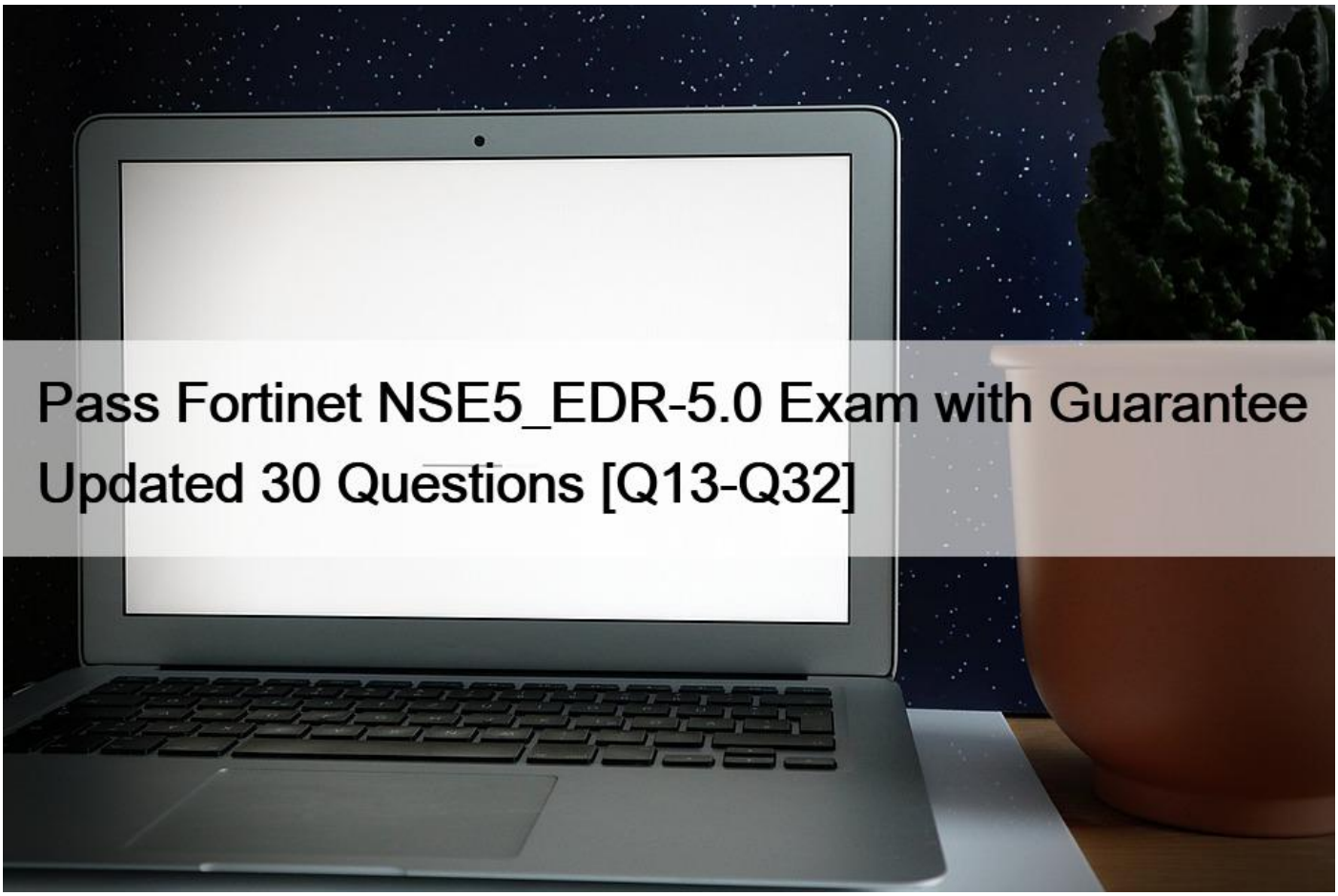
Pass Fortinet NSE5_EDR-5.0 Exam with Guarantee Updated 30 Questions [Q13-Q32

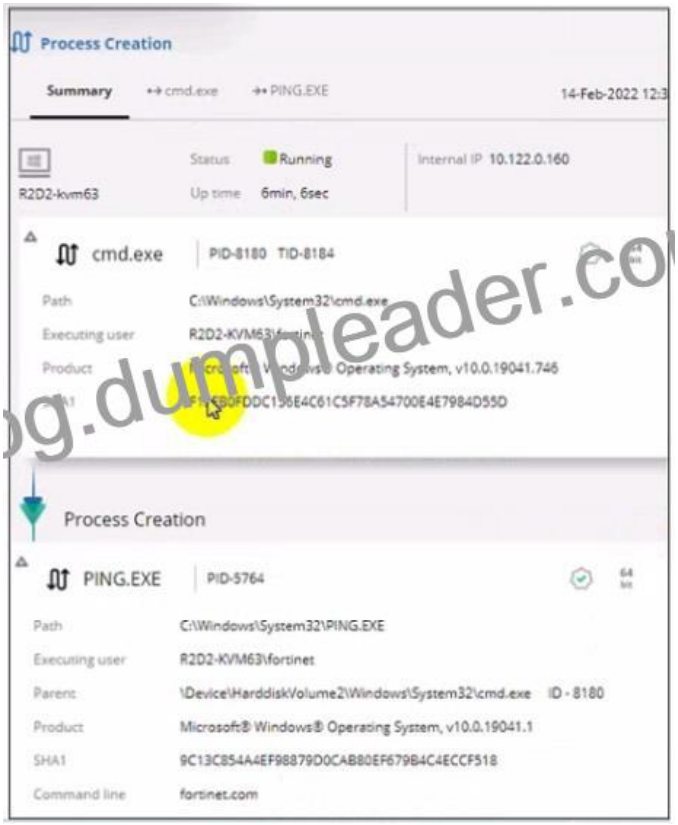


Pass Fortinet NSE5_EDR-5.0 Exam with Guarantee Updated 30 Questions
Latest NSE5_EDR-5.0 Pass Guaranteed Exam Dumps Certification Sample Questions

FortiEDR is an endpoint detection and response solution that provides advanced threat intelligence, detection, and response capabilities. The solution is designed to protect endpoints from advanced threats such as malware, ransomware, and zero-day attacks. FortiEDR integrates with other Fortinet solutions such as FortiGate, FortiSandbox, and FortiClient to provide a comprehensive security solution. The Fortinet NSE5_EDR-5.0 Exam validates the candidate's ability to deploy, manage, and troubleshoot FortiEDR 5.0 solution.

NEW QUESTION 13

Refer to the exhibit.



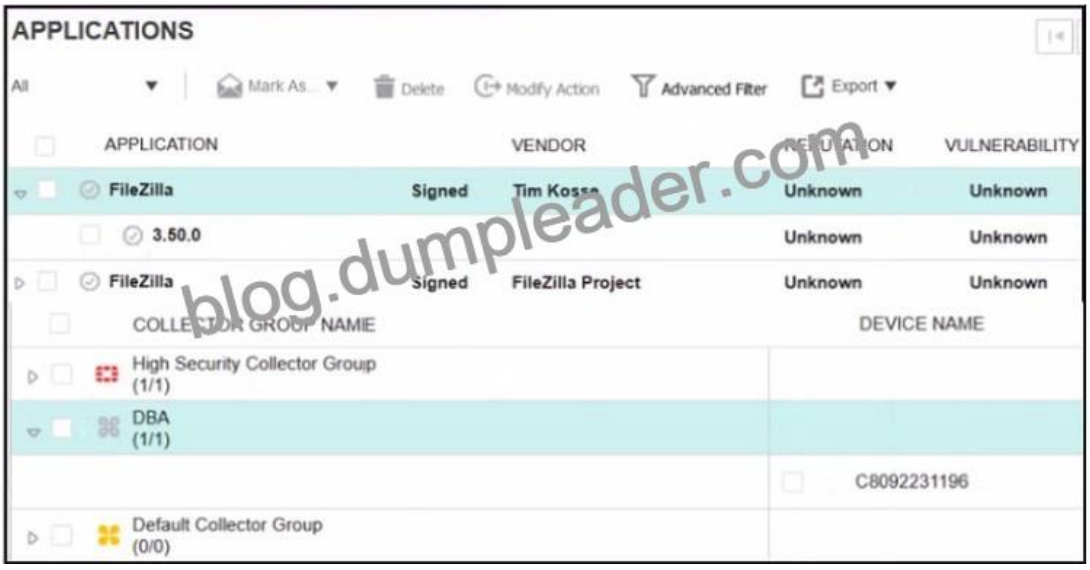
Based on the threat hunting event details shown in the exhibit, which two statements about the event are true?

(Choose two.)

* The PING EXE process was blocked
* The user fortinet has executed a ping command
* The activity event is associated with the file action
* There are no MITRE details available for this event

NEW QUESTION 14

Refer to the exhibits.



blog.dumpleader.com

The exhibits show application policy logs and application details Collector C8092231196 is a member of the Finance group What must an administrator do to block the FileZilia application?

* Deny application in Finance policy
* Assign Finance policy to DBA group
* Assign Finance policy to Default Collector Group
* Assign Simulation Communication Control Policy to DBA group

NEW QUESTION 15

What is the benefit of using file hash along with the file name in a threat hunting repository search?

* It helps to make sure the hash is really a malware
* It helps to check the malware even if the malware variant uses a different file name
* It helps to find if some instances of the hash are actually associated with a different file
* It helps locate a file as threat hunting only allows hash search

NEW QUESTION 16

A company requires a global communication policy for a FortiEDR multi-tenant environment.

How can the administrator achieve this?

* An administrator creates a new communication control policy and shares it with other organizations
* A local administrator creates new a communication control policy and shares it with other organizations
* A local administrator creates a new communication control policy and assigns it globally to all organizations
* An administrator creates a new communication control policy for each organization

NEW QUESTION 17

Refer to the exhibits.

The exhibits show the collector state and active connections. The collector is unable to connect to aggregator IP address 10.160.6.100 using default port.

Based on the netstat command output what must you do to resolve the connectivity issue?
* Reinstall collector agent and use port 443
* Reinstall collector agent and use port 8081
* Reinstall collector agent and use port 555
* Reinstall collector agent and use port 6514

NEW QUESTION 18

What is true about classifications assigned by Fortinet Cloud Sen/ice (FCS)?
* The core is responsible for all classifications if FCS playbooks are disabled
* The core only assigns a classification if FCS is not available
* FCS revises the classification of the core based on its database
* FCS is responsible for all classifications

NEW QUESTION 19

Exhibit.

Based on the forensics data shown in the exhibit, which two statements are true? (Choose two.)

* An exception has been created for this event
* The forensics data is displayed m the stacks view
* The device has been isolated
* The exfiltration prevention policy has blocked this event

NEW QUESTION 20

A FortiEDR security event is causing a performance issue with a third-parry application. What must you do first about the event?

* Contact Fortinet support
* Terminate the process and uninstall the third-party application
* Immediately create an exception
* Investigate the event to verify whether or not the application is safe

NEW QUESTION 21

Refer to the exhibit.

blog.dumpleader.com

Based on the threat hunting query shown in the exhibit which of the following is true?
* RDP connections will be blocked and classified as suspicious
* A security event will be triggered when the device attempts a RDP connection
* This query is included in other organizations
* The query will only check for network category

NEW QUESTION 22

What is the purpose of the Threat Hunting feature?
* Delete any file from any collector in the organization
* Find and delete all instances ofa known malicious file or hash inthe organization
* Identify all instances of a known malicious file or hash and notify affected users
* Execute playbooks to isolate affected collectors in the organization

NEW QUESTION 23

Which two types of remote authentication does the FortiEDR management console support? (Choose two.)
* Radius
* SAML
* TACACS
* LDAP

NEW QUESTION 24

Which threat hunting profile is the most resource intensive?
* Comprehensive
* Inventory
* Default
* Standard Collection

New NSE5_EDR-5.0 Test Materials & Valid NSE5_EDR-5.0 Test Engine:
https://www.dumpleader.com/NSE5_EDR-5.0_exam.html]