



Fortinet

Exam Questions FCSS_SOC_AN-7.4

FCSS - Security Operations 7.4 Analyst

About ExamBible

[Your Partner of IT Exam](#)

Found in 1998

ExamBible is a company specialized on providing high quality IT exam practice study materials, especially Cisco CCNA, CCDA, CCNP, CCIE, Checkpoint CCSE, CompTIA A+, Network+ certification practice exams and so on. We guarantee that the candidates will not only pass any IT exam at the first attempt but also get profound understanding about the certificates they have got. There are so many alike companies in this industry, however, ExamBible has its unique advantages that other companies could not achieve.

Our Advances

* 99.9% Uptime

All examinations will be up to date.

* 24/7 Quality Support

We will provide service round the clock.

* 100% Pass Rate

Our guarantee that you will pass the exam.

* Unique Gurantee

If you do not pass the exam at the first time, we will not only arrange FULL REFUND for you, but also provide you another exam of your claim, ABSOLUTELY FREE!

NEW QUESTION 1

Which two playbook triggers enable the use of trigger events in later tasks as trigger variables? (Choose two.)

- A. EVENT
- B. INCIDENT
- C. ON SCHEDULE
- D. ON DEMAND

Answer: AB

Explanation:

Understanding Playbook Triggers:

Playbook triggers are the starting points for automated workflows within FortiAnalyzer or FortiSOAR.

These triggers determine how and when a playbook is executed and can pass relevant information (trigger variables) to subsequent tasks within the playbook.

Types of Playbook Triggers:

EVENT Trigger:

Initiates the playbook when a specific event occurs.

The event details can be used as variables in later tasks to customize the response.

Selected as it allows using event details as trigger variables.

INCIDENT Trigger:

Activates the playbook when an incident is created or updated.

The incident details are available as variables in subsequent tasks.

Selected as it enables the use of incident details as trigger variables.

ON SCHEDULE Trigger:

Executes the playbook at specified times or intervals.

Does not inherently use trigger events to pass variables to later tasks.

Not selected as it does not involve passing trigger event details.

ON DEMAND Trigger:

Runs the playbook manually or as required.

Does not automatically include trigger event details for use in later tasks.

Not selected as it does not use trigger events for variables.

Implementation Steps:

Step 1: Define the conditions for the EVENT or INCIDENT trigger in the playbook configuration.

Step 2: Use the details from the trigger event or incident in subsequent tasks to customize actions and responses.

Step 3: Test the playbook to ensure that the trigger variables are correctly passed and utilized.

Conclusion:

EVENT and INCIDENT triggers are specifically designed to initiate playbooks based on specific occurrences, allowing the use of trigger details in subsequent tasks.

References:

Fortinet Documentation on Playbook Configuration FortiSOAR Playbook Guide

By using the EVENT and INCIDENT triggers, you can leverage trigger events in later tasks as variables, enabling more dynamic and responsive playbook actions.

NEW QUESTION 2

According to the National Institute of Standards and Technology (NIST) cybersecurity framework, incident handling activities can be divided into phases.

In which incident handling phase do you quarantine a compromised host in order to prevent an adversary from using it as a stepping stone to the next phase of an attack?

- A. Containment
- B. Analysis
- C. Eradication
- D. Recovery

Answer: A

Explanation:

NIST Cybersecurity Framework Overview:

The NIST Cybersecurity Framework provides a structured approach for managing and mitigating cybersecurity risks. Incident handling is divided into several phases to systematically address and resolve incidents.

Incident Handling Phases:

Preparation: Establishing and maintaining an incident response capability.

Detection and Analysis: Identifying and investigating suspicious activities to confirm an incident.

Containment, Eradication, and Recovery:

Containment: Limiting the impact of the incident.

Eradication: Removing the root cause of the incident.

Recovery: Restoring systems to normal operation.

Containment Phase:

The primary goal of the containment phase is to prevent the incident from spreading and causing further damage.

Quarantining a Compromised Host:

Quarantining involves isolating the compromised host from the rest of the network to prevent adversaries from moving laterally and causing more harm.

Techniques include network segmentation, disabling network interfaces, and applying access controls.

NEW QUESTION 3

Refer to the exhibit.

FortiAnalyzer Fabric				
Name	IP Address	Platform	Logs	Serial Number
FAZ-SiteA	10.0.1.236	FortiAnalyzer-VM64		FAZ-VMTM24000905
SiteA				
FortiGate-A2	10.200.2.254	FortiGate-VM64	Real Time	FGVMSLTM24000454
root		vdom	Real Time	
MSSP-Local				
FortiGate-A1	10.0.1.254	FortiGate-VM64	Real Time	FGVMSLTM24000453
root		vdom	Real Time	
FAZ-SiteB	10.200.200.236	FortiAnalyzer-VM64		FAZ-VMTM24000908
root				
Site-B-Fabric				
FortiGate-B1	172.16.200.5	FortiGate-VM64	Real Time	FGVMSLTM24000455
root		vdom	Real Time	
FortiGate-B2	10.200.200.254	FortiGate-VM64	Real Time	FGVMSLTM24000847
root		vdom	Real Time	

Assume that all devices in the FortiAnalyzer Fabric are shown in the image.
Which two statements about the FortiAnalyzer Fabric deployment are true? (Choose two.)

- A. FortiGate-B1 and FortiGate-B2 are in a Security Fabric.
- B. There is no collector in the topology.
- C. All FortiGate devices are directly registered to the supervisor.
- D. FAZ-SiteA has two ADOMs enabled.

Answer: AD

Explanation:

Understanding the FortiAnalyzer Fabric:
The FortiAnalyzer Fabric provides centralized log collection, analysis, and reporting for connected FortiGate devices. Devices in a FortiAnalyzer Fabric can be organized into different Administrative Domains (ADOMs) to separate logs and management.
Analyzing the Exhibit:
FAZ-SiteA and FAZ-SiteB are FortiAnalyzer devices in the fabric.
FortiGate-B1 and FortiGate-B2 are shown under the Site-B-Fabric, indicating they are part of the same Security Fabric.
FAZ-SiteA has multiple entries under it: SiteA and MSSP-Local, suggesting multiple ADOMs are enabled.

Evaluating the Options:
Option A: FortiGate-B1 and FortiGate-B2 are under Site-B-Fabric, indicating they are indeed part of the same Security Fabric.
Option B: The presence of FAZ-SiteA and FAZ-SiteB as FortiAnalyzers does not preclude the existence of collectors. However, there is no explicit mention of a separate collector role in the exhibit.
Option C: Not all FortiGate devices are directly registered to the supervisor. The exhibit shows hierarchical organization under different sites and ADOMs.
Option D: The multiple entries under FAZ-SiteA (SiteA and MSSP-Local) indicate that FAZ-SiteA has two ADOMs enabled.

Conclusion:
FortiGate-B1 and FortiGate-B2 are in a Security Fabric.
FAZ-SiteA has two ADOMs enabled.
References:
Fortinet Documentation on FortiAnalyzer Fabric Topology and ADOM Configuration.
Best Practices for Security Fabric Deployment with FortiAnalyzer.

NEW QUESTION 4

Refer to the exhibit,

Command and Control	T1071.001 Web Protocols (5)
	T1071.002 File Transfer Protocols
16 techniques	T1071.003 Mail Protocols
Application Layer Protocol	T1071.004 DNS (11)
15	

which shows the partial output of the MITRE ATT&CK Enterprise matrix on FortiAnalyzer. Which two statements are true? (Choose two.)

- A. There are four techniques that fall under tactic T1071.
- B. There are four subtechniques that fall under technique T1071.
- C. There are event handlers that cover tactic T1071.
- D. There are 15 events associated with the tactic.

Answer: BC

Explanation:

Understanding the MITRE ATT&CK Matrix:
The MITRE ATT&CK framework is a knowledge base of adversary tactics and techniques based on real-world observations.

Each tactic in the matrix represents the "why" of an attack technique, while each technique represents "how" an adversary achieves a tactic.

Analyzing the Provided Exhibit:

The exhibit shows part of the MITRE ATT&CK Enterprise matrix as displayed on FortiAnalyzer.

The focus is on technique T1071 (Application Layer Protocol), which has subtechniques labeled T1071.001, T1071.002, T1071.003, and T1071.004.

Each subtechnique specifies a different type of application layer protocol used for Command and Control (C2):

T1071.001 Web Protocols

T1071.002 File Transfer Protocols

T1071.003 Mail Protocols

T1071.004 DNS

Identifying Key Points:

Subtechniques under T1071: There are four subtechniques listed under the primary technique T1071, confirming that statement B is true.

Event Handlers for T1071: FortiAnalyzer includes event handlers for monitoring various tactics and techniques. The presence of event handlers for tactic T1071 suggests active monitoring and alerting for these specific subtechniques, confirming that statement C is true.

Misconceptions Clarified:

Statement A (four techniques under tactic T1071) is incorrect because T1071 is a single technique with four subtechniques.

Statement D (15 events associated with the tactic) is misleading. The number 15 refers to the techniques under the Application Layer Protocol, not directly related to the number of events.

Conclusion:

The accurate interpretation of the exhibit confirms that there are four subtechniques under technique T1071 and that there are event handlers covering tactic T1071.

References:

MITRE ATT&CK Framework documentation.

FortiAnalyzer Event Handling and MITRE ATT&CK Integration guides.

NEW QUESTION 5

Which FortiAnalyzer connector can you use to run automation stitches?

- A. FortiCASB
- B. FortiMail
- C. Local
- D. FortiOS

Answer: D

Explanation:

> Overview of Automation Stitches:

> Automation stitches in FortiAnalyzer are predefined sets of automated actions triggered by specific events. These actions help in automating responses to security incidents, improving efficiency, and reducing the response time.

> FortiAnalyzer Connectors:

> FortiAnalyzer integrates with various Fortinet products and other third-party solutions through connectors. These connectors facilitate communication and data exchange, enabling centralized management and automation.

> Available Connectors for Automation Stitches:

> FortiCASB:

> FortiCASB is a Cloud Access Security Broker that helps secure SaaS applications.

However, it is not typically used for running automation stitches within FortiAnalyzer.

NEW QUESTION 6

When configuring a FortiAnalyzer to act as a collector device, which two steps must you perform? (Choose two.)

- A. Enable log compression.
- B. Configure log forwarding to a FortiAnalyzer in analyzer mode.
- C. Configure the data policy to focus on archiving.
- D. Configure Fabric authorization on the connecting interface.

Answer: BD

Explanation:

Understanding FortiAnalyzer Roles:

FortiAnalyzer can operate in two primary modes: collector mode and analyzer mode.

Collector Mode: Gathers logs from various devices and forwards them to another FortiAnalyzer operating in analyzer mode for detailed analysis.

Analyzer Mode: Provides detailed log analysis, reporting, and incident management.

Steps to Configure FortiAnalyzer as a Collector Device:

* A. Enable Log Compression:

While enabling log compression can help save storage space, it is not a mandatory step specifically required for configuring FortiAnalyzer in collector mode.

Not selected as it is optional and not directly related to the collector configuration process.

B. Configure Log Forwarding to a FortiAnalyzer in Analyzer Mode:

Essential for ensuring that logs collected by the collector FortiAnalyzer are sent to the analyzer FortiAnalyzer for detailed processing.

Selected as it is a critical step in configuring a FortiAnalyzer as a collector device.

Step 1: Access the FortiAnalyzer interface and navigate to log forwarding settings.

Step 2: Configure log forwarding by specifying the IP address and necessary credentials of the FortiAnalyzer in analyzer mode.

NEW QUESTION 7

Which statement describes automation stitch integration between FortiGate and FortiAnalyzer?

- A. An event handler on FortiAnalyzer executes an automation stitch when an event is created.
- B. An automation stitch is configured on FortiAnalyzer and mapped to FortiGate using the FortiOS connector.
- C. An event handler on FortiAnalyzer is configured to send a notification to FortiGate to trigger an automation stitch.
- D. A security profile on FortiGate triggers a violation and FortiGate sends a webhook call to FortiAnalyzer.

Answer: D

Explanation:

Overview of Automation Stitches: Automation stitches in Fortinet solutions enable automated responses to specific events detected within the network. This automation helps in swiftly mitigating threats without manual intervention.

FortiGate Security Profiles:

FortiGate uses security profiles to enforce policies on network traffic. These profiles can include antivirus, web filtering, intrusion prevention, and more. When a security profile detects a violation or a specific event, it can trigger predefined actions.

Webhook Calls:

FortiGate can be configured to send webhook calls upon detecting specific security events. A webhook is an HTTP callback triggered by an event, sending data to a specified URL. This allows FortiGate to communicate with other systems, such as FortiAnalyzer.

FortiAnalyzer Integration:

FortiAnalyzer collects logs and events from various Fortinet devices, providing centralized logging and analysis. Upon receiving a webhook call from FortiGate, FortiAnalyzer can further analyze the event, generate reports, and take automated actions if configured to do so.

Detailed Process:

Step 1: A security profile on FortiGate triggers a violation based on the defined security policies.

Step 2: FortiGate sends a webhook call to FortiAnalyzer with details of the violation.

Step 3: FortiAnalyzer receives the webhook call and logs the event.

Step 4: Depending on the configuration, FortiAnalyzer can execute an automation stitch to respond to the event, such as sending alerts, generating reports, or triggering further actions.

References:

Fortinet Documentation: FortiOS Automation Stitches

FortiAnalyzer Administration Guide: Details on configuring event handlers and integrating with FortiGate.

FortiGate Administration Guide: Information on security profiles and webhook configurations. By understanding the interaction between FortiGate and FortiAnalyzer through webhook calls and automation stitches, security operations can ensure a proactive and efficient response to security events.

NEW QUESTION 8

Refer to the exhibits.

Playbook status

Job ID	Playbook	Trigger	Start Time	End Time	Status
2024-03-20 08:32:14 770575-07	DOS attack	event:202403201008	2024-03-20 08:32:15-0700	2024-03-20 08:32:15-0700	Failed

Playbook tasks

Task ID	Task	Start Time	End Time	Status
placeholder_8fab0102_0955_447f_872d_220	Attach_Data_To_Incident	2024-03-20 08:32:16-0700	2024-03-20 08:32:16	upstream_fa
placeholder_fa2a573c_ba4f_4565_ba90_4255d	Get Events	2024-03-20 08:32:17-0700	2024-03-20 08:32:18	success
placeholder_3db75c0a_1765_4479_81b8_2e1	Create SMTP Enumeration incident	2024-03-20 08:32:17-0700	2024-03-20 08:32:18	failed

Raw Logs

```
[2024-03-20T08:32:18.089-0700] {taskinstance.py:1937} ERROR - Task failed with exception
Traceback (most recent call last):
  File "/drive0/private/airflow/plugins/incident_operator.py", line 218, in execute
    self.epid = int(self.epid)
ValueError: invalid literal for int() with base 10: '10.200.200.100'
```

The DOS attack playbook is configured to create an incident when an event handler generates a denial-of-ser/ice (DoS) attack event. Why did the DOS attack playbook fail to execute?

- A. The Create SMTP Enumeration incident task is expecting an integer value but is receiving the incorrect data type
- B. The Get Events task is configured to execute in the incorrect order.
- C. The Attach_Data_To_Incident task failed.
- D. The Attach_Data_To_Incident task is expecting an integer value but is receiving the incorrect data type.

Answer: A

Explanation:

Understanding the Playbook and its Components:

The exhibit shows the status of a playbook named "DOS attack" and its associated tasks. The playbook is designed to execute a series of tasks upon detecting a DoS attack event.

Analysis of Playbook Tasks:

Attach_Data_To_Incident: Task ID placeholder_8fab0102, status is "upstream_failed," meaning it did not execute properly due to a previous task's failure.

Get Events: Task ID placeholder_fa2a573c, status is "success."

Create SMTP Enumeration incident: Task ID placeholder_3db75c0a, status is "failed."

Reviewing Raw Logs:

The error log shows a ValueError: invalid literal for int() with base 10: '10.200.200.100'. This error indicates that the task attempted to convert a string (the IP address '10.200.200.100') to an integer, which is not possible.

Identifying the Source of the Error:

The error occurs in the file "incident_operator.py," specifically in the execute method. This suggests that the task "Create SMTP Enumeration incident" is the one causing the issue because it failed to process the data type correctly.

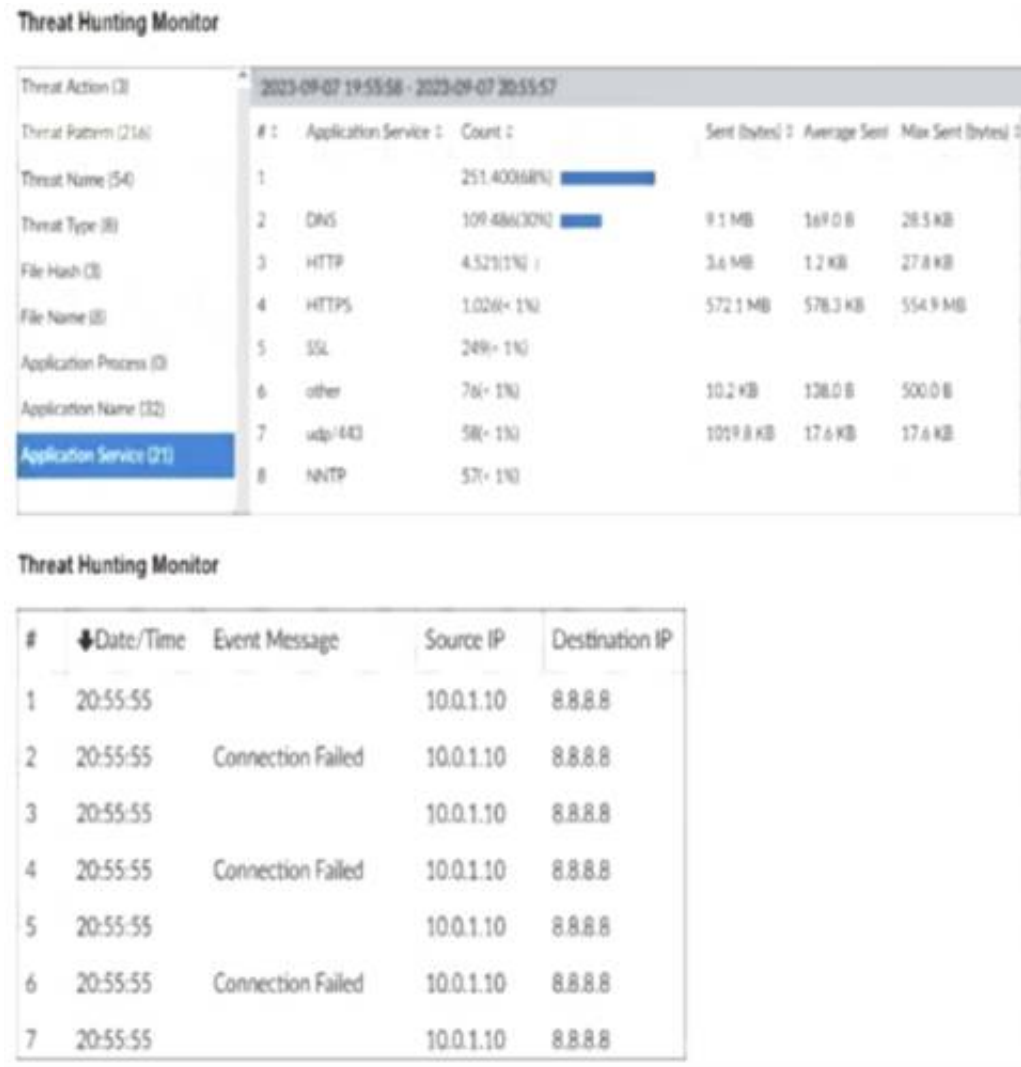
Conclusion:

The failure of the playbook is due to the "Create SMTP Enumeration incident" task receiving a string value (an IP address) when it expects an integer value. This mismatch in data types leads to the error.

References:

Fortinet Documentation on Playbook and Task Configuration.
Python error handling documentation for understanding ValueError.

NEW QUESTION 9
Refer to the exhibits.



What can you conclude from analyzing the data using the threat hunting module?

- A. Spearphishing is being used to elicit sensitive information.
- B. DNS tunneling is being used to extract confidential data from the local network.
- C. Reconnaissance is being used to gather victim identity information from the mail server.
- D. FTP is being used as command-and-control (C&C) technique to mine for data.

Answer: B

Explanation:

Understanding the Threat Hunting Data:
The Threat Hunting Monitor in the provided exhibits shows various application services, their usage counts, and data metrics such as sent bytes, average sent bytes, and maximum sent bytes.
The second part of the exhibit lists connection attempts from a specific source IP (10.0.1.10) to a destination IP (8.8.8.8), with repeated "Connection Failed" messages.
Analyzing the Application Services:
DNS is the top application service with a significantly high count (251,400) and notable sent bytes (9.1 MB).
This large volume of DNS traffic is unusual for regular DNS queries and can indicate the presence of DNS tunneling.
DNS Tunneling:
DNS tunneling is a technique used by attackers to bypass security controls by encoding data within DNS queries and responses. This allows them to extract data from the local network without detection.
The high volume of DNS traffic, combined with the detailed metrics, suggests that DNS tunneling might be in use.
Connection Failures to 8.8.8.8:
The repeated connection attempts from the source IP (10.0.1.10) to the destination IP (8.8.8.8) with connection failures can indicate an attempt to communicate with an external server.
Google DNS (8.8.8.8) is often used for DNS tunneling due to its reliability and global reach.
Conclusion:
Given the significant DNS traffic and the nature of the connection attempts, it is reasonable to conclude that DNS tunneling is being used to extract confidential data from the local network.
Why Other Options are Less Likely:
Spearphishing (A): There is no evidence from the provided data that points to spearphishing attempts, such as email logs or phishing indicators.
Reconnaissance (C): The data does not indicate typical reconnaissance activities, such as scanning or probing mail servers.
FTP C&C (D): There is no evidence of FTP traffic or command-and-control communications using FTP in the provided data.
References:
SANS Institute: "DNS Tunneling: How to Detect Data Exfiltration and Tunneling Through DNS Queries" SANS DNS Tunneling
OWASP: "DNS Tunneling" OWASP DNS Tunneling
By analyzing the provided threat hunting data, it is evident that DNS tunneling is being used to exfiltrate data, indicating a sophisticated method of extracting confidential information from the network.

NEW QUESTION 10
Refer to the Exhibit:



An analyst wants to create an incident and generate a report whenever FortiAnalyzer generates a malicious attachment event based on FortiSandbox analysis. The endpoint hosts are protected by FortiClient EMS integrated with FortiSandbox. All devices are logging to FortiAnalyzer. Which connector must the analyst use in this playbook?

- A. FortiSandbox connector
- B. FortiClient EMS connector
- C. FortiMail connector
- D. Local connector

Answer: A

Explanation:

Understanding the Requirements:

The objective is to create an incident and generate a report based on malicious attachment events detected by FortiAnalyzer from FortiSandbox analysis. The endpoint hosts are protected by FortiClient EMS, which is integrated with FortiSandbox. All logs are sent to FortiAnalyzer.

Key Components:

FortiAnalyzer: Centralized logging and analysis for Fortinet devices.

FortiSandbox: Advanced threat protection system that analyzes suspicious files and URLs.

FortiClient EMS: Endpoint management system that integrates with FortiSandbox for endpoint protection.

Playbook Analysis:

The playbook in the exhibit consists of three main actions: GET_EVENTS, RUN_REPORT, and CREATE_INCIDENT.

EVENT_TRIGGER: Starts the playbook when an event occurs.

GET_EVENTS: Fetches relevant events.

RUN_REPORT: Generates a report based on the events.

CREATE_INCIDENT: Creates an incident in the incident management system.

Selecting the Correct Connector:

The correct connector should allow fetching events related to malicious attachments analyzed by FortiSandbox and facilitate integration with FortiAnalyzer.

Connector Options:

FortiSandbox Connector:

Directly integrates with FortiSandbox to fetch analysis results and events related to malicious attachments.

Best suited for getting detailed sandbox analysis results.

Selected as it is directly related to the requirement of handling FortiSandbox analysis events.

FortiClient EMS Connector:

Used for managing endpoint security and integrating with endpoint logs.

Not directly related to fetching sandbox analysis events.

Not selected as it is not directly related to the sandbox analysis events.

FortiMail Connector:

Used for email security and handling email-related logs and events.

Not applicable for sandbox analysis events.

Not selected as it does not relate to the sandbox analysis.

Local Connector:

Handles local events within FortiAnalyzer itself.

Might not be specific enough for fetching detailed sandbox analysis results.

Not selected as it may not provide the required integration with FortiSandbox.

Implementation Steps:

Step 1: Ensure FortiSandbox is configured to send analysis results to FortiAnalyzer.

Step 2: Use the FortiSandbox connector in the playbook to fetch events related to malicious attachments.

Step 3: Configure the GET_EVENTS action to use the FortiSandbox connector.

Step 4: Set up the RUN_REPORT and CREATE_INCIDENT actions based on the fetched events.

References:

Fortinet Documentation on FortiSandbox Integration FortiSandbox Integration Guide

Fortinet Documentation on FortiAnalyzer Event Handling FortiAnalyzer Administration Guide

By using the FortiSandbox connector, the analyst can ensure that the playbook accurately fetches events based on FortiSandbox analysis and generates the required incident and report.

NEW QUESTION 10

Refer to Exhibit:



A SOC analyst is designing a playbook to filter for a high severity event and attach the event information to an incident. Which local connector action must the analyst use in this scenario?

- A. Get Events
- B. Update Incident
- C. Update Asset and Identity
- D. Attach Data to Incident

Answer: D

Explanation:

Understanding the Playbook Requirements:

The SOC analyst needs to design a playbook that filters for high severity events.

The playbook must also attach the event information to an existing incident.

Analyzing the Provided Exhibit:

The exhibit shows the available actions for a local connector within the playbook.

Actions listed include:

Update Asset and Identity

Get Events

Get Endpoint Vulnerabilities

Create Incident

Update Incident

Attach Data to Incident

Run Report

Get EPEU from Incident

Evaluating the Options:

Get Events: This action retrieves events but does not attach them to an incident.

Update Incident: This action updates an existing incident but is not specifically for attaching event data.

Update Asset and Identity: This action updates asset and identity information, not relevant for attaching event data to an incident.

Attach Data to Incident: This action is explicitly designed to attach additional data, such as event information, to an existing incident.

Conclusion:

The correct action to use in the playbook for filtering high severity events and attaching the event information to an incident is Attach Data to Incident.

References:

Fortinet Documentation on Playbook Actions and Connectors.

Best Practices for Incident Management and Playbook Design in SOC Operations.

NEW QUESTION 11

.....

Relate Links

100% Pass Your FCSS_SOC_AN-7.4 Exam with Exambible Prep Materials

https://www.exambible.com/FCSS_SOC_AN-7.4-exam/

Contact us

We are proud of our high-quality customer service, which serves you around the clock 24/7.

Viste - <https://www.exambible.com/>