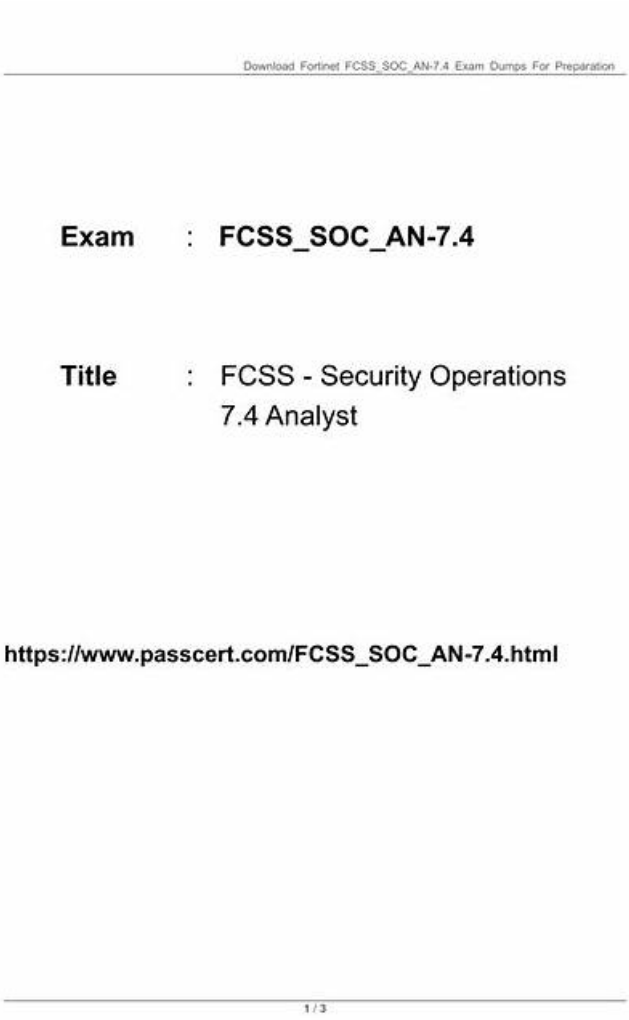
# FCSS_SOC_AN-7.4 Exam Dumps.zip - High Pass-Rate Fortinet FCSS - Security Operations 7.4 Analyst - Study FCSS_SOC_AN-7.4 Center




DOWNLOAD the newest ITexamReview FCSS_SOC_AN-7.4 PDF dumps from Cloud Storage for free: https://drive.google.com/open?id=150UJQn9tM8p6GuegpzyMIsdqaNIcSk07

The FCSS_SOC_AN-7.4 latest exam torrents have different classifications for different qualification examinations, which can enable students to choose their own learning mode for themselves according to the actual needs of users. The FCSS_SOC_AN-7.4 exam questions offer a variety of learning modes for users to choose from, which can be used for multiple clients of computers and mobile phones to study online, as well as to print and print data for offline consolidation. Our reasonable price and FCSS_SOC_AN-7.4 Latest Exam torrents supporting practice perfectly, you will only love our FCSS_SOC_AN-7.4 exam questions.

## Fortinet FCSS_SOC_AN-7.4 Exam Syllabus Topics:

| Topic | Details |
|---|---|
| Topic 1 | • SOC automation: This section of the exam measures the skills of target professionals in the implementation of automated processes within a SOC. It emphasizes configuring playbook triggers and tasks, which are crucial for streamlining incident response. Candidates should be able to configure and manage connectors, facilitating integration between different security tools and systems. |

| | |
|---|---|
| Topic 2 | • Architecture and detection capabilities: This section of the exam measures the skills of SOC analysts in the designing and managing of FortiAnalyzer deployments. It emphasizes configuring and managing collectors and analyzers, which are essential for gathering and processing security data. |
| Topic 3 | • SOC concepts and adversary behavior: This section of the exam measures the skills of Security Operations Analysts and covers fundamental concepts of Security Operations Centers and adversary behavior. It focuses on analyzing security incidents and identifying adversary behaviors. Candidates are expected to demonstrate proficiency in mapping adversary behaviors to MITRE ATT&CK tactics and techniques, which aid in understanding and categorizing cyber threats. |
| Topic 4 | • SOC operation: This section of the exam measures the skills of SOC professionals and covers the day-to-day activities within a Security Operations Center. It focuses on configuring and managing event handlers, a key skill for processing and responding to security alerts. Candidates are expected to demonstrate proficiency in analyzing and managing events and incidents, as well as analyzing threat-hunting information feeds. |



## Study FCSS_SOC_AN-7.4 Center - FCSS_SOC_AN-7.4 Exam Objectives

Our FCSS_SOC_AN-7.4 study materials are different from common study materials, which can motivate you to concentrate on study. Up to now, many people have successfully passed the FCSS_SOC_AN-7.4 exam with our assistance. So you need to be brave enough to have a try. We can guarantee that you will love learning our FCSS_SOC_AN-7.4 Preparation engine as long as you have a try on it. And you can free download the demos of our FCSS_SOC_AN-7.4 learning guide on our website, it is easy, fast and convenient.

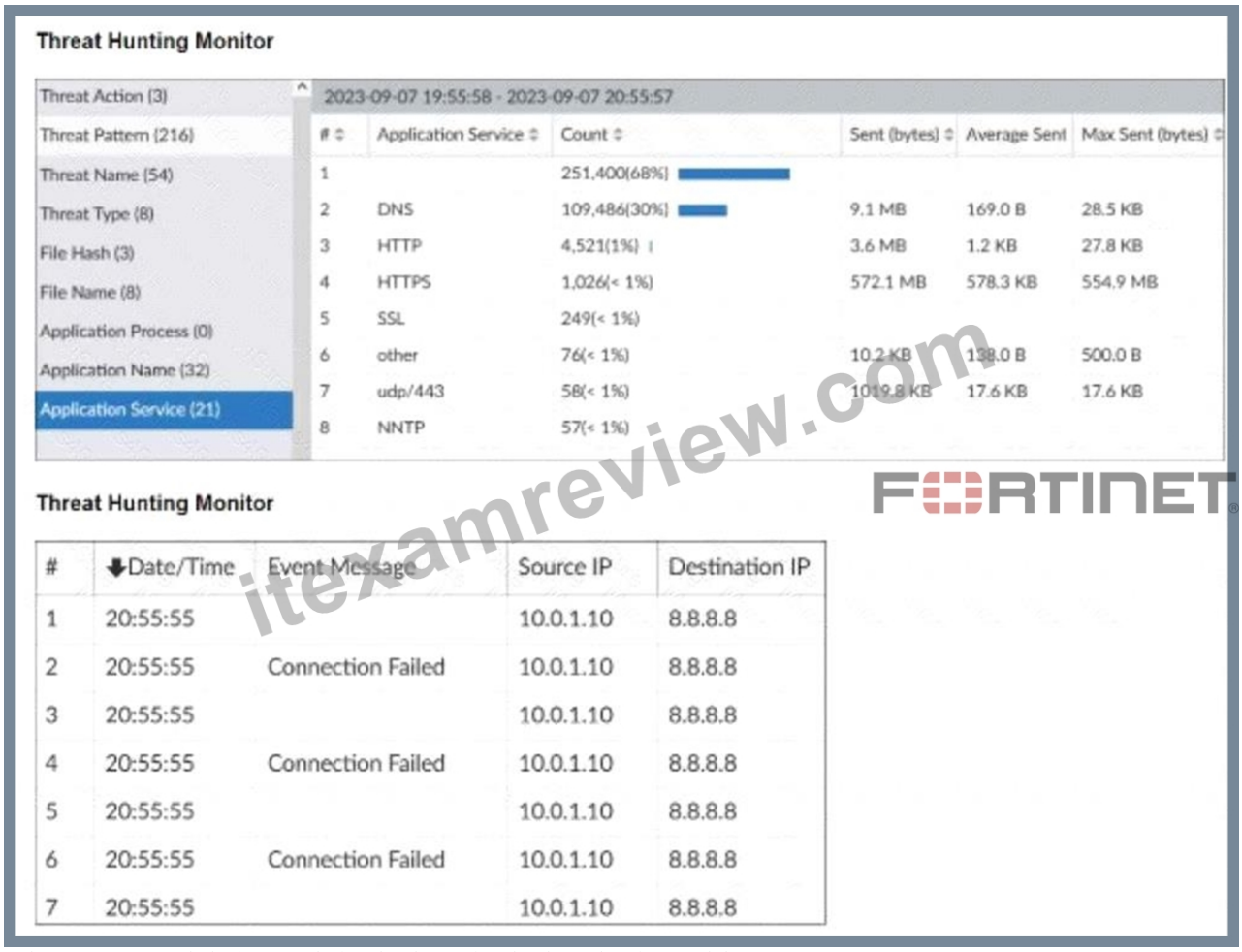
## Fortinet FCSS - Security Operations 7.4 Analyst Sample Questions (Q29-Q34):

**NEW QUESTION # 29**
How do playbook templates benefit SOC operations?

- A. By providing standardized responses to common security scenarios
- B. By increasing the complexity of incident response
- C. By serving as a decorative element in the SOC
- D. By reducing the need for IT personnel

**Answer: A**

**NEW QUESTION # 30**
Refer to the exhibits.





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

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

**Answer: A**

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 # 31**
Which two types of variables can you use in playbook tasks? (Choose two.)

- A. Trigger
- B. Create
- C. Output
- D. input

**Answer: C,D**

Explanation:
Understanding Playbook Variables:
Playbook tasks in Security Operations Center (SOC) playbooks use variables to pass and manipulate data between different steps in the automation process.
Variables help in dynamically handling data, making the playbook more flexible and adaptive to different scenarios.
Types of Variables:
Input Variables:
Input variables are used to provide data to a playbook task. These variables can be set manually or derived from previous tasks.
They act as parameters that the task will use to perform its operations.
Output Variables:
Output variables store the result of a playbook task. These variables can then be used as inputs for subsequent tasks.
They capture the outcome of the task's execution, allowing for the dynamic flow of information through the playbook.
Other Options:
Create: Not typically referred to as a type of variable in playbook tasks. It might refer to an action but not a variable type.
Trigger: Refers to the initiation mechanism of the playbook or task (e.g., an event trigger), not a type of variable.
Conclusion:
The two types of variables used in playbook tasks are input and output.
Reference: Fortinet Documentation on Playbook Configuration and Variable Usage.
General SOC Automation and Orchestration Practices.

**NEW QUESTION # 32**
When configuring playbook triggers, what factor is essential to optimize the efficiency of automated responses?

- A. The geographical location of the SOC
- B. The number of pages in the playbook
- C. The color scheme of the playbook interface
- D. The timing and conditions under which the playbook is triggered

**Answer: D**

**NEW QUESTION # 33**
What should be a priority when configuring playbook tasks to ensure effective SOC automation?

- A. Ensuring tasks are scheduled during office hours only
- B. Limiting tasks to non-critical alerts
- C. Making tasks visible to external stakeholders
- D. Aligning tasks with the specific stages of incident response

**Answer: D**

**NEW QUESTION # 34**

.....

Being a social elite and making achievements in your own field may be the dream of all people. However, only a very few people seize the initiative in their life. Perhaps our research data will give you some help. As long as you spend less time on the game and spend more time on learning, the FCSS_SOC_AN-7.4 study materials can reduce your pressure so that users can feel relaxed and confident during the preparation and certification process. It is believed that many users have heard of the FCSS_SOC_AN-7.4 Study Materials from their respective friends or news stories. So why don't you take this step and try? You will not regret your wise choice.