Vendor: Fortinet

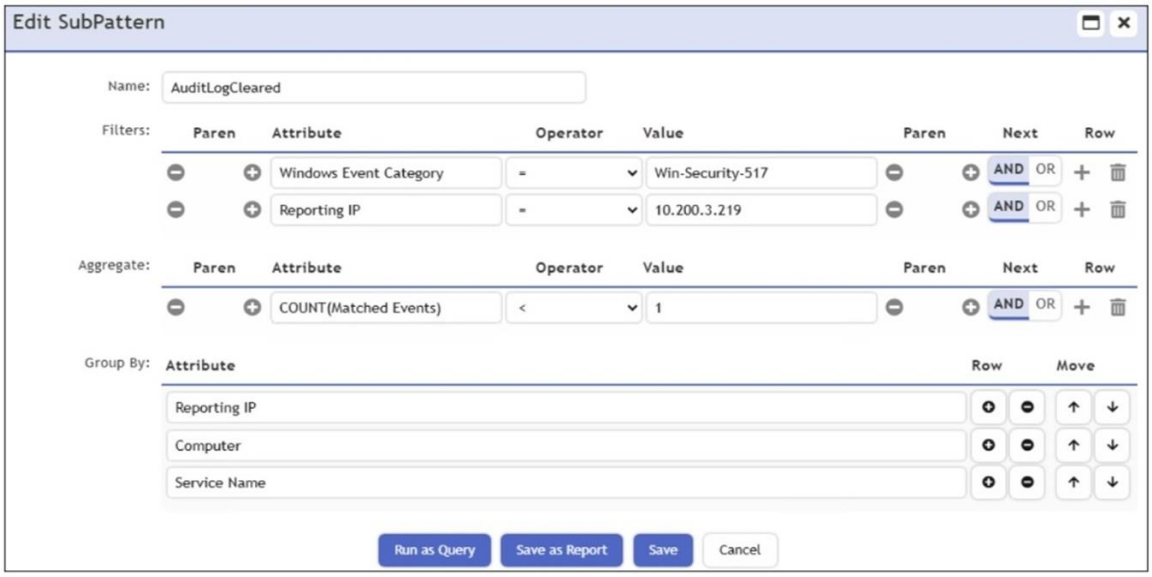
Exam Code: NSE7_SOC_AR-7.6

Exam Name: Fortinet NSE 7 - Security Operations 7.6 Architect

Version: DEMO

QUESTION 1
Refer to the exhibit. What are the two mistakes in the incident subpattern rule configuration? (Choose two.)

Incident subpattern rule configuration



A. The aggregate operator is incorrect.
B. The **Group By** attributes conflict with each other.
C. The subpattern is missing a time window definition.
D. The mandatory **Event Type** attribute is missing.

Answer: AD
Explanation:
The aggregate condition is incorrectly defined because using COUNT (Matched Events) less than 1 does not make sense for detecting an event occurrence and will never trigger as intended. Additionally, the mandatory Event Type attribute is missing, which is required in FortiSIEM subpattern definitions to correctly classify and correlate events.

QUESTION 2
Which two phases are part of the FortiSOAR incident handling process but are not phases in the NIST 800-61 revision 2 model? (Choose two.)

A. Detection
B. Confirmation
C. Identification
D. Preparation

Answer: BC
Explanation:
FortiSOAR includes a Confirmation phase to validate whether an alert represents a true incident, which is not a distinct phase in the NIST 800-61 revision 2 model. It also separates Identification as its own phase, whereas NIST combines identification activities within the broader Detection and Analysis phase rather than treating it as a standalone phase.

QUESTION 3
When configuring an **Ingest Bulk Feed** playbook step, which two restrictions must you consider? (Choose two.)

A. It will not trigger **On Create** triggers.
B. It is slower than the **Create Record** step.
C. It will not trigger **On Update** triggers.
D. It cannot use step output from a connector action.

Answer: AC
Explanation:
The Ingest Bulk Feed step ingests records directly into the database without invoking standard record lifecycle processing. As a result, it does not trigger On Create triggers or On Update triggers, which are only executed when records are created or modified through standard create or update actions.

QUESTION 4
You want to automate a workflow on FortiSOAR so that whenever an incident with critical severity is moved to the containment phase, it is automatically reassigned to an L3 analyst as the incident lead.

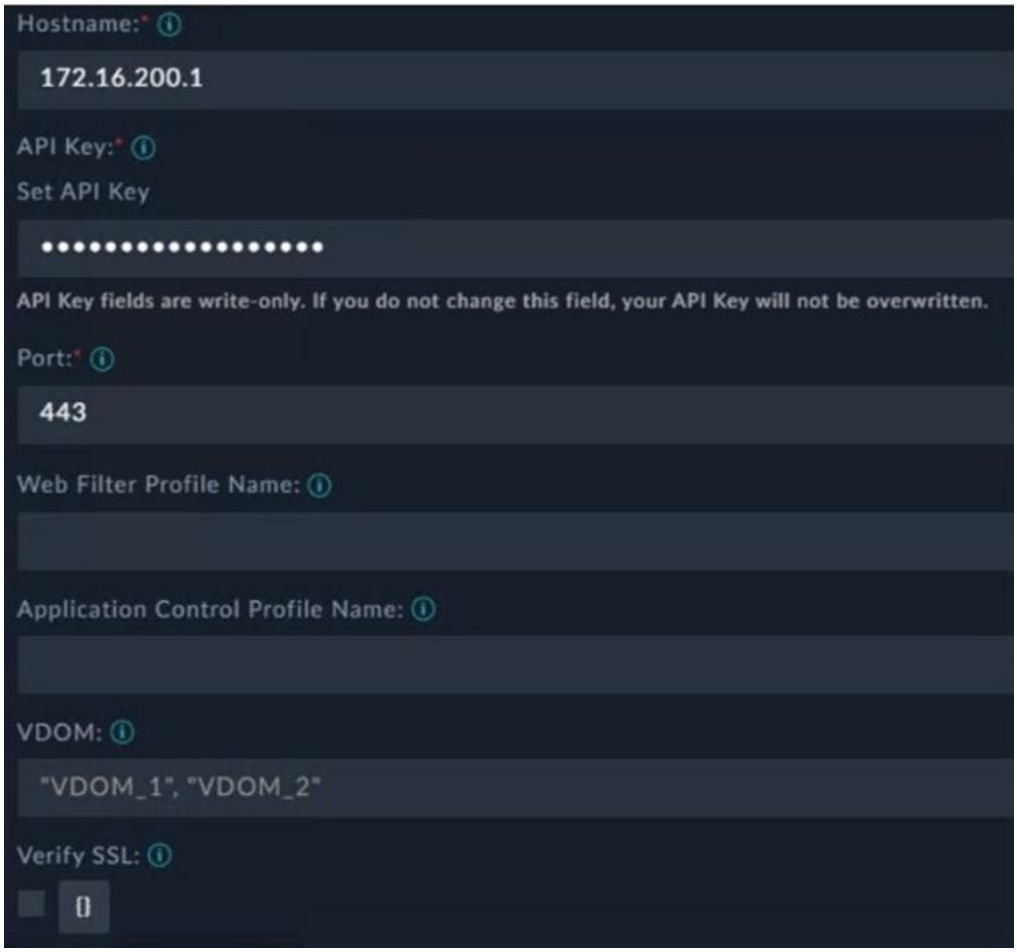
Which two steps will accomplish this task? (Choose two.)

A. Create a **Find Record** step to find matching incidents.
B. Create a **Condition** step to check the incident phase and update the incident lead.
C. Create an **Update Record** step to set the incident lead.
D. Create an **On Update** trigger with trigger conditions that match the containment phase and critical severity.
E. Set the playbook schedule to run persistently.

Answer: CD
Explanation:
An On Update trigger is required so the playbook runs automatically when an incident is modified, with trigger conditions matching both critical severity and the containment phase. An Update Record step is then used to change the incident lead to the appropriate L3 analyst when those conditions are met.

QUESTION 5
Refer to the exhibit. You must configure the FortiGate connector to allow FortiSOAR to perform actions on a firewall. However, the connection fails.

Configuration wizard



Which two configurations are required? (Choose two.)

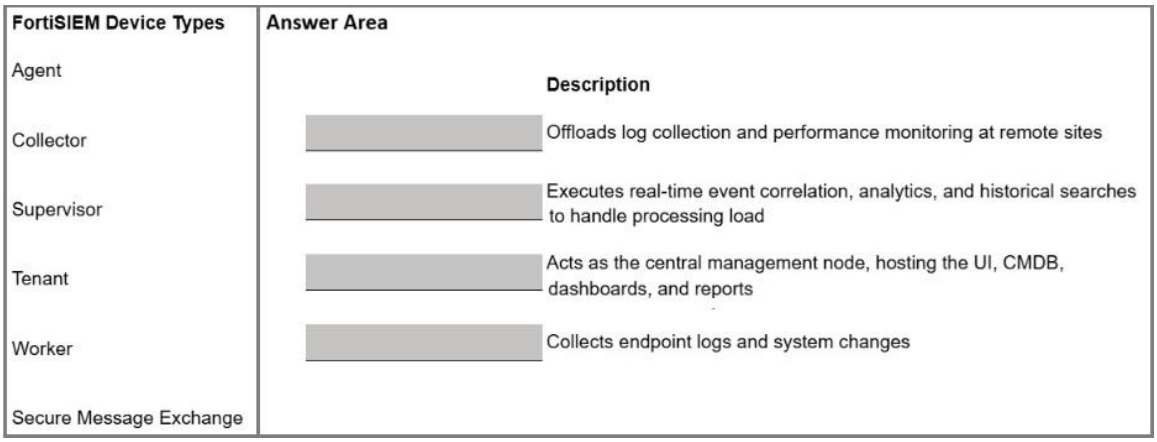
A. Trusted hosts must be enabled and the FortiSOAR IP address must be permitted.
B. An API administrator must be created on FortiGate with the appropriate profile, along with a generated API key to configure on the connector.
C. The VDOM name must be specified, or set to `VDOM_1`, if VDOMs are not enabled on FortiGate.
D. HTTPS must be enabled on the FortiGate interface that FortiSOAR will communicate with.

Answer: BD
Explanation:
FortiSOAR requires an API administrator account on the FortiGate with the appropriate permissions and a generated API key to authenticate and perform actions. In addition, HTTPS must be enabled on the FortiGate interface used for communication, because the connector communicates with the FortiGate API over HTTPS.

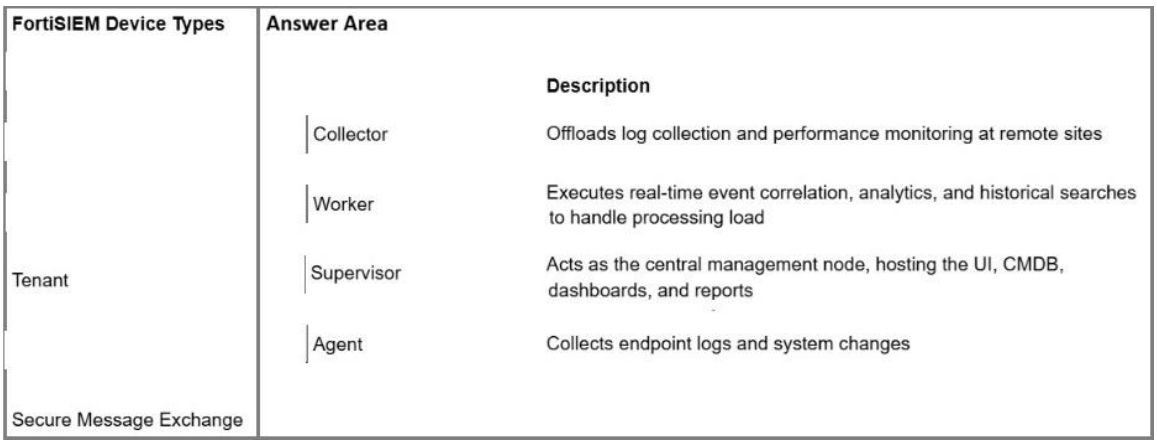
QUESTION 6
Drag and Drop Question

Match the FortiSIEM device type to its description.

Select each FortiSIEM device type in the left column, hold and drag it to the blank space next to its corresponding description in the column on the right. Once you match a device type to its description, you can move it again if you want to change your answer by clicking on the device type name. You need to match four device types to its description in the work area.



Answer:



Explanation:
The collector offloads log collection and performance monitoring at remote sites. The worker executes real-time correlation, analytics, and historical searches to handle processing load. The supervisor acts as the central management node hosting the UI, CMDB, dashboards, and reports. The agent is responsible for collecting endpoint logs and system changes.

QUESTION 7
You are trying to create a playbook that creates a manual task that shows a list of public IPv6 addresses.

You were successful in extracting all IP addresses om a previous action into a variable called `ip_list`, which has a mix of private and public IPv4 and IPv6 addresses. Now, you must filter the results to display only public IPv6 addresses.

Which two Jinja expressions can accomplish this task? (Choose two.)

A. `{{ vars.ip_list | ipaddr(!private) | ipv6 }}`

B. `{{ vars.ip_list | ipv6 | ipaddr('public') }}`
C. `{{ vars.ip_list | ipv6addr('public') }}`
D. `{{ vars.ip_list | ipaddr('public') | ipv6 }}`

Answer: BD
Explanation:
You can first filter the list to IPv6 addresses and then keep only public addresses, or first keep only public addresses and then filter to IPv6. Both approaches correctly narrow ip_list down to public IPv6 entries.

QUESTION 8
A partner organization recently had sensitive data exfiltrated by a well-known adversary group. You are tasked with threat hunting to see your organization is also affected.

Which action must you take first?

A. Use threat intelligence to enrich the IP addresses of all destinations.
B. Review the tactics, techniques, and procedures of the adversary.
C. Use a packet analyzer to capture and review all traffic flows on critical devices.
D. Review historical logs to establish a baseline for normal bandwidth usage.

Answer: B
Explanation:
Threat hunting begins by understanding the adversary's known tactics, techniques, and procedures so you can form a focused hypothesis and identify relevant behaviors, indicators, and data sources to hunt for potential compromise in your environment.

QUESTION 9
Review the incident report.

```
Packet captures show a host maintaining periodic TLS sessions that
imitate normal HTTPS traffic but run on TCP 8443 to a single external
host. An analyst flags the traffic as potential command-and-control.
During the same period, the host issues frequent DNS queries with
oversized TXT payloads to an attacker-controlled domain, transferring
staged files.
```

Which two MITRE ATT&CK techniques best describe this activity? (Choose two.)

A. Exploitation of Remote Services
B. Non-Standard Port
C. Exfiltration Over Alternative Protocol
D. Hide Artifacts

Answer: BC
Explanation:
The TLS sessions over TCP port 8443 represent the use of a non-standard port to disguise command-and-control traffic as normal HTTPS. The transfer of staged files using oversized DNS TXT records is an example of exfiltration over an alternative protocol, abusing DNS for data exfiltration.

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**