KaozhengPro

IT認證考試題庫

專業平臺

考證寶提供最新考古題與模擬試題
協助您高效通過認證考試

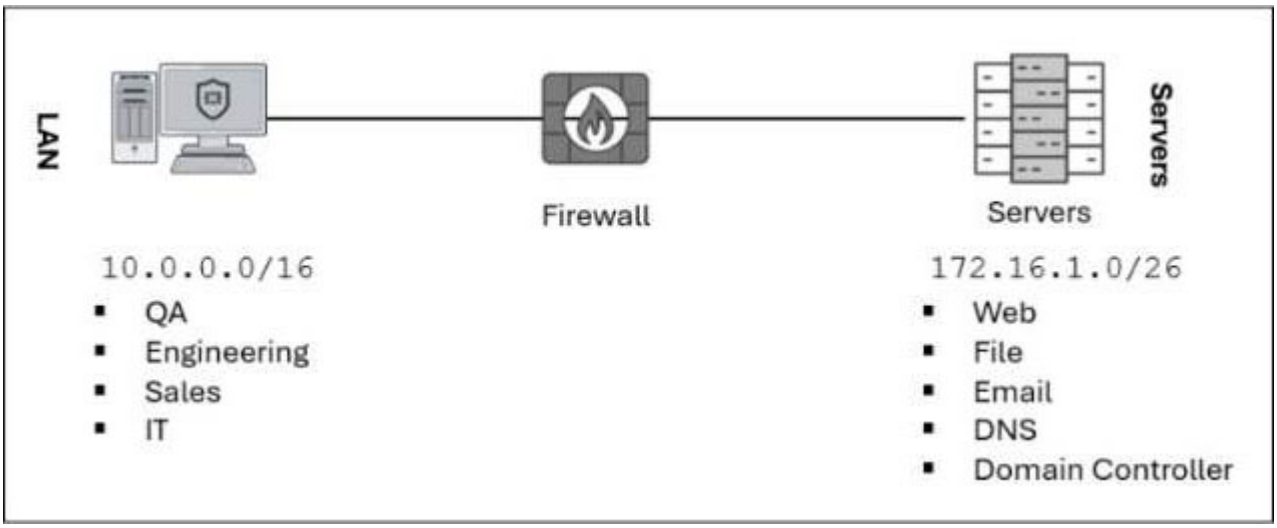
www.kaozhengpro.com

Exam : **NSE7_SOC_AR-7.6**

Title : Fortinet NSE 7 - Security Operations 7.6 Architect

Version : DEMO

1.Refer to the exhibit.



Which method most effectively reduces the attack surface of this organization?

A. Remove unused devices.

B. Enable deep inspection on firewall policies.

C. Forward all firewall logs to the security information and event management (SIEM) system.

D. Implement macrosegmentation.

Answer: D

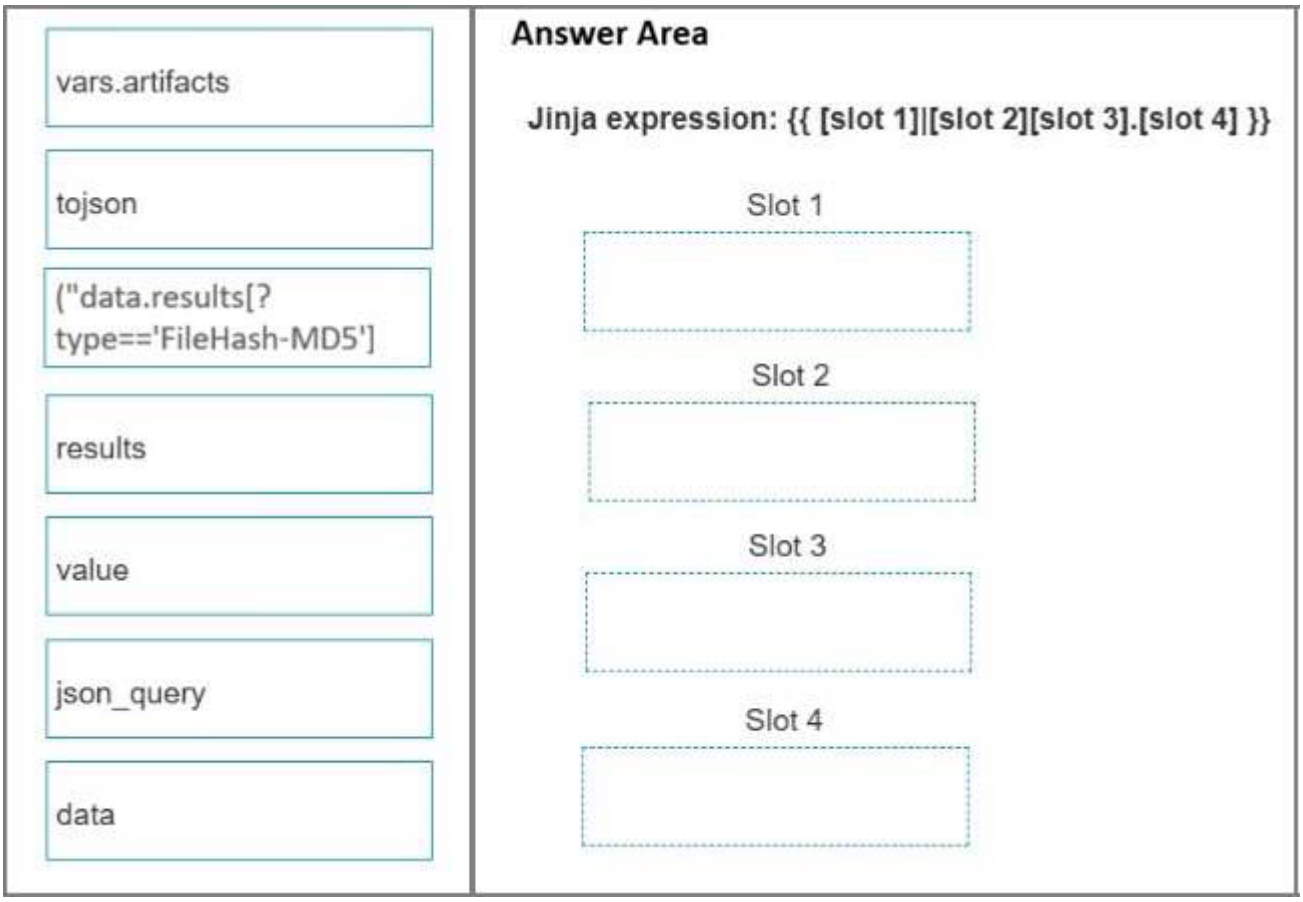
2.DRAG DROP -

Refer to the exhibit.

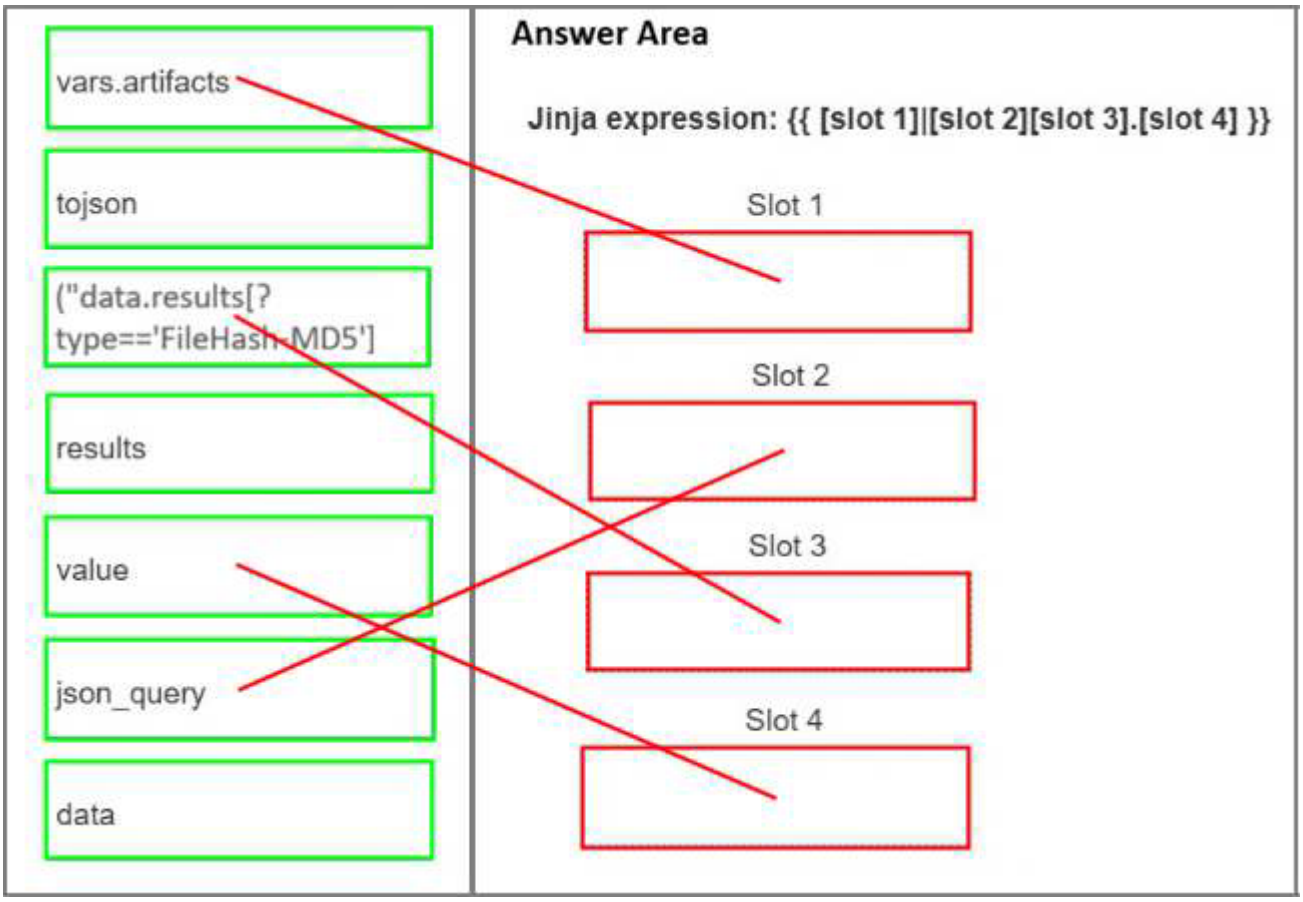
What is the correct Jinja expression to filter the results to show only the MD5 hash values?

{{ [slot 1]|[slot 2][slot 3].[slot 4] }}

Select the jinja expression in the left column, hold and drag it to a blank position on the right. Place the four correct steps in order, placing the first step in the first slot. Once you place an expression, you can move it again if you want to change your answer before moving to the next question. You need to drop four jinja expressions in the work area. Select and drag the screen divider to change the viewable area of the source and work areas.

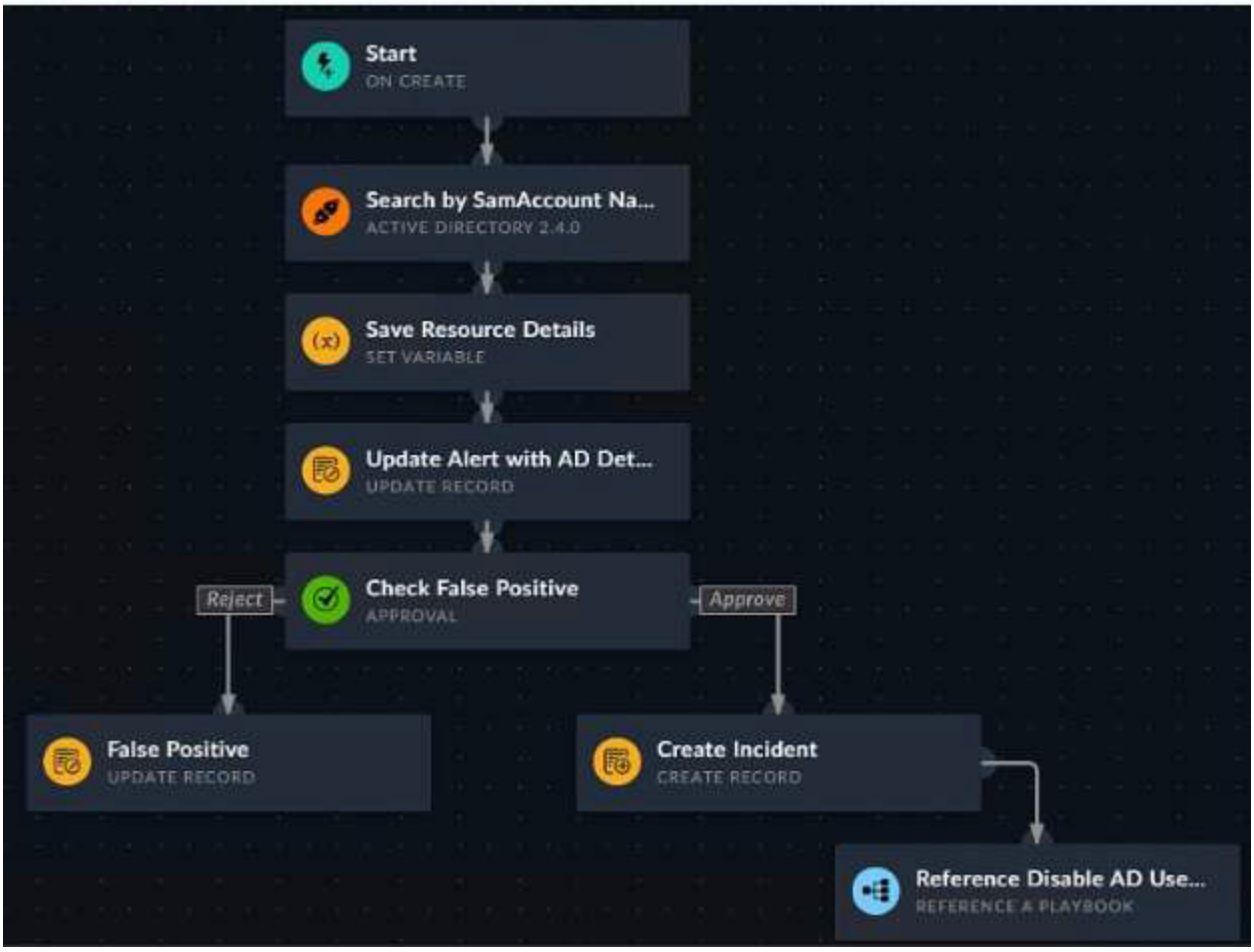

vars.artifacts
tojson
("data.results[?type=='FileHash-MD5']
results
value
json_query
data
Answer Area
Jinja expression: {{ [slot 1]|[slot 2][slot 3].[slot 4] }}
Slot 1
Slot 2
Slot 3
Slot 4

Answer:

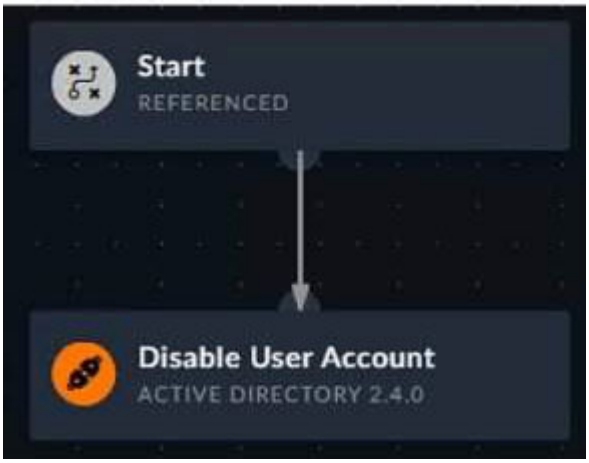


3.DRAG DROP
Refer to the exhibits.

Parent playbook



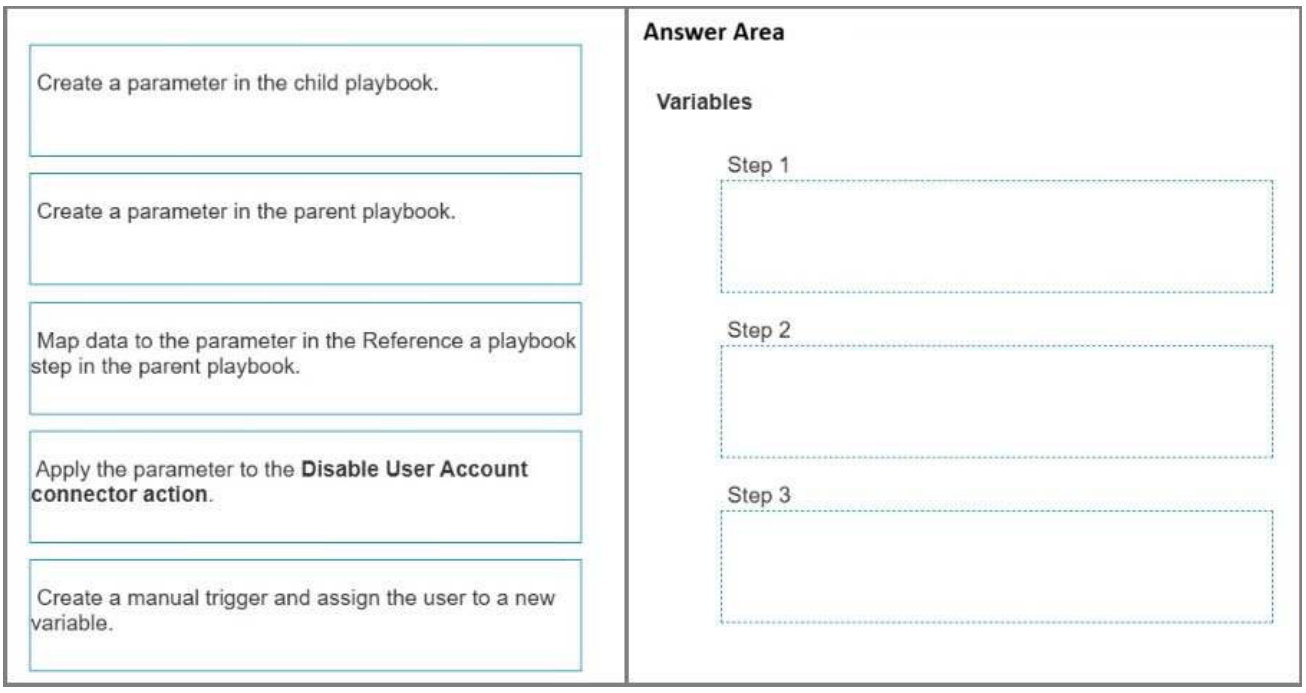
Child playbook



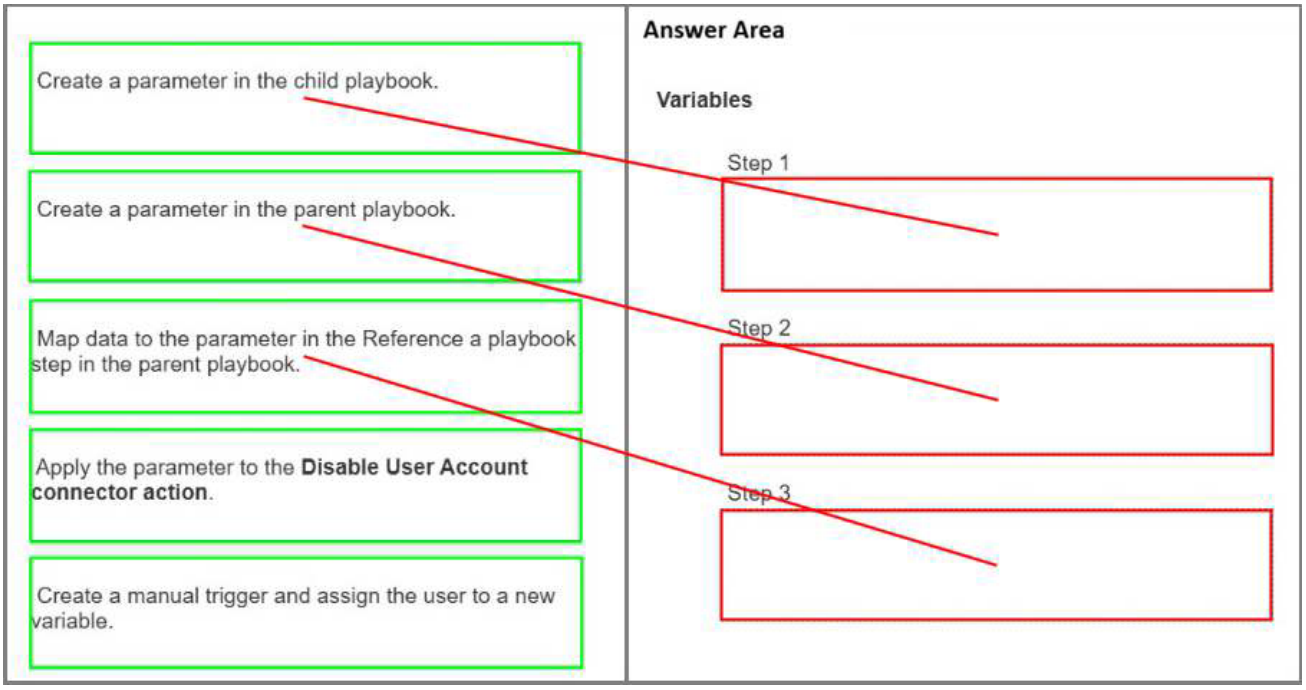
You have a playbook that, depending on whether an analyst deems the alert to be a true positive, could reference a child playbook. You need to pass variables from the parent playbook to the child playbook. Place the steps needed to accomplish this in the correct order.

Select the step in the left column, hold and drag it to a blank position on the right. Place the three correct steps in order, placing the first step in the first position at the top of the column. Once you place a step, you can move it again if you want to change your answer before moving to the next question. You need to drop three steps in the work area.

Select and drag the screen divider to change the viewable area of the source and work areas.

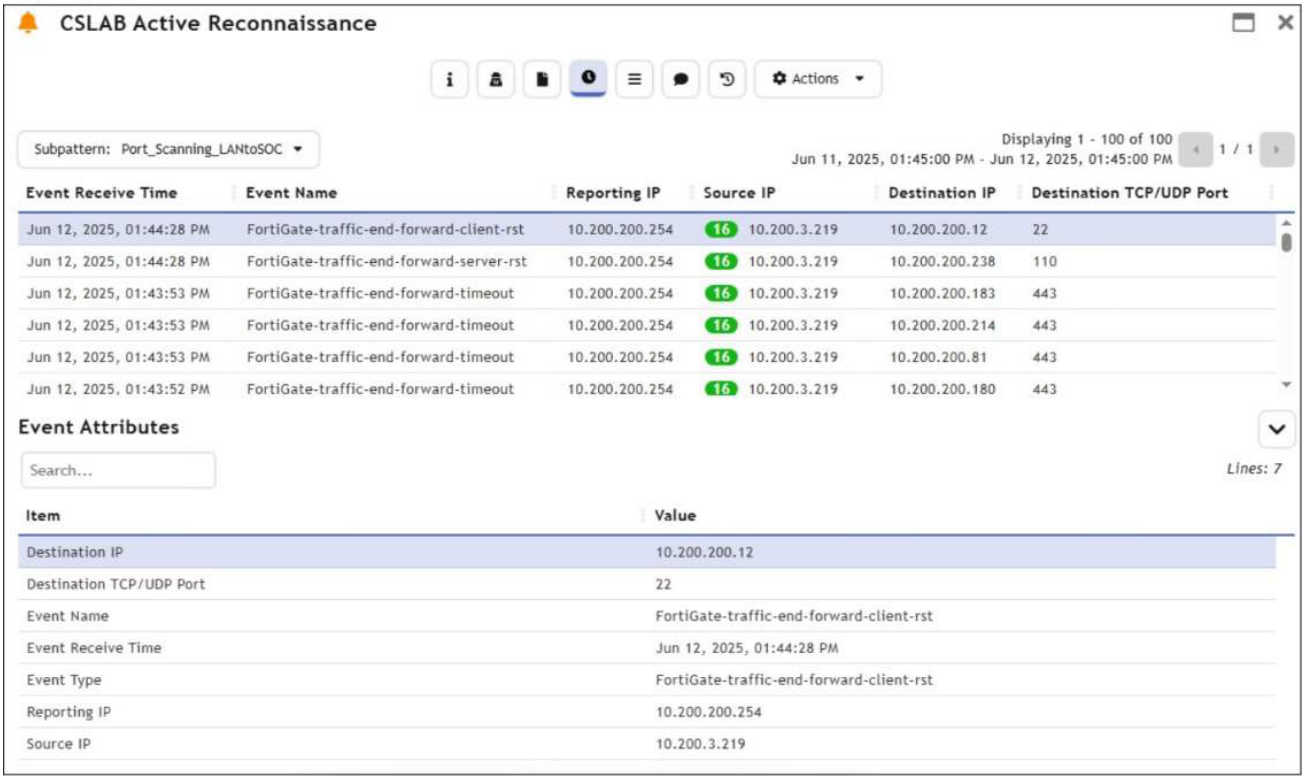


Answer:



4.Refer to the exhibit.

Triggering events



You are reviewing the Triggering Events page for a FortiSIEM incident. You want to remove the Reporting IP column because you have only one firewall in the topology.
How do you accomplish this?
A. Customize the display columns for this incident.
B. Remove the Reporting IP attribute from the raw logs using parsing rules.
C. Disable correlation for the Reporting IP field in the rule subpattern.
D. Clear the Reporting IP field from the Triggered Attributes section when you configure the Incident Action.
Answer: A

5.Based on the Pyramid of Pain model, which two statements accurately describe the value of an indicator and how it is for an adversary to change? (Choose two.)
A. Tactics, techniques, and procedures are hard because adversaries must adapt their methods.
B. Tools are easy because often, multiple alternatives exist.
C. IP addresses are easy because adversaries can spoof them or move them to new resources.
D. Artifacts are easy because adversaries can alter file paths or registry keys.
Answer: AC