

# Fortinet

## Exam Questions NSE7\_OTS-6.4

Fortinet NSE 7 - OT Security 6.4



#### NEW QUESTION 1

An OT supervisor needs to protect their network by implementing security with an industrial signature database on the FortiGate device. Which statement about the industrial signature database on FortiGate is true?

- A. A supervisor must purchase an industrial signature database and import it to the FortiGate.
- B. An administrator must create their own database using custom signatures.
- C. By default, the industrial database is enabled.
- D. A supervisor can enable it through the FortiGate CLI.

**Answer:** D

#### NEW QUESTION 2

An OT network architect needs to secure control area zones with a single network access policy to provision devices to any number of different networks. On which device can this be accomplished?

- A. FortiGate
- B. FortiEDR
- C. FortiSwitch
- D. FortiNAC

**Answer:** D

#### NEW QUESTION 3

What two advantages does FortiNAC provide in the OT network? (Choose two.)

- A. It can be used for IoT device detection.
- B. It can be used for industrial intrusion detection and prevention.
- C. It can be used for network micro-segmentation.
- D. It can be used for device profiling.

**Answer:** CD

#### NEW QUESTION 4

When you create a user or host profile, which three criteria can you use? (Choose three.)

- A. Host or user group memberships
- B. Administrative group membership
- C. An existing access control policy
- D. Location
- E. Host or user attributes

**Answer:** ADE

#### NEW QUESTION 5

An administrator wants to use FortiSoC and SOAR features on a FortiAnalyzer device to detect and block any unauthorized access to FortiGate devices in an OT network.

Which two statements about FortiSoC and SOAR features on FortiAnalyzer are true? (Choose two.)

- A. You must set correct operator in event handler to trigger an event.
- B. You can automate SOC tasks through playbooks.
- C. Each playbook can include multiple triggers.
- D. You cannot use Windows and Linux hosts security events with FortiSoC.

**Answer:** BC

#### Explanation:

Ref: <https://docs.fortinet.com/document/fortianalyzer/7.0.0/administration-guide/268882/fortisoc>

#### NEW QUESTION 6

As an OT administrator, it is important to understand how industrial protocols work in an OT network. Which communication method is used by the Modbus protocol?

- A. It uses OSI Layer 2 and the primary device sends data based on request from secondary device.
- B. It uses OSI Layer 2 and both the primary/secondary devices always send data during the communication.
- C. It uses OSI Layer 2 and both the primary/secondary devices send data based on a matching token ring.
- D. It uses OSI Layer 2 and the secondary device sends data based on request from primary device.

**Answer:** D

#### NEW QUESTION 7

An OT administrator configured and ran a default application risk and control report in FortiAnalyzer to learn more about the key application crossing the network. However, the report output is empty despite the fact that some related real-time and historical logs are visible in the FortiAnalyzer.

What are two possible reasons why the report output was empty? (Choose two.)

- A. The administrator selected the wrong logs to be indexed in FortiAnalyzer.
- B. The administrator selected the wrong time period for the report.
- C. The administrator selected the wrong devices in the Devices section.
- D. The administrator selected the wrong hcache table for the report.

**Answer:** BD

#### NEW QUESTION 8

Refer to the exhibit.



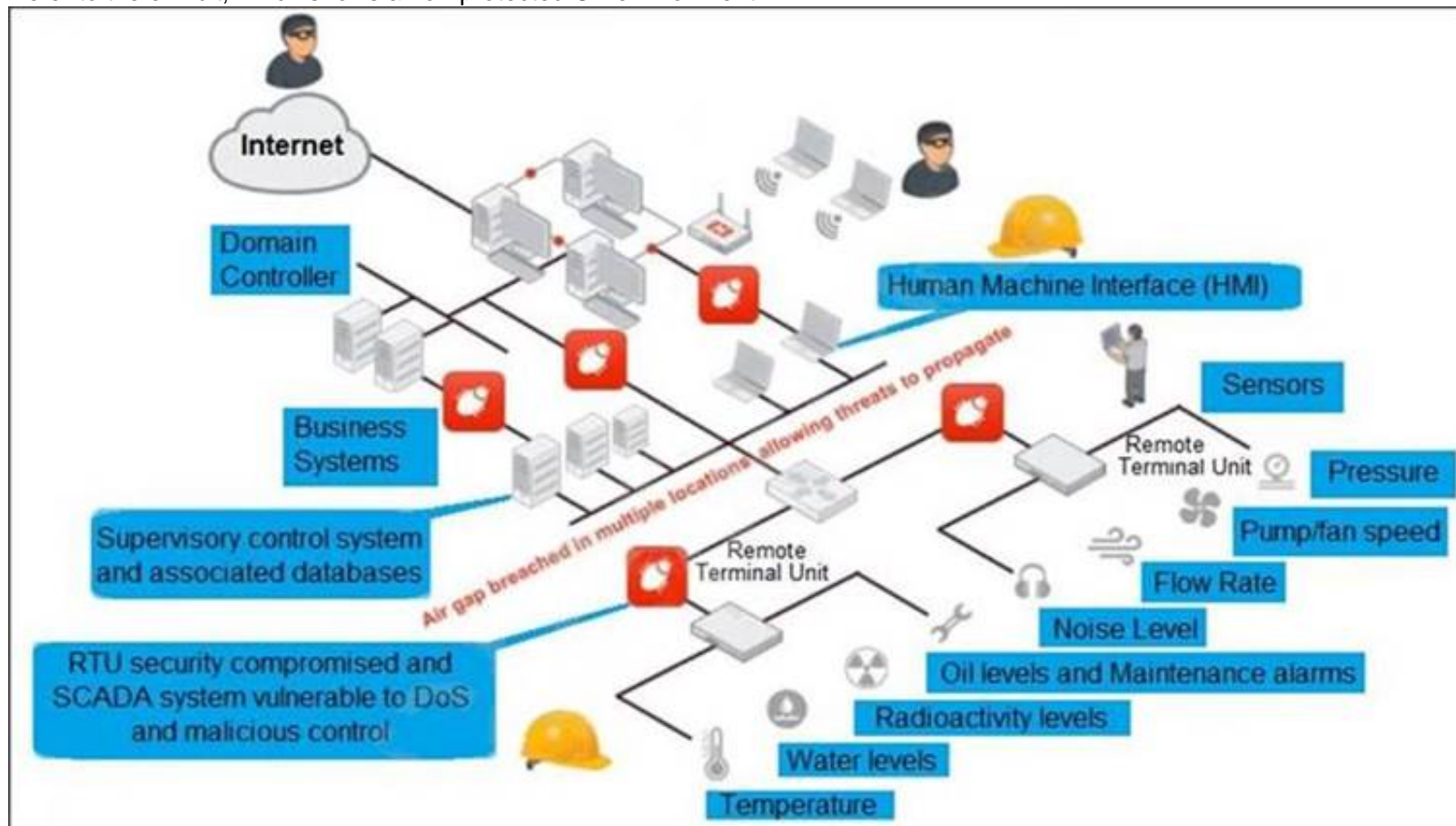
Based on the Purdue model, which three measures can be implemented in the control area zone using the Fortinet Security Fabric? (Choose three.)

- A. FortiGate for SD-WAN
- B. FortiGate for application control and IPS
- C. FortiNAC for network access control
- D. FortiSIEM for security incident and event management
- E. FortiEDR for endpoint detection

**Answer:** BCD

#### NEW QUESTION 9

Refer to the exhibit, which shows a non-protected OT environment.



An administrator needs to implement proper protection on the OT network.

Which three steps should an administrator take to protect the OT network? (Choose three.)

- A. Deploy an edge FortiGate between the internet and an OT network as a one-arm sniffer.
- B. Deploy a FortiGate device within each ICS network.
- C. Configure firewall policies with web filter to protect the different ICS networks.
- D. Configure firewall policies with industrial protocol sensors
- E. Use segmentation

**Answer:** ACD

#### NEW QUESTION 10

When device profiling rules are enabled, which devices connected on the network are evaluated by the device profiling rules?

- A. Known trusted devices, each time they change location
- B. All connected devices, each time they connect
- C. Rogue devices, only when they connect for the first time

D. Rogue devices, each time they connect

**Answer:** C

**NEW QUESTION 10**

An OT administrator is defining an incident notification policy using FortiSIEM and would like to configure the system with a notification policy. If an incident occurs, the administrator would like to be able to intervene and block an IP address or disable a user in Active Directory from FortiSIEM. Which step must the administrator take to achieve this task?

- A. Configure a fabric connector with a notification policy on FortiSIEM to connect with FortiGate.
- B. Create a notification policy and define a script/remediation on FortiSIEM.
- C. Define a script/remediation on FortiManager and enable a notification rule on FortiSIEM.
- D. Deploy a mitigation script on Active Directory and create a notification policy on FortiSIEM.

**Answer:** C

**NEW QUESTION 13**

An OT administrator deployed many devices to secure the OT network. However, the SOC team is reporting that there are too many alerts, and that many of the alerts are false positive. The OT administrator would like to find a solution that eliminates repetitive tasks, improves efficiency, saves time, and saves resources. Which products should the administrator deploy to address these issues and automate most of the manual tasks done by the SOC team?

- A. FortiSIEM and FortiManager
- B. FortiSandbox and FortiSIEM
- C. FortiSOAR and FortiSIEM
- D. A syslog server and FortiSIEM

**Answer:** C

**NEW QUESTION 14**

What are two benefits of a Nozomi integration with FortiNAC? (Choose two.)

- A. Enhanced point of connection details
- B. Direct VLAN assignment
- C. Adapter consolidation for multi-adapter hosts
- D. Importation and classification of hosts

**Answer:** AB

**NEW QUESTION 17**












What can be assigned using network access control policies?

- A. Layer 3 polling intervals
- B. FortiNAC device polling methods
- C. Logical networks
- D. Profiling rules

**Answer:** D

**NEW QUESTION 21**

Refer to the exhibit.

Maint	Device	Type	Organization	Avail Status	Perf Status	Security Status
	FG240D3913800441	Fortinet FortiOS	Super			
	SJ-QA-F-Lnx-CHK	Checkpoint FireWall	Super			
	FAPS321C-default	Fortinet FortiAP	Super			

You are navigating through FortiSIEM in an OT network. How do you view information presented in the exhibit and what does the FortiGate device security status tell you?

- A. In the PCI logging dashboard and there are one or more high-severity security incidents for the FortiGate device.
- B. In the summary dashboard and there are one or more high-severity security incidents for the FortiGate device.
- C. In the widget dashboard and there are one or more high-severity incidents for the FortiGate device.
- D. In the business service dashboard and there are one or more high-severity security incidents for the FortiGate device.

**Answer:** B

**NEW QUESTION 26**

.....

## Thank You for Trying Our Product

### We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questions and Answers in PDF Format

### NSE7\_OTS-6.4 Practice Exam Features:

- \* NSE7\_OTS-6.4 Questions and Answers Updated Frequently
- \* NSE7\_OTS-6.4 Practice Questions Verified by Expert Senior Certified Staff
- \* NSE7\_OTS-6.4 Most Realistic Questions that Guarantee you a Pass on Your FirstTry
- \* NSE7\_OTS-6.4 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year

**100% Actual & Verified — Instant Download, Please Click**  
**[Order The NSE7\\_OTS-6.4 Practice Test Here](#)**