



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



CERTIFICATION TEST

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

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: C

Community vote distribution

A (100%)

Demian2 **Highly Voted** 1 year, 5 months ago

correct it's A.

upvoted 6 times

khanchand **Highly Voted** 1 year, 7 months ago

It should be A

upvoted 5 times

50f3ed5 **Most Recent** 2 weeks, 1 day ago

Selected Answer: A

I think correct answer is A.

upvoted 1 times

burcort21 6 months, 3 weeks ago

Selected Answer: D

Option C ("FCS is responsible for all classifications") might appear correct at first glance, as the Fortinet Cloud Service (FCS) indeed plays a significant role in classifications by leveraging cloud intelligence to determine application and threat reputations. However, this statement is incomplete because the Core also has classification responsibilities under specific conditions, such as when FCS playbooks are disabled or unavailable.

Option D provides a more complete view of the situation, as it accounts for scenarios where FCS is not in use.

upvoted 1 times

Latrel 7 months, 2 weeks ago

Correct it's A

upvoted 1 times

thinasci01 9 months, 2 weeks ago

the correct answer is A.

upvoted 1 times

joeytrib 1 year, 1 month ago

Selected Answer: A

page 94 study guide

upvoted 1 times

Chogi_ 1 year, 5 months ago

Correct ans. is A

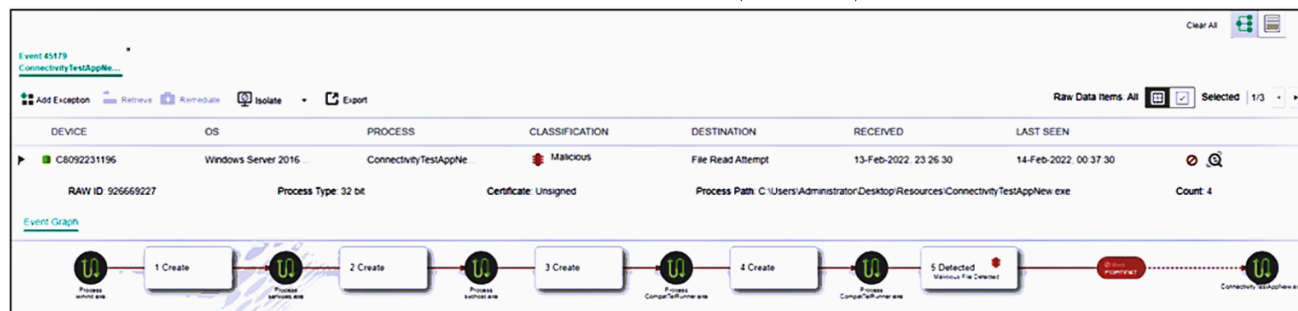
upvoted 4 times

fontabest99 1 year, 6 months ago

it should be A

upvoted 5 times

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: CD

Community vote distribution

AB (100%)

fontabest99 Highly Voted 1 year, 6 months ago

Selected Answer: AB

they are the real answer
upvoted 5 times

Latrel Most Recent 7 months, 2 weeks ago

A & B

Remediate Button is Greyed out and execution prevention policie block.

This questions is available on the FortiEDR Lab Guide pag 32

upvoted 2 times

thinasci01 9 months, 2 weeks ago

the correct answer is A and B.
upvoted 1 times

yonandres 1 year, 3 months ago

Selected Answer: AB

A & B are the answer
upvoted 2 times

Computerhigh 1 year, 5 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

Refer to the exhibit.

TestApplication.exe.exe (3 events) ❗ Malicious 15-Feb-2022, 13:31:39

5894314 ■ R2D2-kvm63 TestApplication.exe.exe ❗ Malicious 8.8.8.8 15-Feb-2022, 13:31:39 15-Feb-2022, 13:31:39

Logged-in User: R2D2-KVM63\fortinet Process owner: R2D2-KVM63\fortinet Certificate: Unsigned Process path: C:\Users\fortinet\Desktop

CLASSIFICATION DETAILS

❗ Malicious **Fortinet**

Threat name: Unknown
Threat family: Unknown
Threat type: Unknown

History

❗ Malicious, by Fortinet, on 15-Feb-2022, 13:31:41

Triggered Rules

Exfiltration Prevention

- Invalid Checksum - Connection Attempt from Application wi...
- Malicious File Detected
- Suspicious Packer - Activity by an Application packed by a S...
- Writeable Code - Identified an Executable with Writable Code

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: AB

Community vote distribution

CD (63%)

AC (38%)

Agent1994 Highly Voted 1 year, 11 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

Chogi_ 1 year, 11 months ago

Ans. are C&D - exact explanation.

upvoted 2 times

rac_sp Most Recent 12 months ago

Selected Answer: CD

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

Latrel 1 year, 1 month ago

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

🗨️ 👤 **thinasci01** 1 year, 3 months ago

the correct answer is C and D.

upvoted 1 times

🗨️ 👤 **joeytrib** 1 year, 7 months ago

Selected Answer: CD

CD is the right answer !

upvoted 1 times

🗨️ 👤 **thommy88** 1 year, 7 months ago

Selected Answer: CD

a= false because NGAV is exectuion prevention

b= false because i is not "by fortinetCloudServices

upvoted 2 times

🗨️ 👤 **BrunoLu** 1 year, 9 months ago

Selected Answer: AC

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

🗨️ 👤 **BrunoLu** 1 year, 9 months ago

B.It's history say by fortinet

upvoted 1 times

🗨️ 👤 **headhunter24** 1 year, 11 months ago

correct answer A & C

upvoted 2 times

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

Community vote distribution

B (100%)

  **Miccyg** Highly Voted 1 year, 5 months ago

Selected Answer: B

"post-infection"

upvoted 7 times

  **thinasci01** Most Recent 9 months, 2 weeks ago

the correct answer is B.

upvoted 1 times

  **Adancorrea** 1 year, 2 months ago

Selected Answer: B

B - Correct Answer

upvoted 1 times

  **soporte127** 11 months, 3 weeks ago

why b?

upvoted 1 times

  **defiantbear** 11 months, 3 weeks ago

It says "post-infection", meaning the program was able to be launched. The next layer that comes after execution prevention is Exfiltration Prevention.

FortiEDR 5.0 Study Guide Pag. 94



upvoted 1 times

  **ebenav11** 1 year, 2 months ago

Option C

FortiEDR is the only solution that detects and stops advanced attacks in real time, even when the endpoint has been compromised. No breaches, no data loss, no problem. FortiEDR eliminates dwell time and provides a suite of automated endpoint detection and response (EDR) features to detect, defuse, investigate, respond to, and remediate incidents.

upvoted 1 times

  **Chogi_** 1 year, 5 months ago

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

upvoted 3 times

Which scripting language is supported by the FortiEDR action manager?

- A. TCL
- B. Bash
- C. Perl
- D. Python

Suggested Answer: *D*

🗲️ 👤 **Chogi_** Highly Voted 1 year, 5 months ago

Ans. D - Python
upvoted 5 times

🗲️ 👤 **burcurt21** Most Recent 6 months, 3 weeks ago

Selected Answer: D

The scripting language supported by the FortiEDR Action Manager is Python.
upvoted 1 times

🗲️ 👤 **thinasci01** 9 months, 2 weeks ago

the correct answer is D. Python
upvoted 1 times

🗲️ 👤 **torrespdr** 11 months ago

D - Python
upvoted 1 times

🗲️ 👤 **ebenav11** 1 year, 2 months ago

Python
upvoted 2 times

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: D

Community vote distribution

C (100%)

  **edcwsxqaz** Highly Voted 1 year, 5 months ago

Selected Answer: C

The correct answer is Device Control.

upvoted 10 times

  **fontabest99** Highly Voted 1 year, 6 months ago

The correct answer is Device Control.



FortiEDR_5.0_Study_Guide-Online.pdf page 83

upvoted 6 times

  **Latrel** Most Recent 7 months, 2 weeks ago

The correct answer is Device Control.

upvoted 1 times

  **thinasci01** 9 months, 2 weeks ago

the correct answer is C. Device Control

upvoted 1 times

  **ebenav11** 1 year, 2 months ago

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

  **khanchand** 1 year, 6 months ago

Can you please confirm this answer ?

upvoted 1 times


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

CLASSIFICATION DETAILS



 Malicious **FORTINET**

Automated analysis steps completed by Fortinet Details

History

- ▼  Malicious, by FortinetCloudServices, on 10-Feb-2022, 10:20:25
 - Device **R2D2-kvm63** was moved from collector group **Training** to collector group **High Security Collector Group** once

Triggered Rules

- ▼  Training-eXtended Detection
 - ▷  Suspicious network activity Detected


- 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: AD

Community vote distribution


AD (83%)

BD (17%)

🗨️  **rac_sp** 11 months, 3 weeks ago

Selected Answer: AD

first, it was an extended detection. So automation plays a rule here. Extended detections operates in simulation mode
upvoted 2 times

🗨️  **Latrel** 1 year, 1 month ago

the correct answer is A and D
upvoted 1 times

🗨️  **thinasci01** 1 year, 3 months ago

the correct answer is A and D.
upvoted 1 times

🗨️  **nse_student** 1 year, 5 months ago


Selected Answer: AD

A & D Correct
upvoted 1 times

🗨️  **pgg1896** 1 year, 6 months ago

Selected Answer: AD

eXtended Detection Policy operates only in simulation mode, A&D are correct
upvoted 3 times

🗨️  **joeytrib** 1 year, 6 months ago

Selected Answer: BD

BD are the right answers study guide p96
upvoted 1 times

🗨️  **ebnav11** 1 year, 8 months ago

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

  **BrunoLu** 1 year, 9 months ago

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

upvoted 2 times

  **fontabest99** 2 years ago

the correct answer are B and D,

FortiEDR study guide pag 96

upvoted 3 times

  **RodrigoG** 1 year, 11 months ago

that is incorrect, A and D are correct, the device was moved to the HSG (by playbook), it wasnt isolated

upvoted 2 times

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

- A. FortiSandbox
- B. FortiSiem
- C. FortiNAC
- D. FortiGate

Suggested Answer: AB

Community vote distribution

CD (100%)

🗳️ 👤 **Agent1994** Highly Voted 👍 2 years, 5 months ago

C & D

FortiEDR_5.0_Study_Guide page 106

upvoted 8 times

🗳️ 👤 **fontabest99** Highly Voted 👍 2 years, 6 months ago

it must be C & D

upvoted 5 times

🗳️ 👤 **DataConsult** Most Recent 🕒 10 months, 1 week ago

C & D are Correct

FortiNAC to Isolate a device

FortiGate to block a malicious IP

upvoted 1 times

🗳️ 👤 **thinasci01** 1 year, 9 months ago

the correct answer is C. FortiNAC and D. FortiGate

upvoted 1 times

🗳️ 👤 **edcwsxqaz** 2 years, 5 months ago

Selected Answer: CD

the correct are C & D

upvoted 4 times

🗳️ 👤 **khanchand** 2 years, 7 months ago

It must be C & D

upvoted 5 times

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: C

Community vote distribution

B (100%)


 **[Removed]**  1 year, 3 months ago

Selected Answer: B

B is correct

FortiEDR guide page 15

upvoted 6 times

 **fontabest99**  1 year, 6 months ago

FortiEDR Threat Hunting Repository : fortiedr guide page 15:

FIND AND DELETE KNOWN MALWARE ON ANY DEVICE WITHIN THE SYSTEM

upvoted 6 times

 **thinasci01**  9 months, 2 weeks ago

the correct answer is B.


upvoted 1 times

 **Adancorrea** 1 year, 2 months ago

Selected Answer: B

B - Correct Answer

upvoted 2 times

 **Chogi_** 1 year, 5 months ago

Ans. is B

upvoted 3 times

Which threat hunting profile is the most resource intensive?

- A. Inventory
- B. Comprehensive
- C. Standard Collection
- D. Default

Suggested Answer: B

Community vote distribution

B (100%)

🗳️ 👤 **4ng3l0v** 8 months, 3 weeks ago

B is correct, pag 176
upvoted 1 times

🗳️ 👤 **thinasci01** 9 months, 2 weeks ago

the correct answer is B. Comprehensive
upvoted 1 times

🗳️ 👤 **Adancorrea** 1 year, 2 months ago

Selected Answer: B

B - Comprehensive
upvoted 2 times

🗳️ 👤 **[Removed]** 1 year, 3 months ago

Selected Answer: B

Comprehensive Profile collects almost all data from endpoints and is the most resource-intensive profile
FortiEDR Study guide 176
upvoted 4 times

🗳️ 👤 **neojosele** 1 year, 4 months ago

B - Comprehensive
upvoted 2 times

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: B

Community vote distribution

D (100%)

🗳️ 👤 **Latrel** 7 months, 2 weeks ago

D is the correct answer
upvoted 1 times

🗳️ 👤 **thinasci01** 9 months, 2 weeks ago

the correct answer is D.
upvoted 1 times

🗳️ 👤 **joeytrib** 1 year ago

Selected Answer: D
D is the correct answer
upvoted 1 times

🗳️ 👤 **Adancorrea** 1 year, 2 months ago

Selected Answer: D
D - Corrent Answer
upvoted 2 times

🗳️ 👤 **Agent1994** 1 year, 5 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** 1 year, 5 months ago

Corrent Answer D
upvoted 4 times

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

🗨️ 👤 **e93df3f** 6 months, 1 week ago

Selected Answer: C

Correct Answer.

upvoted 1 times

🗨️ 👤 **Latrel** 1 year, 1 month ago

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

🗨️ 👤 **Dani_Prime** 6 months, 3 weeks ago

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

upvoted 1 times

🗨️ 👤 **thinasci01** 1 year, 3 months ago

the answer C. is correct.

upvoted 2 times

🗨️ 👤 **soporte127** 1 year, 5 months ago

For me option D is the correct one.

upvoted 1 times

🗨️ 👤 **ebenav11** 1 year, 8 months ago

Option C

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

upvoted 2 times

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

DEVICE	OS	PROCESS	CLASSIFICATION	DESTINATION	RECEIVED	LAST SEEN
c3po-kvm48	Windows 10 Pro	bot.exe	Malicious	File Read Attempt	01-jan-2022, 04:33:09	04-jan-2022, 13:16:16

RAW ID: 119330467 Process Type: 32 bit Certificate: Unsigned Process Path: C:\Users\fortinet\Desktop\bot.exe Count: 135

ESS CREATION PARENT PROCESS CREATION PARENT PROCESS CREATION PARENT PROCESS CREATION PARENT PROCESS CREATION PARENT PROCESS CREATION FILE READ ATTEMPT PRE EXECUTE

- 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: AD

Community vote distribution

BD (100%)

headhunter24 Highly Voted 2 years, 5 months ago

Correct answer B & D

upvoted 6 times

[Removed] Highly Voted 2 years, 3 months ago

Selected Answer: BD

B- The Red icon on the device indicate isolation icon

D- At the top right corner the Green icon is gray out indicating that is the selected view

upvoted 5 times

DataConsult Most Recent 10 months, 1 week 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 1 year, 7 months ago

Correct answer B & D

upvoted 2 times

thinasci01 1 year, 9 months ago

the correct answer is B and D

upvoted 1 times

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

Community vote distribution

A (100%)

🗨️ 👤 **DataConsult** 10 months, 1 week ago

A is the Correct answer
upvoted 1 times

🗨️ 👤 **Josuerive01** 1 year, 10 months ago

Selected Answer: A

I think is A.
upvoted 3 times

🗨️ 👤 **hugojt** 2 years, 3 months ago

It should be the C
upvoted 3 times

🗨️ 👤 **soporte127** 1 year, 11 months ago

why option c ?
upvoted 2 times

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

Community vote distribution

A (100%)

🗲️ 👤 **thinasci01** 9 months, 2 weeks ago

the correct answer is A.

upvoted 1 times

🗲️ 👤 **Adancorrea** 1 year, 1 month ago

Selected Answer: A

Option A

upvoted 1 times

🗲️ 👤 **Chogi_** 1 year, 5 months ago

Ans. is A

upvoted 2 times

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: D

Community vote distribution

B (100%)

🗳️ 👤 **Agent1994** Highly Voted 👍 2 years, 5 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

🗳️ 👤 **burcurt21** Most Recent ⌚ 6 months, 3 weeks 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** 10 months, 1 week ago

B is the correct answer

upvoted 1 times

🗳️ 👤 **Latrel** 1 year, 7 months ago

the correct answer is B

upvoted 1 times

🗳️ 👤 **thinasci01** 1 year, 9 months ago

the correct answer is B

upvoted 1 times

🗳️ 👤 **Adancorrea** 2 years, 2 months ago

Selected Answer: B

B - Correct answer

upvoted 2 times

Refer to the exhibit.

```
Administrator: Command Prompt
Microsoft Windows [Version 10.0.19043.1526]
(c) Microsoft Corporation. All rights reserved.

C:\WINDOWS\system32>"C:\Program Files\Fortinet\FortiEDR\FortiEDRCollectorService.exe" --status
FortiEDR Service: Up
FortiEDR Driver: Up
FortiEDR Status: Degraded (no configuration)
```

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: CD

Community vote distribution

BC (100%)

 **Latrel** Highly Voted 7 months, 2 weeks ago

Selected Answer: BC

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** Most Recent 7 months, 3 weeks ago

Selected Answer: BC

B AND ARE TRUE

upvoted 1 times

 **joeytrib** 1 year ago

Selected Answer: BC

Study guide p246

upvoted 1 times

 **Agent1994** 1 year, 5 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

 **Agent1994** 1 year, 5 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

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: *CD*

Community vote distribution

BC (83%)

AC (17%)

🗳️ 👤 **Miccyg** Highly Voted 👍 1 year, 5 months ago

Selected Answer: BC

It should be B & C

upvoted 8 times

🗳️ 👤 **fabrizzz** Most Recent 🕒 7 months, 2 weeks ago

Selected Answer: BC

B AND C

upvoted 1 times

🗳️ 👤 **thinasci01** 9 months, 2 weeks ago

the correct answer is B and C.

upvoted 1 times

🗳️ 👤 **joeytrib** 1 year ago

Selected Answer: BC

b -- page 15 FortiEDR study guide

c -- page 9 FortiEDR study guide

upvoted 1 times

🗳️ 👤 **SIEM23** 1 year, 2 months ago

b -- page 15 FortiEDR study guide

c -- page 9 FortiEDR study guide

upvoted 3 times

🗳️ 👤 **khanchand** 1 year, 6 months ago

Selected Answer: AC

It should be A & C

upvoted 2 times

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

- A. TACACS
- B. LDAP
- C. SAML
- D. Radius

Suggested Answer: AD

Community vote distribution

BC (100%)

🗳️ 👤 **BrunoLu** Highly Voted 👍 1 year, 3 months ago

Selected Answer: BC

correct answer is b & c, page 32

upvoted 5 times

🗳️ 👤 **khanchand** Highly Voted 👍 1 year, 6 months ago

Selected Answer: BC

correct answer is b & c

upvoted 5 times

🗳️ 👤 **4ng3l0v** Most Recent 🕒 8 months, 3 weeks ago

b, c, page 32

upvoted 1 times

🗳️ 👤 **thinasci01** 9 months, 2 weeks ago

the correct answer is B and C.

upvoted 1 times

🗳️ 👤 **Adancorrea** 1 year, 2 months ago

Selected Answer: BC

correct answers are B and C

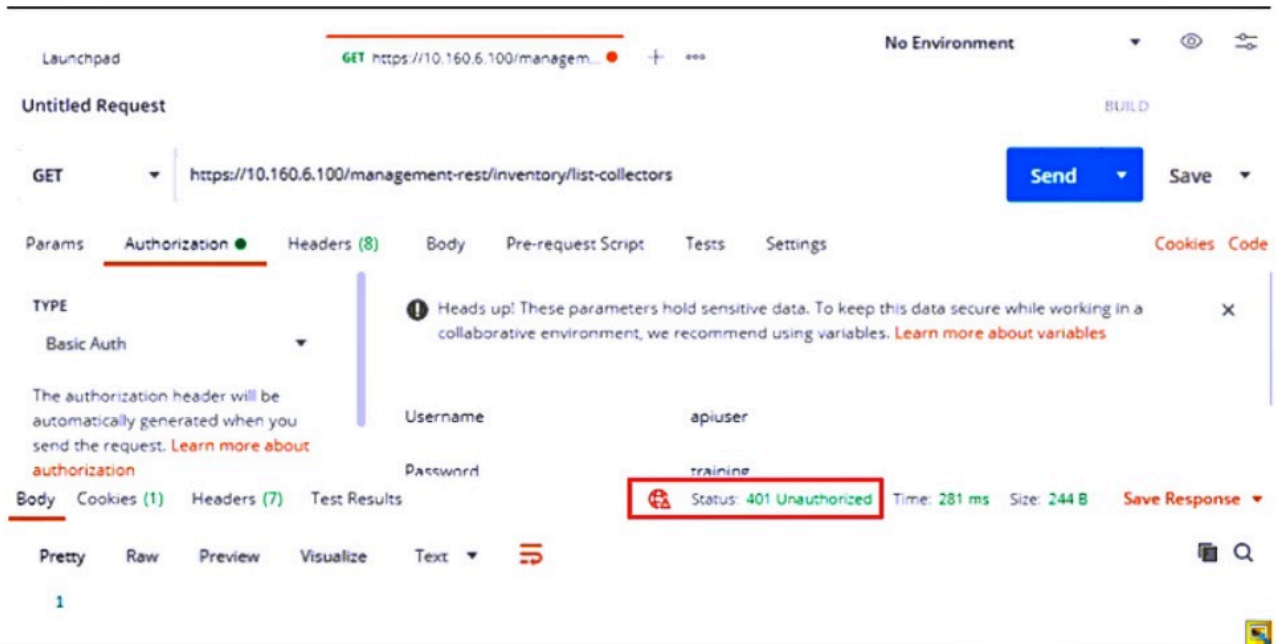
upvoted 2 times

🗳️ 👤 **ebenav11** 1 year, 2 months ago

Correct options are B & C

upvoted 2 times

Refer to the exhibit.



Based on the postman output shown in the exhibit, why is the user getting an unauthorized error?

- A. Postman cannot reach the central manager.
- B. API access is disabled on the central manager.
- C. The user has been assigned Admin and Rest API roles.
- D. FortiEDR requires a password reset the first time a user logs in.

Suggested Answer: B

Community vote distribution

D (100%)

- Agent1994** Highly Voted 1 year, 5 months ago

D

FortiEDR 5.0 Study Guide 227

upvoted 8 times
- headhunter24** Highly Voted 1 year, 5 months ago

answer D

upvoted 5 times
- Latrel** Most Recent 7 months, 2 weeks ago

Selected Answer: D

the correct answer is D

upvoted 1 times
- thinasci01** 9 months, 2 weeks ago

the correct answer is D.

upvoted 1 times
- joeytrib** 1 year ago

Selected Answer: D

FortiEDR 5.0 Study Guide 227

upvoted 1 times
- thommy88** 1 year, 1 month ago

Selected Answer: D

d is correct

upvoted 1 times

  **thommy88** 1 year, 1 month ago

answer D

upvoted 1 times

Refer to the exhibit.

The screenshot displays the Windows Task Manager interface, specifically the 'Process Creation' tab. It shows two processes: 'cmd.exe' and 'PING.EXE'. The 'cmd.exe' process is running, with a status of 'Running' and an internal IP of '10.122.0.160'. It was created by 'R2D2-KVM63' and has a PID of 8180 and TID of 8184. The 'PING.EXE' process is also running, with a status of 'Running' and an internal IP of '10.122.0.160'. It was created by 'R2D2-KVM63' and has a PID of 5764. The parent process of 'PING.EXE' is 'cmd.exe' with PID 8180. The command line for 'PING.EXE' is 'fortinet.com'.

Process Name	Status	Internal IP	Up time	PID	TID	Path	Executing user	Product	SHA1	Command line
cmd.exe	Running	10.122.0.160	6min, 6sec	8180	8184	C:\Windows\System32\cmd.exe	R2D2-KVM63\fortinet	Microsoft Windows Operating System, v10.0.19041.746	F1EFB0FDDC156E4C61C5F78A54700E4E7984D55D	
PING.EXE	Running	10.122.0.160		5764		C:\Windows\System32\PING.EXE	R2D2-KVM63\fortinet	Microsoft Windows Operating System, v10.0.19041.1	9C13C854A4EF98879D0CA880EF679B4C4ECCF518	fortinet.com

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

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

Suggested Answer: AC

Community vote distribution

BD (100%)

thinasci01 9 months, 2 weeks ago

the correct answer is B and D.

upvoted 1 times

joeytrib 1 year ago

Selected Answer: BD

The correct answers are B & D

upvoted 1 times

Adancorrea 1 year, 1 month ago

Selected Answer: BD

Correct Answer are B and D

upvoted 2 times

Chogi_ 1 year, 4 months ago