ATMIC NETWORKS
YOUR GUIDE TO GLOBAL CERTIFIATION

"Please note that these files may not be up to date. However, the questions will help you understand the exam format and typical question patterns."

www.atmicnetworks .com

Warning: Keep connected with our support team for latest updates

Question: 1

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.

Answer: C

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: 2

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

Answer: C, D

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: 3

The Create Record and Update Record steps are categorized under which playbook step'

A. Evaluate

B. Execute

C. Core

D. Reference

Answer: C

Explanation:

In FortiSOAR playbooks, the "Create Record" and "Update Record" steps are categorized under the "Core" category of playbook steps. Core steps are essential actions that are frequently used in playbooks to interact with records in the FortiSOAR database. They include fundamental operations such as creating, reading, updating, or deleting records within modules. These steps are crucial for the automation of tasks such as data management, where playbooks need to create new entries or update existing data as part of incident response workflows.

Question: 4

When configuring the system proxy on FortiSOAR. which two URLs should be accessible from the proxy server? (Choose two.)

A. https://fortiguard.coin

B. https: //licensing, fortinet .net

C. https://iepo.fortisoar.fcrtinet.ccm

D. https://globalupdate.fortinet.net

Answer: C, D

Explanation:

When configuring the system proxy for FortiSOAR, it is essential to ensure connectivity to certain URLs to maintain system updates and licensing. For FortiSOAR, access to https://iepo.fortisoar.fortinet.com is required for incident enrichment and analysis, while https://globalupdate.fortinet.net is necessary for global updates to keep the system up-to-date with the latest threat information. These connections allow FortiSOAR to communicate with Fortinet's servers to fetch updated threat intelligence and system updates, which are critical for the operational effectiveness of FortiSOAR.

Question: 5

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

Answer: A, C

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: 6

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

A. Alerts

B. Indicators

C. Incidents

D. Tasks

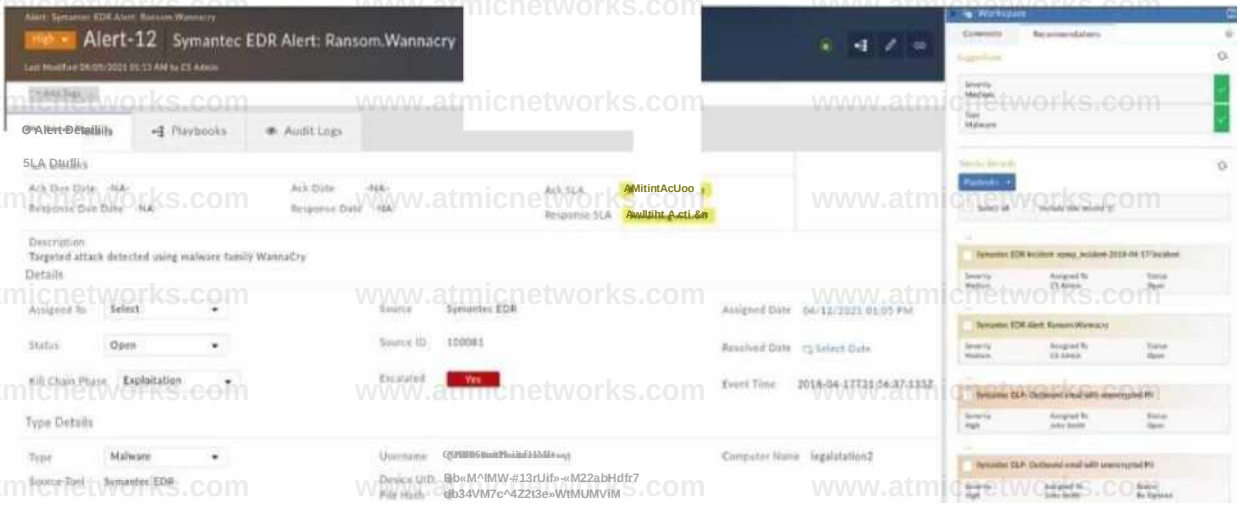
Answer: A, B

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.

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

Answer: B, D

Explanation:

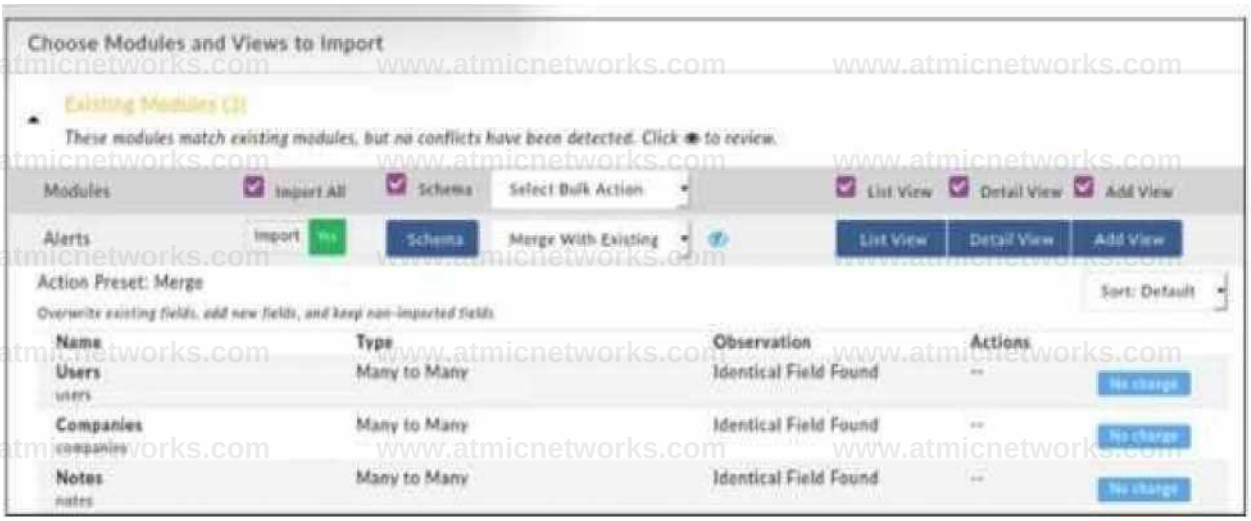
The Recommendation Engine in FortiSOAR is designed to assist in alert triage by suggesting values for certain fields based on historical data and machine learning models. In this case, the engine is

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.

Answer: D

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

Answer: B

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.

Answer: B, D

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.

Answer: D

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

Answer: D

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

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.

Answer: C, D

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: 14

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

A. Twilio

B. Google Authenticator

C. 2factor

D. Telesign

Answer: D

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: 15

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.

Answer: A, C, D

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: 16

Which two statements about appliance users are true? (Choose two.)

A. Appliance users do not have a login ID and do not add to the license count.

B. Appliance users represent non-human users.

C. Appliance users use two-factor authentication for messages sent to the API.

D. Appliance users use time-expiring tokens for primary authentication.

Answer: A, B

Explanation:

In FortiSOAR, appliance users are accounts that represent non-human entities, such as system processes or integrations. These users do not require login IDs and therefore do not contribute to the licensing user count. Appliance users are configured for backend tasks or to interact with external systems, enabling automated processes without consuming standard user licenses. This approach optimizes system resources and keeps licensing costs manageable.

Question: 17

Which two statements about Elasticsearch are true? (Choose two.)

A. Elasticsearch allows you to store, search, and analyze huge volumes of data quickly. In near real time, and return answers in milliseconds.

B. To change the location of your Elasticsearch instance from the local instance to a remote location, you must update the falcon. conf file.

C. The minimum version of the Elasticsearch cluster must be 6.0.2. if you want to externalize the Elasticsearch data.

D. The global search mechanism in FortiSOAR leverages an Elasticsearch database to achieve rapid, efficient searches across the entire record system.

Answer: A, D

Explanation:

Elasticsearch in FortiSOAR is used for its robust data handling capabilities, allowing rapid storage, searching, and analysis of vast amounts of data in near real-time. Its integration with FortiSOAR's global search enables efficient querying across all records, providing quick response times and a seamless user experience. The Elasticsearch database is crucial for handling extensive datasets and delivering swift search results, making it integral to FortiSOAR's performance and data management capabilities.

Question: 18

Refer to the exhibit.

Which statement correctly describes the user's login behavior?

A. The user is sent to a waiting queue if there are named users logged in.

B. The user can log in only if there are enough seats available.

C. The user will always be able to draw from the concurrent pool and log in.

D. The user has an active concurrent session that does not time out.

Answer: B

Explanation:

In FortiSOAR, when a user is configured with "Concurrent" access type, their ability to log in depends on the availability of concurrent user seats. This means the user can only log in if there are available seats in the concurrent pool. If all seats are occupied, the user must wait until a seat becomes free. This configuration allows multiple users to share a pool of licenses, making it suitable for environments where not all users need constant access.

Question: 19

An administrator wants to collect and review all FortiSOAR log tiles to troubleshoot an issue. Which two methods can they use to accomplish this? (Choose two.)

A. Enter the csacta services —status command, and then copy the output.

B. Download the logs from the GUI.

C. Enter the caacta log —collect directory command.

D. Review the contents of /var/log/messages.

Answer: B, C

Explanation:

Administrators can collect and review FortiSOAR logs for troubleshooting in two primary ways. First, they can download logs directly from the GUI, which provides access to various logs through an intuitive interface. Secondly, using the command-line interface, the csacta log --collect command can be used to gather all logs within a specified directory, enabling more detailed ofline analysis. Both methods offer comprehensive log collection to aid in diagnosing and resolving issues.

Question: 20

Which three activities can be achieved using the FortiSOAR queue and shift management feature? (Choose three)

A. Initiate shift handovers

B. Designate a coordinator to monitor queues and shifts

C. Generate shift leads and shift members

D. Set up queue meeting rooms

E. Create queue rules based on matching conditions

Answer: A, C, E

Explanation:

The FortiSOAR queue and shift management feature enables several key activities for managing shifts and queues. Administrators can initiate shift handovers, allowing for smooth transitions between shift leads and members. They can also designate specific roles within shifts, including shift leads and members, to define responsibilities. Additionally, queue rules can be established based on certain conditions, ensuring that incidents and tasks are assigned according to predefined criteria, which helps streamline operations and improve response times.

Question: 21

Refer to the exhibit.

The former primary node was relegated to the secondary rote but is stuck in the Faulted state.

Which two steps must you take to restore operation in the high availability (HA) cluster? (Choose two.)

A. Perform a fire drill to test the database integrity of the node that is in the Faulted state.

B. On the node that is in the Faulted state, enter the csadm ha leave-cluster command.

C. Enter the csadm ha join-cluster command to have the node that is in the Faulted state rejoin the HA cluster as a secondary node.

D. Restart the node that is in the Faulted state to trigger another election.

Answer: B, C

Explanation:

In a FortiSOAR HA cluster, if the former primary node is relegated to a secondary role but is stuck in a Faulted state, it indicates that the node has lost sync or faced a failure during a role change. To restore its functionality, first, you should remove it from the cluster using the csadm ha leave-cluster command. Once it has left the cluster, you can use the csadm ha join-cluster command to re-add the node as a secondary node. This process will allow it to sync back up with the cluster and resume its role as intended.

Question: 22

Which two ports must be open between FortiSOAR HA nodes'* (Choose two.)

A. Port 5432

B. Port 25

C. Port 6380

D. Port 9200

Answer: A, D

Explanation:

In a FortiSOAR HA configuration, certain ports must be open for communication between nodes. Port 5432 is required for PostgreSQL database communication, which is essential for data replication between HA nodes. Port 9200 is used by Elasticsearch, which FortiSOAR leverages for indexing and search functions across the nodes. These ports must be accessible between nodes to ensure seamless operation and data consistency within the cluster.

Question: 23

Which two statements about FortiSOAR virtual instance deployment requirements are true? (Choose two.)

A. FortiSOAR Cloud is a subscription service that allows you to deploy an instance hosted on FortlCloud.

B. There are size limits for the records database, but no charges or fees for storing months or years worth of data.

C. FortiSOAR is supported on VMWare ESXi and Amazon Web Services (AWS).

D. While memory and storage can be added based on requirements, charges are required for every vCPU that is added to the FortiSOAR VM.

Answer: A, C

Explanation:

FortiSOAR offers flexibility in deployment environments, including FortiSOAR Cloud, which is a subscription service that enables hosting on FortiCloud. This provides cloud-hosted management with scalable resources. Additionally, FortiSOAR supports deployment on VMware ESXi and Amazon Web Services (AWS), allowing organizations to choose based on their infrastructure preferences. This flexibility ensures that FortiSOAR can be integrated into various IT environments depending on business needs.

Question: 24

Which CLI command will not work when the PostgreSQL database on FortiSOAR is externalized?

A. csada ha firedrill

B. csadmin ha show-health —all-nodes

C. csadm ha takeover

D. csadm ha export-conf

Answer: A

Explanation:

When the PostgreSQL database is externalized in FortiSOAR, certain HA-related CLI commands become inapplicable. Specifically, the csada ha firedrill command, which is used to test the integrity of the HA cluster by simulating failures, is not applicable in scenarios where the database is managed outside FortiSOAR. Externalizing the database changes how FortiSOAR manages database connections, making some internal commands like firedrill redundant.

Question: 25

Which log file contains license synchronization logs on FortiSOAR?

A. fdn.log

B. beat.log

C. celery.log

D. falcon.log

Answer: A

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: 26

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

Answer: A

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: 27

On FortiSOAR. which default role is used to assign privileges to other teams and is recommended to not be removed?

A. Application Administrator

B. Full App Permissions

C. Playbook Administrator

D. Security Administrator

Answer: A

Explanation:

In FortiSOAR, the "Application Administrator" role is a default role that holds broad privileges, including the ability to assign permissions to other teams. This role is fundamental to system administration and is recommended not to be removed as it provides crucial administrative capabilities. Removing or modifying this role could impact FortiSOAR's ability to manage user roles

and permissions effectively, which could hinder system operations and user management.

Question: 28

Refer to the exhibit.

How long after the syops-ha service goes down will the heartbeat missed notification be sent to the administrator?

A. 15 minutes

B. 60 minutes

C. 5 minutes

D. 3 minutes

Answer: B

Explanation:

In FortiSOAR's high availability (HA) setup, if the cyops-ha service becomes unresponsive, the system is configured to send a "heartbeat missed" notification after a specified period, which in this case is 60 minutes. This delay allows for transient issues to be resolved without triggering immediate alerts,

while also ensuring that administrators are informed of prolonged service disruptions. Timely notifications about the cyops-ha service's status help maintain the reliability and responsiveness of the HA environment.

Question: 29

What are two features of the FortiSOAR perpetual trial license? (Choose two.).

A. It is a multi-tenant type license.

B. It provides access to FortiSOAR for a limited amount of time per day.

C. It has restrictions on the number of users.

D. It has restrictions on the number of actions that can be performed.

Answer: C, D

Explanation:

The FortiSOAR perpetual trial license includes limitations on both the number of users and the number of actions that can be performed. These restrictions are in place to provide prospective users with a functional evaluation of FortiSOAR while limiting its usage in a production environment. The trial license does not support multi-tenancy and restricts the overall capacity for scaling, making it suitable only for testing and familiarization with FortiSOAR's capabilities.

Question: 30

Which edition of license, when deployed, will serve as a primary node in a distributed deployment?

A. MT

B. MT_Tenant

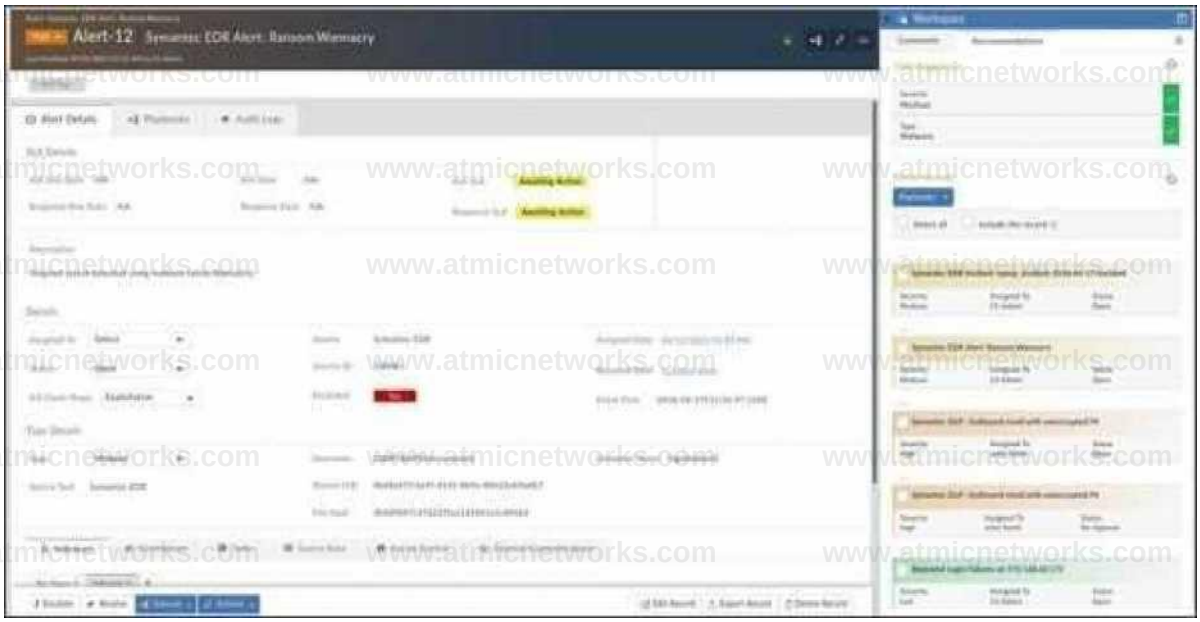
C. MT_RegionalSOC

D. Enterprise

Answer: A

Explanation:

Question: 31



View the exhibit. The dataset on FortiSOAR has been trained to predict which record field?

A. Assigned To

B. Status

C. Playbooks

D. Severity

Answer: D

Explanation:

Question: 32

Which three roles are defined as SAML roles?

(Choose three.)

A. Service provider

B. Role

C. Identity provider

D. Attribute map

E. Principal

Answer: ACE

Explanation:

Question: 33

What are two different services that you can configure for monitoring system and cluster health statuses on FortiSOAR?
(Choose two.)

A. Exchange

B. POP

C. IMAP

D. SMTP

Answer: AD

Explanation:

Question: 34

Which product is essential to level 3 of the SOC automation model?

A. FortiAnalyzer

B. FortiAuthenticator

C. FortiManager

D. FortiSOAR

Answer: D

Explanation:

Question: 35

Which two relationship types are configurable on FortiSOAR?

(Choose two.)

A. Siblings

B. Grandparents

C. Parents

D. Relatives

Answer: AC

Explanation:

Question: 36

What are two use cases for configuring a FortiSOAR HA cluster?

(Choose two.)

A. Disaster recovery

B. Multi-tenancy

C. Data externalization

D. Scaling

Answer: AD

Explanation:

Question: 37

Which two system monitoring reports are available on the System Monitoring widget?

(Choose two.)

A. RAM Usage

B. CPU Usage

C. Service Status

D. Playbook Health Status

Answer: BC

Explanation:

Question: 38

View the exhibit:

What does the command output mean?

```
rootafortisoar -H cMdm db —check-connection
The file db^external_confi^.yml does not exist. Failed to connect the instance
[tOGtgfortisoar ']#
```

A. The configuration to enable database externalization has not been completed.

B. The local PostgreSQL database is disabled on the FortiSOAR instance.

C. The local PostgreSQL database is configured on the FortiSOAR instance.

D. There is no connectivity between the PostgreSQL databases of the primary and secondary FortiSOAR instances.

Answer: A

Explanation:

Question: 39

Select two statements that are true about FortiSOAR themes.

(Choose two.)

A. There are three theme options available: Dark, Light, and Sky.

B. Non-administrator users can change the theme by editing their user profile.

C. FortiSOAR theme can be configured to apply to all users on the system.

D. Selecting Revert Theme allows the user to revert the user profile theme.

Answer: BC

Explanation:

Question: 40

Which two roles are default roles configured on FortiSOAR? (Choose two answers)

A. T1 Analyst

B. T3 Analyst

C. FortiSOAR Agent

D. Connector Administrator

Answer: A, D

Explanation:

Comprehensive and Detailed Explanation From FortiSOAR 7.3 Exact Extract study guide:

FortiSOAR comes with several pre-defined (out-of-the-box) roles designed to align with common Security Operations Center (SOC) functions. According to the FortiSOAR 7.3 Administration Guide under the "Security Management" section:

T1 Analyst (Tier 1): This role is a default configuration intended for front-line analysts who perform initial triaging of alerts and basic incident response tasks.

Connector Administrator: This is a specialized default role that grants permissions specifically for configuring,

updating, and managing the lifecycle of connectors within the environment.

While FortiSOAR is highly customizable and allows for the creation of T2 or T3 roles, they are not always present as specific "default" named roles in the same way the T1 Analyst is across all base installations. Furthermore, "FortiSOAR Agent" refers to a technical component or a deployment architecture rather than a standard user RBAC (Role-Based Access Control) role. Other common default roles include Security Administrator, Application Administrator, and Full Access.

Question: 41

What two permissions must you assign to a user to allow the purge of audit logs for all users? (Choose two answers)

A. Delete permission on the Security module

B. Delete permission on the Audit Log Activities module

C. Delete permission on the People module

D. Delete permission on the Users module

Answer: A, B

Explanation:

Comprehensive and Detailed Explanation From FortiSOAR 7.3 Exact Extract study guide:

According to the FortiSOAR 7.3 Administration Guide under the "Audit Logs" and "Role-Based Access Control (RBAC)" sections, managing the lifecycle of system logs requires elevated administrative privileges.

To perform a manual purge of audit logs, the system validates permissions across two specific areas:

Audit Log Activities Module: The user must have Delete permissions on this specific module because it is the repository where the actual log records are stored. Without "Delete" rights here, the application cannot remove the database entries.

Security Module: Because the purging of audit logs is a sensitive security operation that affects the system's accountability trail, FortiSOAR requires the Delete permission on the Security module. This acts as a secondary administrative guardrail to ensure only authorized security administrators can permanently remove audit trails.

Permissions on the People or Users modules (Options C and D) are used for managing user profiles and account attributes, but they do not grant the authority to manipulate system-level audit

databases.

Question: 42

Which statement about licensing on FortiSOAR is true? (Choose one answer)

A. A FortiSOAR VM with a perpetual license needs access to update.fortiguard.net.1

B. The subscription license requires connectivity to globalupdate.fortinet.net to retrieve information.

C. The perpetual trial license has a limit on actions per day but no limit on user count.2

D. The evaluation license has an expiry date but no limit on user count.3

Answer: B

Explanation:

Comprehensive and Detailed Explanation From FortiSOAR 7.3 Exact Extract study guide:

According to the FortiSOAR 7.3 Deployment and Administration Guide under the "Licensing FortiSOAR" section:

Connectivity Requirements: For the FortiSOAR license deployment and validation process to succeed, the instance must have outbound connectivity to https://globalupdate.fortinet.net. This URL is specifically used by the FortiSOAR license manager to fetch entitlements, verify the subscription status, and retrieve product information from the Fortinet licensing servers. If this connectivity is blocked (and a FortiManager is not being used as a local FDN proxy), the license deployment will fail.4

License Limits: Every FortiSOAR license—whether Perpetual, Subscription, or Trial—strictly enforces a maximum number of active users (concurrent or named) and often a limit on the number of automation actions per day.5

Perpetual Trial Licenses (often called "Free Trial") are restricted to a specific user count (typically 2 or 3) and a daily action limit (e.g., 200 or 1000 actions). Therefore, options C and D are incorrect as they suggest "no limit on user count."

URL Clarification: While update.fortiguard.net is a common Fortinet endpoint for security signatures (IPS/AV), FortiSOAR's specific licensing and entitlement communication is directed to the globalupdate.fortinet.net service.

Question: 43

Which three features are installed with the FortiSOAR Incidence Response Content Pack? (Choose three answers)

A. System monitoring connectors1

B. Sample data for playbooks

C. Sample alerts and incidents

D. System playbooks2

E. SLA template module

Answer: B, C, D

Explanation:

Comprehensive and Detailed Explanation From FortiSOAR 7.3 Exact Extract study guide:

The FortiSOAR Incidence Response Content Pack (which is essentially the predecessor or foundational component of the SOAR Framework Solution Pack in version 7.3) is designed to provide users with an immediate, functional environment. According to the FortiSOAR 7.3 Administration Guide and Content Hub documentation:

Sample Alerts and Incidents (C): The content pack includes a set of demo records.3 Upon installation and clicking the "Demo IR Records" button, the system populates the Alerts and Incidents modules with pre-configured samples, including associated indicators and assets, to demonstrate how records are handled.4

System Playbooks (D): It installs a comprehensive collection of "out-of-the-box" (OOB) playbooks. These include system-level playbooks used for triaging, indicator extraction, and managing standard record lifecycles (such as auto-populating dates when a record is closed).5

Sample Data for Playbooks (B): Along with the records themselves, the pack includes simulation and training data (often referred to as "Playbook Samples" or "Mock Data").6 This allows administrators to test playbook logic and workflows without requiring live feeds from third-party security tools.

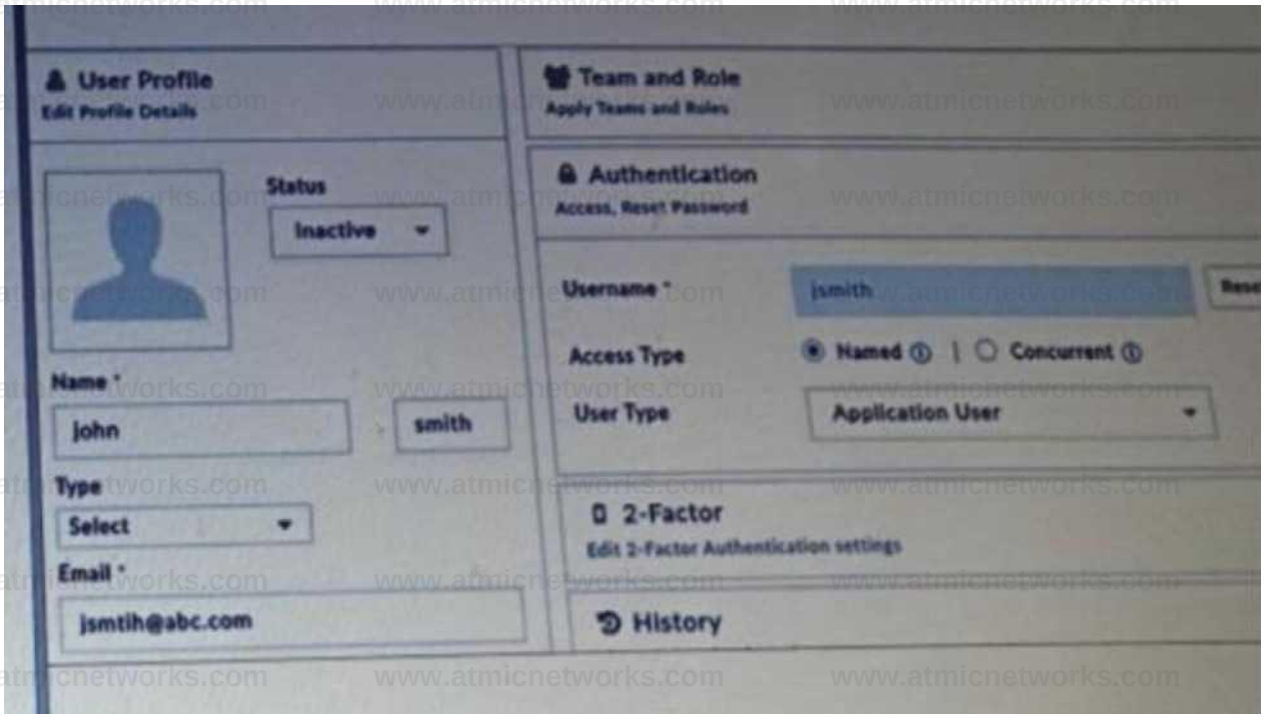
Why other options are incorrect:

System monitoring connectors (A): While the pack may configure some basic internal connectors (like the Code Snippet connector), "system monitoring connectors" are generally standalone integrations or part of specific device solution packs rather than the core IR pack.

SLA template module (E): Although the pack includes playbooks that manage SLAs (calculating response and resolution times), the "SLA Management" or "SLA Template" capability is often categorized as an additional module or handled via the Module Editor, rather than being a specific "feature" installed solely by the IR pack.

Question: 44

Refer to the exhibit.



Why is this user's account inactive? (Choose one answer)

A. The user has exceeded the maximum number of authentication tries for a one-hour period.

B. The user does not have a valid email ID for the account.

C. The user has not reset the password for the account.

D. The user has exceeded the maximum number of allowed user accounts.

Answer: D

Explanation:

Comprehensive and Detailed Explanation From FortiSOAR 7.3 Exact Extract study guide:

According to the FortiSOAR 7.3 Administration and Deployment Guides, specifically in the "Licensing FortiSOAR" and "Security Management" sections:

Licensing Enforcement: FortiSOAR strictly enforces the number of active users based on the installed license. The license specifies the maximum number of active users allowed in the system at any given point in time.

User Status (Active vs. Inactive): When the number of active users reaches the limit defined by the license, any additional users created or imported will be set to an Inactive status by default. An administrator cannot change their status to "Active" until an existing active user is deactivated or deleted, or the license is upgraded to support more users.

Locked Status (Option A): It is important to distinguish between "Inactive" and "Locked." Users become temporarily locked out of FortiSOAR when they exceed the configured number of authentication attempts (defaulting to 5 times) within a specific period. A locked user profile will typically display a "Locked" indicator

or a checkbox to "Unlock" rather than a simple "Inactive" status.

Other Options: While an email ID is required for account creation, its validity does not automatically trigger an "Inactive" status (Option B). Similarly, a required password reset (Option C) forces a password change upon login but does not disable the account.