



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

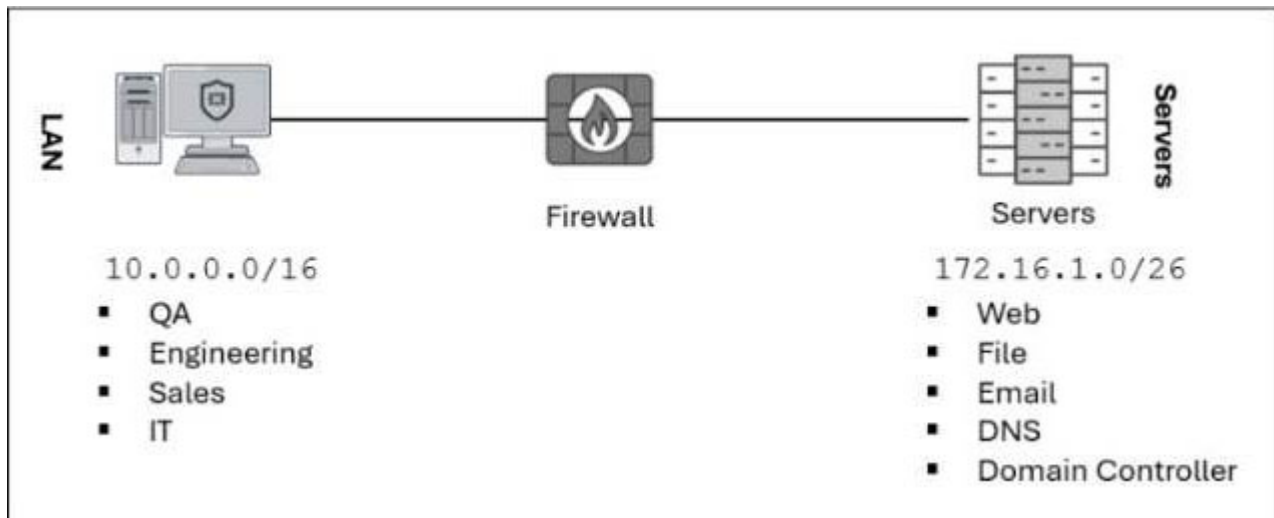
www.kaozhengpro.com

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.

```

{
  "vars": {
    "artifacts": {
      "data": {
        "results": [
          {
            "type": "Host",
            "value": "malicious-site.com",
            "picklist_iri": "/api/3/picklists/3272abd8-aae-4663-8c47-6d1195e684d9"
          },
          {
            "type": "IP Address",
            "value": "123.123.123.123",
            "picklist_iri": "/api/3/picklists/c0beeda4-2c7a-4214-b7e5-53ba1649539c"
          },
          {
            "type": "Host",
            "value": "fortinet.com",
            "picklist_iri": "/api/3/picklists/3272abd8-aae-4663-8c47-6d1195e684d9"
          },
          {
            "type": "File",
            "value": "org.apache.tika.parser.pdf",
            "picklist_iri": "/api/3/picklists/0162241b-f5bf-4917-a150-00e920be47bd"
          },
          {
            "type": "FileHash-MD5",
            "value": "6aad63bcc3dd4e148f3724808955f912",
            "picklist_iri": "/api/3/picklists/0ca054f2-d923-4992-a4a7-c516e6df281e"
          },
          {
            "type": "FileHash-MD5",
            "value": "9fd2b1c0e4a37658bca9d0f1e2c34567",
            "picklist_iri": "/api/3/picklists/9a8b7c6d-5e4f-41a0-b123-0fedcba98765"
          }
        ]
      }
    }
  }
}

```

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.

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

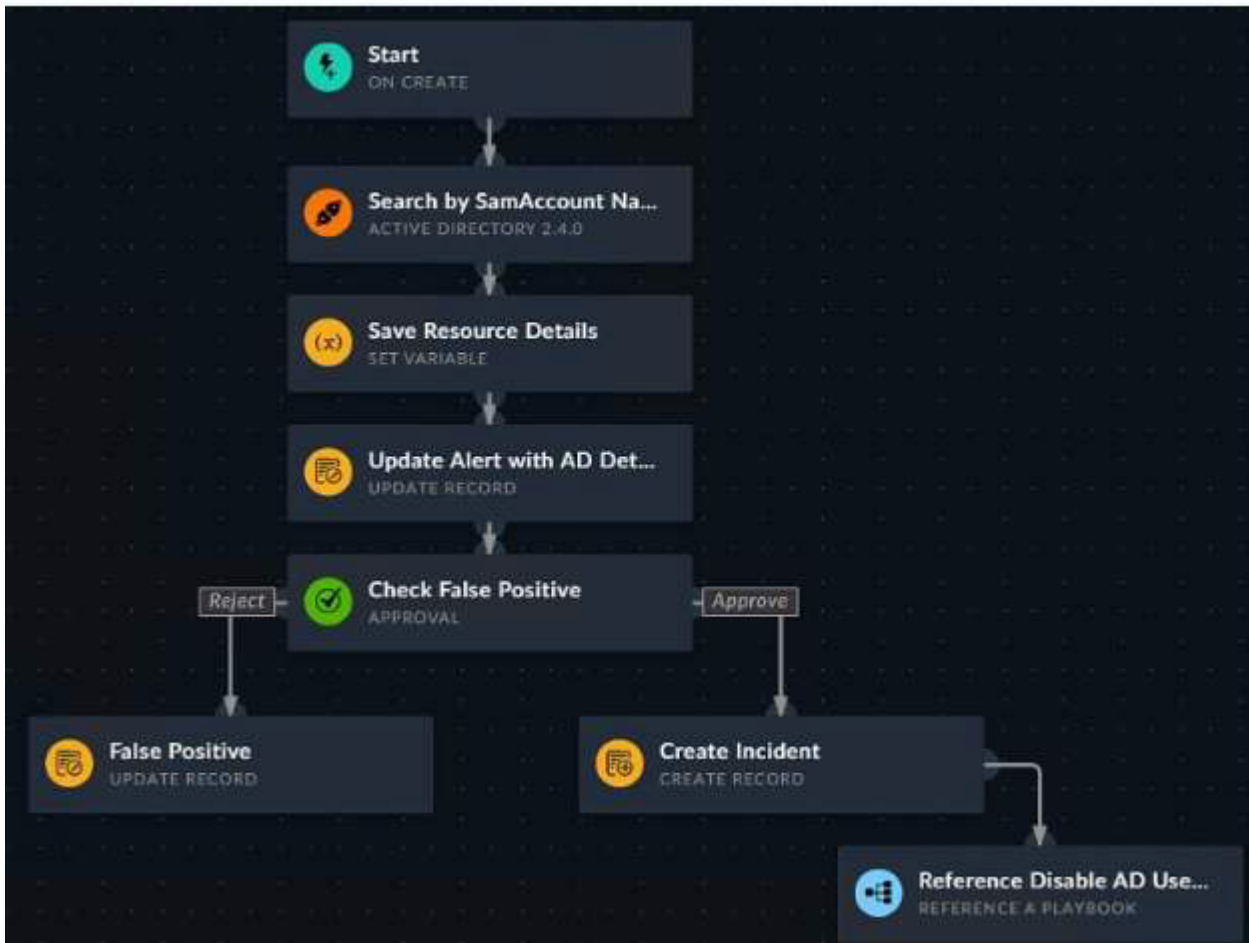
Answer:

<div data-bbox="183 224 574 324">vars.artifacts</div> <div data-bbox="183 347 574 448">tojson</div> <div data-bbox="183 470 574 571">("data.results[? type=='FileHash:MD5']</div> <div data-bbox="183 593 574 694">results</div> <div data-bbox="183 716 574 817">value</div> <div data-bbox="183 840 574 940">json_query</div> <div data-bbox="183 963 574 1064">data</div>	<p>Answer Area</p> <p>Jinja expression: {{ [slot 1] [slot 2] [slot 3].[slot 4] }}</p> <div data-bbox="726 380 1117 526">Slot 1 <input type="text"/></div> <div data-bbox="726 548 1117 694">Slot 2 <input type="text"/></div> <div data-bbox="726 716 1117 862">Slot 3 <input type="text"/></div> <div data-bbox="726 884 1117 1041">Slot 4 <input type="text"/></div>
--	---

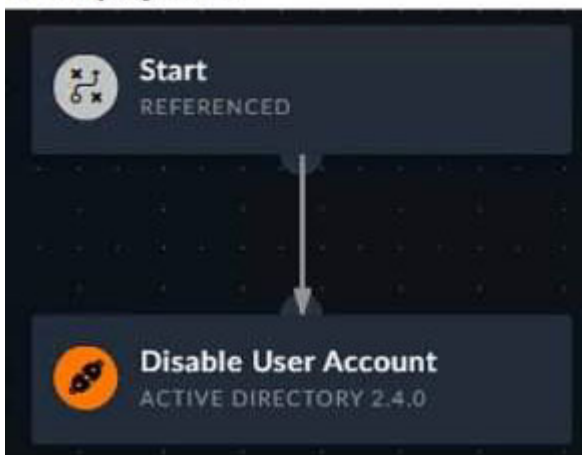
3.DRAG DROP

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.

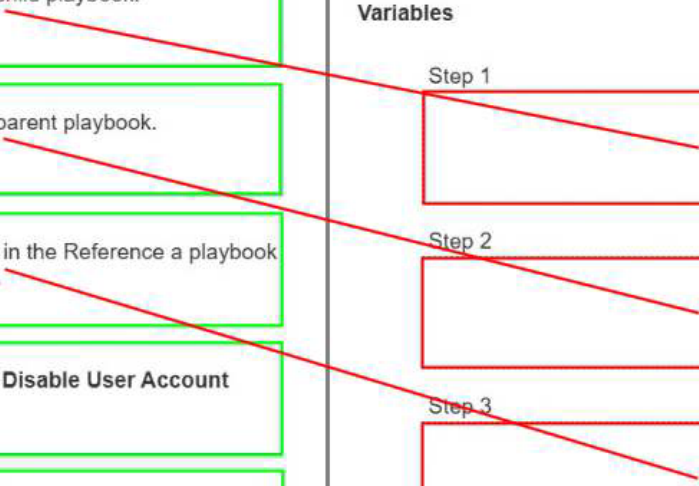
Select the step in the left column, hold and drag it to a blank position on the right. Place the three correct steps in order, placing the first step in the first position at the top of the column. Once you place a step, you can move it again if you want to change your answer before moving to the next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

<p>Create a parameter in the child playbook.</p>	Answer Area
<p>Create a parameter in the parent playbook.</p>	Variables
<p>Map data to the parameter in the Reference a playbook step in the parent playbook.</p>	Step 1
<p>Apply the parameter to the Disable User Account connector action.</p>	
<p>Create a manual trigger and assign the user to a new variable.</p>	Step 2
	Step 3

Answer:

<p>Create a parameter in the child playbook.</p>	Answer Area
<p>Create a parameter in the parent playbook.</p>	Variables
<p>Map data to the parameter in the Reference a playbook step in the parent playbook.</p>	Step 1
<p>Apply the parameter to the Disable User Account connector action.</p>	
<p>Create a manual trigger and assign the user to a new variable.</p>	Step 2
	Step 3



4.Refer to the exhibit.

Triggering events

CSLAB Active Reconnaissance

Subpattern: Port_Scanning_LANtoSOC

Displaying 1 - 100 of 100
Jun 11, 2025, 01:45:00 PM - Jun 12, 2025, 01:45:00 PM

Event Receive Time	Event Name	Reporting IP	Source IP	Destination IP	Destination TCP/UDP Port
Jun 12, 2025, 01:44:28 PM	FortiGate-traffic-end-forward-client-rst	10.200.200.254	16 10.200.3.219	10.200.200.12	22
Jun 12, 2025, 01:44:28 PM	FortiGate-traffic-end-forward-server-rst	10.200.200.254	16 10.200.3.219	10.200.200.238	110
Jun 12, 2025, 01:43:53 PM	FortiGate-traffic-end-forward-timeout	10.200.200.254	16 10.200.3.219	10.200.200.183	443
Jun 12, 2025, 01:43:53 PM	FortiGate-traffic-end-forward-timeout	10.200.200.254	16 10.200.3.219	10.200.200.214	443
Jun 12, 2025, 01:43:53 PM	FortiGate-traffic-end-forward-timeout	10.200.200.254	16 10.200.3.219	10.200.200.81	443
Jun 12, 2025, 01:43:52 PM	FortiGate-traffic-end-forward-timeout	10.200.200.254	16 10.200.3.219	10.200.200.180	443

Event Attributes

Search...

Item	Value
Destination IP	10.200.200.12
Destination TCP/UDP Port	22
Event Name	FortiGate-traffic-end-forward-client-rst
Event Receive Time	Jun 12, 2025, 01:44:28 PM
Event Type	FortiGate-traffic-end-forward-client-rst
Reporting IP	10.200.200.254
Source IP	10.200.3.219

Lines: 7

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