Free Questions for NSE5_FSM-6.3

Shared by Bird on 04-10-2024

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

How is a subpattern for a rule defined?

Options:

A- Filters, Aggregation, Group by definitions

B- Filters, Group By definitions, Threshold

C- Filters, Threshold, Time Window definitions

D- Filters, Aggregation, Time Window definitions

Answer:

C

Question 2

Question Type: MultipleChoice

Where do you configure rule notifications and automated remediation on FortiSIEM?

Options:

A- Notification policy

B- Remediation policy

C- Notification engine

D- Remediation engine

Answer:

A

Explanation:

Rule Notifications and Automated Remediation: In FortiSIEM, notifications and automated remediation actions can be configured to respond to specific incidents or alerts generated by rules.

Notification Policy: This is the section where administrators configure the settings for notifications and specify the actions to be taken when a rule triggers an alert.

Configuration Options: Includes defining the recipients of notifications, the type of notifications (e.g., email, SMS), and any automated remediation actions that should be executed.

Importance: Proper configuration of notification policies ensures timely alerts and automated responses to incidents, enhancing the effectiveness of the SIEM system.

Reference: FortiSIEM 6.3 User Guide, Notifications and Automated Remediation section, which details how to configure notification policies for rule-triggered actions and responses.

Question 3

Question Type: MultipleChoice

How is a subparttern for a rule defined?

Options:

A- Filters Aggregation. Group By definition

B- Filters Group By definitions. Threshold

C- Filters Threshold Time Window definitions

D- Filters Aggregation Time Window definitions

Answer:

D

Explanation:

Rule Subpattern Definition: In FortiSIEM, a subpattern within a rule is used to define specific conditions and criteria that must be met for the rule to trigger an incident or alert.

Components of a Subpattern: The subpattern includes the following elements:

Filters: Criteria to filter the events that the rule will evaluate.

Aggregation: Conditions that define how events should be aggregated or grouped for analysis.

Time Window Definitions: Specifies the time frame over which the events will be evaluated to determine if the rule conditions are met.

Explanation: Together, these components allow the system to efficiently and accurately detect patterns of interest within the event data.

Reference: FortiSIEM 6.3 User Guide, Rules and Patterns section, which explains the structure and configuration of rule subpatterns, including the use of filters, aggregation, and time window definitions.

Question 4

Question Type: MultipleChoice

Which is a requirement for implementing FortiSIEM disaster recovery?

Options:

A- All worker nodes must access both supervisor nodes using IP.

B- SNMP, and WMI ports must be open between the two supervisor nodes.

C- The two supervisor nodes must have layer 2 connectivity.

D- DNS names must be used for the worker upload addresses.

Answer:

D

Explanation:

Disaster Recovery (DR) Implementation: For FortiSIEM to effectively support disaster recovery, specific requirements must be met to ensure seamless failover and data integrity.

Layer 2 Connectivity: One of the critical requirements for implementing FortiSIEM DR is that the two supervisor nodes must have layer 2 connectivity.

Layer 2 Connectivity: This ensures that the supervisors can communicate directly at the data link layer, which is necessary for synchronous data replication and other DR processes.

Importance of Connectivity: Layer 2 connectivity between the supervisor nodes ensures that they can maintain consistent and up-to-date state information, which is essential for a smooth failover in the event of a disaster.

Reference: FortiSIEM 6.3 Administration Guide, Disaster Recovery section, which details the requirements and configurations needed for setting up disaster recovery, including the necessity for layer 2 connectivity between supervisor nodes.

Question 5

Question Type: **MultipleChoice**

Consider the storage of anomaly baseline date that is calculated for different parameters. Which database is used for storing this data?

Options:

A- Event DB

B- Profile DB

C- SVNDB

D- CMDB

Answer:

D

Explanation:

Anomaly Baseline Data: Anomaly baseline data refers to the statistical profiles and baselines calculated for various parameters to detect deviations indicative of potential security incidents.

Profile DB: The Profile DB is specifically designed to store such baseline data in FortiSIEM.

Purpose: It maintains statistical profiles for different monitored parameters to facilitate anomaly detection.

Usage: This data is used by FortiSIEM to compare real-time metrics against the established baselines to identify anomalies.

Reference: FortiSIEM 6.3 User Guide, Database Architecture section, which describes the different databases used in FortiSIEM and their purposes, including the Profile DB for storing anomaly baseline data.

Question 6

Question Type: MultipleChoice

What does the Frequency field determine on a rule?

Options:

A- How often the rule will evaluate the subpattern.

B- How often the rule will trigger for the same condition.

C- How often the rule will trigger.

D- How often the rule will take a clear action.

Answer:

B

Explanation:

Rule Evaluation in FortiSIEM: Rules in FortiSIEM are evaluated periodically to check if the defined conditions or subpatterns are met.

Frequency Field: The Frequency field in a rule determines the interval at which the rule's subpattern will be evaluated.

Evaluation Interval: This defines how often the system will check the incoming events against the rule's subpattern to determine if an incident should be triggered.

Impact on Performance: Setting an appropriate frequency is crucial to balance between timely detection of incidents and system performance.

Examples:

If the Frequency is set to 5 minutes, the rule will evaluate the subpattern every 5 minutes.

This means that every 5 minutes, the system will check if the conditions defined in the subpattern are met by the incoming events.

Reference: FortiSIEM 6.3 User Guide, Rules and Incidents section, which explains the Frequency field and how it impacts the evaluation of subpatterns in rules.

Question 7

Question Type: **MultipleChoice**

In me FortiSIEM CLI. which command must you use to determine whether or not syslog is being received from a network device?

Options:

A- tcpdump

B- OphSyslogRecorder

C- Onetcat

D- phDeviceTest

Answer:

A

Explanation:

Syslog Reception Verification: To verify whether syslog messages are being received from a network device, a network packet capture tool can be used.

tcpdump Command: tcpdump is a powerful command-line packet analyzer tool available in Unix-like operating systems. It allows administrators to capture and analyze network traffic.

Usage: By using tcpdump with the appropriate filters (e.g., port 514 for syslog), administrators can monitor the incoming syslog messages in real-time to verify if they are being received.

Example Command: tcpdump -i <interface> port 514 captures the syslog messages on the specified network interface.

Reference: FortiSIEM 6.3 User Guide, CLI Commands section, which details the usage of tcpdump for network traffic analysis and verification of syslog reception.