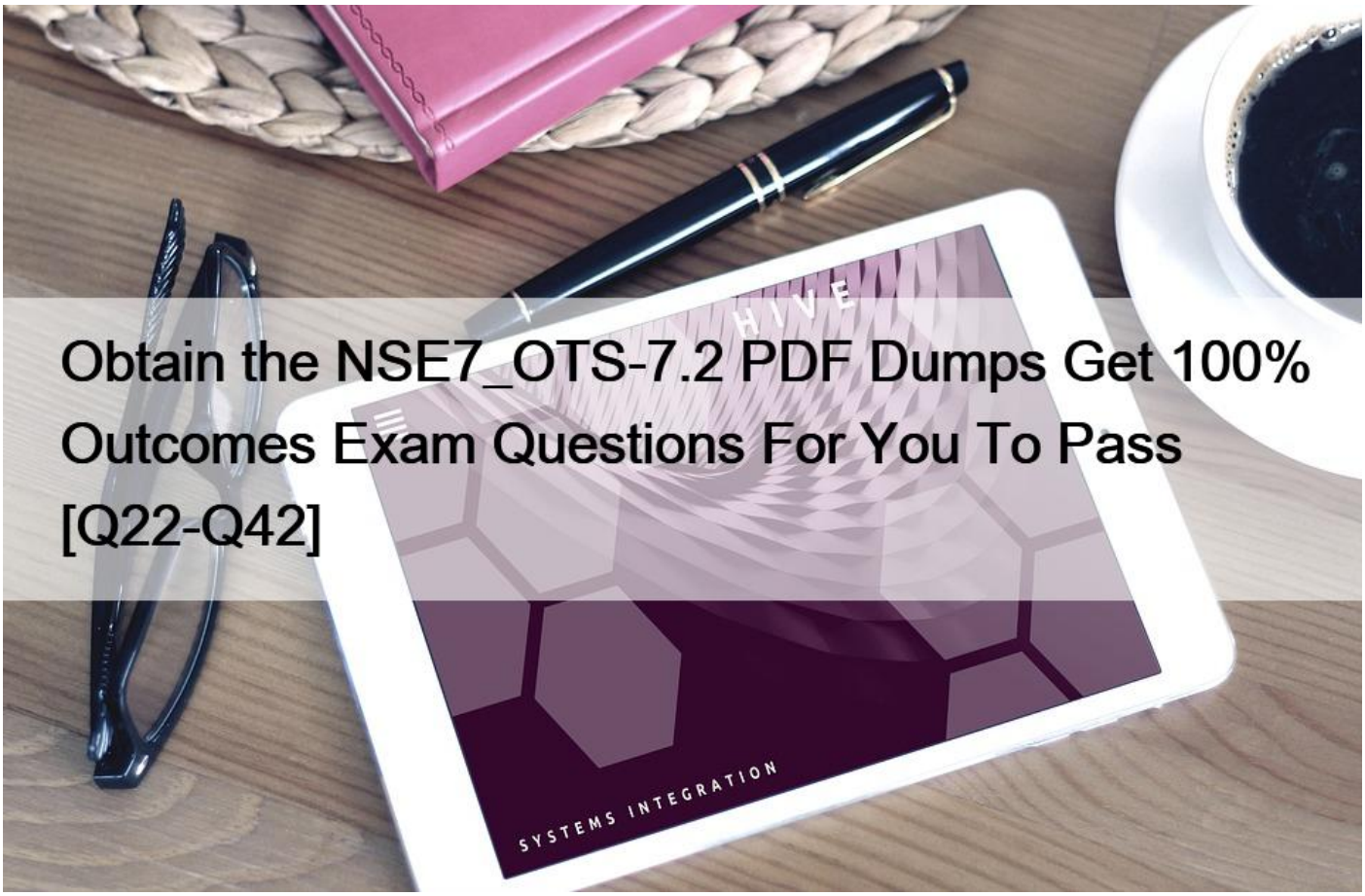
Obtain the NSE7_OTS-7.2 PDF Dumps Get 100% Outcomes Exam Questions For You To Pass [Q22-Q42



Obtain the NSE7_OTS-7.2 PDF Dumps Get 100% Outcomes Exam Questions For You To Pass
NSE7_OTS-7.2 Exam Dumps Contains FREE Real Quesions from the Actual Exam

Fortinet NSE7_OTS-7.2 certification exam is designed to validate the knowledge and skills of network security professionals in the field of operational technology (OT) security. Operational technology refers to the use of technology to control and monitor physical processes in industries such as manufacturing, energy, and transportation. As these industries become increasingly digitized, the need for skilled professionals who can secure these systems against cyber threats is growing. The NSE7_OTS-7.2 exam covers topics such as OT security fundamentals, network security architecture, access control, threat detection and response, and incident response. Passing the exam demonstrates a high level of proficiency in securing OT networks and devices.

NEW QUESTION 22

An OT architect has deployed a Layer 2 switch in the OT network at Level 1 the Purdue model-process control. The purpose of the Layer 2 switch is to segment traffic between PLC1 and PLC2 with two VLANs.

All the traffic between PLC1 and PLC2 must first flow through the Layer 2 switch and then through the FortiGate device in the Level 2 supervisory control network.

What statement about the traffic between PLC1 and PLC2 is true?
* The Layer 2 switch rewrites VLAN tags before sending traffic to the FortiGate device.
* The Layer 2 switches routes any traffic to the FortiGate device through an Ethernet link.
* PLC1 and PLC2 traffic must flow through the Layer-2 switch trunk link to the FortiGate device.
* In order to communicate, PLC1 must be in the same VLAN as PLC2.

Explanation

The statement that is true about the traffic between PLC1 and PLC2 is that PLC1 and PLC2 traffic must flow through the Layer-2 switch trunk link to the FortiGate device.

NEW QUESTION 23

How can you achieve remote access and internel availability in an OT network?
* Create a back-end backup network as a redundancy measure.
* Implement SD-WAN to manage traffic on each ISP link.
* Add additional internal firewalls to access OT devices.
* Create more access policies to prevent unauthorized access.

NEW QUESTION 24

Refer to the exhibit.

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?

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

NEW QUESTION 25

What are two benefits of a Nozomi integration with FortiNAC? (Choose two.)
* Enhanced point of connection details
* Direct VLAN assignment
* Adapter consolidation for multi-adapter hosts
* Importation and classification of hosts

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 26

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?
* FortiSIEM and FortiManager
* FortiSandbox and FortiSIEM
* FortiSOAR and FortiSIEM
* A syslog server and FortiSIEM

NEW QUESTION 27

Which three common breach points can be found in a typical OT environment? (Choose three.)
* Global hat
* Hard hat
* VLAN exploits
* Black hat
* RTU exploits

NEW QUESTION 28

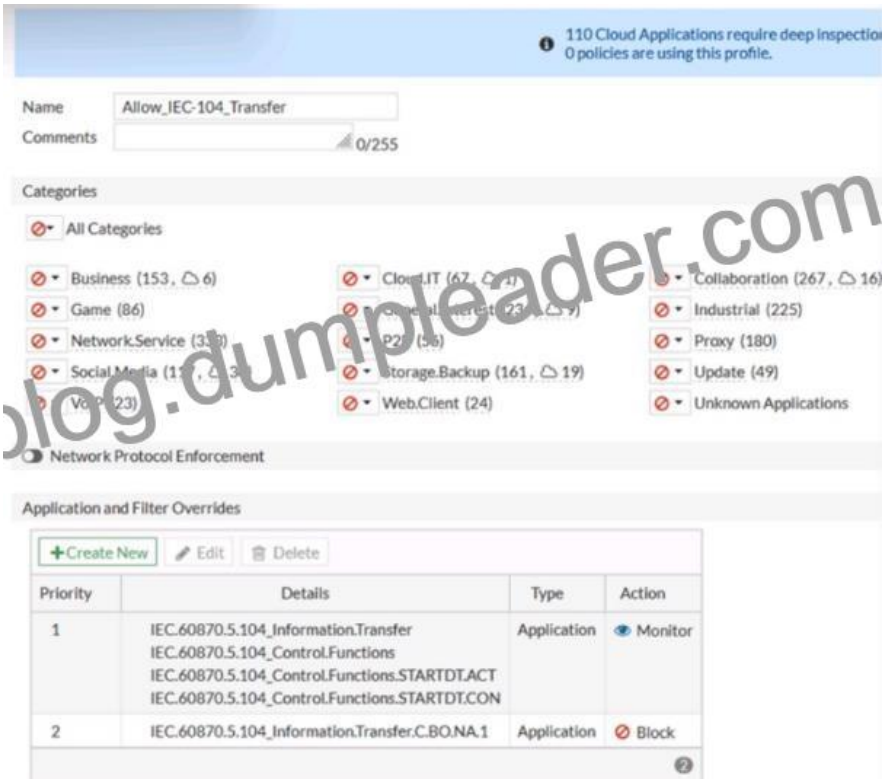
Which type of attack posed by skilled and malicious users of security level 4 (SL 4) of IEC 62443 is designed to defend against intentional attacks?
* Users with access to moderate resources
* Users with low access to resources
* Users with unintentional operator error
* Users with substantial resources

NEW QUESTION 29

What are two benefits of a Nozomi integration with FortiNAC? (Choose two.)
* Adapter consolidation for multi-adapter hosts
* Direct VLAN assignment
* Importation and classification of hosts
* Enhanced point of connection details

NEW QUESTION 30

Refer to the exhibit.



An OT network security audit concluded that the application sensor requires changes to ensure the correct security action is committed against the overrides filters.

Which change must the OT network administrator make?
* Set all application categories to apply default actions.
* Change the security action of the industrial category to monitor.
* Set the priority of the C.BO.NA.1 signature override to 1.
* Remove IEC.60870.5.104 Information.Transfer from the first filter override.

Explanation

According to the Fortinet NSE 7 – OT Security 6.4 exam guide1, the application sensor settings allow you to configure the security action for each application category andnetwork protocol override. The security action determines how the FortiGate unit handles traffic that matches the application category or network protocol override. The security action can be one of the following:

Allow: The FortiGate unit allows the traffic without any further inspection.

Monitor: The FortiGate unit allows the traffic and logs it for monitoring purposes.

Block: The FortiGate unit blocks the traffic and logs it as an attack.

The priority of the network protocol override determines the order in which the FortiGate unit applies the security action to the traffic. The lower the priority number, the higher the priority. For example, a priority of 1 is higher than a priority of 10.

In the exhibit, the application sensor has the following settings:

The industrial category has a security action of allow, which means that the FortiGate unit will not inspect or log any traffic that belongs to this category.

The IEC.60870.5.104 Information.Transfer network protocol override has a security action of block, which means that the FortiGate unit will block and log any traffic that matches this protocol.

The IEC.60870.5.104 Control.Functions network protocol override has a security action of monitor, which means that the FortiGate unit will allow and log any traffic that matches this protocol.

The IEC.60870.5.104 Start/Stop network protocol override has a security action of allow, which means that the FortiGate unit will not inspect or log any traffic that matches this protocol.

The IEC.60870.5.104 Transfer.C.BO.NA.1 network protocol override has a security action of block, which means that the FortiGate unit will block and log any traffic that matches this protocol.

The problem with these settings is that the IEC.60870.5.104 Transfer.C.BO.NA.1 network protocol override has a lower priority than the IEC.60870.5.104 Information.Transfer network protocol override. This means that if the traffic matches both protocols, the FortiGate unit will apply the security action of the higher priority override, which is block. However, the IEC.60870.5.104 Transfer.C.BO.NA.1 protocol is used to transfer binary outputs, which are essential for controlling OT devices. Therefore, blocking this protocol could have negative consequences for the OT network.

To fix this issue, the OT network administrator must set the priority of the IEC.60870.5.104 Transfer.C.BO.NA.1 network protocol override to 1, which is higher than the priority of the IEC.60870.5.104 Information.Transfer network protocol override. This way, the FortiGate unit will apply the security action of the lower priority override, which is allow, to the traffic that matches both protocols. This will ensure that the FortiGate unit does not block the traffic that is used to transfer binary outputs, while still blocking the traffic that is used to transfer information.

1: NSE 7 Network Security Architect – Fortinet

NEW QUESTION 31

When you create a user or host profile, which three criteria can you use? (Choose three.)
* Host or user group memberships
* Administrative group membership
* An existing access control policy
* Location
* Host or user attributes

Explanation

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

NEW QUESTION 32

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

NEW QUESTION 33

An OT network architect must deploy a solution to protect fuel pumps in an industrial remote network. All the fuel pumps must be closely monitored from the corporate network for any temperature fluctuations.

How can the OT network architect achieve this goal?
* Configure a fuel server on the remote network, and deploy a FortiSIEM with a single pattern temperature security rule on the corporate network.
* Configure a fuel server on the corporate network, and deploy a FortiSIEM with a single pattern temperature performance rule on the remote network.
* Configure a fuel server on the remote network, and deploy a FortiSIEM with a single pattern temperature performance rule on the corporate network.
* Configure both fuel server and FortiSIEM with a single-pattern temperature performance rule on the corporate network.
Explanation

This way, FortiSIEM can discover and monitor everything attached to the remote network and provide security visibility to the corporate network

NEW QUESTION 34

As an OT network administrator, you are managing three FortiGate devices that each protect different levels on the Purdue model. To increase traffic visibility, you are required to implement additional security measures to detect exploits that affect PLCs.

Which security sensor must implement to detect these types of industrial exploits?
* Intrusion prevention system (IPS)
* Deep packet inspection (DPI)
* Antivirus inspection
* Application control

NEW QUESTION 35

Refer to the exhibit.

```
config system interface
     edit VLAN101_dmz
          set forward-domain 101
next
     edit VLAN101_internal
          set forward-domain 101
end
```

Given the configurations on the FortiGate, which statement is true?
* FortiGate is configured with forward-domains to reduce unnecessary traffic.
* FortiGate is configured with forward-domains to forward only domain controller traffic.
* FortiGate is configured with forward-domains to forward only company domain website traffic.
* FortiGate is configured with forward-domains to filter and drop non-domain controller traffic.

NEW QUESTION 36

An OT administrator has configured FSSO and local firewall authentication. A user who is part of a user group is not prompted from credentials during authentication.

What is a possible reason?
* FortiGate determined the user by passive authentication
* The user was determined by Security Fabric
* Two-factor authentication is not configured with RADIUS authentication method
* FortiNAC determined the user by DHCP fingerprint method

NEW QUESTION 37

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.

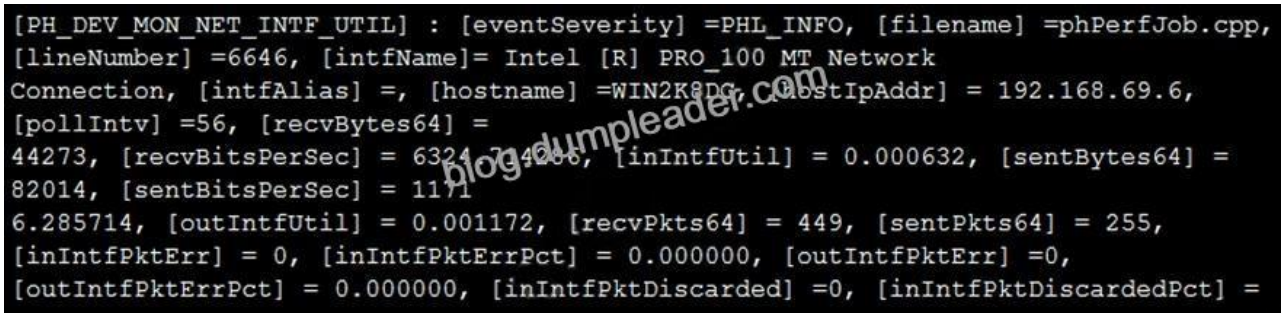
What are two possible reasons why the report output was empty? (Choose two.)
* The administrator selected the wrong logs to be indexed in FortiAnalyzer.
* The administrator selected the wrong time period for the report.
* The administrator selected the wrong devices in the Devices section.
* The administrator selected the wrong hcache table for the report.

Explanation

https://fortinetweb.s3.amazonaws.com/docs.fortinet.com/v2/attachments/32cb817d-a307-11eb-b70b-0050569258

NEW QUESTION 38

Refer to the exhibit and analyze the output.



Which statement about the output is true?
* This is a sample of a FortiAnalyzer system interface event log.
* This is a sample of an SNMP temperature control event log.
* This is a sample of a PAM event type.
* This is a sample of FortiGate interface statistics.

NEW QUESTION 39

What are two critical tasks the OT network auditors must perform during OT network risk assessment and management? (Choose two.)
* Planning a threat hunting strategy
* Implementing strategies to automatically bring PLCs offline
* Creating disaster recovery plans to switch operations to a backup plant
* Evaluating what can go wrong before it happens

NEW QUESTION 40

An OT network consists of multiple FortiGate devices. The edge FortiGate device is deployed as the secure gateway and is only allowing remote operators to access the ICS networks on site.

Management hires a third-party company to conduct health and safety on site. The third-party company must have outbound access to external resources.

As the OT network administrator, what is the best scenario to provide external access to the third-party company while continuing to secure the ICS networks?
* Configure outbound security policies with limited active authentication users of the third-party company.
* Create VPN tunnels between downstream FortiGate devices and the edge FortiGate to protect ICS network traffic.
* Split the edge FortiGate device into multiple logical devices to allocate an independent VDOM for the third-party company.
* Implement an additional firewall using an additional upstream link to the internet.

NEW QUESTION 41

What two advantages does FortiNAC provide in the OT network? (Choose two.)
* It can be used for IoT device detection.
* It can be used for industrial intrusion detection and prevention.
* It can be used for network micro-segmentation.
* It can be used for device profiling.

Explanation

Typically, in a microsegmented network, NGFWs are used in conjunction with VLANs to implement security policies and to inspect and filter network communications. Fortinet FortiSwitch and FortiGate NGFW offer an integrated approach to microsegmentation.

Use Real Fortinet Achieve the NSE7_OTS-7.2 Dumps - 100% Exam Passing Guarantee:
https://www.dumpleader.com/NSE7_OTS-7.2_exam.html]