



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

-  **Instant Download** After Purchase
-  **100% Money Back** Guarantee
-  **365 Days** Free Update
-  **800,000+** Satisfied Customers





QUESTION 1

When installing a FortiEDR collector, why is a `Registration Password` for collectors needed?

- A. To restrict installation and uninstallation of collectors
- B. To verify Fortinet support request
- C. To restrict access to the management console
- D. To verify new group assignment

Correct Answer: A

QUESTION 2

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

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

Correct Answer: BD

QUESTION 3

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

- A. Device Control
- B. Ransomware Prevention
- C. Execution Prevention
- D. Exfiltration Prevention

Correct Answer: A

QUESTION 4

What is true about classifications assigned by Fortinet Cloud Sen/ice (FCS)?

- A. The core is responsible for all classifications if FCS playbooks are disabled
- B. The core only assigns a classification if FCS is not available
- C. FCS revises the classification of the core based on its database



D. FCS is responsible for all classifications

Correct Answer: C

QUESTION 5

Exhibit.

DEVICE	OS	PROCESS	CLASSIFICATION	DESTINATION	RECEIVED	LAST SEEN
RAVIC-S0688227	Windows Server 2016	C:\Users\Administrator\Desktop\ConnectivityTestApp.exe	Malicious	File Share Storage	12 Feb 2023 15:30:35	12 Feb 2023 15:17:30

Process Type: 32 bit
Certificate: Unsigned
Process Path: C:\Users\Administrator\Desktop\Resources\ConnectivityTestApp.exe
Count: 4

Event Graph: 1 Create, 2 Create, 3 Create, 4 Create, 5 Deleted, 6 Deleted



Event 45179
ConnectivityTestAppNe...

Add Exception | Retrievs | Remediate | Isolate | Export

DEVICE	OS	PROCESS	CLASSIFICATION
C8092231196	Windows Server 2016	ConnectivityTestAppNe...	Malicious

RAW ID: 926669227 Process Type: 32 bit Certificate: Unsigned

Event Graph

```

graph LR
    P1((Process Initial state)) --> A1[1 Create]
    A1 --> P2((Process Initial state))
    P2 --> A2[2 Create]
    A2 --> P3((Process Initial state))
    P3 --> A3[3 Create]
  
```

Clear All

Raw Data Items: All | Selected 1/3

DESTINATION	RECEIVED	LAST SEEN
File Read Attempt	13-Feb-2022, 23:26:30	14-Feb-2022, 00:37:30

Process Path: C:\Users\Administrator\Desktop\Resources\ConnectivityTestAppNew.exe Count: 4

```

graph LR
    P1((Process Computer.exe)) --> A1[4 Create]
    A1 --> P2((Process Computer.exe))
    P2 --> A2[5 Detected Malicious File Detected]
    A2 --> A3[Blocked]
    A3 -.-> P3((ConnectivityTestAppNew.exe))
  
```

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

- A. The device cannot be remediated
- B. The event was blocked because the certificate is unsigned
- C. Device C8092231196 has been isolated
- D. The execution prevention policy has blocked this event.

Correct Answer: AD