



300-215^{Q&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.geekcert.com/300-215.html>

100% Passing Guarantee
100% Money Back Assurance

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

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





QUESTION 1

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 2

A scanner detected a malware-infected file on an endpoint that is attempting to beacon to an external site. An analyst has reviewed the IPS and SIEM logs but is unable to identify the file's behavior. Which logs should be reviewed next to evaluate this file further?

- A. email security appliance
- B. DNS server
- C. Antivirus solution
- D. network device

Correct Answer: B

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

```
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

QUESTION 5

System Number of events: 572

Level	Date and Time	Source	Event ID	Task Category
Information	4/26/2015 12:42:14 PM	Service Control Man...	7045	None
Information	4/26/2015 12:38:28 PM	Service Control Man...	7045	None

Event 7045, Service Control Manager

General Details

A service was installed in the system.

Service Name: DIIAOHHNMPMMRqji
Service File Name: [\\127.0.0.1\admin\\$\EgnBqKWm.exe](#)
Service Type: user mode service
Service Start Type: demand start
Service Account: LocalSystem

Refer to the exhibit. An HR department submitted a ticket to the IT helpdesk indicating slow performance on an internal share server. The helpdesk engineer checked the server with a real-time monitoring tool and did not notice anything suspicious. After checking the event logs, the engineer noticed an event that occurred 48 hour prior. Which two indicators of compromise should be determined from this information? (Choose two.)

- A. unauthorized system modification
- B. privilege escalation
- C. denial of service attack
- D. compromised root access
- E. malware outbreak

Correct Answer: AD

[300-215 VCE Dumps](#)

[300-215 Practice Test](#)

[300-215 Braindumps](#)