

Fortinet

Exam Questions NSE7_OTS-7.2

Fortinet NSE 7 - OT Security 7.2



NEW QUESTION 1

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: BC

Explanation:

https://fortinetweb.s3.amazonaws.com/docs.fortinet.com/v2/attachments/32cb817d-a307-11eb-b70b-00505692583a/FortiAnalyzer-7.0.0-Administration_Guide.pdf

NEW QUESTION 2

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 3

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: BCE

NEW QUESTION 4

Refer to the exhibit.

	Name	Type	IP/Netmask	VLAN ID
Physical Interface 14				
	port1	Physical Interface	10.200.1.1/255.255.255.0	
	port1-vlan10	VLAN	10.1.10.1/255.255.255.0	10
	port1-vlan1	VLAN	10.200.5.1/255.255.255.0	1
	port10	Physical Interface	10.0.11.1/255.255.255.0	
	port2	Physical Interface	10.200.2.1/255.255.255.0	
	port2-vlan10	VLAN	10.0.10.1/255.255.255.0	10
	port2-vlan1	VLAN	10.0.5.1/255.255.255.0	1

Which statement about the interfaces shown in the exhibit is true?

- A. port2, port2-vlan10, and port2-vlan1 are part of the software switch interface.
- B. The VLAN ID of port1-vlan1 can be changed to the VLAN ID 10.
- C. port1-vlan10 and port2-vlan10 are part of the same broadcast domain
- D. port1, port1-vlan10, and port1-vlan1 are in different broadcast domains

Answer: D

NEW QUESTION 5

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: AD

Explanation:

The two benefits of a Nozomi integration with FortiNAC are enhanced point of connection details and importation and classification of hosts. Enhanced point of connection details allows for the identification and separation of traffic from multiple points of connection, such as Wi-Fi, wired, cellular, and VPN. Importation and classification of hosts allows for the automated importing and classification of host and device information into FortiNAC. This allows for better visibility and control of the network.

NEW QUESTION 6

Which three methods of communication are used by FortiNAC to gather visibility information? (Choose three.)

- A. SNMP
- B. ICMP
- C. API
- D. RADIUS
- E. TACACS

Answer: ACD

NEW QUESTION 7

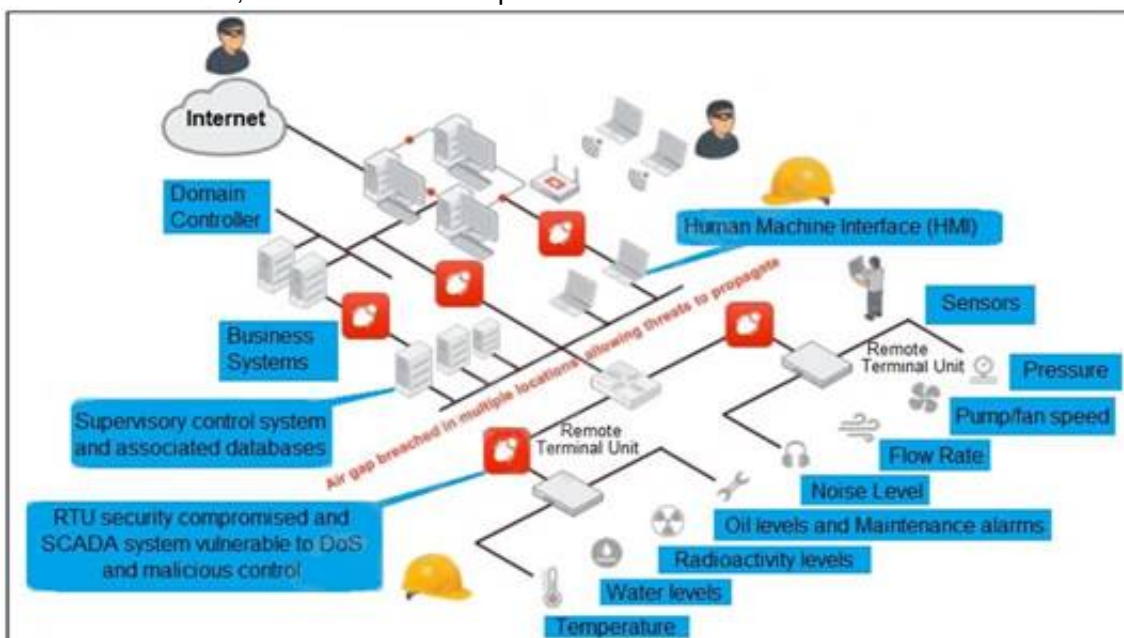
You are investigating a series of incidents that occurred in the OT network over past 24 hours in FortiSIEM. Which three FortiSIEM options can you use to investigate these incidents? (Choose three.)

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

Answer: CDE

NEW QUESTION 8

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 9

The OT network analyst runs different level of reports to quickly explore threats that exploit the network. Such reports can be run on all routers, switches, and firewalls. Which FortiSIEM reporting method helps to identify these type of exploits of image firmware files?

- A. CMDB reports
- B. Threat hunting reports
- C. Compliance reports
- D. OT/IoT reports

Answer: B

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: B

Explanation:

<https://fusecommunity.fortinet.com/blogs/silviu/2022/04/12/fortisiempublishingscript>

NEW QUESTION 10

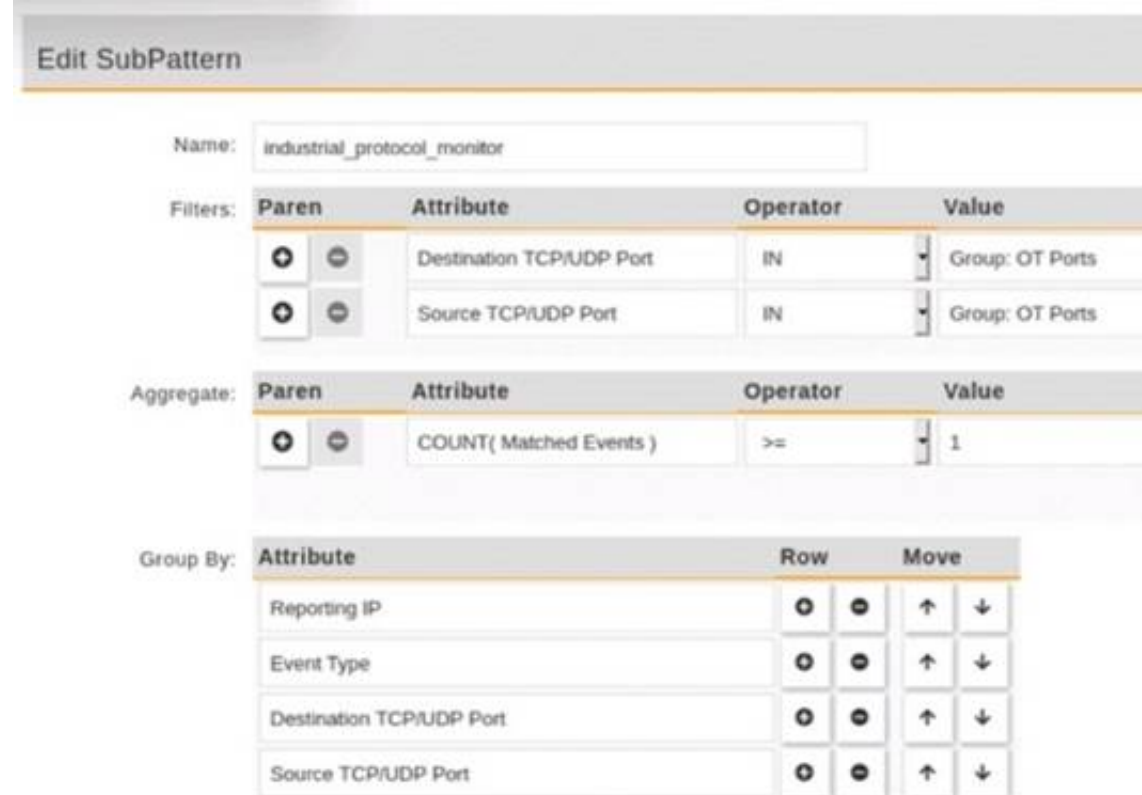
Which two statements about the Modbus protocol are true? (Choose two.)

- A. Modbus uses UDP frames to transport MBAP and function codes.
- B. Most of the PLC brands come with a built-in Modbus module.
- C. You can implement Modbus networking settings on internetworking devices.
- D. Modbus is used to establish communication between intelligent devices.

Answer: BC

NEW QUESTION 15

Refer to the exhibit.



Edit SubPattern

Name: industrial_protocol_monitor

Filters:

Paren	Attribute	Operator	Value
<input type="radio"/>	Destination TCP/UDP Port	IN	Group: OT Ports
<input type="radio"/>	Source TCP/UDP Port	IN	Group: OT Ports

Aggregate:

Paren	Attribute	Operator	Value
<input type="radio"/>	COUNT(Matched Events)	>=	1

Group By:

Attribute	Row	Move
Reporting IP	<input type="radio"/>	<input type="radio"/>
Event Type	<input type="radio"/>	<input type="radio"/>
Destination TCP/UDP Port	<input type="radio"/>	<input type="radio"/>
Source TCP/UDP Port	<input type="radio"/>	<input type="radio"/>

An operational technology rule is created and successfully activated to monitor the Modbus protocol on FortiSIEM. However, the rule does not trigger incidents despite Modbus traffic and application logs being received correctly by FortiSIEM. Which statement correctly describes the issue on the rule configuration?

- A. The first condition on the SubPattern filter must use the OR logical operator.
- B. The attributes in the Group By section must match the ones in Fitters section.
- C. The Aggregate attribute COUNT expression is incompatible with the filters.
- D. The SubPattern is missing the filter to match the Modbus protocol.

Answer: B

NEW QUESTION 18

Refer to the exhibit and analyze the output.


```
[PH_DEV_MON_NET_INTF_UTIL] : [eventSeverity] =PHL_INFO, [filename] =phPerfJob.cpp,
[lineNumber] =6646, [intfName]= Intel [R] PRO_100 MT Network
Connection, [intfAlias] =, [hostname] =WIN2K8DC, [hostIpAddr] = 192.168.69.6,
[pollIntv] =56, [recvBytes64] =
44273, [recvBitsPerSec] = 6324.714286, [inIntfUtil] = 0.000632, [sentBytes64] =
82014, [sentBitsPerSec] = 1171
6.285714, [outIntfUtil] = 0.001172, [recvPkts64] = 449, [sentPkts64] = 255,
[inIntfPktErr] = 0, [inIntfPktErrPct] = 0.000000, [outIntfPktErr] =0,
[outIntfPktErrPct] = 0.000000, [inIntfPktDiscarded] =0, [inIntfPktDiscardedPct] =
```

Which statement about the output is true?

- A. This is a sample of a FortiAnalyzer system interface event log.
- B. This is a sample of an SNMP temperature control event log.
- C. This is a sample of a PAM event type.
- D. This is a sample of FortiGate interface statistics.

Answer: C

NEW QUESTION 22

What are two critical tasks the OT network auditors must perform during OT network risk assessment and management? (Choose two.)

- A. Planning a threat hunting strategy
- B. Implementing strategies to automatically bring PLCs offline
- C. Creating disaster recovery plans to switch operations to a backup plant
- D. Evaluating what can go wrong before it happens

Answer: BC

NEW QUESTION 26

What triggers Layer 2 polling of infrastructure devices connected in the network?

- A. A failed Layer 3 poll
- B. A matched security policy
- C. A matched profiling rule
- D. A linkup or linkdown trap

Answer: D

NEW QUESTION 28

Which type of attack posed by skilled and malicious users of security level 4 (SL 4) of IEC 62443 is designed to defend against intentional attacks?

- A. Users with access to moderate resources
- B. Users with low access to resources
- C. Users with unintentional operator error
- D. Users with substantial resources

Answer: C

NEW QUESTION 33

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

Explanation:

<https://docs.fortinet.com/document/fortinac/9.2.0/administration-guide/15797/user-host-profiles>

NEW QUESTION 37

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: AB

Explanation:

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

NEW QUESTION 39

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 43

.....

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-7.2 Practice Exam Features:

- * NSE7_OTS-7.2 Questions and Answers Updated Frequently
- * NSE7_OTS-7.2 Practice Questions Verified by Expert Senior Certified Staff
- * NSE7_OTS-7.2 Most Realistic Questions that Guarantee you a Pass on Your FirstTry
- * NSE7_OTS-7.2 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year

100% Actual & Verified — Instant Download, Please Click
[Order The NSE7_OTS-7.2 Practice Test Here](#)