NSE5_EDR-5.0^{Q&As}

Fortinet NSE 5 - FortiEDR 5.0

Pass Fortinet NSE5_EDR-5.0 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.passapply.com/nse5_edr-5-0.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by Fortinet
Official Exam Center

QUESTION 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 new a communication control policy and shares it with other organizations

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

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

Correct Answer: C

QUESTION 2

An administrator finds that a newly installed collector does not display on the INVENTORY tab in the central manager.

What two troubleshooting steps must the administrator perform? (Choose two.)

A. Export the collector logs from the central manager.

B. Verify the central manager has connectivity to FCS.

C. Verify TCP ports 8081 and 555 are open.

D. Check if the FortiEDR services are running on the collector device.

Correct Answer: CD

QUESTION 3

Refer to the exhibit.

The exhibit shows an event viewer.

▾ All	ID	DEVICE	PROCESS
Payroll Manager.exe (3 events)			
☐ ▶	9715	▣ cwinserv-32 🖳	Payroll Manager.exe
▷ 🏢 User: CWINSERV-32\Administrator		Certificate: Unsigned	Process path: .
☐ ▶	9695	▣ cwinserv-32 🖳	Payroll Manager.exe
☐ ▶	8878	▣ cwinserv-32 🖳	Payroll Manager.exe
CryptoLocker2.exe (1 event)			

CLASSIFICATION ▲	DESTINATIONS	RECEIVED ▾	LAST UPDATED	
⬢ Suspicious		25-Nov-2020, 06:09:07		
⬢ Suspicious	74.125.235.20	25-Nov-2020, 06:09:07	25-Nov-2020, 06:09:07	⊘
..inistrator\Downloads\Resources\TestFiles\Fake Malware\Payroll Manager.exe Raw data items: 1				
⬢ Suspicious	74.125.235.20	25-Nov-2020, 06:07:43	25-Nov-2020, 06:07:43	⊘
⬢ Suspicious	74.125.235.20	21-Sep-2020, 06.45.53	21-Sep-2020, 11.21.11	⊘
⬢ Malicious		28-Sep-2020, 05:46:35		

What is true about the Payroll Manager.exe event?

A. An event has not been handled by a console admin

B. An event has been deleted

C. A rule assigned action is set to block but the policy is in simulation mode

D. An event has been handled by the communication control policy

Correct Answer: C

QUESTION 4

How does FortiEDR implement post-infection protection?

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

B. By using methods used by traditional EDR

C. By insurance against ransomware

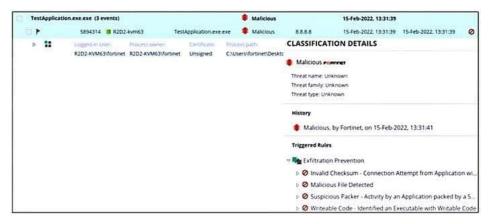D. By real-time filtering to prevent malware from executing

Correct Answer: A

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

QUESTION 5

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\Deskto	**CLASSIFICATION DETAILS**			

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

---

☐ **TestApplication.exe.exe (3 events)**   ● **Malicious**

☐ ▶   5894314   ■ R2D2-kvm63   TestApplication.exe.exe   ● **Malicious**

▷ ∷

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

---

15-Feb-2022, 13:31:39

8.8.8.8   15-Feb-2022, 13:31:39   15-Feb-2022, 13:31:39   ⊘

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. TestApplication exe is sophisticated malware

C. The user was able to launch TestApplication exe

D. FCS classified the event as malicious

Correct Answer: BC

NSE5_EDR-5.0 PDF
Dumps

NSE5_EDR-5.0 VCE
Dumps

NSE5_EDR-5.0 Braindumps