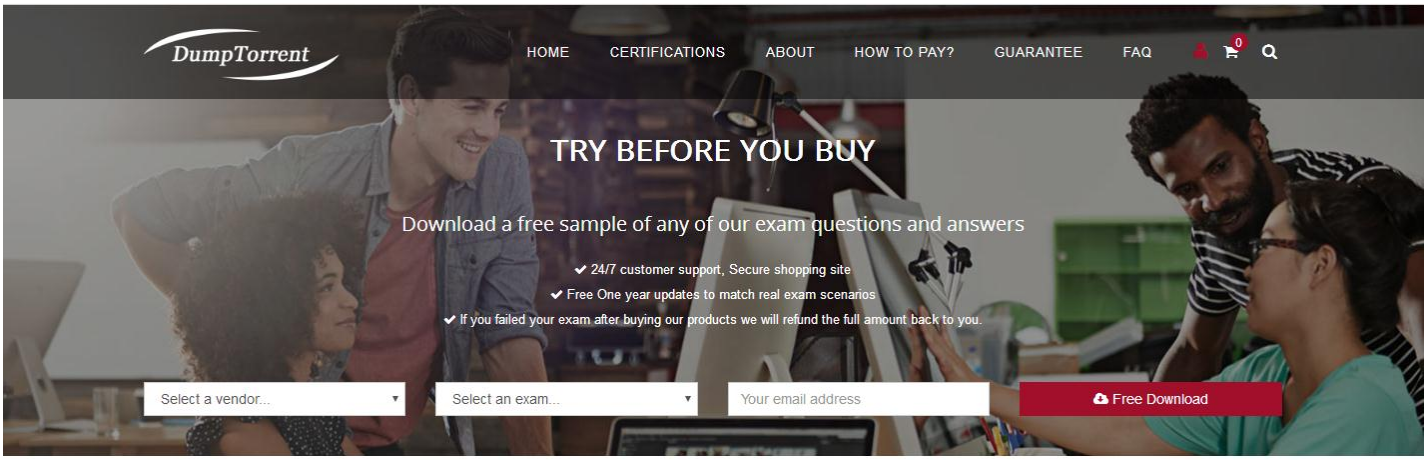
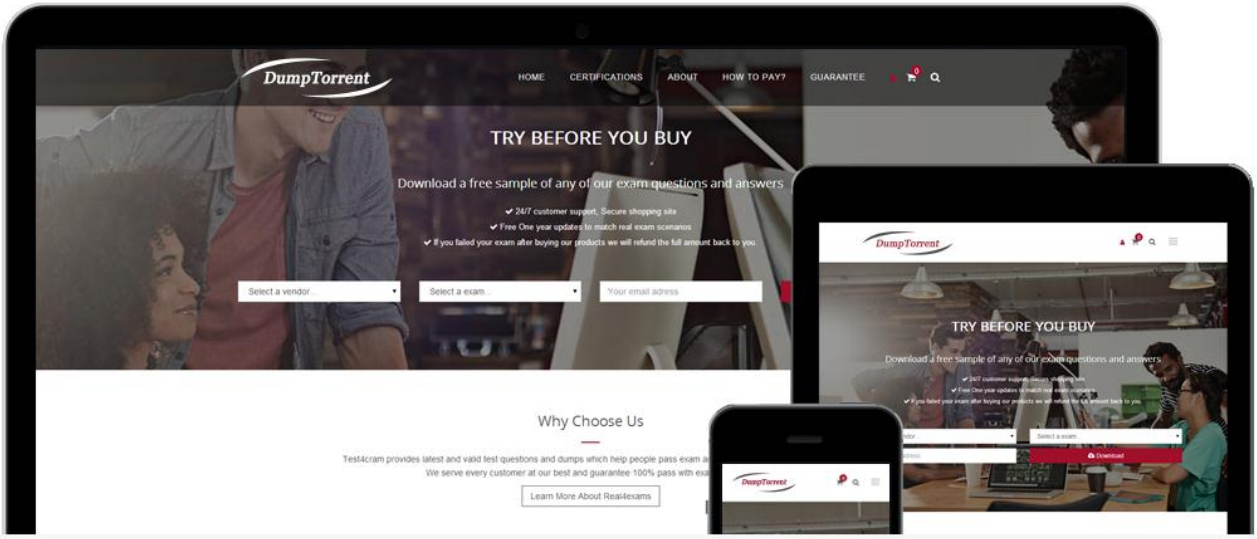
DumpTorrent





QUALITY AND VALUE

ExamsTorrent Practice Exams are written to the highest standards of technical accuracy, using only certified subject matter experts and published authors for development - no all vce.

TESTED AND APPROVED

We are committed to the process of vendor and third party approvals. We believe professionals and executives alike deserve the confidence of quality coverage these authorizations provide.

EASY TO PASS

If you prepare for the exams using our ExamsTorrent testing engine, It is easy to succeed for all certifications in the first attempt. You don't have to deal with all dumps or any free torrent / rapidshare all stuff.

TRY BEFORE BUY

ExamsTorrent offers free demo of each product. You can check out the interface, question quality and usability of our practice exams before you decide to buy.

http://www.dumptorrent.com

High-quality Exam Torrent & Valid Test Dumps & Reliable Guide Torrent

Exam : **FCSS_SOC_AN-7.4**

Title : FCSS - Security Operations 7.4 Analyst

Vendor : Fortinet

Version : DEMO

NO.1 In monitoring SOC playbooks, what is a critical indicator of a need for updates or adjustments?
A. A decrease in coffee consumption by SOC staff
B. An increase in unresolved security alerts
C. The number of visitors to the SOC
D. The frequency of team-building activities
Answer: B

NO.2 What is the advantage of integrating advanced analytics in the management of events and incidents in a SOC?
A. It reduces the necessity for manual data processing.
B. It increases the workload on SOC analysts.
C. It diminishes the importance of cybersecurity.
D. It focuses on marketing data analysis.
Answer: A

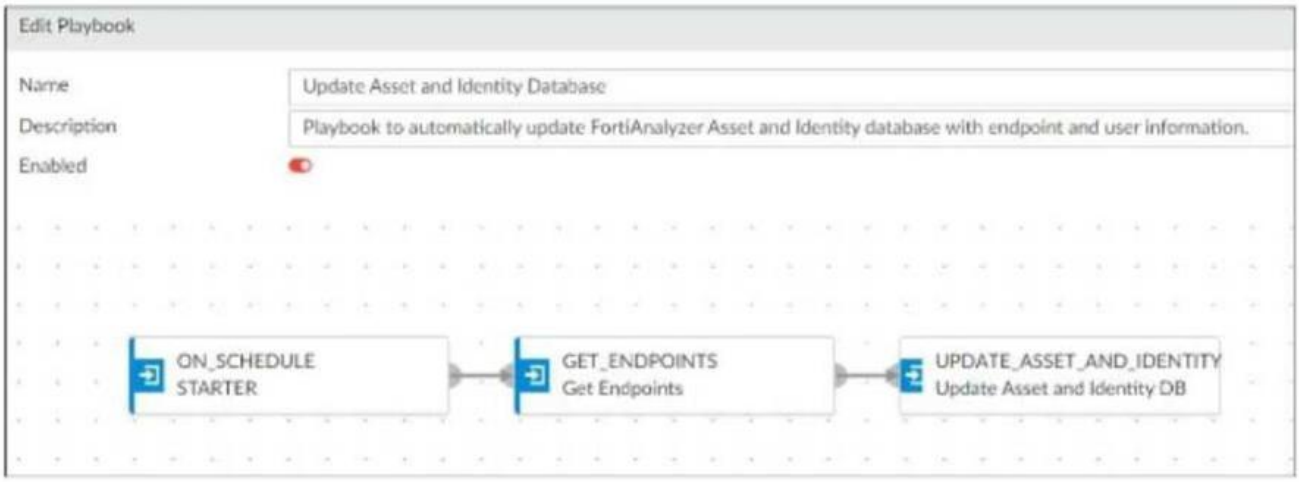
NO.3 Which FortiAnalyzer connector can you use to run automation stitches9
A. FortiCASB
B. FortiMail
C. Local
D. FortiOS
Answer: D
Explanation:
Overview of Automation Stitches:
Automation stitches in FortiAnalyzer are predefined sets of automated actions triggered by specific events. These actions help 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.
Reference: Fortinet FortiCASB Documentation FortiCASB
FortiMail:
FortiMail is an email security solution. While it can send logs and events to FortiAnalyzer, it is not primarily used for running automation stitches.
Reference: Fortinet FortiMail Documentation FortiMail
Local:
The local connector refers to FortiAnalyzer's ability to handle logs and events generated by itself. This is useful for internal processes but not specifically for integrating with other Fortinet devices for automation stitches.
Reference: Fortinet FortiAnalyzer Administration Guide FortiAnalyzer Local FortiOS:

FortiOS is the operating system that runs on FortiGate firewalls. FortiAnalyzer can use the FortiOS connector to communicate with FortiGate devices and run automation stitches. This allows FortiAnalyzer to send commands to FortiGate, triggering predefined actions in response to specific events.
Reference: Fortinet FortiOS Administration Guide FortiOS Detailed Process:
Step 1: Configure the FortiOS connector in FortiAnalyzer to establish communication with FortiGate devices.
Step 2: Define automation stitches within FortiAnalyzer that specify the actions to be taken when certain events occur.
Step 3: When a triggering event is detected, FortiAnalyzer uses the FortiOS connector to send the necessary commands to the FortiGate device.
Step 4: FortiGate executes the commands, performing the predefined actions such as blocking an IP address, updating firewall rules, or sending alerts. Conclusion:
The FortiOS connector is specifically designed for integration with FortiGate devices, enabling FortiAnalyzer to execute automation stitches effectively.
Reference: Fortinet FortiOS Administration Guide: Details on configuring and using automation stitches.
Fortinet FortiAnalyzer Administration Guide: Information on connectors and integration options.
By utilizing the FortiOS connector, FortiAnalyzer can run automation stitches to enhance the security posture and response capabilities within a network.

NO.4 A key benefit of mapping adversary behaviors to MITRE ATT&CK tactics in SOC operations is:
A. Decreasing the dependency on external consultants
B. Enhancing preventive security measures
C. Streamlining software development processes
D. Improving public relations
Answer: B

NO.5 What is a key consideration when managing playbook templates for SOC automation?
A. The color coordination of playbook interfaces
B. The comprehensiveness and adaptability of the templates
C. The entertainment value of playbook simulations
D. The popularity of templates among SOC analysts
Answer: B

NO.6 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 a local connector.

B. The playbook is using a FortiMail connector.

C. The playbook is using an on-demand trigger.

D. The playbook is using a FortiClient EMS connector.

Answer: A 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.

Reference: Fortinet Documentation on Playbook Actions and Connectors.

FortiAnalyzer and FortiClient EMS Integration Guides.

NO.7 You are tasked with configuring automation to quarantine infected endpoints.
Which two Fortinet SOC components can work together to fulfill this task?
(Choose two.)
A. FortiAnalyzer
B. FortiClient EMS
C. FortiMail
D. FortiSandbox
Answer: A B

NO.8 Which feature is most important when selecting a connector for integration into a SOC playbook?
A. The ability to display colorful graphics
B. The compatibility with existing security infrastructure
C. The connector's country of origin
D. The size of the connector's installation file
Answer: B

NO.9 Which two assets are available with the outbreak alert licensed feature on FortiAnalyzer?
(Choose two.)
A. Custom event handlers from FortiGuard
B. Outbreak-specific custom playbooks
C. Custom connectors from FortiGuard
D. Custom outbreak reports
Answer: A D