Fortinet

NSEI_OTS_AR-7.6

Fortinet NSE I - OT Security 7.6 Architect

For More Information – Visit link below:

https://www.examsempire.com/

Product Version

1. Up to Date products, reliable and verified.
2. Questions and Answers in PDF Format.

Latest Version: 6.0

Question: 1

Which three device profiling methods of FortiNAC are considered non-direct?
(Choose three.)

A. Location
B. TCP
C. IP range
D. SSH
E. Network traffic

Answer: A,C,E

Question: 2

Which protocol and port is used by the Modbus protocol?

A. TCP port214
B. UDP port500
C. TCP port443
D. TCP port502

Answer: D

Question: 3

You are investigating a series of incidents that occurred in the OT network over past 24 hours in FortiSIEM. Which three FortiSIEM options can you use to investigate these incidents?
(Choose three.)

A. Security
B. IPS
C. List
D. Risk
E. Overview

Answer: C,D,E

Question: 4

An administrator needs to group FortiGate wireless interfaces in NAT mode with multiple physical interfaces. What interface type must the administrator select to group multiple FortiGate interfaces with the wireless interface?

A. Aggregate interface
B. VLAN interface
C. Software switch interface
D. Redundant interface

Answer: A

Question: 5

Which deployment option allows an administrator to detect intrusions without any modifications to production traffic?

A. Offline IPS
B. Offline IDS
C. Virtual patching
D. Inline IPS and IDS

Answer: B

Question: 6

Which three protocols are used as industrial Ethernet protocols?
(Choose three.)

A. M12
B. EtherCAT
C. RJ45
D. PROFINET
E. EtherNet/IP

Answer: B,D,E

Question: 7

In the context of FortiNAC, what is a key feature of a logical network?

A. It creates a one-to-one association between a network access policy and a VLAN.
B. It groups up to 10 VLANs into a single policy.
C. It simplifies network access policy management by reducing the number of policies needed.
D. It can identify several endpoints with a single rule.

Answer: C

Question: 8

Which two statements about FortiSIEM are true?
(Choose two.)

A. FortiSIEM can receive data from certain devices in SQL format.
B. FortiSIEM can receive and collect data from network devices and applications.
C. FortiSIEM can receive data from any network device and application.
D. FortiSIEM cannot receive data from a Windows server without an agent.

Answer: B,D

Question: 9

A supervisor is configuring an application filter sensor to block Modbus traffic between PLC-1 and PLC-2.
When creating a new application sensor, the supervisor is not able see any industrial signatures.
Which change must the supervisor must make in order to see all the industrial signatures in the application filter?

A. The supervisor must contact the FortiGuard team to collect the industrial signature database.
B. The supervisor must configure exclude-signatures to none.
C. The supervisor must enable the FortiGuard industrial signatures under config system global.
D. The supervisor must generate some Modbus logs in order to see the Modbus signatures.

Answer: B

Question: 10

What is the main difference between real-time logs and historical logs on FortiAnalyzer?

A. Historical logs are indexed in the SQL database, but real-time logs are not.
B. Real-time logs are indexed in the SQL database, but historical logs are not.
C. Historical logs are compressed and real-time logs are indexed in the SQL database.

D. Real-time logs are indexed while historical logs are compressed in the SQL database.

Answer: A

Thank You for Trying Our Product

Special 16 USD Discount Coupon: NSZUBG3X

Email: support@examsempire.com

Check our Customer Testimonials and ratings available on every product page.

Visit our website.

https://examsempire.com/