NSE5_EDR-5.0$^{Q\&As}$

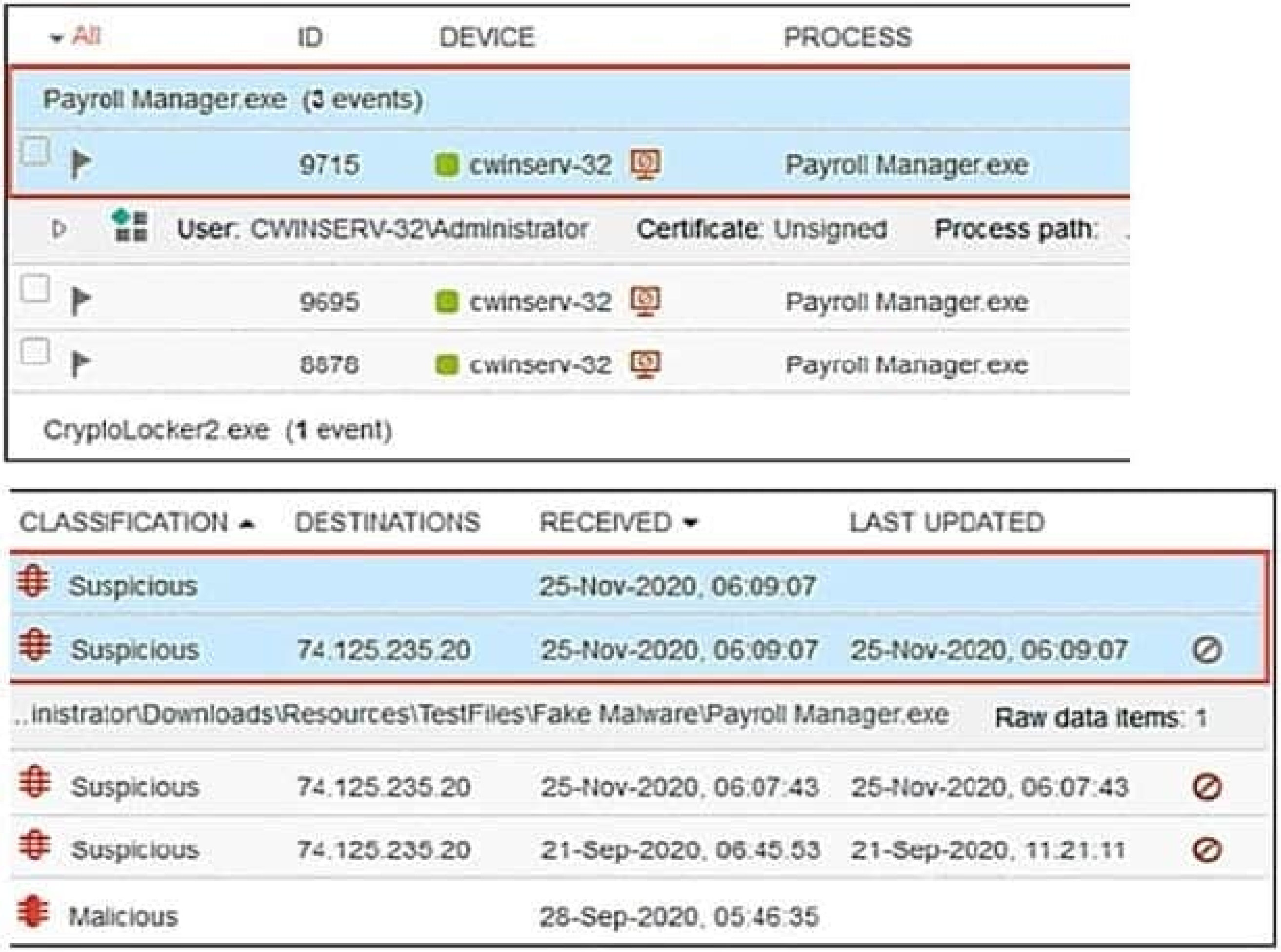
Fortinet NSE 5 - FortiEDR 5.0

Pass Fortinet NSE5_EDR-5.0 Exam with 100% Guarantee

QUESTION 1

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 2

FortiXDR relies on which feature as part of its automated extended response?

A. Playbooks

B. Security Policies

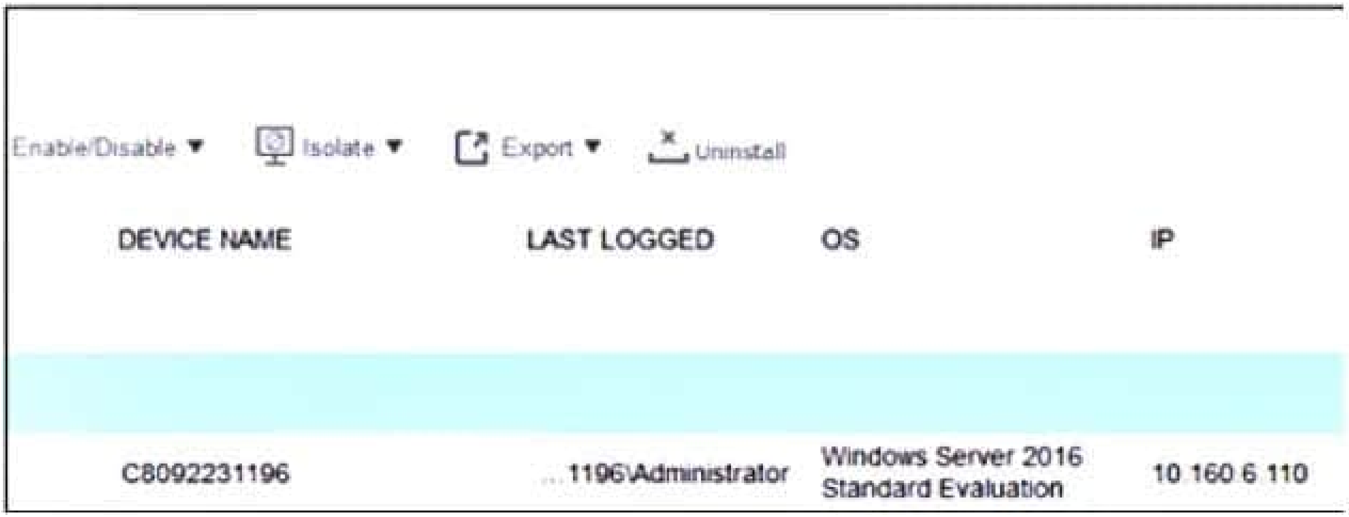
C. Forensic

D. Communication Control

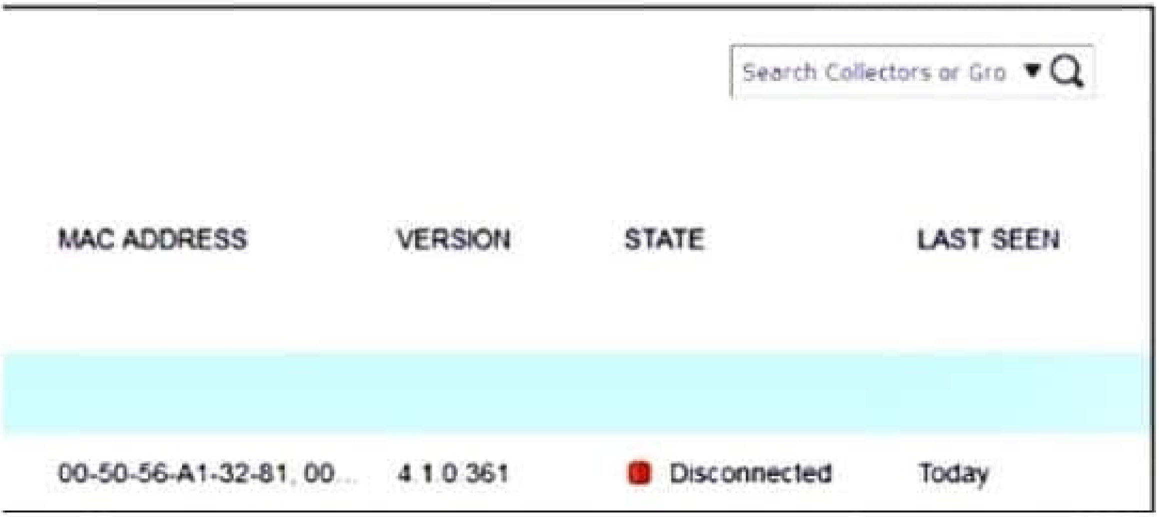
Correct Answer: A

QUESTION 3

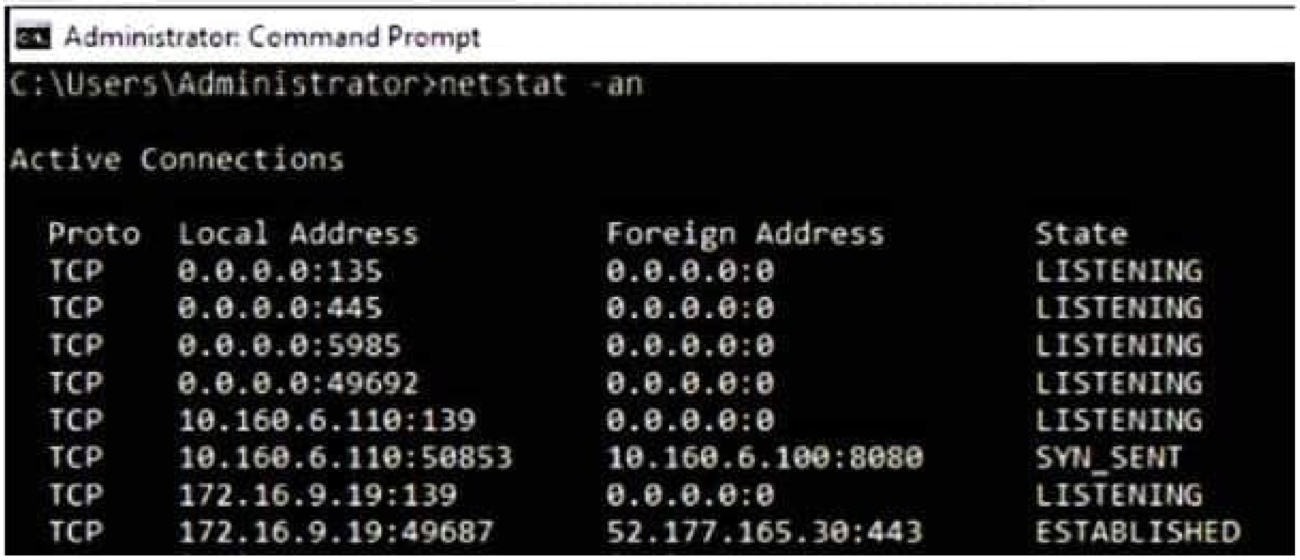
Refer to the exhibits.



DEVICE NAME	LAST LOGGED	OS	IP
C8092231196	...1196\Administrator	Windows Server 2016 Standard Evaluation	10 160 6 110



MAC ADDRESS	VERSION	STATE	LAST SEEN
00-50-56-A1-32-81, 00...	4 1 0 361	● Disconnected	Today



```
C:\Users\Administrator>netstat -an

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    0.0.0.0:135            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:445            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:5985           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49692          0.0.0.0:0              LISTENING
  TCP    10.160.6.110:139       0.0.0.0:0              LISTENING
  TCP    10.160.6.110:50853     10.160.6.100:8080      SYN_SENT
  TCP    172.16.9.19:139        0.0.0.0:0              LISTENING
  TCP    172.16.9.19:49687      52.177.165.30:443      ESTABLISHED
```

The exhibits show the collector state and active connections. The collector is unable to connect to aggregator IP address 10.160.6.100 using default port. Based on the netstat command output what must you do to resolve the connectivity issue?

A. Reinstall collector agent and use port 443

B. Reinstall collector agent and use port 8081

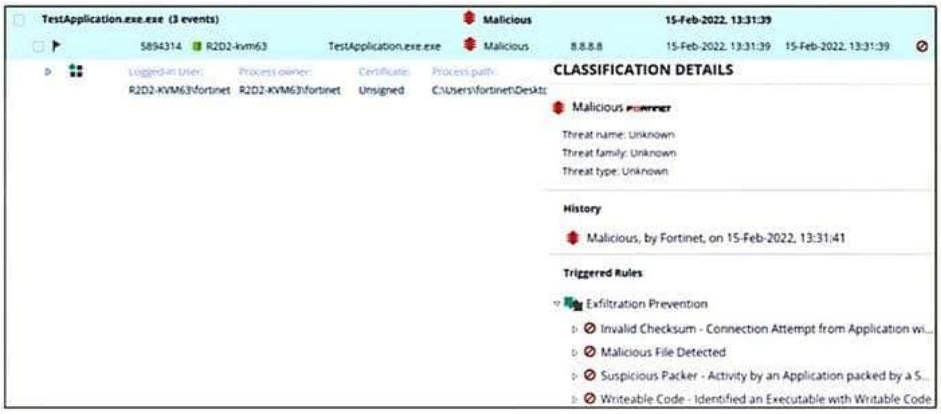
C. Reinstall collector agent and use port 555

D. Reinstall collector agent and use port 6514

Correct Answer: B

QUESTION 4

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\Desktc

CLASSIFICATION DETAILS

Malicious FORTINET

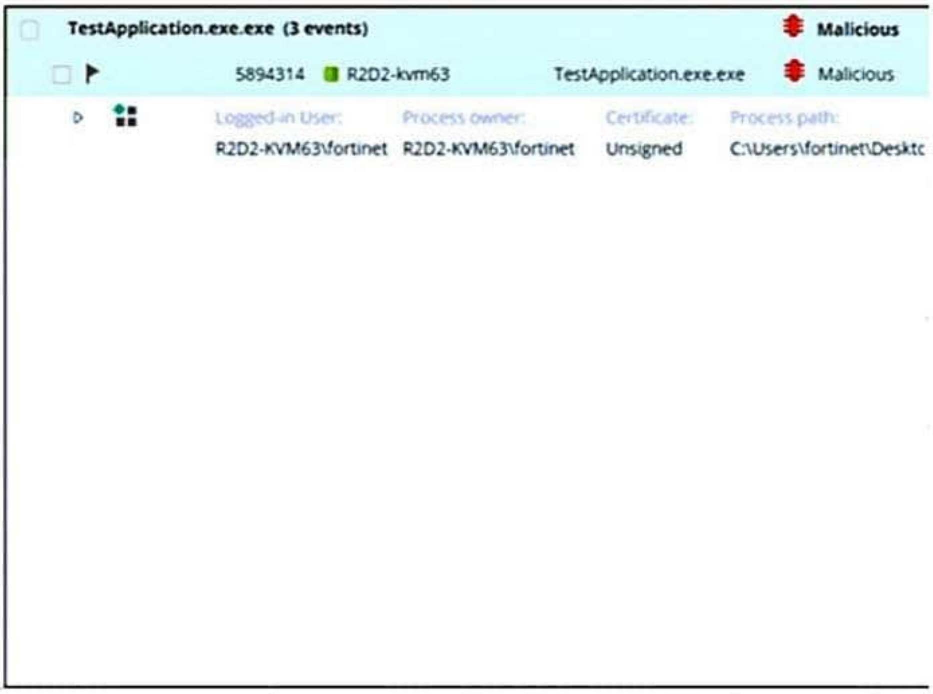
Threat name: Unknown
Threat family: Unknown
Threat type: Unknown

History

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

Triggered Rules

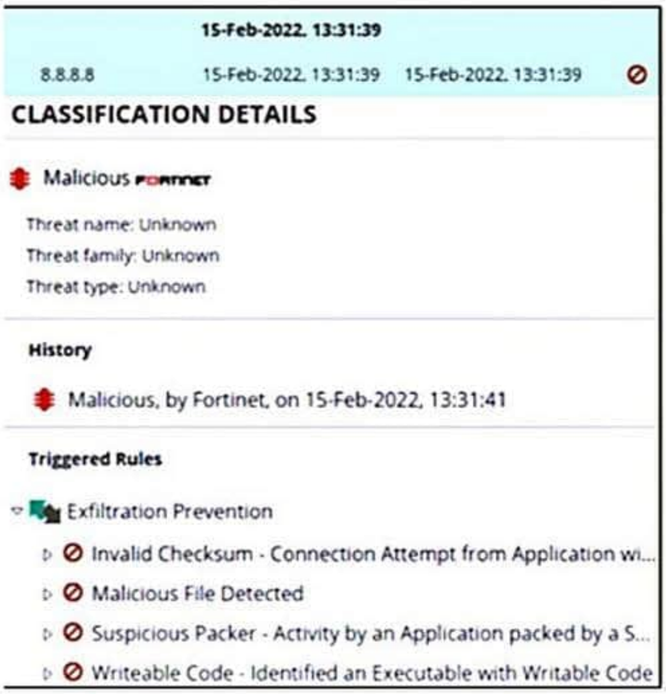
Exfiltration Prevention
- Invalid Checksum - Connection Attempt from Application wi...
- Malicious File Detected
- Suspicious Packer - Activity by an Application packed by a S...
- Writeable Code - Identified an Executable with Writable Code



TestApplication.exe.exe (3 events) Malicious

5894314 R2D2-kvm63 TestApplication.exe.exe Malicious

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



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

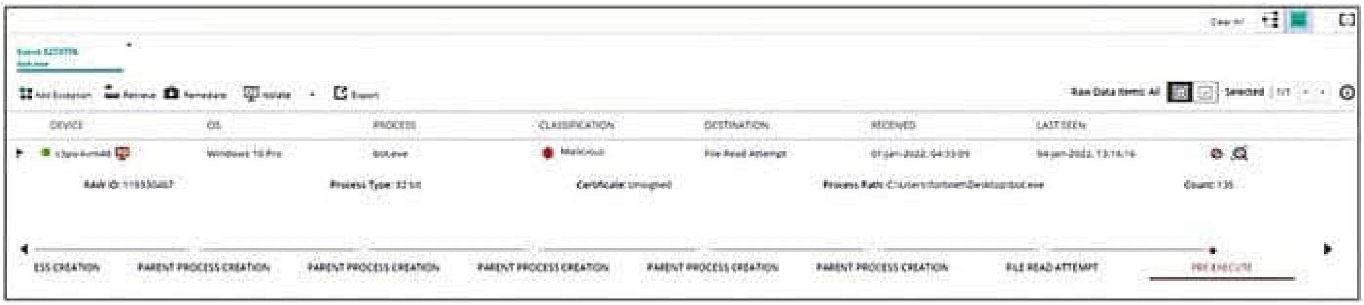
C. The user was able to launch TestApplication exe

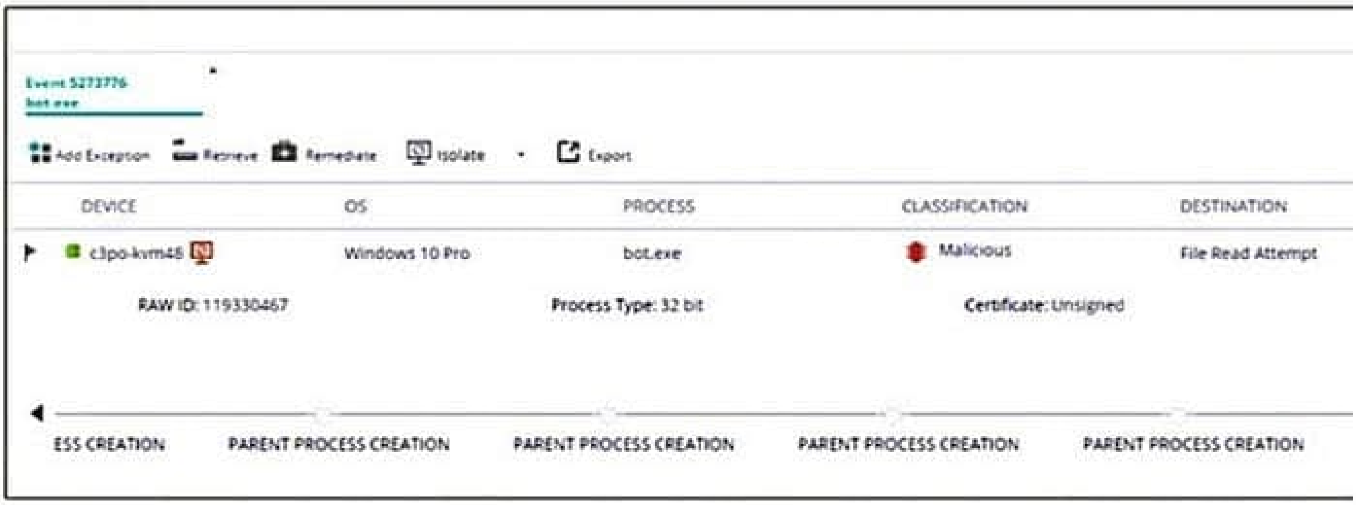
D. FCS classified the event as malicious

Correct Answer: BC

QUESTION 5

Exhibit.



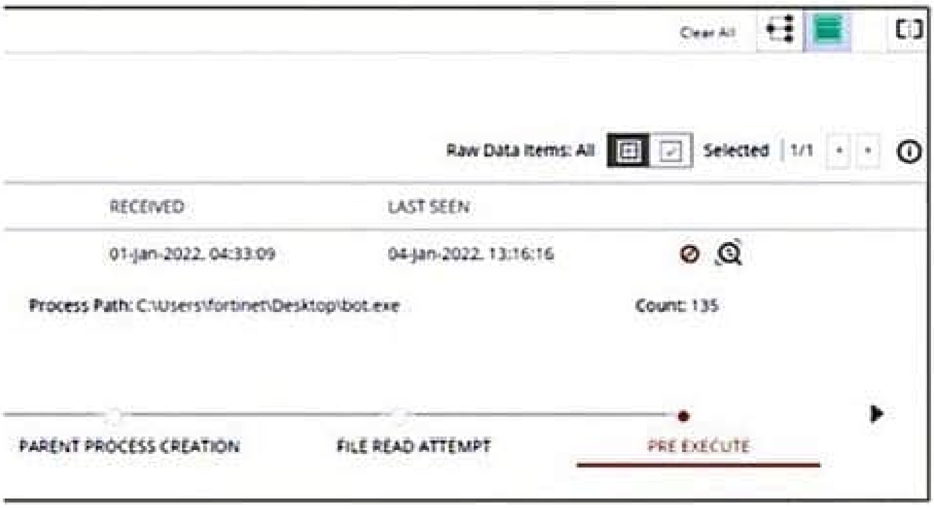


Event 5273776
bot.exe

Add Exception | Retrieve | Remediate | Isolate | Export

DEVICE	OS	PROCESS	CLASSIFICATION	DESTINATION
c3po-kvm48	Windows 10 Pro	bot.exe	Malicious	File Read Attempt

RAW ID: 119330467
Process Type: 32 bit
Certificate: Unsigned



Raw Data Items: All | Selected 1/1

RECEIVED	LAST SEEN
01-Jan-2022, 04:33:09	04-Jan-2022, 13:16:16

Process Path: C:\Users\fortinet\Desktop\bot.exe
Count: 135

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 forensics data is displayed m the stacks view

C. The device has been isolated

D. The exfiltration prevention policy has blocked this event

Correct Answer: BC