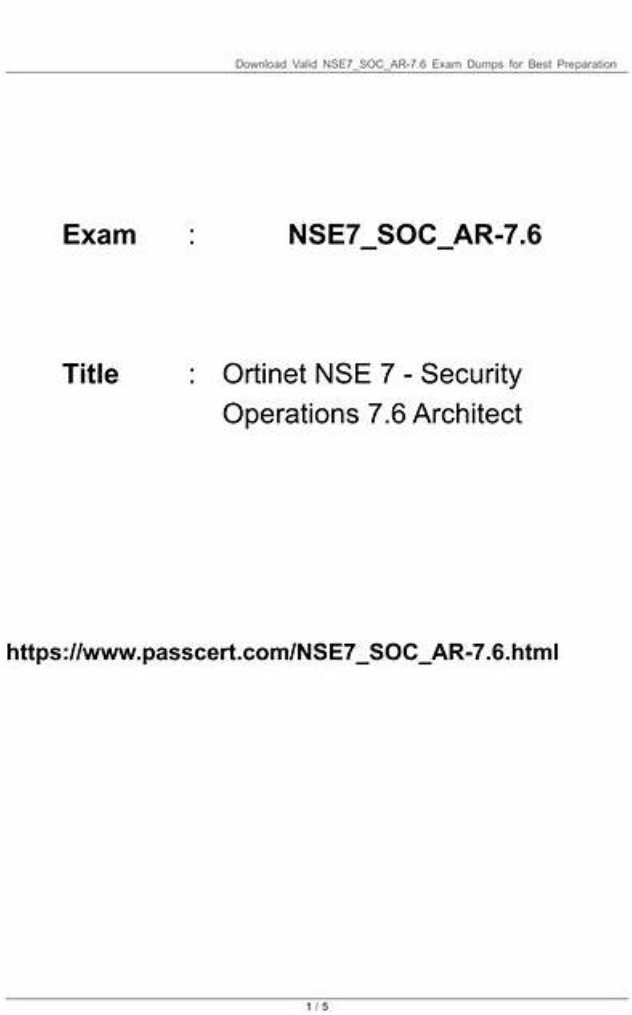
検証するNSE7_SOC_AR-7.6｜ハイパスレートのNSE7_SOC_AR-7.6日本語問題集試験｜試験の準備方法Fortinet NSE 7 - Security Operations 7.6 Architect復習範囲



BONUS！！！ MogiExam NSE7_SOC_AR-7.6ダンプの一部を無料でダウンロード：https://drive.google.com/open?id=1xbu4UqXjG8IISQa3ebqZce7UxQtboNjl

NSE7_SOC_AR-7.6学習教材は、業界の経験豊富な専門家によって作成されているため、品質と効率を保証できます。 NSE7_SOC_AR-7.6学習ガイドの内容は、常に命題法に準拠しています。最良のリファレンスとは言えませんが、あなたを失望させないでしょう。私たちは、試験に合格し、認定資格を取得することに熱心な受験者に最適です。 NSE7_SOC_AR-7.6の実際の試験は、証明書を取得するという夢を実現するのに役立ちます。

Fortinet NSE7_SOC_AR-7.6 認定試験の出題範囲：

トピック	出題範囲
トピック 1	• Detection Capabilities: Focuses on configuring FortiSIEM incident rules, building log queries, and analyzing incidents for effective threat detection.

トピック 2	• SOAR Playbook Development: Covers configuring playbooks and connectors, using Jinja filters for data handling, and troubleshooting FortiSOAR automation workflows.
トピック 3	• SOAR Incident Handling and Threat Hunting: Includes threat hunting analysis, managing FortiSOAR incidents, workload coordination, and using war rooms for incident response.
トピック 4	• SOC Concepts and Frameworks: Covers analyzing security incidents, identifying adversary behaviors, understanding Fortinet SOC architecture, and recognizing common attack vectors.

>> NSE7_SOC_AR-7.6日本語問題集 <<

NSE7_SOC_AR-7.6試験の準備方法｜信頼的なNSE7_SOC_AR-7.6日本語問題集試験｜有効的なFortinet NSE 7 - Security Operations 7.6 Architect復習範囲

最短時間でNSE7_SOC_AR-7.6試験に合格し、関連する認定資格を取得する場合、当社のNSE7_SOC_AR-7.6トレーニング資料を選択することは、すべての人々の利益になります。あなたのNSE7_SOC_AR-7.6試験に合格し、想像を超える最短時間で関連する認定資格を取得することが非常に簡単になることを確認できます。ウェブからNSE7_SOC_AR-7.6認定トレーニング資料の手順を知ることができます。また、NSE7_SOC_AR-7.6試験問題のデモを無料でダウンロードして、支払い前に確認することもできます。

Fortinet NSE 7 - Security Operations 7.6 Architect 認定 NSE7_SOC_AR-7.6 試験問題 (Q47-Q52):

質問 # 47
When you use a manual trigger to save user input as a variable, what is the correct Jinja expression to reference the variable? (Choose one answer)

- A. {{ vars.item.<variable_name> }}
- B. {{ vars.input.params.<variable_name> }}
- C. {{ vars.steps.<variable_name> }}
- D. {{ globalVars.<variable_name> }}

正解：B

解説：
Comprehensive and Detailed Explanation From FortiSOAR 7.6., FortiSIEM 7.3 Exact Extract study guide:
InFortiSOAR 7.6, the playbook engine utilizes Jinja2 expressions to handle dynamic data. When a playbook is configured with aManual Trigger, the administrator can define input fields (such as text, picklists, or checkboxes) that an analyst must fill out when executing the playbook from a record.
* Input Parameter Mapping:Any data entered by the user during this manual trigger phase is automatically mapped to the input.params dictionary within the vars object. Therefore, the syntax to retrieve a specific input value is {{ vars.input.params.variable_name }}.
* Scope of Variables:This specific path ensures that the variable is pulled from the initial user input rather than from the output of a subsequent step (vars.steps) or a globally defined variable (globalVars).

質問 # 48
Refer to the exhibits.
What can you conclude from analyzing the data using the threat hunting module?

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

正解：C

解説：
* 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.

質問 # 49
Refer to the exhibits.
You configured a custom event handler and an associated rule to generate events whenever FortiMail detects spam emails.
However, you notice that the event handler is generating events for both spam emails and clean emails.
Which change must you make in the rule so that it detects only spam emails?

- A. In the Log filter by Text field, type type==spam.
- B. In the Log Type field, select Anti-Spam Log (spam)
- C. Disable the rule to use the filter in the data selector to create the event.
- D. In the Trigger an event when field, select Within a group, the log field Spam Name (snane) has 2 or more unique values.

正解：B

解説：
* Understanding the Custom Event Handler Configuration:
* The event handler is set up to generate events based on specific log data.
* The goal is to generate events specifically for spam emails detected by FortiMail.
* Analyzing the Issue:
* The event handler is currently generating events for both spam emails and clean emails.
* This indicates that the rule's filtering criteria are not correctly distinguishing between spam and non-spam emails.
* Evaluating the Options:
* Option A:Selecting the "Anti-Spam Log (spam)" in the Log Type field will ensure that only logs related to spam emails are considered. This is the most straightforward and accurate way to filter for spam emails.
* Option B:Typing type==spam in the Log filter by Text field might help filter the logs, but it is not as direct and reliable as selecting the correct log type.
* Option C:Disabling the rule to use the filter in the data selector to create the event does not address the issue of filtering for spam logs specifically.
* Option D:Selecting "Within a group, the log field Spam Name (snane) has 2 or more unique values" is not directly relevant to filtering spam logs and could lead to incorrect filtering criteria.

* Conclusion:
* The correct change to make in the rule is to select "Anti-Spam Log (spam)" in the Log Type field. This ensures that the event handler only generates events for spam emails.
References:
Fortinet Documentation on Event Handlers and Log Types.
Best Practices for Configuring FortiMail Anti-Spam Settings.

質問 # 50
Refer to the exhibit.

You must configure the FortiGate connector to allow FortiSOAR to perform actions on a firewall. However, the connection fails. Which two configurations are required? (Choose two answers)

- A. HTTPS must be enabled on the FortiGate interface that FortiSOAR will communicate with.
- B. Trusted hosts must be enabled and the FortiSOAR IP address must be permitted.
- C. The VDOM name must be specified, or set to VDOM_1, if VDOMs are not enabled on FortiGate.
- D. An API administrator must be created on FortiGate with the appropriate profile, along with a generated API key to configure on the connector.

正解：A、D

解説：
Comprehensive and Detailed Explanation From FortiSOAR 7.6., FortiSIEM 7.3 Exact Extract study guide:
To establish a successful integration betweenFortiSOAR 7.6and aFortiGatefirewall via the FortiGate connector, specific administrative and network requirements must be met on the FortiGate side:
* API Administrator and Key (D):FortiSOAR does not use standard UI login credentials. Instead, it requires aREST API Administratoraccount to be created on the FortiGate. This account must be assigned an administrative profile with the necessary permissions (e.g., Read/Write for Firewall policies or Address objects). Upon creation, the FortiGate generates a uniqueAPI Key, which must be entered into the "API Key" field of the FortiSOAR configuration wizard as shown in the exhibit.
* HTTPS Management Access (C):The connector communicates with the FortiGate using REST API calls overHTTPS(port 443 by default). Therefore, the physical or logical interface on the FortiGate that corresponds to the "Hostname" IP (172.16.200.1) must haveHTTPSenabled under "Administrative Access" in its network settings. If HTTPS is disabled, the connection will time out or be

refused.
Why other options are incorrect:
* Trusted hosts (A):While it is a best practice to restrict API access to specific IPs (like the FortiSOAR IP), the integration can technically function without "Trusted hosts" enabled if the network allows the traffic. However, theabsenceof an API key or HTTPS access will definitively cause a failure regardless of trusted host settings.
* VDOM name (B):In the exhibit, the VDOM field contains multiple values ("VDOM_1", "VDOM_2").
If VDOMs are disabled on the FortiGate, this field should generally be left blank or set to the default "root." Setting it specifically to "VDOM_1" when VDOMs are disabled is not a universal requirement for connectivity; the primary handshake depends on the API key and HTTPS connectivity.

質問 # 51
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. FortiClient EMS connector
- B. Local connector
- C. FortiSandbox connector
- D. FortiMail connector

正解：C

解説：
* 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.

質問 # 52
.....

Fortinet認証に伴って、この認証の重要性を発見する人が多くなっています。最近仕事を探すのは難しいですが、NSE7_SOC_AR-7.6認証を取得して、あなたの就職チャンスを増加することができます。あなたは試験に合格したいなら、我々のNSE7_SOC_AR-7.6問題集を利用することができます。