DUMPSQUEEN

Fortinet NSE 5 - FortiEDR 5.0 Exam

Fortinet NSE5_EDR-5.0

Version Demo

Total Demo Questions: 5

Total Premium Questions: 30

Buy Premium PDF

dumpsqueen.com

QUESTION NO: 1

Which connectors can you use for the FortiEDR automated incident response? (Choose two.)

A. FortiNAC

B. FortiGate

C. FortiSiem

D. FortiSandbox

ANSWER: B C

QUESTION NO: 2

Refer to the exhibits.

APPLICATION DETAILS
FileZilla

Policies

Policy		Action	
Default Communication Control ... FORTINET		Allow	According to policy
Servers Policy FORTINET		Deny	According to policy
Finance Policy		Deny	Manually
Simulation Communication Control Policy		Allow	According to policy
Isolation Policy FORTINET		Deny	According to policy

ASSIGNED COLLECTOR GROUPS
Finance Policy
Unassign Group

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 FileZilla application?

A. Deny application in Finance policy

B. Assign Finance policy to DBA group

C. Assign Finance policy to Default Collector Group

D. Assign Simulation Communication Control Policy to DBA group

ANSWER: D

QUESTION NO: 3

Which two types of remote authentication does the FortiEDR management console support? (Choose two.)

A. Radius

B. SAML

C. TACACS

D. LDAP

ANSWER: A D

QUESTION NO: 4

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

A. Contact Fortinet support

B. Terminate the process and uninstall the third-party application

C. Immediately create an exception

D. Investigate the event to verify whether or not the application is safe

ANSWER: C

QUESTION NO: 5

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

A. It helps to make sure the hash is really a malware

B. It helps to check the malware even if the malware variant uses a different file name

C. It helps to find if some instances of the hash are actually associated with a different file

D. It helps locate a file as threat hunting only allows hash search

ANSWER: C