Vendor: Fortinet

Exam Code: NSE5_FSM-6.3

Exam Name: Fortinet NSE 5 - FortiSIEM 6.3

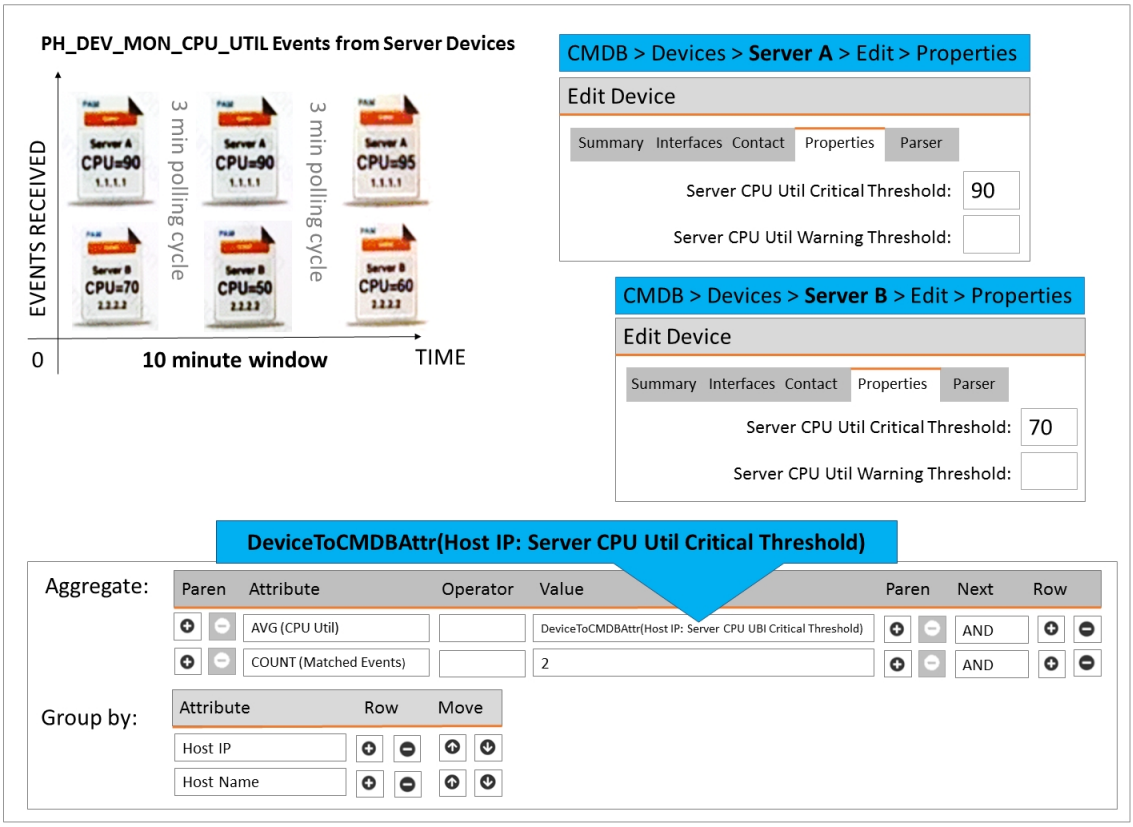
Version: DEMO

QUESTION 1
Which process converts raw log data to structured data?

A. Data classification
B. Data validation
C. Data parsing
D. Data enrichment

Answer: C
Explanation:
Raw Log Data: When devices send logs to FortiSIEM, the data arrives in a raw, unstructured format.
Data Parsing Process: The process that converts this raw log data into a structured format is known as data parsing.
Data Parsing: This involves extracting relevant fields from the raw log entries and organizing them into a structured format, making the data usable for analysis, reporting, and correlation.
Significance of Structured Data: Structured data is essential for effective event correlation, alerting, and generating meaningful reports.

QUESTION 2
Refer to the exhibits. Three events are collected over a 10-minute time period from two servers: Server A and Server B.
Based on the settings being used for the rule subpattern, how many incidents will the servers generate?



A. Server A will generate one incident and Server B will generate one incident.

B. Server A will generate one incident and Server B will not generate any incidents.
C. Server B will generate one incident and Server A will not generate any incidents.
D. Server A will not generate any incidents and Server B will not generate any incidents.

Answer: B
Explanation:
Event Collection Overview: The exhibits show three events collected over a 10-minute period from two servers, Server A and Server B.
Rule Subpattern Settings: The rule subpattern specifies two conditions:
AVG(CPU Util) > DeviceToCMDBAttr(Host IP : Server CPU Util Critical Threshold): This checks if the average CPU utilization exceeds the critical threshold defined for each server.
COUNT(Matched Events) >= 2: This requires at least two matching events within the specified period.
Server A Analysis:
Events: Three events (CPU=90, CPU=90, CPU=95).
Average CPU Utilization: (90+90+95)/3 = 91.67, which exceeds the critical threshold of 90.
Matched Events Count: 3, which meets the condition of being greater than or equal to 2.
Incident Generation: Server A meets both conditions, so it generates one incident.
Server B Analysis:
Events: Three events (CPU=70, CPU=50, CPU=60).
Average CPU Utilization: (70+50+60)/3 = 60, which does not exceed the critical threshold of 90.
Matched Events Count: 3, but since the average CPU utilization condition is not met, no incident is generated.
Conclusion: Based on the rule subpattern, Server A will generate one incident, and Server B will not generate any incidents.

QUESTION 3
In me FortiSIEM CLI. which command must you use to determine whether or not syslog is being received from a network device?

A. tcpdump
B. phSyslogRecorder
C. netcat
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.

QUESTION 4
What does the Frequency field determine on a rule?

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: A
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.

QUESTION 5
Consider the storage of anomaly baseline date that is calculated for different parameters. Which database is used for storing this data?

A. Event DB
B. Profile DB
C. SVNDB
D. CMDB

Answer: B
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.

QUESTION 6
Which is a requirement for implementing FortiSIEM disaster recovery?

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:
DNS Names are used for the Supervisor nodes at the two sites. Make sure that users, collectors, and agents can access both Supervisor nodes by their DNS names.
DNS Names are used for the Worker upload addresses.
https://docs.fortinet.com/document/fortisiem/5.4.0/disaster-recovery-procedures-nfs/565771/disaster-recovery

QUESTION 7
How is a subpattern for a rule defined?

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.

QUESTION 8
Which FortiSIEM components are capable of performing device discovery?

A. FortiSIEM Windows agent
B. Worker
C. FortiSIEM Linux agent
D. Collector

Answer: D
Explanation:
Device Discovery in FortiSIEM: Device discovery is the process by which FortiSIEM identifies and adds devices to its management scope.
Role of Collectors: Collectors are responsible for gathering data from network devices, including discovering new devices in the network.
Functionality: Collectors use protocols such as SNMP, WMI, and others to discover devices and gather their details.
Capability: While agents (Windows and Linux) primarily gather data from their host systems, the collectors actively discover devices across the network.

Thank You for Trying Our Product

Lead2pass Certification Exam Features:

★ More than **99,900** Satisfied Customers Worldwide.

★ Average **99.9%** Success Rate.

★ **Free Update** to match latest and real exam scenarios.

★ **Instant Download** Access! No Setup required.

★ Questions & Answers are downloadable in **PDF** format and **VCE** test engine format.

★ Multi-Platform capabilities - **Windows, Laptop, Mac, Android, iPhone, iPod, iPad**.

★ **100%** Guaranteed Success or **100%** Money Back Guarantee.

★ **Fast**, helpful support **24x7**.

View list of all certification exams: http://www.lead2pass.com/all-products.html

10% Discount Coupon Code: **ASTR14**