Number: NSE6_FSR-7.3
Passing Score: 800
Time Limit: 120
File Version: 4.0

Exam Code: NSE6_FSR-7.3

Exam Name: Fortinet NSE 6 - FortiSOAR 7.3 Administrator

Exam A

QUESTION 1
Which two statements about upgrading a FortiSOAR HA cluster are true7 (Choose two.)

A. Nodes can be upgraded while the primary node or secondary node are in the HA cluster.
B. Upgrading a FortiSOAR HA cluster requires no downtime.
C. The upgrade procedure for an active-active cluster and an active-passive cluster are the same.
D. It is recommended that the passive secondary node be upgraded first, and then the active primary node.

Correct Answer: C, D
Section:
Explanation:
Upgrading a FortiSOAR HA cluster follows the same procedure regardless of whether it is configured in an active-active or active-passive setup. The process generally involves upgrading one node at a time to minimize service disruption. Best practices recommend upgrading the passive secondary node first before moving to the active primary node. This sequence helps maintain cluster stability and ensures that at least one node remains operational during the upgrade.

QUESTION 2
Which SMS vendor does FortiSOAR support for two-factor authentication?

A. Twilio
B. Google Authenticator
C. 2factor
D. Telesign

Correct Answer: D
Section:
Explanation:
For two-factor authentication (2FA) via SMS, FortiSOAR supports integration with Telesign. This vendor provides SMS-based 2FA services, enabling FortiSOAR to leverage Telesign's API for sending verification codes as part of its security features. Telesign's service is compatible with FortiSOAR, ensuring secure user authentication when accessing the platform or certain features.

QUESTION 3
Which three actions can be performed from within the war room? (Choose three)

A. View graphical representation of all records linked to an incident in the Artifacts lab
B. Change the room's status to Escalated to enforce hourly updates.
C. Investigate issues by tagging results as evidence.
D. Use the Task Manager tab to create, manage, assign, and track tasks.
E. Integrate a third-party instant messenger directly into the collaboration workspace.

Correct Answer: A, C, D
Section:
Explanation:
In FortiSOAR's War Room, users can perform several actions to manage incidents effectively. They can view a graphical representation of records linked to an incident in the Artifacts lab, which helps visualize connections and dependencies. Additionally, the War Room supports tagging investigation results as evidence, allowing for a structured approach to incident documentation. Users can also manage tasks via the Task Manager tab, facilitating

task creation, assignment, and tracking within the incident response workflow.

QUESTION 4
Several users have informed you that the FortiSOAR GUI Is not reachable. When troubleshooting, which step should you take first?

A. Enter the csadm license --show-details command to check if there is a duplicate license.
B. Enter the csadm services --restart ngiax command to restart only the Nginx process.
C. Enter the systemct1 status nginx command to gather more information.
D. Review the connecters.log file to see what is happening to the HTTPS connections.

Correct Answer: C
Section:
Explanation:
When troubleshooting the issue of the FortiSOAR GUI not being reachable, the first step should be to check the status of the nginx service, which is responsible for managing web requests. Using the command systemctl status nginx will provide information on whether the service is running and any potential issues or errors related to it. This approach is more efficient as it directly addresses the service responsible for the web interface, making it possible to diagnose and resolve common issues such as service failure, configuration errors, or connectivity problems.

QUESTION 5
Which log file contains license synchronization logs on FortiSOAR?

A. fdn.log
B. beat.log
C. celery.log
D. falcon.log

Correct Answer: A
Section:
Explanation:
The fdn.log file in FortiSOAR contains logs related to license synchronization activities. This log file records events and errors associated with license checks and synchronization with Fortinet's licensing servers, ensuring that the FortiSOAR instance remains compliant with licensing requirements. Monitoring fdn.log can help administrators troubleshoot issues related to license synchronization and ensure the system operates within the licensed limits.

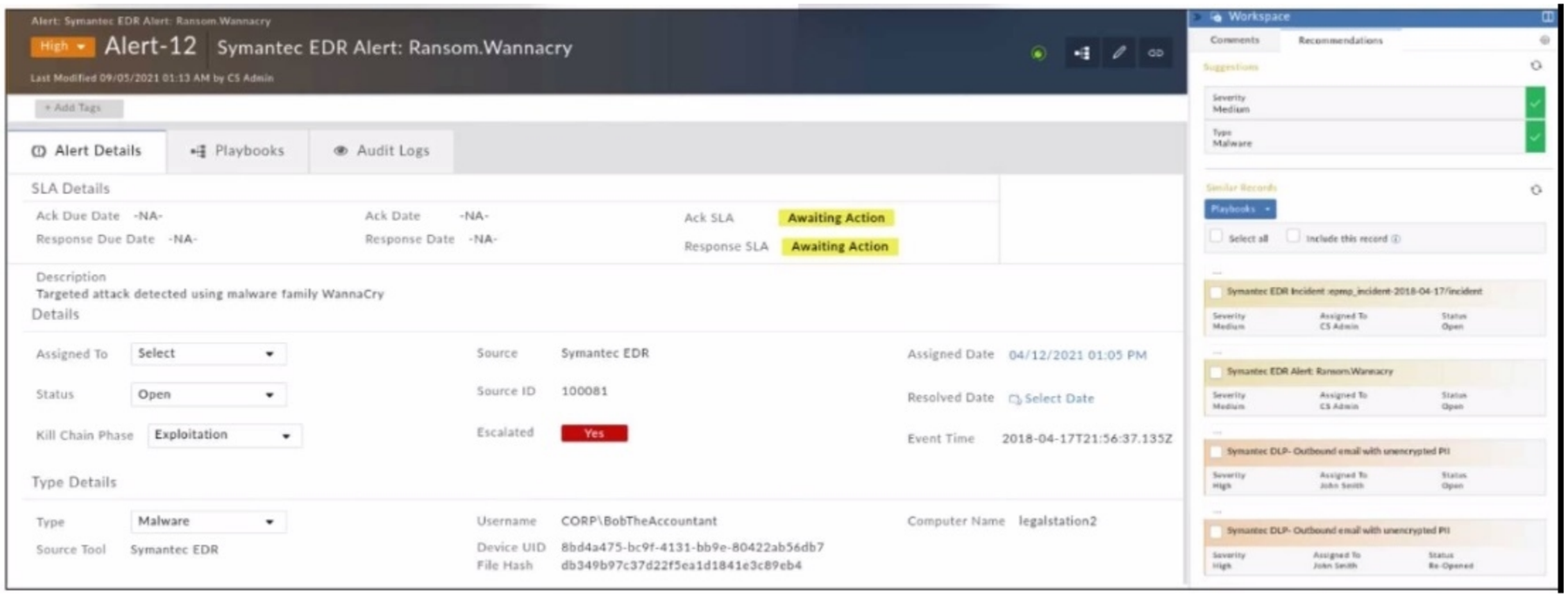
QUESTION 6
Which playbook collection includes system-level playbooks that FortiSOAR uses to auto-populate date fields when the status of incident or alert records changes to Resolved or Closed?

A. SLA Management Playbooks
B. Utilities Playbooks
C. Schedule Management Playbooks
D. Approval/Manual Task Playbooks

Correct Answer: A
Section:
Explanation:
The SLA Management Playbooks collection in FortiSOAR includes system-level playbooks designed to auto-populate date fields when the status of incident or alert records changes to Resolved or Closed. This functionality ensures that relevant date fields, such as resolution date or closure date, are accurately filled based on SLA criteria. By using SLA Management Playbooks, FortiSOAR automatically maintains date-related data integrity, which is essential for tracking and reporting purposes.

QUESTION 7

Refer to the exhibit.

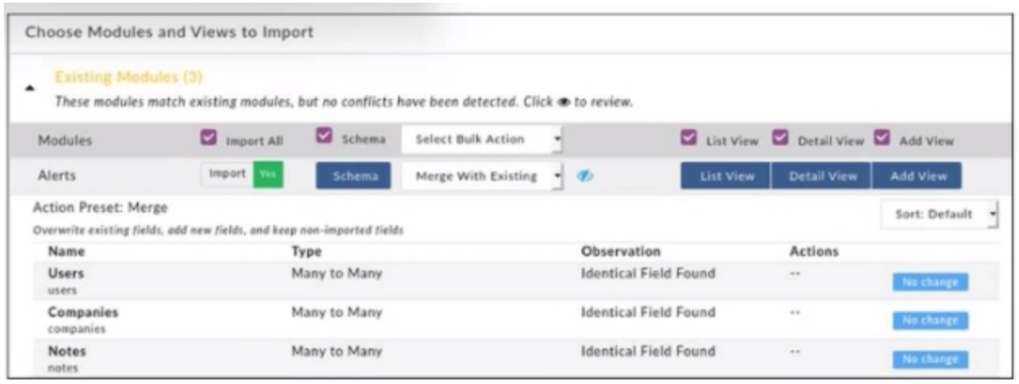


Which two statements about the recommendation engine are true? (Choose two.)

A. There are no playbooks that can be run on the recommended alerts using the recommendation panel
B. The dataset is trained to predict the Severity and Type fields.
C. The recommendation engine is set to automatically accept suggestions.
D. The alert severity is High, but the recommendation is for it to be set to Medium

Correct Answer: B, D
Section:
Explanation:
The Recommendation Engine in FortiSOAR is designed to assist in alert triage by suggesting values for certain fields based on historical data and machine learning models. In this case, the engine is trained to predict both the Severity and Type fields, suggesting values that align with past incidents and threat intelligence. Although the current alert severity is High, the recommendation engine has suggested adjusting it to Medium based on the pattern of similar past alerts, indicating a less critical threat level than initially perceived. This functionality helps analysts by providing data-driven insights, which can optimize alert handling and resource allocation.

QUESTION 8
Refer to the exhibit.



When importing modules to FortiSOAR using the configuration wizard, what actions are applied to fields it you select Merge with Existing as the Bulk action?

A. Existing fields are kept, new fields are added, and non-imported fields are deleted.
B. Existing Holds are overwritten, now fields are added, and non-imported fields are deleted.
C. Existing fields are kept, new fields are added, and non-imported fields are kept.
D. Existing fields are overwritten, new fields are added, and non-Imported fields are kept.

Correct Answer: D
Section:
Explanation:
When importing modules into FortiSOAR using the configuration wizard and selecting 'Merge with Existing' as the bulk action, the behavior for field handling is as follows: any fields that already exist in the system are overwritten with the imported values. New fields from the imported module are added to the system, while fields that are not part of the imported module remain unaffected and are retained in the system. This option ensures that existing data structures are updated with new information without losing existing, but non-imported, fields.

QUESTION 9
Which service on FortiSOAR is the playbook scheduler?

A. cyops-torccat
B. colcrybeatd
C. celeryd
D. uwsgi

Correct Answer: B
Section:
Explanation:
In FortiSOAR, the service responsible for the playbook scheduling functionality is colcrybeatd. This service manages the timing and execution of scheduled playbooks, allowing for the automation of various tasks at specified intervals. It ensures that playbooks execute according to their configured schedules, which can include tasks such as data ingestion, threat detection, or incident response actions. Proper functioning of this service is essential for the reliable automation of time-dependent processes within FortiSOAR.

QUESTION 10
A security analyst has reported unauthorized access to System Configuration. You must review the user's current level of access, and then restrict their access according to your organization's requirements. As part of your auditing process, which two actions should you perform? (Choose two.)

A. Remove the create, read, update, and delete (CRUD) permissions or roles that the user does not require.
B. View the user's effective role permissions, and then investigate which role is providing that access.
C. Remove all record ownership that is assigned to the user.

D. Review the user's learn hierarchy to ensure that the appropriate relationships are configured.

Correct Answer: B, D
Section:
Explanation:
To audit and restrict a user's access within FortiSOAR, particularly in response to unauthorized access reports, it's necessary to review the user's effective role permissions. This involves checking which roles grant the user access to the System Configuration module and adjusting as needed. Additionally, reviewing the user's team hierarchy ensures that the user's access aligns with the organization's policies. Misconfigurations in team relationships can sometimes inadvertently provide elevated access; hence, confirming that the team setup is correct is a critical part of the auditing process.

QUESTION 11
An administrator is issuing the following command on a node trying to join a FortiSOAR duster as a standby: csadm ha join-cluster --status active ---role secondary --primary-node 10.0.1.160
The node fails to join the cluster. What is the issue?

A. The role value should be worker.
B. The primary node needs to be resolvable via FQDN.
C. The IP address should be for secondary-node Instead of primary-node.
D. The status value should be passive.

Correct Answer: D
Section:
Explanation:
When joining a FortiSOAR cluster as a standby node, the correct status value should be passive. Using active would imply that the node is trying to join as an active node, which could cause conflicts in the cluster setup. In FortiSOAR, standby nodes must be set as passive to ensure they are recognized correctly and to avoid conflicts with the primary node or other active nodes within the cluster. Therefore, setting the status to passive will resolve the issue and allow the node to join the cluster as intended.

QUESTION 12
When deleting a user account on FortiSOAR, you must enter the user ID in which file on FortiSOAR?

A. userDelete.txt.
B. config_yml
C. scripts
D. usersToDelete.txt

Correct Answer: D
Section:
Explanation:
When deleting a user account in FortiSOAR, the user ID must be entered into the usersToDelete.txt file. This file is specifically used to list users that are marked for deletion. Once the user IDs are listed in this file, the system can process the deletion of these accounts as part of its user management operations. This method ensures that only specified users are deleted, as referenced in FortiSOAR's administrative controls.

QUESTION 13
What are two system-level logs that can be purged using application configuration? (Choose two.)

A. Connector logs
B. Reporting logs
C. Audit togs
D. Executed Playbook logs

Correct Answer: C, D

Section:
Explanation:
In FortiSOAR, system-level logs that can be purged include both 'Audit logs' and 'Executed Playbook logs.' These types of logs can be configured to be purged periodically to free up storage space and ensure that unnecessary logs do not impact system performance. The application configuration allows administrators to schedule automatic purges, which can be especially useful in high-activity environments where log data accumulates quickly. Purging these logs helps maintain a cleaner and more efficient system.

QUESTION 14
When configuring an HA cluster with an externalized PostgreSQL database, which two tiles on the database server need to be configured to trust all FortiSOAR nodes' incoming connections? (Choose two.)

A. pg_hba.conf
B. db_external_config.yml.
C. postgreaq1.conf
D. db_config.yml

Correct Answer: A, C
Section:
Explanation:
In a FortiSOAR High Availability (HA) cluster setup with an externalized PostgreSQL database, it is necessary to configure the database server to allow incoming connections from all FortiSOAR nodes. This configuration involves modifying the pg_hba.conf file to set up host-based authentication and control which IP addresses can connect. The postgresql.conf file must also be adjusted to enable listening on all necessary IP addresses, which is critical for FortiSOAR nodes to connect to the database server securely and reliably. Together, these configurations ensure that all FortiSOAR nodes can access the database, facilitating effective HA functionality.

QUESTION 15
For which two modules on FortiSOAR can you create SLA templates7 (Choose two.)

A. Alerts
B. Indicators
C. Incidents
D. Tasks

Correct Answer: A, B
Section:
Explanation:
In FortiSOAR, SLA (Service Level Agreement) templates can be created for specific modules, including Alerts and Indicators. These templates are essential for tracking response and resolution times, ensuring compliance with defined service levels. By configuring SLAs on the Alerts and Indicators modules, organizations can monitor the time taken to address these items, which is critical in maintaining efficient incident response and management practices. The SLA templates can be customized according to specific business requirements and are applied to records within these modules to enforce timely actions.