Prepare Smart for Success Free Fortinet NSE6_OTS_AR-7.6 Exam Questions and Answers

Ready to pass faster? Grab free and updated Fortinet NSE 6 - OT Security 7.6 Architect exam PDF questions now. Get authentic NSE6_OTS_AR-7.6 dumps packed with verified answers and secure your certification success with PrepBolt NSE6_OTS_AR-7.6 exam pdf questions and answers.

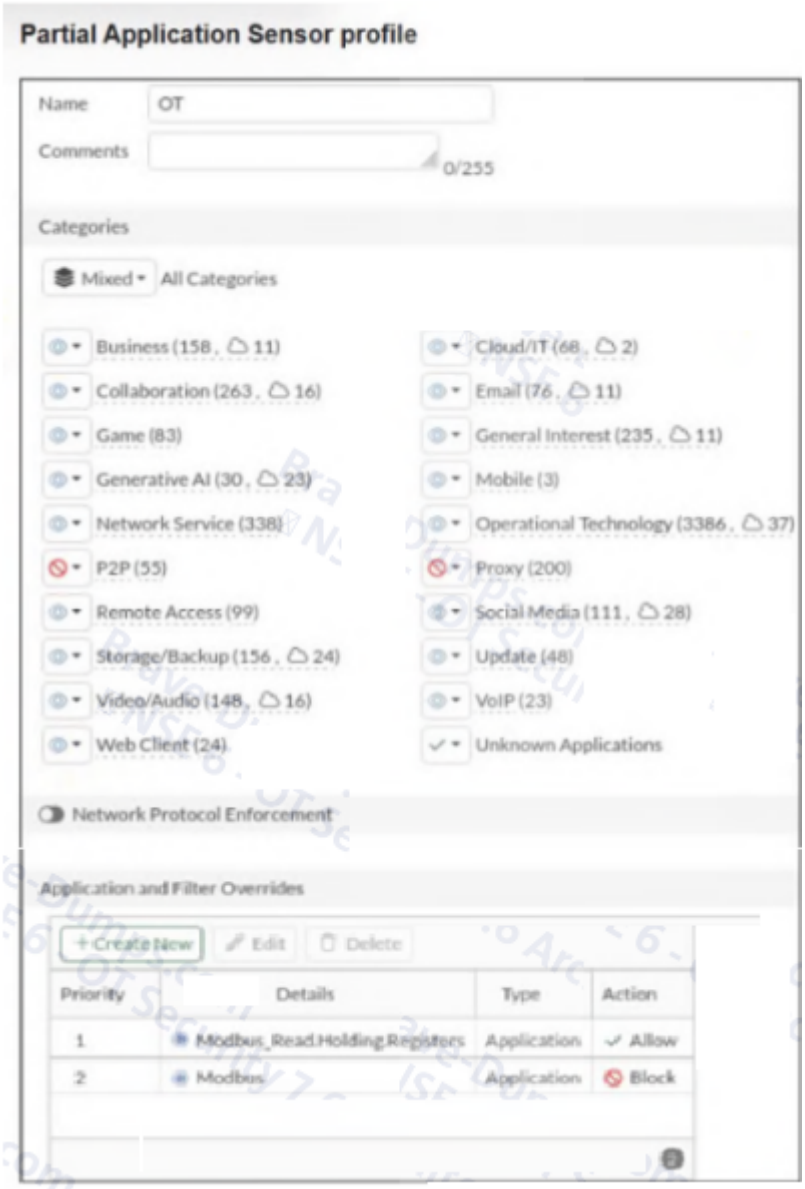
Thank you for Downloading NSE6_OTS_AR-7.6 exam PDF Demo

https://prepbolt.com/NSE6_OTS_AR-7.6.html

Question 1

Question Type: MultipleChoice

Refer to the exhibit.



A partial Application Sensor profile is shown. When you apply this profile in firewall policy, which two statements are correct? (Choose two answers)

Options:

A- OT signatures are enabled.

B- All OT protocols are monitored.

C- Modbus write commands are blocked.

D- A log is provided for each Modbus read holding registers command.

Answer:

A, C

Explanation:

The correct answers are A and C. The study guide explains that ''You can use application control signatures to detect OT protocols'' and that application control provides ''granular message type identification.'' In the exhibit, the Operational Technology application category is included in the Application Sensor profile, so OT application signatures are enabled in this profile.

Option C is also correct because the override table shows Modbus_Read.Holding.Registers = Allow and Modbus = Block. The study guide states that you can use specific granular application control signatures to allow a specific Modbus command and block all others, and it also shows that application control can identify read and write commands separately at message level. Therefore, Modbus write commands are blocked by this profile.

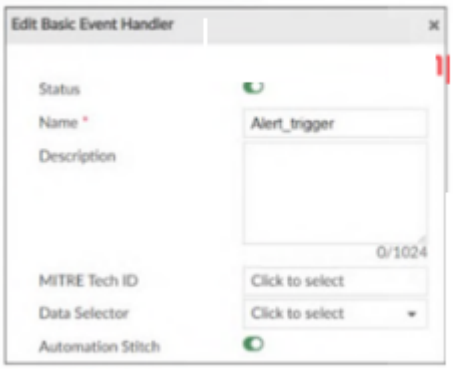
Option B is incorrect because the profile is not simply monitoring all OT protocols; it contains a Block action for Modbus. Option D is incorrect because the study guide links OT protocol visibility specifically to the monitor status, while in the exhibit Modbus_Read.Holding.Registers is set to Allow, not Monitor.

Question 2

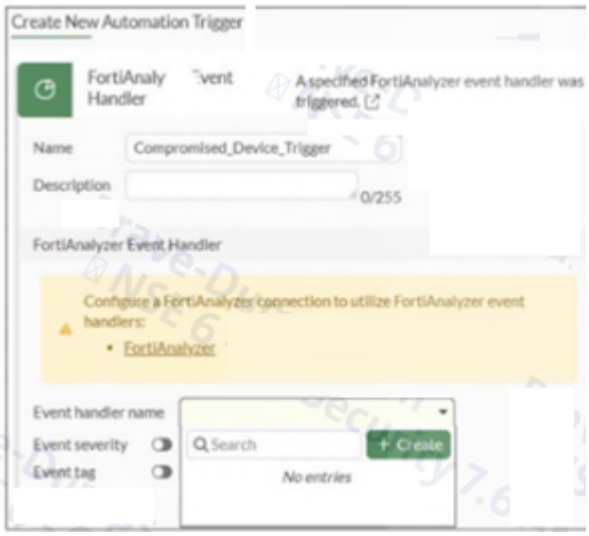
Question Type: MultipleChoice

Refer to the exhibits.

Partial Basic Event Handler page



Creation of a trigger



A partial Basic Event Handler page on FortiAnalyzer and the creation of a trigger in a FortiGate device are shown. To improve the protection of your OT network, you want to automate the handling of compromised devices notified through FortiAnalyzer. You have configured an event handler named Alert_trigger as shown in the exhibit. When you create the trigger on the FortiGate device, the Event handler name field does not provide the Alert_trigger option. What two actions must you perform to make the Alert_trigger option available? (Choose two answers)

Options:

A- You must click + Create in the Event handler name field.
B- You must authorize the FortiGate device on FortiAnalyzer.
C- You must configure the FortiAnalyzer setting on the FortiGate device.
D- You must configure the trigger on the root FortiGate.

Answer:

C, D

Explanation:

The correct answers are C and D.

Option C is correct because the study guide explains that when ''a handler generates an event with

the automation stitch option enabled, FortiAnalyzer sends a notification'' and, in the Security Fabric workflow, ''FortiAnalyzer parses the logs and notifies the root FortiGate.'' This means FortiGate must first have the FortiAnalyzer connection configured so it can consume FortiAnalyzer event handlers and use them in automation. The wizard message in the exhibit also points to this requirement by indicating that a FortiAnalyzer connection must be configured.

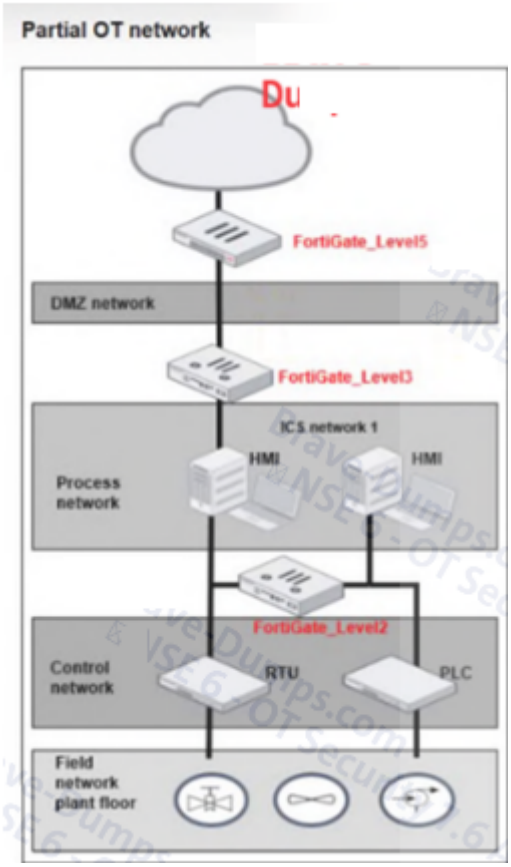
Option D is also correct because the study guide explicitly says that in this automation flow ''the root FortiGate triggers the action'' and shows ''Stitches configured on root FortiGate.'' Therefore, if you want the FortiAnalyzer event handler to appear and be usable for automation, the trigger must be configured on the root FortiGate, not on an arbitrary downstream FortiGate.

Option A is incorrect because + Create is only a GUI control and does not solve the missing-event-handler visibility problem. Option B is not identified in the study guide as the requirement for making a FortiAnalyzer event handler available in the FortiGate automation trigger list.

Question 3

Question Type: MultipleChoice

Refer to the exhibit.



A partial OT network is shown. In this OT network, you must add additional security measures to detect OT protocols and, therefore, increase the traffic visibility. Which security sensor must you implement to detect the OT protocols in this network? (Choose one answer)

Options:

A- Device detection on all the FortiGate interfaces.
B- Inline IDS on FortiGate_Level3.
C- Application sensor set to monitor on all the FortiGate devices.
D- IPS sensor on FortiGate_Level5.

Answer:

C

Explanation:

The correct answer is C. Application sensor set to monitor on all the FortiGate devices.

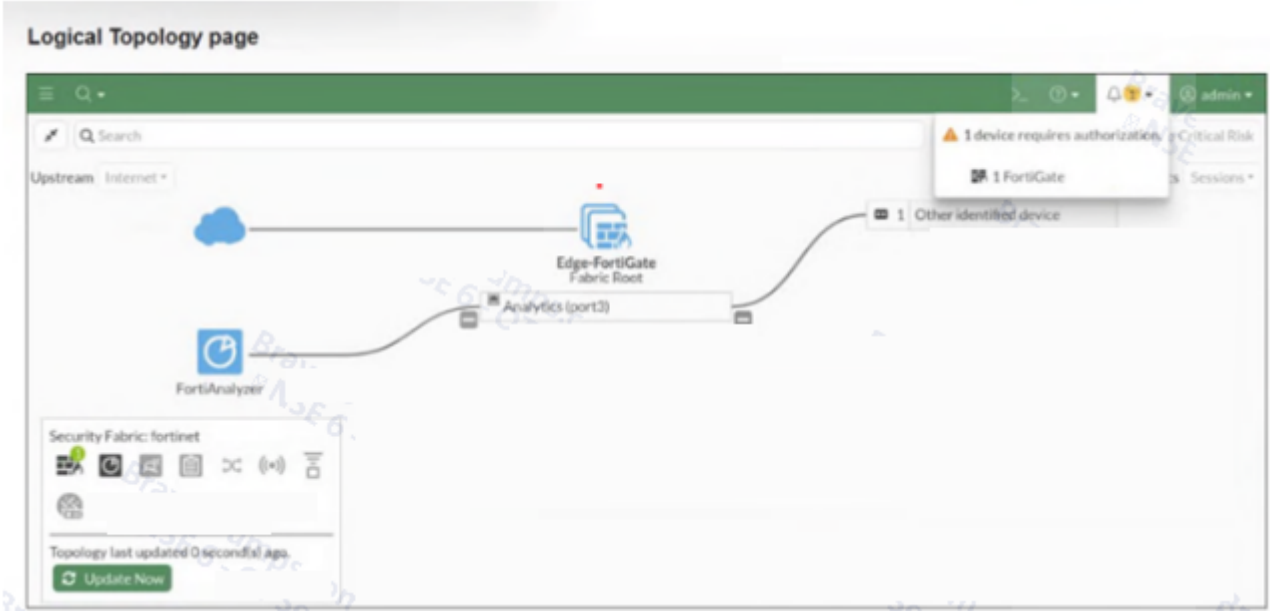
The study guide clearly explains that application control is the feature used to identify OT protocols. It states that ''application control detects the protocols used in applications like Modbus, IEC 104, and the contents of the telecontrol messages'' and also says ''You can use application control signatures to detect OT protocols.'' It further shows an example where a Modbus application control profile is enabled on a firewall policy ''for OT protocol visibility in the monitor status.'' This directly matches the requirement in the question, which is to detect OT protocols and increase traffic visibility.

The other options do not fit the requirement as precisely. Device detection is for identifying devices and collecting endpoint information, not for detecting industrial protocols. Inline IDS and IPS are focused more on detecting or blocking attacks, exploits, protocol abnormalities, and known vulnerabilities. While IPS can inspect some OT traffic, the study guide distinguishes it from application control by stating that IPS signatures tend to detect exploits, whereas application control signatures tend to provide protocol detection at various levels. Therefore, the required security sensor for OT protocol detection and traffic visibility is the application sensor in monitor mode.

Question 4

Question Type: MultipleChoice

Refer to the exhibit.



A Logical Topology page of a FortiGate device is shown. Your OT company wants to gain visibility into the network. You decide to implement device detection with the Security Fabric. Based on the exhibit, which statement is correct? (Choose one answer)

Options:

A- Device Detection is enabled on the other identified device.
B- The other identified device must be authorized on the root FortiGate.
C- The other identified device must be authorized on FortiAnalyzer.
D- Device Detection is enabled on port3.

Answer:

A

Explanation:

The correct answer is A. Device Detection is enabled on the other identified device.

The study guide explains that device identification is a ''useful feature for the Security Fabric topology view'' and that ''FortiGate detects most third-party devices in your network and adds them to the topology view of the Security Fabric.'' It also states that in the interfaces section, you can enable device detection, and this detection is what allows FortiGate to identify devices based on observed traffic.

In the exhibit, the tooltip distinguishes between ''1 device requires authorization'' and ''1 other identified device.'' That means the unauthorized device is a separate FortiGate/Fabric member issue, while the other identified device is simply a detected third-party device shown in the topology because device detection is working. Therefore, the correct interpretation is that device detection is enabled for that identified device. Option B is incorrect because the exhibit does not say the other identified device requires authorization. Option C is not supported by the study guide, and option D is too specific because no evidence in the exhibit confirms that the detection was enabled specifically on

port3.

Question 5

Question Type: MultipleChoice

Which industrial protocol does not support VLANs? (Choose one answer)

Options:

A- [Not clearly visible in the exhibit]
B- Ethernet over industrial protocol
C- EtherCAT
D- Modbus over TCP

Answer:

C

Explanation:

The correct answer is C. EtherCAT.

The study guide states that for industrial Ethernet protocols, ''such as Ethernet/IP and Modbus/TCP, you can use VLANs to segment your physical LAN into multiple logical LANs.'' This directly confirms that Ethernet/IP and Modbus/TCP support VLAN-based segmentation in the OT context.

By contrast, the guide explains that ''EtherCAT skips layers 3 to 6 to deliver real-time communication'' and describes it as an ''Open-Software Modified-Ethernet'' approach. Because it does not operate like the standard Ethernet/IP model used for normal VLAN-based segmentation, EtherCAT is the protocol identified here as not supporting VLANs in the way Ethernet/IP and Modbus/TCP do.

So, based on the study guide comparison, the verified answer is EtherCAT.

Question 6

Question Type: MultipleChoice

Refer to the exhibit.

Event Brave-Dumps.com	Event Status	Event Type	Count	Severity	First Occurrence	Last Update	Handler Brave-Dumps.com	Device Name
Schneider.Electric.Modicon.	Mitigated	IPS	16	Medium	a day ago	an hour ago	Default-Malicious-Code-Detection-By-Threat	Edge-FortiGate
Triangle.Research.Nano-10.	Mitigated	IPS	6	Medium	19 hours ago	19 hours ago	Default-Malicious-Code-Detection-By-Threat	Edge-FortiGate

Based on the information provided on the partial Event Monitor page shown in the exhibit, how was the attack detected? (Choose one answer)

Options:

A- Automatically by a stitch
B- Manually by an administrator
C- Automatically by a playbook
D- Automatically by an event handler

Answer:

D

Explanation:

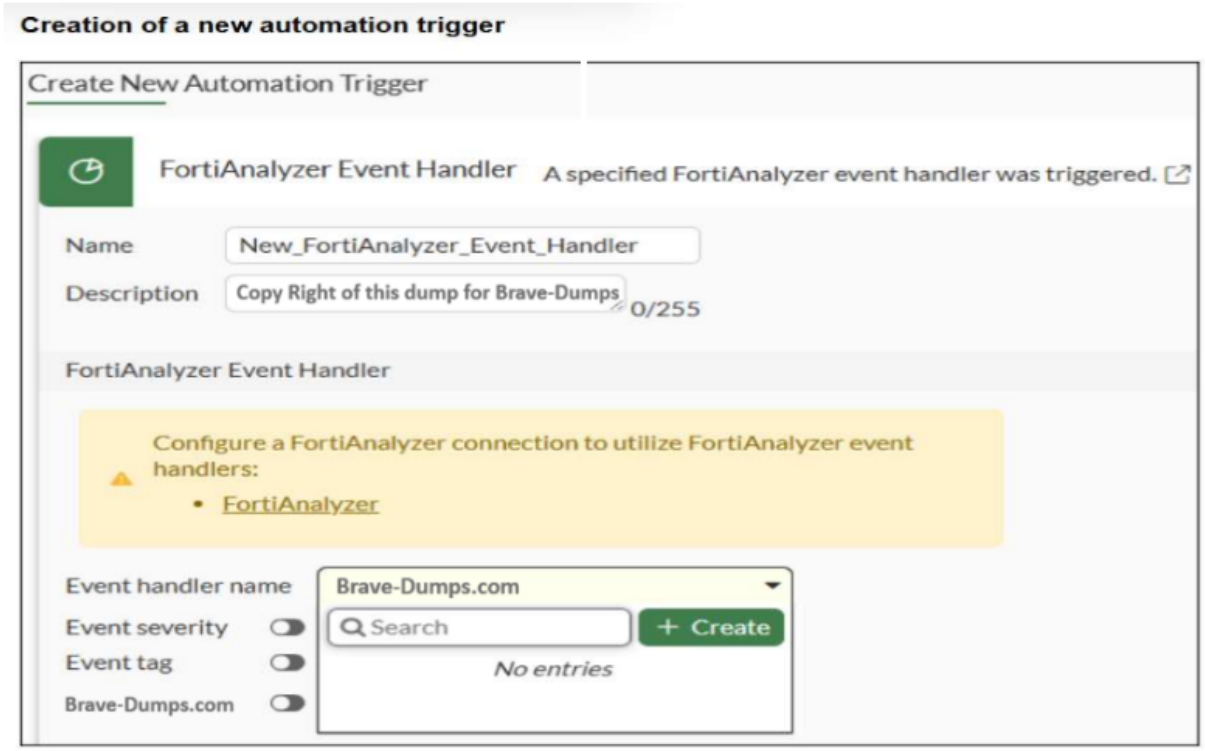
The correct answer is D. Automatically by an event handler. The study guide explicitly states that ''Event handlers generate events on FortiAnalyzer'' and ''FortiAnalyzer uses event handlers to filter all incoming logs. If the logs received match the conditions set in the event handlers, FortiAnalyzer generates an event.'' It also says ''You can view all generated events on the Event Monitor page.'' This directly matches the exhibit, which is showing entries on the Event Monitor page. Therefore, the attack shown there was detected automatically through an event handler.

The guide also explains the detection flow: ''FortiAnalyzer receives logs,'' ''FortiAnalyzer parses logs,'' and ''FortiAnalyzer generates an event if a rule is matched in an event handler.'' In addition, the Event Monitor view includes the Handler column, which identifies the event handler that generated the event. That is why the attack is not considered manually detected, and it is not primarily detected by a playbook or stitch. Playbooks and stitches are used for subsequent automation actions, but the event appearing in Event Monitor is created by the event handler mechanism.

Question 7

Question Type: MultipleChoice

Refer to the exhibit.



An automation trigger creation wizard is shown. You want to automate some tasks in your OT network. In a FortiGate device, you create a new automation trigger based on a FortiAnalyzer event handler. When you want to configure the Event handler name field, the event handler created in FortiAnalyzer is not shown. What are two reasons for this? (Choose two answers)

Options:

A- You must configure the Fabric settings on the FortiGate device.
B- You must enable Automation Stitch in the event handler on FortiAnalyzer.
C- You must click + Create in the Event handler name field.
D- You must add the FortiGate device to FortiAnalyzer and authorize it.

Answer:

A, B

Explanation:

The correct answers are A and B.

Option B is correct because the study guide states that ''When a handler generates an event with the automation stitch option enabled, FortiAnalyzer sends a notification'' to FortiGate. If Automation Stitch is not enabled in the FortiAnalyzer event handler, that handler will not be usable for the FortiGate automation-stitch workflow. The guide also explains that the configuration of each event handler can include ''Automation stitches'' and ''Rules,'' showing that this is a required part of the FortiAnalyzer-to-FortiGate automation path.

Option A is also correct. The study guide explains the automation flow in the Security Fabric: ''FortiAnalyzer parses the logs and notifies the root FortiGate'' and then ''The root FortiGate triggers the action.'' That means FortiGate must have the FortiAnalyzer connection configured through the Security Fabric side before it can consume FortiAnalyzer event handlers. The warning in the exhibit about configuring a FortiAnalyzer connection also points directly to that requirement.

Option C is incorrect because + Create is not the reason the existing event handler is missing; it is only an interface control. Option D is not the best answer for this item because the question is about why the event handler name list on FortiGate is empty for FortiAnalyzer-triggered automation. The study guide's verified requirements for that workflow are the FortiAnalyzer-to-FortiGate Fabric connection and enabling Automation Stitch on the FortiAnalyzer event handler.

Thank You for trying NSE6_OTS_AR-7.6 PDF Demo

To try our NSE6_OTS_AR-7.6 practice exam software visit link below

https://prepbolt.com/NSE6_OTS_AR-7.6.html

Start Your NSE6_OTS_AR-7.6 Preparation

Use Coupon “SAVE50” for extra 50% discount on the purchase of Practice Test Software. Test your NSE6_OTS_AR-7.6 preparation with actual exam questions.