agent time zone M

upvoted 1 times

MrBravo 2 years ago

vancouver ebook p. 231

upvoted 1 times

Sazeka 2 years, 4 months ago

ebook page 198: Factirs to consider when auto-assigning security incidents to agents: 1 Timezone 2 Location 3 Skilld/capabilities Therefore D is correct

upvoted 2 times

Question #36 *Topic 1*

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

A. Workflow

B. Orchestration

C. Subflows

D. Integration Hub

Suggested Answer: *D*

Official Answer: D

Community vote distribution

D (100%)

NokoNice Most Recent 1 year, 7 months ago

D is correct

upvoted 1 times

Sazeka 1 year, 10 months ago

According to the Ebook of Security Incident Response (Tokyo) page 258 IntegrationHub Extends Flow Designer to integrate business processes with other systems. Allow developers to encapsulate code so process analyst may reuse integration steps without needing to know how to code.

upvoted 2 times

Question #37 *Topic 1*

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

Suggested Answer: *C*
Official Answer: C

Community vote distribution
C (100%)

NokoNice Most Recent 1 year, 8 months ago
https://www.servicenow.com/docs/bundle/xanadu-build-workflows/page/administer/integrationhub/reference/secops-spoke.html
upvoted 1 times

Sazeka 1 year, 10 months ago
ebook page 265: the security operations spoke provides security operations actions for flow designers to manage security incident response flow templates:
upvoted 2 times

sephereth 2 years, 1 month ago
Explanation: checked in OOB instance, under plugin -> Security Operations Spoke, description: Security orchestration flows & actions
upvoted 1 times

stophs 2 years, 2 months ago
C IS CORECT https://docs.servicenow.com/bundle/rome-servicenow-platform/page/administer/integrationhub/reference/secops-spoke.htmlchecked in OOB instance, under plugin -> Security Operations Spoke, description: Security orchestration flows & actions
upvoted 2 times

stophs 2 years, 2 months ago
Selected Answer: C
C IS CORECT https://docs.servicenow.com/bundle/rome-servicenow-platform/page/administer/integrationhub/reference/secops-spoke.html
upvoted 2 times

sephereth 2 years, 1 month ago
checked in OOB instance, under plugin -> Security Operations Spoke, description: Security orchestration flows & actions
upvoted 1 times

Question #38 *Topic 1*

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

Suggested Answer: *B*

Official Answer: B

Community vote distribution

B (100%)

c396608 Most Recent 1 year, 5 months ago

Process Definition provides the ability to create many, Process Selection dictates which one is in use

upvoted 1 times

Sazeka 1 year, 10 months ago

Ebook page 218: these definitions can be found by navigating to security incident-> Administration -> Process Definitions. The one in use will be found at Security Incident -> Administration -> Process Selection.

upvoted 1 times

sephereth 2 years, 1 month ago

Explanation: Process Definition [sn_si_process_definition] table is where the definition is kepted, Process Selection is where process definition record is selected to be used. both under Security Incident -> Administration

upvoted 1 times

Question #39 *Topic 1*

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

Suggested Answer: *D*

Official Answer: D

Community vote distribution

A (100%)

Krzyk Most Recent 2 years, 1 month ago

A is correct

upvoted 1 times

Sazeka 2 years, 10 months ago

A is correct

upvoted 1 times

sephereth 3 years, 1 month ago

Explanation: ebook p.58, Adding new items to the Security Incidetn Catalog requires the sn_si.admin role.

upvoted 2 times

Remo878 3 years, 2 months ago

Sn_si.admin role

upvoted 2 times

Question #40 *Topic 1*

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

Suggested Answer: *B*

Official Answer: B

Community vote distribution

D (100%)

Sazeka Most Recent 1 year, 10 months ago

According to the eBook of Security Incident Response (Tokyo) page 227 The Risk Score is calculated as an arithmetic mean, representing the risk based on CI business impact, Security Incident Business Impact, Security Incident Priority, Sec Incident Severity and User Business Impact

upvoted 1 times

stophs 2 years, 2 months ago

D IS CORRECT https://docs.servicenow.com/bundle/tokyo-security-management/page/product/security-incident-response/reference/setup-assistant-reference.html#title_create-process-definition-sir

upvoted 3 times

Question #41 *Topic 1*

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

A. User Reporting Phishing (for Forwarded emails)

B. Scan email for threats

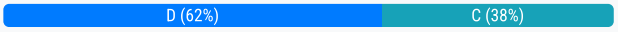
C. User Reporting Phishing (for New emails)

D. Create Phishing Email

Suggested Answer: *A*

Official Answer: A

Community vote distribution



Alice_the_2nd Most Recent 1 year, 9 months ago

The User Reported Phishing inbound actions available prior to the Security Incident Response 9.0 release are now disabled. Security incidents are no longer created through the disabled inbound actions. A new Create Phishing Email inbound action is now available. https://docs.servicenow.com/en-US/bundle/vancouver-security-management/page/product/security-incident-response/concept/urp-about.html

upvoted 1 times

Sazeka 1 year, 10 months ago

D is correct. The existing User Reported Phishing email inbound actions (Type = Forward and Type = New) have been disabled. A new Create Phishing Email inbound action is now available. ref: https://docs.servicenow.com/bundle/sandiego-security-management/page/product/security-incident-response/concept/urp-about.html

upvoted 1 times

sgawas 2 years ago

User Reported Phishing determines whether inbound email should be processed as Phishing email.

upvoted 1 times

sephereth 2 years, 1 month ago

in the course provided SN instance, only the "Create Phishing Email" inbound action is active, both the "User Reported Phishing" (there are 2) have active set to false, additionally, it's calling a script include called "EmailUserReportedPhishing" under the description of that script include record, it states "Email User Reported Phishing V2 details methods to determine if this is a phishing." So correct answer should be D

upvoted 3 times

Dharshu98 2 years, 1 month ago

D is correct

upvoted 2 times

stophs 2 years, 2 months ago

c is correct

upvoted 2 times

Question #42 *Topic 1*

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

Suggested Answer: *A*

Official Answer: A

Community vote distribution

B (100%)

MrBravo Most Recent 2 years ago

Vancouver eBook p. 335: "Once the SI Phisging Email record is created, it triggers the Transform flow. That flow creates the SI record.

upvoted 1 times

sephereth 2 years, 7 months ago

Explanation: ebook p.312, Once the Security Incident Phishing Email record is created, it triggers the Transform flow. Thta flow creates the Security incident record and determines if this is a new phishing attempt or whether it should be aggregated with existing incidents.

upvoted 1 times

Remo878 2 years, 8 months ago

B. Transform flow

upvoted 2 times

Question #43 *Topic 1*

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

Suggested Answer: *D*

Official Answer: D

Community vote distribution

D (100%)

Sazeka Most Recent 1 year, 9 months ago

The correct Answer is D: According to the Ebook page 152: there are over 20 integration cards available baseline, and other integration can be added from the ServiceNow store.

upvoted 1 times

Question #44 *Topic 1*

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

Suggested Answer: *A, B*
Official Answer: AB

Community vote distribution
AB (100%)

sephereth Most Recent 2 years, 1 month ago
Explanation: services and CI are impacted, https://docs.servicenow.com/bundle/paris-it-service-management/page/product/incident-management/concept/c_IncidentManagement.html
upvoted 2 times

Question #45 *Topic 1*

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

Suggested Answer: *A*

Official Answer: A

Community vote distribution

A (100%)

Sazeka Most Recent 1 year, 9 months ago

A is correct.

upvoted 1 times

sephereth 2 years, 1 month ago

Explanation: ebook p.38, ... "Organize - Analyze - Prioritize - Contain" ...correct!

upvoted 2 times

sephereth 2 years, 1 month ago

Selected Answer: A

Explanation: ebook p.38, ... "Organize - Analyze - Prioritize - Contain" ...

upvoted 2 times

Sazeka 1 year, 9 months ago

correct!

upvoted 1 times

Question #46 *Topic 1*

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

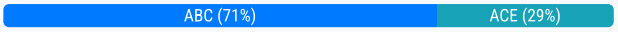
D. Reduce the number of incidents assigned to the Platform Admin

E. Preserve the security image in the company

Suggested Answer: *B, C, D*

Official Answer: BCD

Community vote distribution



Sazeka Most Recent 1 year, 10 months ago

Option B, "Allow SIR Teams to control the assignment of security roles," is not necessarily "wrong," but it may not be one of the primary reasons for separating the Platform Administrator and Security Incident Administrator roles in the context of maintaining security and compliance in ServiceNow. Option E instead preserve the security image in the company: Having a clear separation of roles, especially when it comes to security-related tasks, can help enhance the company's security posture and reputation. It demonstrates a commitment to maintaining a strong security culture and minimizes the potential for unauthorized access or mishandling of security incidents.

upvoted 2 times

sgawas 2 years ago

right answers

upvoted 2 times

sephereth 2 years, 1 month ago

i am guessing A B and C Explanation: here are my thought processes - By separating the Platform (System) Administrator role from the Security Incident administrator role, organizations can restrict access to security incident data to those who need it. (a) - By separating the Platform (System) Administrator role from the Security Incident administrator role, organizations can allow the SIR team to control the assignment of security roles. This ensures that only those who are authorized to do so have access to security incident data and can perform security incident response activities. (b) - By separating the Platform (System) Administrator role from the Security Incident administrator role, organizations can implement the principle of separation of duty. This helps to prevent unauthorized access to security incident data and ensures that security incidents are responded to effectively. (c)

upvoted 3 times

Question #47 *Topic 1*

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

Suggested Answer: *C*

Official Answer: C

Community vote distribution

D (100%)

ademir_amaral Most Recent 1 year, 8 months ago

D is correct!

upvoted 1 times

Sazeka 2 years, 3 months ago

D is correct

upvoted 2 times

sephereth 2 years, 7 months ago

Selected Answer: D

Explanation: ebook p.295, using the KB articles for your Playbooks tasks also gives you the enhanced ability to create and present concise, descriptive tasks for your analysts.

upvoted 2 times

sephereth 2 years, 7 months ago

Explanation: ebook p.295, using the KB articles for your Playbooks tasks also gives you the enhanced ability to create and present concise, descriptive tasks for your analysts.correct

upvoted 2 times

Sazeka 2 years, 3 months ago

correct

upvoted 1 times

Dharshu98 2 years, 7 months ago

D is correct

upvoted 3 times

Question #48 *Topic 1*

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

Suggested Answer: *A*

Official Answer: A

Community vote distribution

D (100%)

MrBravo Most Recent 2 years ago

Vancouver ebook p 335: "URP v2 creates a record in a new table - Security Incident Phising Emails"

upvoted 1 times

fraga02 2 years, 1 month ago

D is correct

upvoted 1 times

sephereth 2 years, 7 months ago

Explanation: ebook p.318, This Script will generate a record in the Security Incident Phishing Email [sn_si_phishing_email] table. *note, actual description on script include states "processes an email for user reported phishing. Each attached eml file will be parsed for headers creates sn_si_phishing_email/sn_si_phishing_email_header" meaning record is also created on the [sn_si_phishing_email_header] table

upvoted 1 times

stophs 2 years, 8 months ago

D IS CORRECT

upvoted 2 times

Question #49 *Topic 1*

A flow consists of _____. (Choose two.)

A. Scripts

B. Actions

C. Processes

D. Actors

E. Triggers

Suggested Answer: *B, E*

Official Answer: BE

Community vote distribution

BE (100%)

NokoNice Most Recent 1 year, 8 months ago

1. Triggers - The event that starts the flow. 2. Actions - The steps that the flow takes. 3. Conditions - The criteria that must be met for the flow to continue.

upvoted 1 times

sephereth 2 years, 1 month ago

Explanation: Components of a flow are: 1. Triggers - The event that starts the flow. 2. Actions - The steps that the flow takes. 3. Conditions - The criteria that must be met for the flow to continue. 4. Branches - The paths that the flow can take based on conditions.

upvoted 2 times

Question #50 *Topic 1*

Which of the following process definitions are not provided baseline?

A. NIST Open

B. SAN Stateful

C. NIST Stateful

D. SANS Open

Suggested Answer: *A*

Official Answer: A

Community vote distribution

B (100%)

Remo878 Highly Voted 2 years, 8 months ago

Sans stateful

upvoted 5 times

fraga02 Most Recent 2 years, 1 month ago

SANS Stateful

upvoted 3 times

sephereth 2 years, 7 months ago

Explanation: oob configuration has - NIST Stateful - NIST Open - SANS Open - Example *note, Stateful means step by step (can't skip to any statues), while Open allows skipping steps

upvoted 3 times