300-215Q&As

Conducting Forensic Analysis and Incident Response Using Cisco Technologies for CyberOps (CBRFIR)

Pass Cisco 300-215 Exam with 100% Guarantee

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

https://www.lead4pass.com/300-215.html

100% Passing Guarantee
100% Money Back Assurance

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

QUESTION 1

What is the goal of an incident response plan?

A. to identify critical systems and resources in an organization

B. to ensure systems are in place to prevent an attack

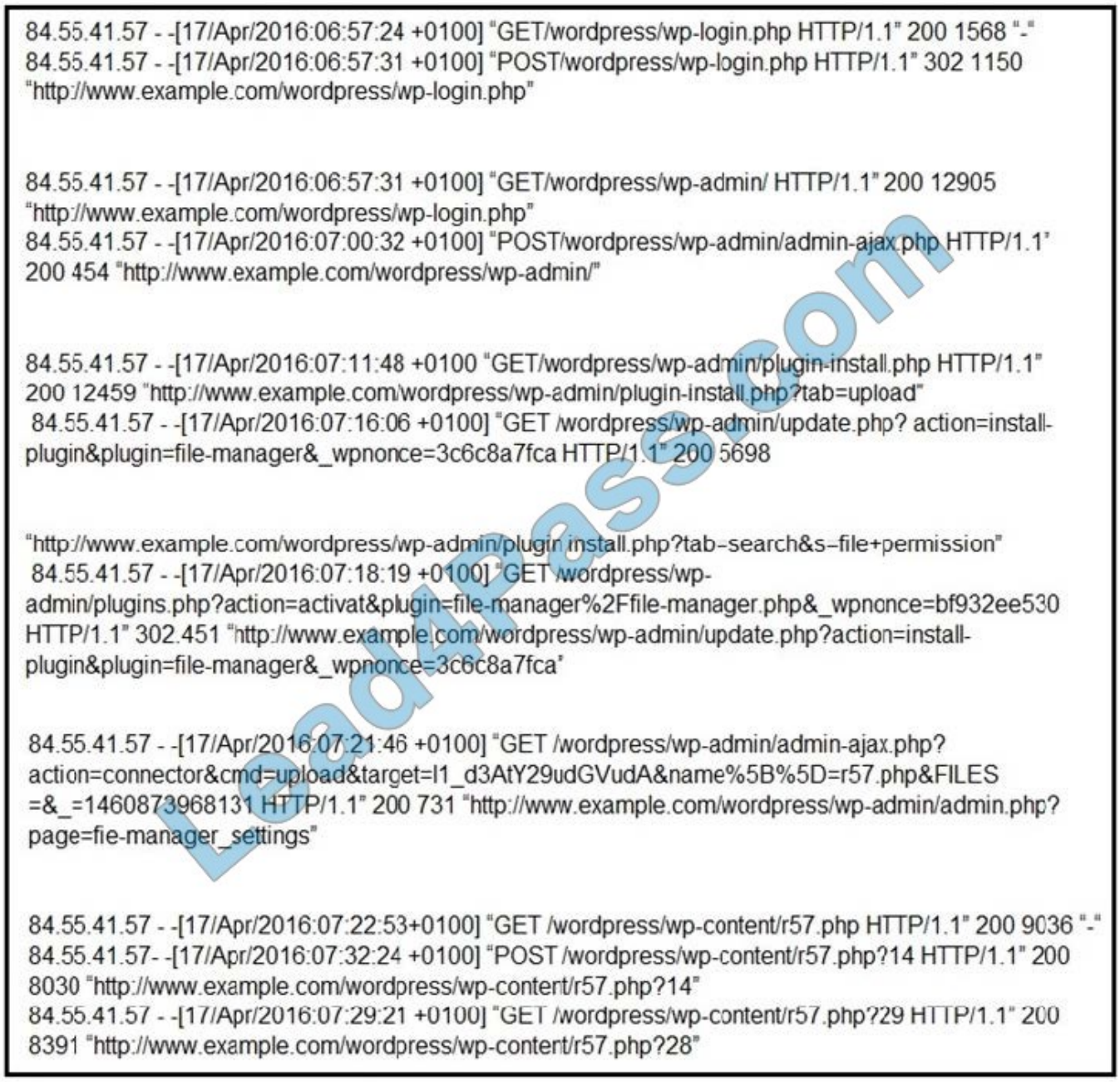
C. to determine security weaknesses and recommend solutions

D. to contain an attack and prevent it from spreading

Correct Answer: D

Reference: https://www.forcepoint.com/cyber-edu/incident-response

QUESTION 2



Refer to the exhibit. Which two determinations should be made about the attack from the Apache access logs? (Choose two.)

A. The attacker used r57 exploit to elevate their privilege.

B. The attacker uploaded the word press file manager trojan.

C. The attacker performed a brute force attack against word press and used sql injection against the backend database.

D. The attacker used the word press file manager plugin to upoad r57.php.

E. The attacker logged on normally to word press admin page.

Correct Answer: CD

QUESTION 3

```
alert tcp $LOCAL_NET any -> $HTTP_SERVERS $HTTP_PORTS (msg: "WEB-IIS unicode
directory traversal attempt"; flow:to_server, established; content: "/..%c0%af../";
nocase; classtype:web-application-attack; reference:cve, CVE-2000-0884; threshold:
type limit, track_by_dst, count 1, seconds 60; sid: 981; rev6;)
```

Refer to the exhibit. A company that uses only the Unix platform implemented an intrusion detection system. After the initial configuration, the number of alerts is overwhelming, and an engineer needs to analyze and classify the alerts. The highest number of alerts were generated from the signature shown in the exhibit. Which classification should the engineer assign to this event?

A. True Negative alert

B. False Negative alert

C. False Positive alert

D. True Positive alert

Correct Answer: C

QUESTION 4

A threat actor attempts to avoid detection by turning data into a code that shifts numbers to the right four times. Which anti-forensics technique is being used?

A. encryption

B. tunneling

C. obfuscation

D. poisoning

Correct Answer: C

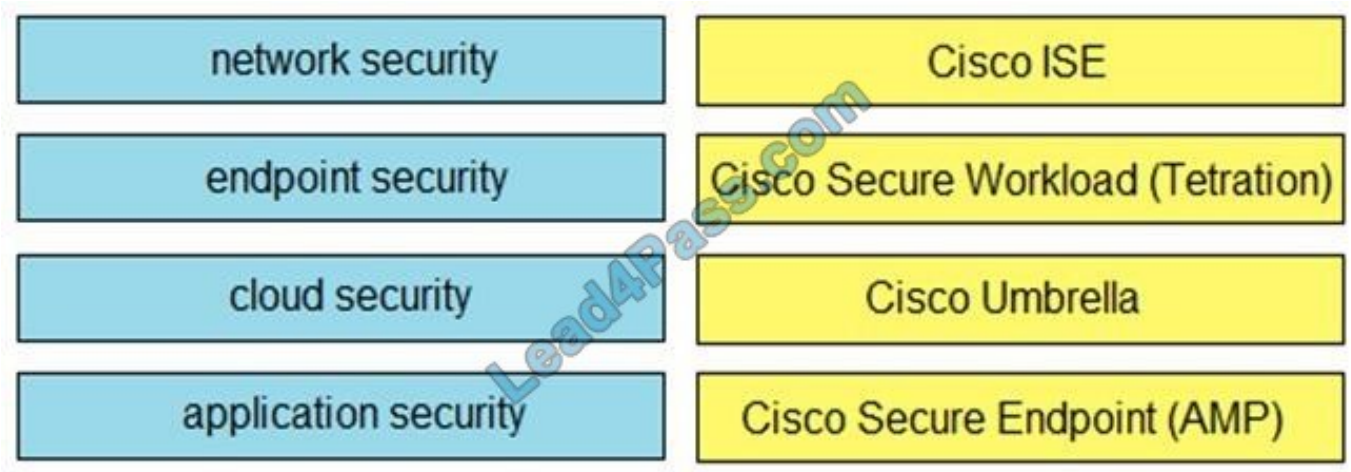
Reference: https://www.vadesecure.com/en/malware-analysis-understanding-code-obfuscation-techniques/#:~:text=Obfuscation%20of%20character%20strings%20is,data%20when%20the%20code%20executes.

QUESTION 5

DRAG DROP

Drag and drop the capabilities on the left onto the Cisco security solutions on the right.

Select and Place:



Correct Answer:

QUESTION 6

An engineer is investigating a ticket from the accounting department in which a user discovered an unexpected application on their workstation. Several alerts are seen from the intrusion detection system of unknown outgoing internet traffic from this workstation. The engineer also notices a degraded processing capability, which complicates the analysis process. Which two actions should the engineer take? (Choose two.)

A. Restore to a system recovery point.

B. Replace the faulty CPU.

C. Disconnect from the network.

D. Format the workstation drives.

E. Take an image of the workstation.

Correct Answer: AE

QUESTION 7

An incident response team is recommending changes after analyzing a recent compromise in which:

a large number of events and logs were involved;

team members were not able to identify the anomalous behavior and escalate it in a timely manner;

several network systems were affected as a result of the latency in detection;

security engineers were able to mitigate the threat and bring systems back to a stable state; and

the issue reoccurred shortly after and systems became unstable again because the correct information was not gathered during the initial identification phase.

Which two recommendations should be made for improving the incident response process? (Choose two.)

A. Formalize reporting requirements and responsibilities to update management and internal stakeholders throughout the incident-handling process effectively.

B. Improve the mitigation phase to ensure causes can be quickly identified, and systems returned to a functioning state.

C. Implement an automated operation to pull systems events/logs and bring them into an organizational context.

D. Allocate additional resources for the containment phase to stabilize systems in a timely manner and reduce an attack\\'s breadth.

E. Modify the incident handling playbook and checklist to ensure alignment and agreement on roles, responsibilities, and steps before an incident occurs.

Correct Answer: CE

QUESTION 8

A network host is infected with malware by an attacker who uses the host to make calls for files and shuttle traffic to bots. This attack went undetected and resulted in a significant loss. The organization wants to ensure this does not happen in the future and needs a security solution that will generate alerts when command and control communication from an infected device is detected. Which network security solution should be recommended?

A. Cisco Secure Firewall ASA

B. Cisco Secure Firewall Threat Defense (Firepower)

C. Cisco Secure Email Gateway (ESA)

D. Cisco Secure Web Appliance (WSA)

Correct Answer: B

QUESTION 9

An attacker embedded a macro within a word processing file opened by a user in an organization\\'s legal department. The attacker used this technique to gain access to confidential financial data. Which two recommendations should a security expert make to mitigate this type of attack? (Choose two.)

A. controlled folder access

B. removable device restrictions

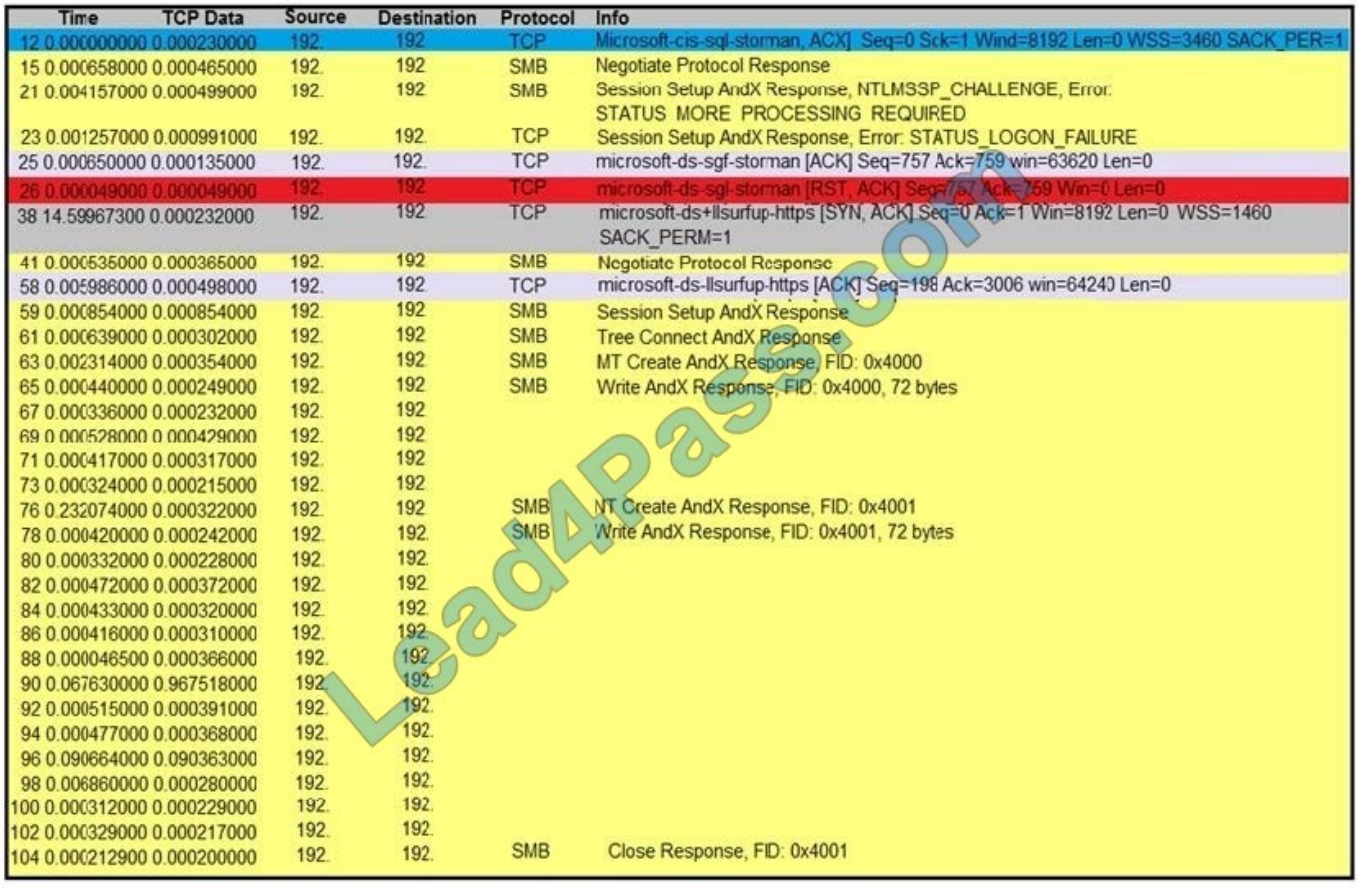
C. signed macro requirements

D. firewall rules creation

E. network access control

Correct Answer: AC

QUESTION 10



Time	TCP Data	Source	Destination	Protocol	Info
12 0.000000000	0.000230000	192.	192	TCP	Microsoft-cis-sql-storman, ACK] Seq=0 Sck=1 Wind=8192 Len=0 WSS=3460 SACK_PER=1
15 0.000658000	0.000465000	192.	192	SMB	Negotiate Protocol Response
21 0.004157000	0.000499000	192.	192	SMB	Session Setup AndX Response, NTLMSSP_CHALLENGE, Error: STATUS_MORE_PROCESSING_REQUIRED
23 0.001257000	0.000991000	192.	192.	TCP	Session Setup AndX Response, Error: STATUS_LOGON_FAILURE
25 0.000650000	0.000135000	192.	192.	TCP	microsoft-ds-sgf-storman [ACK] Seq=757 Ack=759 win=63620 Len=0
26 0.000049000	0.000049000	192.	192	TCP	microsoft-ds-sgf-storman [RST, ACK] Seq=757 Ack=759 Win=0 Len=0
38 14.59967300	0.000232000	192.	192	TCP	microsoft-ds+llsurfup-https [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 WSS=1460 SACK_PERM=1
41 0.000535000	0.000365000	192.	192	SMB	Negotiate Protocol Response
58 0.005986000	0.000498000	192.	192	TCP	microsoft-ds-llsurfup-https [ACK] Seq=198 Ack=3006 win=64240 Len=0
59 0.000854000	0.000854000	192.	192	SMB	Session Setup AndX Response
61 0.000639000	0.000302000	192.	192	SMB	Tree Connect AndX Response
63 0.002314000	0.000354000	192.	192	SMB	MT Create AndX Response, FID: 0x4000
65 0.000440000	0.000249000	192.	192	SMB	Write AndX Response, FID: 0x4000, 72 bytes
67 0.000336000	0.000232000	192.	192		
69 0.000528000	0.000429000	192.	192		
71 0.000417000	0.000317000	192.	192		
73 0.000324000	0.000215000	192.	192		
76 0.232074000	0.000322000	192.	192	SMB	NT Create AndX Response, FID: 0x4001
78 0.000420000	0.000242000	192.	192.	SMB	Write AndX Response, FID: 0x4001, 72 bytes
80 0.000332000	0.000228000	192.	192.		
82 0.000472000	0.000372000	192.	192		
84 0.000433000	0.000320000	192.	192		
86 0.000416000	0.000310000	192.	192.		
88 0.000046500	0.000366000	192.	192.		
90 0.067630000	0.967518000	192.	192.		
92 0.000515000	0.000391000	192.	192.		
94 0.000477000	0.000368000	192.	192.		
96 0.090664000	0.090363000	192.	192.		
98 0.006860000	0.000280000	192.	192.		
100 0.000312000	0.000229000	192.	192.		
102 0.000329000	0.000217000	192.	192.		
104 0.000212900	0.000200000	192.	192.	SMB	Close Response, FID: 0x4001

Refer to the exhibit. An engineer is analyzing a TCP stream in a Wireshark after a suspicious email with a URL. What should be determined about the SMB traffic from this stream?

A. It is redirecting to a malicious phishing website,

B. It is exploiting redirect vulnerability C. It is requesting authentication on the user site.

D. It is sharing access to files and printers.

Correct Answer: B

QUESTION 11

Over the last year, an organization\\'s HR department has accessed data from its legal department on the last day of each month to create a monthly activity report. An engineer is analyzing suspicious activity alerted by a threat intelligence platform that an authorized user in the HR department has accessed legal data daily for the last week. The engineer pulled the network data from the legal department\\'s shared folders and discovered above average-size data dumps. Which threat actor is implied from these artifacts?

A. privilege escalation

B. internal user errors

C. malicious insider

D. external exfiltration

Correct Answer: C

QUESTION 12

```
[**] [1:2008186:5] ET SCAN DirBuster Web App Scan in Progress [**]
[Classification: Web Application Attack] [Priority: 1]
04/20-13:02:21.250000 192.168.100.100:51022 -> 192.168.50.50:80
TCP TTL:63 TOS:0x0 ID:20054 IpLen:20 DgmLen:342 DF
***AP*** Seq: 0x369FB652 Ack: 0x9CF06FD8 Win: 0xFA60 TcpLen: 32
[Xref => http://doc.emergingthreats.net/2008186] [Xref => http://owasp.org]
```


Refer to the exhibit. According to the SNORT alert, what is the attacker performing?

A. brute-force attack against the web application user accounts

B. XSS attack against the target webserver

C. brute-force attack against directories and files on the target webserver

D. SQL injection attack against the target webserver

Correct Answer: C

QUESTION 13

Metadata	
Drive type	Fixed (Hard disk)
Drive serial number	1CBDB2C4
Full path	C:\Windows\System32\WIndowsPowerShell\v1.0\powershell.exe
NetBIOS name	user-pc
Lnk file name	ds7002.pdf
Relative path	..\..\..\..\..\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
Arguments	-noni –ep bypass $zk = 'JHB0Z3Q9MHgwMDA1ZTJiZTskdmNxPTB4MDAwNjlzYjY7.
Target file size (bytes)	452608
Droid volume	c59b0b22-7202-4410-b323-894349c1d75b
Birth droid volume	c59b0b22-7202-4410-b323-894349c1d75b
Droid file	bf069f66-8be6-11e6-b3d9-0800279224e5
Birth droid file	bf069f66-8be6-11e6-b3d9-0800279224e5
File attribute	The file or directory is an archive file
Target file access time (UTC)	13.07.2009 23:32:37
Target file creation time (UTC)	13.07.2009 23:32:37
Target file modification time (UTC)	14.07.2009 1:14:24
Header flags	HasTargetIdList, HasLinkInfo, HasName, HasRelativePath, HasArguments, HasIcc
MAC vendor	Cadmus Computer Systems
Target path	My Computer\C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
Target MFT entry number	0x7E21

Refer to the exhibit. An engineer is analyzing a .LNK (shortcut) file recently received as an email attachment and blocked by email security as suspicious. What is the next step an engineer should take?

A. Delete the suspicious email with the attachment as the file is a shortcut extension and does not represent any threat.

B. Upload the file to a virus checking engine to compare with well-known viruses as the file is a virus disguised as a legitimate extension.

C. Quarantine the file within the endpoint antivirus solution as the file is a ransomware which will encrypt the documents of a victim.

D. Open the file in a sandbox environment for further behavioral analysis as the file contains a malicious script that runs on execution.

Correct Answer: D

QUESTION 14

00386078	64	44	45	33	4C	6A	41	34	4C	6A	4D	78	4C	6B	5A	44
00386088	4D	44	59	78	4E	79	34	31	4E	54	41	32	4C	6A	55	31
00386098	4D	44	59	75	4E	6A	67	7A	4E	77	3D	3D	00	AB	AB	AB

Refer to the exhibit. Which encoding technique is represented by this HEX string?

A. Unicode

B. Binary

C. Base64

D. Charcode

Correct Answer: B

Reference: https://www.suse.com/c/making-sense-hexdump/

QUESTION 15

```
indicator:Observable id= "example:Observable-Pattern-5f1dedd3-ece3-4007-94cd-7d52784c1474">
<cybox:Object id= "example:Object-3a7aa9db-d082-447c-a422-293b78e24238">
<cybox:Properties xsi:type= "EmailMessageObj:EmailMessageObjectType">
<EmailMessageObj:Header>
<EmailMessageObj:From category= "e-mail">
<AddressObj:Address_Value condition= "Contains">@state.gov</AddressObj:Address Value>
</EmailMessageObj:From>
</EmailMessageObj:Header>
</cybox:Properties>
<cybox:Related_Objects>
<cybox:Related_Object>
<cybox:Properties xsi:type= "FileObj:FileObjectType">
<FileObj:File_Extension>pdf</FileObj:File_Extension>
<FileObj:Size_In_Bytes>87022</FileObj:Size_In_Bytes>
<FileObj:Hashes>
<cyboxCommon:Hash>
<cyboxCommon:Type xsi type= 'cyboxVocabs:HashNameVocab- 1.0">MD5</cyboxCommon:Type>
<cyboxCommn:Simple_Hash_Value>cf2b3ad32a8a4cfb05e9dfc45875bd70</cyboxCommon:Simple_Ha
sh_Value>
</cyboxCommon:Hash>
</FileObj:Hashes>
</cybox:Properties>
<cybox:Relationship xsi:type= "cyboxVocabs:ObjectRelatiobshipVocab-
1.0">Contains</cybox:Relationship>
</cybox:Related_Object>|
</cybox:Related_Objects>
</cybox:Object>
</indicator:Observable>
```


Refer to the exhibit. Which two actions should be taken as a result of this information? (Choose two.)

A. Update the AV to block any file with hash "cf2b3ad32a8a4cfb05e9dfc45875bd70".

B. Block all emails sent from an @state.gov address.

C. Block all emails with pdf attachments.

D. Block emails sent from Admin@state.net with an attached pdf file with md5 hash "cf2b3ad32a8a4cfb05e9dfc45875bd70".

E. Block all emails with subject containing "cf2b3ad32a8a4cfb05e9dfc45875bd70".

Correct Answer: AB