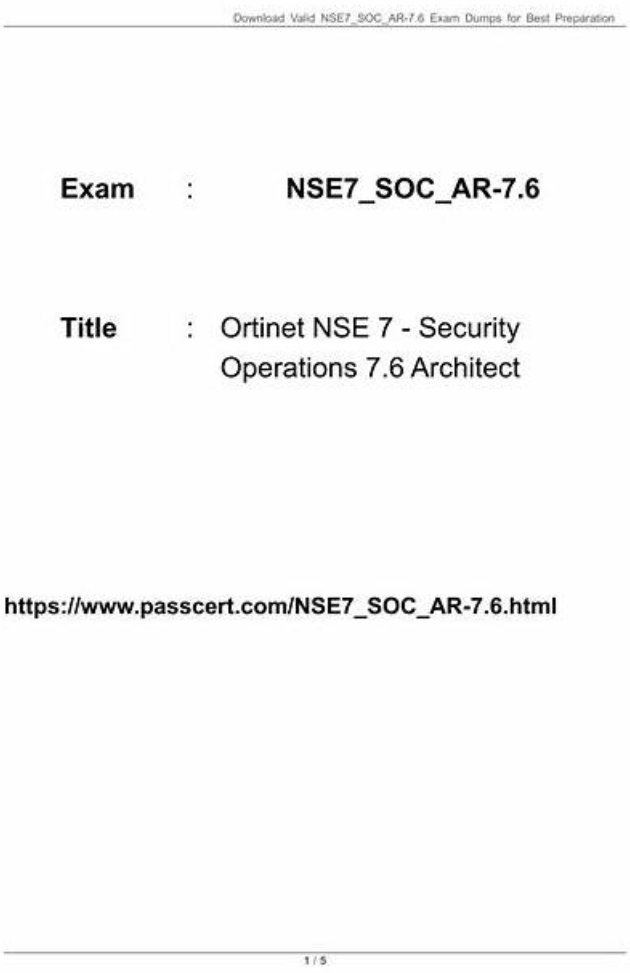
NSE7_SOC_AR-7.6 Exam Fee, NSE7_SOC_AR-7.6 Reliable Dumps Book



DOWNLOAD the newest Free4Torrent NSE7_SOC_AR-7.6 PDF dumps from Cloud Storage for free: https://drive.google.com/open?id=1rqNPxQp7uWuq0X0gWDE9bGbbXMD8ak7L

The Free4Torrent is one of the top-rated and reliable platforms that has been helping the Fortinet NSE7_SOC_AR-7.6 exam candidates for many years. Over this long time period, countless NSE7_SOC_AR-7.6 exam candidates have passed their Fortinet exam with good scores. In their success one thing is common and that is the usage of Free4Torrent NSE7_SOC_AR-7.6 Exam Practice test questions.

Our NSE7_SOC_AR-7.6 test questions are available in three versions, including PDF versions, PC versions, and APP online versions. Each version has its own advantages and features, NSE7_SOC_AR-7.6 test material users can choose according to their own preferences. The most popular version is the PDF version of NSE7_SOC_AR-7.6 exam prep. The PDF version of NSE7_SOC_AR-7.6 Test Questions can be printed out to facilitate your learning anytime, anywhere, as well as your own priorities. The PC version of NSE7_SOC_AR-7.6 exam prep is for Windows users. If you use the APP online version, just download the application. Program, you can enjoy our NSE7_SOC_AR-7.6 test material service.

>> NSE7_SOC_AR-7.6 Exam Fee <<

NSE7_SOC_AR-7.6 Reliable Dumps Book & NSE7_SOC_AR-7.6 Learning Materials

We have considered that your time may be very tight, and you can only use some fragmented time to learn. Therefore, it is really important to be able to read our NSE7_SOC_AR-7.6 study materials anytime, anywhere. So we have developed our NSE7_SOC_AR-7.6 exam questions to three different versions: the PDF, Software and APP online. They have covered all conditions that you will be in to study on our NSE7_SOC_AR-7.6 learning guide. For example, the time you want to study on phone, computer, laptop, paper and so on.

Fortinet NSE7_SOC_AR-7.6 Exam Syllabus Topics:

Topic	Details
Topic 1	• SOAR Incident Handling and Threat Hunting: Includes threat hunting analysis, managing FortiSOAR incidents, workload coordination, and using war rooms for incident response.
Topic 2	• SOC Concepts and Frameworks: Covers analyzing security incidents, identifying adversary behaviors, understanding Fortinet SOC architecture, and recognizing common attack vectors.
Topic 3	• SOAR Playbook Development: Covers configuring playbooks and connectors, using Jinja filters for data handling, and troubleshooting FortiSOAR automation workflows.
Topic 4	• Detection Capabilities: Focuses on configuring FortiSIEM incident rules, building log queries, and analyzing incidents for effective threat detection.

Fortinet NSE 7 - Security Operations 7.6 Architect Sample Questions (Q57-Q62):

NEW QUESTION # 57
Refer to the exhibits.
What can you conclude from analyzing the data using the threat hunting module?

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

Answer: C

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.
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.

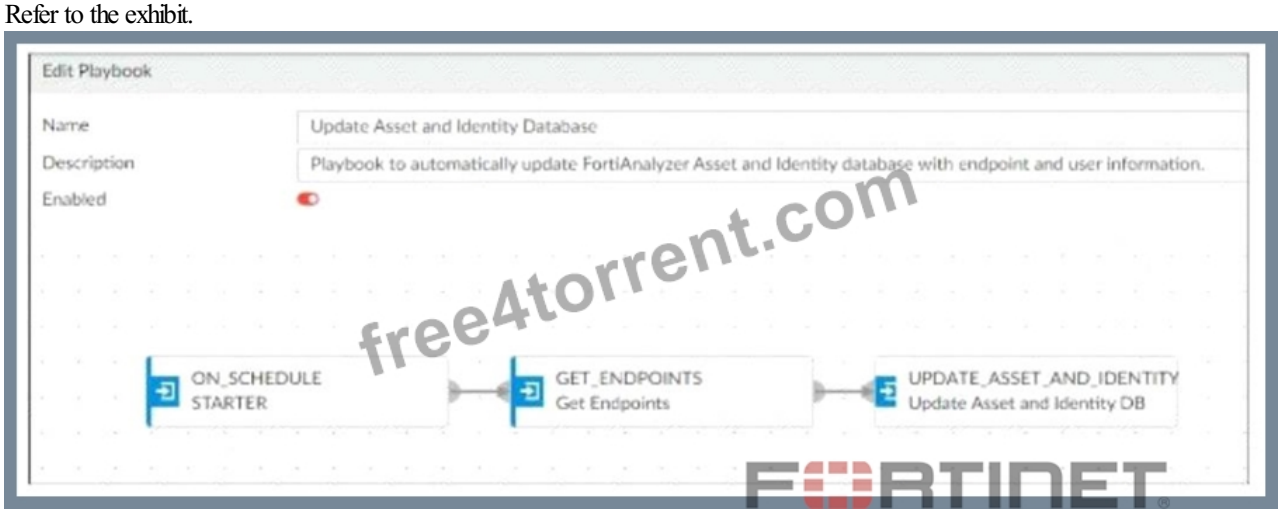
NEW QUESTION # 58
Review the incident report:
Packet captures show a host maintaining periodic TLS sessions that imitate normal HTTPS traffic but run on TCP 8443 to a single external host. An analyst flags the traffic as potential command-and-control. During the same period, the host issues frequent DNS queries with oversized TXT payloads to an attacker-controlled domain, transferring staged files.
Which two MITRE ATT&CK techniques best describe this activity? (Choose two answers)

- A. Hide Artifacts
- B. Exploitation of Remote Services
- C. Exfiltration Over Alternative Protocol
- D. Non-Standard Port

Answer: C,D

Explanation:
Comprehensive and Detailed Explanation From FortiSOAR 7.6., FortiSIEM 7.3 Exact Extract study guide:
In accordance with the MITRE ATT&CK mapping utilized byFortiSIEM 7.3andFortiSOAR 7.6, the described behaviors correspond to the following techniques:
* Non-Standard Port (T1571):This technique involves adversaries communicating using a protocol and port pairing that are typically not associated. The incident report identifies HTTPS (TLS) traffic running onTCP 8443rather than the standard port 443.FortiSIEMspecifically includes built-in correlation rules, such as "Suspicious Typical Malware Back Connect Ports," designed to detect these protocol-port mismatches.
* Exfiltration Over Alternative Protocol (T1048):This technique describes adversaries stealing data by exfiltrating it over a different protocol than the primary command and control (C2) channel. In this scenario, while the C2 channel is established via HTTPS on port 8443, the adversary is transferring staged files usingDNS queries with oversized TXT payloads. DNS is a common "alternative protocol" used to bypass standard data transfer monitoring and egress filtering.
Analysis of Incorrect Options:
* Exploitation of Remote Services (B):This technique falls underInitial AccessorLateral Movementtactics, focusing on gaining entry into a system via vulnerabilities in network services like SMB or RDP. It does not apply to the maintenance of an established C2 channel or the exfiltration of data.
* Hide Artifacts (D):This is aDefense Evasiontechnique where an adversary attempts to conceal their presence by removing traces such as log files or registry keys. While the attacker is "imitating normal traffic," the specific acts of using a non-standard port and DNS exfiltration are primary behavioral signatures defined by their own more specific techniques.

NEW QUESTION # 59
Refer to the exhibit.



Which two options describe how the Update Asset and Identity Database playbook is configured? (Choose two.)

- A. The playbook is using an on-demand trigger.
- B. The playbook is using a FortiMail connector.
- C. The playbook is using a FortiClient EMS connector.
- D. The playbook is using a local connector.

Answer: C,D

Explanation:
* Understanding the Playbook Configuration:
* The playbook named "Update Asset and Identity Database" is designed to update the FortiAnalyzer Asset and Identity database with endpoint and user information.
* The exhibit shows the playbook with three main components: ON_SCHEDULE STARTER, GET_ENDPOINTS, and UPDATE_ASSET_AND_IDENTITY.
* Analyzing the Components:
* ON_SCHEDULE STARTER:This component indicates that the playbook is triggered on a schedule, not on-demand.
* GET_ENDPOINTS:This action retrieves information about endpoints, suggesting it interacts with an endpoint management system.
* UPDATE_ASSET_AND_IDENTITY:This action updates the FortiAnalyzer Asset and Identity database with the retrieved information.
* Evaluating the Options:
* Option A:The actions shown in the playbook are standard local actions that can be executed by the FortiAnalyzer, indicating the use of a local connector.
* Option B:There is no indication that the playbook uses a FortiMail connector, as the tasks involve endpoint and identity management, not email.
* Option C:The playbook is using an "ON_SCHEDULE" trigger, which contradicts the description of an on-demand trigger.
* Option D:The action "GET_ENDPOINTS" suggests integration with an endpoint management system, likely FortiClient EMS, which manages endpoints and retrieves information from them.
* Conclusion:
* The playbook is configured to use a local connector for its actions.
* It interacts with FortiClient EMS to get endpoint information and update the FortiAnalyzer Asset and Identity database.
References:
Fortinet Documentation on Playbook Actions and Connectors.
FortiAnalyzer and FortiClient EMS Integration Guides.

NEW QUESTION # 60
Your company is doing a security audit To pass the audit, you must take an inventory of all software and applications running on all Windows devices Which FortiAnalyzer connector must you use?

- A. FortiClient EMS
- B. FortiCASB
- C. Local Host
- D. ServiceNow

Answer: A

Explanation:
* Requirement Analysis:
* The objective is to inventory all software and applications running on all Windows devices within the organization.
* This inventory must be comprehensive and accurate to pass the security audit.
* Key Components:
* FortiClient EMS (Endpoint Management Server):
* FortiClient EMS provides centralized management of endpoint security, including software and application inventory on Windows devices.
* It allows administrators to monitor, manage, and report on all endpoints protected by FortiClient.
* Connector Options:
* FortiClient EMS:
* Best suited for managing and reporting on endpoint software and applications.
* Provides detailed inventory reports for all managed endpoints.

* Selected as it directly addresses the requirement of taking inventory of software and applications on Windows devices.
* ServiceNow:
* Primarily a service management platform.
* While it can be used for asset management, it is not specifically tailored for endpoint software inventory.
* Not selected as it does not provide direct endpoint inventory management.
* FortiCASB:
* Focuses on cloud access security and monitoring SaaS applications.
* Not applicable for managing or inventorying endpoint software.
* Not selected as it is not related to endpoint software inventory.
* Local Host:
* Refers to handling events and logs within FortiAnalyzer itself.
* Not specific enough for detailed endpoint software inventory.
* Not selected as it does not provide the required endpoint inventory capabilities.
* Implementation Steps:
* Step 1: Ensure all Windows devices are managed by FortiClient and connected to FortiClient EMS.
* Step 2: Use FortiClient EMS to collect and report on the software and applications installed on these devices.
* Step 3: Generate inventory reports from FortiClient EMS to meet the audit requirements.
Fortinet Documentation on FortiClient EMS FortiClient EMS Administration Guide By using the FortiClient EMS connector, you can effectively inventory all software and applications on Windows devices, ensuring compliance with the security audit requirements.

NEW QUESTION # 61
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. Local connector
- B. FortiClient EMS connector
- C. FortiSandbox connector
- D. FortiMail connector

Answer: C

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.
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 # 62
.....

- techonpage.com, deacontjhn261830.blogs100.com, aliviavkrs742750.blog-mall.com, zaynwjca698126.qodsblog.com, prestonedib434428.tkzblog.com, fraserlkfl678771.blogs100.com, prestonevyr909393.digitollblog.com, francesyxrt018346.wikikali.com, tomasxhvq389026.atualblog.com, iwantqoe827209.wikigiogio.com, Disposable vapes

What's more, part of that Free4Torrent NSE7_SOC_AR-7.6 dumps now are free: https://drive.google.com/open?id=1rqNPxQp7uWuq0X0gWDE9bGbbXMD8ak7L