EXAMTOPICS

-Expert Verified, Online, **Free**.



CERTIFICATION TEST

-CertificationTest.net - Cheap & Quality Resources With Best Support

Question #1 *Topic 1*

What is true about classifications assigned by Fortinet Cloud Service (FCS)?

A. FCS revises the classification of the core based on its database.

B. The core only assigns a classification if FCS is not available.

C. FCS is responsible for all classifications.

D. The core is responsible for all classifications if FCS playbooks are disabled.

Suggested Answer: *A*
Official Answer: C

Demian2 Highly Voted 8 months ago
correct it's A.
upvoted 6 times

fontabest99 Highly Voted 8 months ago
it should be A
upvoted 5 times

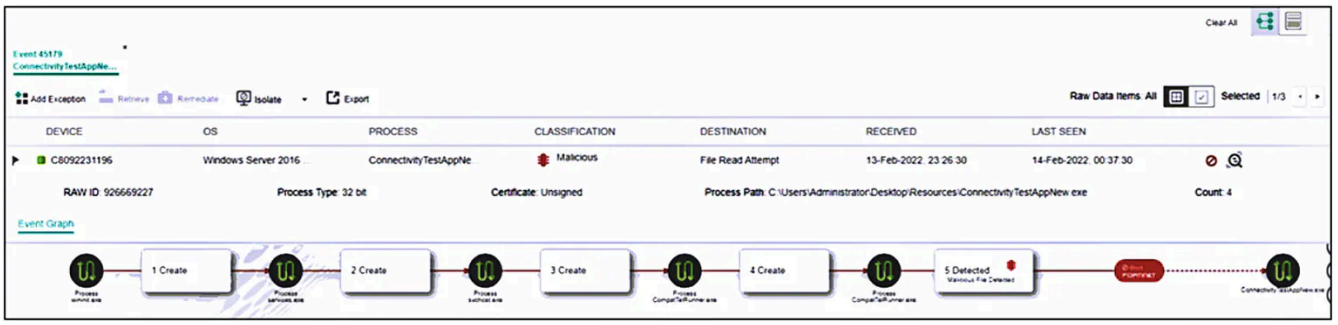
khanchand 8 months ago
It should be A
upvoted 5 times

Chogi_ 8 months ago
Correct ans. is A
upvoted 4 times

50f3ed5 Most Recent 8 months ago
Selected Answer: A
I think correct answer is A.
upvoted 1 times

Question #2 *Topic 1*

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



A. The device cannot be remediated.

B. The execution prevention policy has blocked this event.

C. The event was blocked because the certificate is unsigned.

D. Device C8092231196 has been isolated.

Suggested Answer: *A, B*
Official Answer: CD

fontabest99 Highly Voted 8 months ago

Selected Answer: A, B

they are the real answer

upvoted 5 times

Computerhigh 8 months ago

A and B are the correct Answers If you look the Remediate Button is Greyed out so it cannot be remediated You also don't see the Icon for Isolation so the Collector is not isolated Unsigned Certificates don't necessarily trigger an action. Hard to see from the picture but the malicious action was taken during the execution phase , and the red block icon is visible

upvoted 4 times

Latrel 8 months ago

A & B Remediate Button is Greyed out and execution prevention policie block. This questions is avaliable on the FortiEDR Lab Guide pag 32

upvoted 2 times

yonandres 8 months ago

Selected Answer: A, B

A & B are the answer

upvoted 2 times

thinasci01 Most Recent 8 months ago

Selected Answer: A, B

the correct answer is A and B.

upvoted 1 times

Question #3 *Topic 1*

Refer to the exhibit.

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



A. The NGAV policy has blocked TestApplication.exe.

B. FCS classified the event as malicious.

C. TestApplication.exe is sophisticated malware.

D. The user was able to launch TestApplication.exe.

Suggested Answer: *C, D*
Official Answer: AB

Agent1994 Highly Voted 8 months ago

A. False. NGAV is execution prevention. https://docs.fortinet.com/document/fortiedr/5.2.1/administration-guide/354083/introducing-fortiedr B. False. It should say "by FortinetCloudServices" C. True. Mostly because A & B are false. D. True. Exfiltration happens after execution.

upvoted 5 times

Latrel 8 months ago

Selected Answer: C, D

the correct answer is C and D. Similar cenario available on the FortiEDR Lab Guide pag 38 "Stop and think! Why wasn't the process caught by the Execution Prevention policy like you saw earlier? Because, in some cases, with brand new or very sophisticated malware, NGAV cannot detect the attack. This is when the post-infection prevention policies really shine. An unrecognized malicious program may occasionally be allowed to launch, but FortiEDR will stop it before it is able to cause harm."

upvoted 3 times

BrunoLu 8 months ago

Selected Answer: A, C

A. TRUE. NGAV is execution prevention."This blocks the execution of files that are identified as malicious or suspected to be malicious." I find this in the link: https://docs.fortinet.com/document/fortiedr/5.2.1/administration-guide/354083/introducing-fortiedr B. False. It should say "by FortinetCloudServices" C. True. D. FALSE. The NGAV will block it

upvoted 3 times

Chogi_ 8 months ago

Ans. are C&D - exact explanation.

upvoted 2 times

rac_sp Most Recent 8 months ago

Selected Answer: C, D

The file was executed. As you can see in the screenshot the Exfiltration Policy was invoked, therefore this policy is invoked in the post infection phase of the EDR protection method. So if it is in the post infection phase, then NGAV was not capable to block the execution of the file.

upvoted 2 times

Question #4 *Topic 1*

How does FortiEDR implement post-infection protection?

A. By insurance against ransomware

B. By preventing data exfiltration or encryption even after a breach occurs

C. By real-time filtering to prevent malware from executing

D. By using methods used by traditional EDR

Suggested Answer: *B*
Official Answer: B

Miccyg Highly Voted 8 months ago

Selected Answer: B

"post-infection"

upvoted 7 times

Chogi_ 8 months ago

Ans. is C - https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortiedr.pdf

upvoted 3 times

thinasci01 8 months ago

Selected Answer: B

the correct answer is B.

upvoted 1 times

Adancorrea 8 months ago

Selected Answer: B

B - Correct Answer

upvoted 1 times

soporte127 Most Recent 8 months ago

why b?

upvoted 1 times

Question #5 *Topic 1*

Which scripting language is supported by the FortiEDR action manager?

A. TCL

B. Bash

C. Perl

D. Python

Suggested Answer: *D*
Official Answer: D

Chogi_ Highly Voted 8 months ago
Ans. D - Phyton
upvoted 5 times

ebenav11 8 months ago
Python
upvoted 2 times

burcurt21 8 months ago
Selected Answer: D
The scripting language supported by the FortiEDR Action Manager is Python.
upvoted 1 times

thinasci01 8 months ago
Selected Answer: D
the correct answer is D. Python
upvoted 1 times

torrespdr Most Recent 8 months ago
D - Phyton
upvoted 1 times

Question #6 *Topic 1*

Which security policy has all of its rules disabled by default?

A. Exfiltration Prevention

B. Execution Prevention

C. Device Control

D. Ransomware Prevention

Suggested Answer: *C*
Official Answer: D

edcwsxqaz Highly Voted 8 months ago

Selected Answer: C

The correct answer is Device Control.

upvoted 10 times

fontabest99 Highly Voted 8 months ago

The correct answer is Device Control. FortiEDR_5.0_Study_Guide-Online.pdf page 83

upvoted 6 times

Latrel 8 months ago

The correct answer is Device Control.

upvoted 1 times

thinasci01 8 months ago

Selected Answer: C

the correct answer is C. Device Control

upvoted 1 times

ebenav11 Most Recent 8 months ago

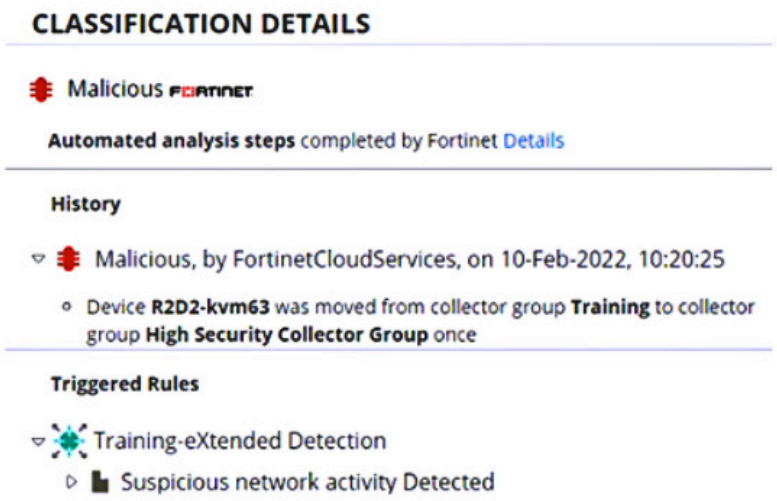
Selected Answer: C

Option C SECURITY POLICIES Device Control USB Application Specific Device Detected Block Disabled USB Audio Device Detected Block Disabled USB Audio/Video Device Detected Block Disabled USB Base Class Device Detected Block Disabled USB Billboard Device Detected Block Disabled USB CDC-Data Device Detected Block Disabled USB Communications and CDC Control Device Detected Block Disabled USB Content Security Device Detected Block Disabled

upvoted 1 times

Question #7 *Topic 1*

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



A. The policy is in simulation mode.

B. The device is moved to isolation.

C. The event has been blocked.

D. Playbooks is configured for this event.

Suggested Answer: *A, D*
Official Answer: AD

pgg1896 8 months ago

Selected Answer: A, D

eXtended Detection Policy operates only in simulation mode, A&D are correct

upvoted 3 times

ebenav11 8 months ago

Selected Answer: B, D

The correct answer are B and D Any policy in Simulation Mode, has the next label Simulation Device PC-X was moved from collector group Default-Group to collector group High Security Collector Group once Simulation Device PC-Y was isolated once In this case device wasnt isolated.

upvoted 3 times

fontabest99 8 months ago

Selected Answer: B, D

the correct answer are B and D, FortiEDR study guide pag 96

upvoted 3 times

rac_sp 8 months ago

Selected Answer: A, D

first, it was an extended detection. So automation plays a rule here. Extended detections operates in simulation mode

upvoted 2 times

BrunoLu Most Recent 8 months ago

A&D,I check the FortiEDR study guide pag 96,but i think A and D is correct

upvoted 2 times

Question #8 *Topic 1*

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

A. FortiSandbox

B. FortiSiem

C. FortiNAC

D. FortiGate

Suggested Answer: *C, D*
Official Answer: AB

Agent1994 Highly Voted 8 months ago
C & D FortiEDR_5.0_Study_Guide page 106
upvoted 8 times

fontabest99 Highly Voted 8 months ago
it must be C & D
upvoted 5 times

khanchand 8 months ago
It must be C & D
upvoted 5 times

edcwsxqaz 8 months ago
Selected Answer: C, D
the correct are C & D
upvoted 4 times

DataConsult Most Recent 8 months ago
C & D are Correct FortiNAC to Isolate a device FortiGate to block a milicious IP
upvoted 1 times

Question #9 *Topic 1*

Which FortiEDR component is required to find malicious files on the entire network of an organization?

A. FortiEDR Aggregator

B. FortiEDR Threat Hunting Repository

C. FortiEDR Central Manager

D. FortiEDR Core

Suggested Answer: *B*
Official Answer: C

fontabest99 Highly Voted 8 months ago
FortiEDR Threat Hunting Repository : fortiedr guide page 15: FIND AND DELETE KNOWN MALWARE ON ANY DEVICE WITHIN THE SYSTEM
upvoted 6 times

Chogi_ 8 months ago
Ans. is B
upvoted 3 times

Adancorrea 8 months ago
Selected Answer: B
B - Correct Answer
upvoted 2 times

thinasci01 Most Recent 8 months ago
Selected Answer: B
the correct answer is B.
upvoted 1 times

Question #10 *Topic 1*

Which threat hunting profile is the most resource intensive?

A. Inventory

B. Comprehensive

C. Standard Collection

D. Default

Suggested Answer: *B*
Official Answer: B

Adancorrea 8 months ago

Selected Answer: B

B - Comprehensive

upvoted 2 times

neojosele 8 months ago

B - Comprehensive

upvoted 2 times

4ng3l0v 8 months ago

B is correct, pag 176

upvoted 1 times

thinasci01 Most Recent 8 months ago

Selected Answer: B

the correct answer is B. Comprehensive

upvoted 1 times

Question #11 *Topic 1*

What is the role of a collector in the communication control policy?

A. A collector is used to change the reputation score of any application that collector runs

B. A collector can quarantine unsafe applications from communicating

C. A collector blocks unsafe applications from running

D. A collector records applications that communicate externally

Suggested Answer: *D*
Official Answer: B

Agent1994 8 months ago
A: False. B: False. The collector doesn't quarantine, it blocks the communication. C: False. It's not execution prevention. D: True.
FortiEDR_5.0_Study_Guide page 117
upvoted 4 times

headhunter24 8 months ago
Selected Answer: D
Corrent Answer D
upvoted 4 times

Adancorrea 8 months ago
Selected Answer: D
D - Corrent Answer
upvoted 2 times

Latrel 8 months ago
D is the correct answer
upvoted 1 times

thinasci01 Most Recent 8 months ago
Selected Answer: D
the correct answer is D.
upvoted 1 times

Question #12 *Topic 1*

A company requires a global communication policy for a FortiEDR multi-tenant environment.
How can the administrator achieve this?

A. An administrator creates a new communication control policy and shares it with other organizations.

B. A local administrator creates a new communication control policy and shares it with other organizations.

C. An administrator creates a new communication control policy for each organization.

D. A local administrator creates a new communication control policy and assigns it globally to all organizations.

Suggested Answer: *C*
Official Answer: C

Latrel 8 months ago

Selected Answer: C

The correct answer is C. I performed this test in my lab and it requires the admin user to create a new communication control rule in each organization. The local admin user can only create the rule in the organization he belongs to. The hoster view does not enable the applications and policies sub-item on the Communication control tab.

upvoted 3 times

thinasci01 8 months ago

Selected Answer: C

the answer C. is correct.

upvoted 2 times

ebenav11 8 months ago

Opction C https://docs.fortinet.com/document/fortiedr/5.2.1/administration-guide/967281/communication-control

upvoted 2 times

e93df3f 8 months ago

Selected Answer: C

Correct Answer.

upvoted 1 times

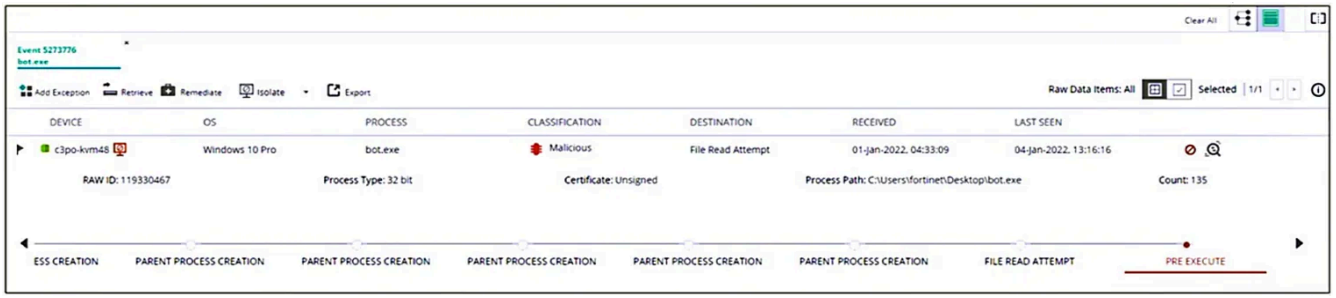
Dani_Prime Most Recent 8 months ago

Totally agree!! I check it on my FortiEDR console.

upvoted 1 times

Question #13 *Topic 1*

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



A. An exception has been created for this event.

B. The device has been isolated.

C. The exfiltration prevention policy has blocked this event.

D. The forensics data is displayed in the stacks view.

Suggested Answer: *B, D*
Official Answer: AD

headhunter24 Highly Voted 8 months ago

Selected Answer: B

Correct answer B & D

upvoted 6 times

DataConsult 8 months ago

C & D 1- The exe was blocked so there is no exception 2-the Isolate Button is clickable so the device is not isolated 3-TRUE: you can see the processes created so the exe was launched 4-True: you can see from the view selected in the top right corner

upvoted 2 times

Latrel 8 months ago

Selected Answer: B

Correct answer B & D

upvoted 2 times

thinasci01 Most Recent 8 months ago

Selected Answer: B, D

the correct answer is B and D

upvoted 1 times

Question #14 *Topic 1*

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

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

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

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.

Suggested Answer: *A*
Official Answer: A

Josuerive01 8 months ago

Selected Answer: A

I think is A.

upvoted 3 times

hugojt 8 months ago

It should be the C

upvoted 3 times

soporte127 8 months ago

Selected Answer: C

why option c ?

upvoted 2 times

DataConsult Most Recent 8 months ago

A is the Correct answer

upvoted 1 times

Question #15 *Topic 1*

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

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

B. Contact Fortinet support

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

D. Immediately create an exception

Suggested Answer: *A*
Official Answer: A

Chogi_ 8 months ago
Ans. is A
upvoted 2 times

thinasci01 8 months ago
Selected Answer: A
the correct answer is A.
upvoted 1 times

Adancorrea Most Recent 8 months ago
Selected Answer: A
Option A
upvoted 1 times

Question #16 *Topic 1*

What is the purpose of the Threat Hunting feature?

A. Execute playbooks to isolate affected collectors in the organization

B. Find and delete all instances of a known malicious file or hash in the organization

C. Delete any file from any collector in the organization

D. Identify all instances of a known malicious file or hash and notify affected users

Suggested Answer: *B*
Official Answer: D

Agent1994 Highly Voted 8 months ago
B FortiEDR 5.0 Study Guide 174 "Threat hunting allows management console users to find and remediate dormant threats before they execute. Essentially it's a search and destroy operation."
upvoted 8 times

Adancorrea 8 months ago
Selected Answer: B
B - Correct answer
upvoted 2 times

burcurt21 8 months ago
Selected Answer: D
The primary purpose of Threat Hunting is to identify threats by detecting their presence (via hashes, IOCs, or other signals) within an organization's network. While the feature can identify instances of malware and compromised files, the actual removal or deletion from endpoints typically requires manual investigation or remediation playbooks, not automatic deletion by Threat Hunting itself
upvoted 1 times

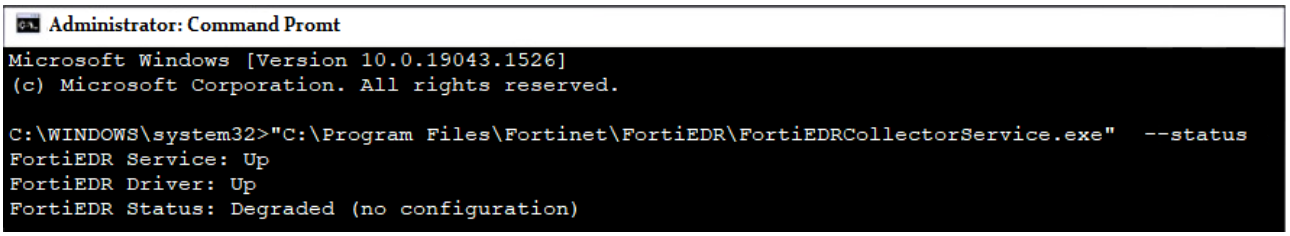
DataConsult 8 months ago
B is the correct answer
upvoted 1 times

Latrel Most Recent 8 months ago
Selected Answer: B
the correct answer is B
upvoted 1 times

Question #17 *Topic 1*

Refer to the exhibit.

Based on the FortiEDR status output shown in the exhibit, which two statements about the FortiEDR collector are true? (Choose two.)



A. The collector device has windows firewall enabled.

B. The collector has been installed with an incorrect port number.

C. The collector has been installed with an incorrect registration password.

D. The collector device cannot reach the central manager.

Suggested Answer: *B, C*

Official Answer: CD

Agent1994 Highly Voted 8 months ago

I'll correct myself. A. False B. True C. True D. The collector doesn't connect to the central manager, just the aggregator and core.

upvoted 8 times

Latrel Highly Voted 8 months ago

Selected Answer: B, C

I performed 2 tests in my lab and validated that the correct answer is B and C. The collector installer allows you to install with the wrong registration password and the status of the collector is Degraded. If you install the collector with the wrong port, the status of the collector is also Degraded. If the windows firewall blocks any connectivity, the status becomes Disconnected.

upvoted 5 times

fabrizzz 8 months ago

Selected Answer: B, C

B AND ARE TRUE

upvoted 1 times

joeytrib 8 months ago

Selected Answer: B, C

Study guide p246

upvoted 1 times

Agent1994 Most Recent 8 months ago

A. False, Windows Firewall won't usually block outbound connections. B. True. It could be the reason for D. C. False. Though I dont have it installed yet, I believe that there should be a more specific error for the registration password. D. True.

upvoted 1 times

Question #18 *Topic 1*

Which two statements about the FortiEDR solution are true? (Choose two.)

A. It provides point-to-point protection

B. It provides central management

C. It provides pre-infection and post-infection protection

D. It is Windows OS only

Suggested Answer: *B, C*
Official Answer: CD

Miccyg Highly Voted 8 months ago

Selected Answer: B, C

It should be B & C

upvoted 8 times

SIEM23 8 months ago

b -- page 15 FortiEDR study guide c -- page 9 FortiEDR study guide

upvoted 3 times

khanchand 8 months ago

Selected Answer: A, C

It should be A & C

upvoted 2 times

fabrizzz 8 months ago

Selected Answer: B, C

B AND C

upvoted 1 times

thinasci01 Most Recent 8 months ago

Selected Answer: B, C

the correct answer is B and C.

upvoted 1 times