

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.pass2lead.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 website administrator has an output of an FTP session that runs nightly to download and unzip files to a local staging server. The download includes thousands of files, and the manual process used to find how many files failed to download is time-consuming. The administrator is working on a PowerShell script that will parse a log file and summarize how many files were successfully downloaded versus ones that failed. Which script will read the contents of the file one line at a time and return a collection of objects?

- A. `Get-Content-Folder \\Server\FTPFolder\Logfiles\ftpfiles.log | Show-From "ERROR", "SUCCESS"`
- B. `Get-Content -ifmatch \\Server\FTPFolder\Logfiles\ftpfiles.log | Copy-Marked "ERROR", "SUCCESS"`
- C. `Get-Content -Directory \\Server\FTPFolder\Logfiles\ftpfiles.log | Export-Result "ERROR", "SUCCESS"`
- D. `Get-Content -Path \\Server\FTPFolder\Logfiles\ftpfiles.log | Select-String "ERROR", "SUCCESS"`

Correct Answer: D

QUESTION 2

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 3

An "unknown error code" is appearing on an ESXi host during authentication. An engineer checks the authentication logs but is unable to identify the issue. Analysis of the vCenter agent logs shows no connectivity errors. What is the next log file the engineer should check to continue troubleshooting this error?

- A. `/var/log/syslog.log`
- B. `/var/log/vmksummary.log`
- C. `var/log/shell.log`
- D. `var/log/general/log`

Correct Answer: A

Reference: <https://docs.vmware.com/en/VMware-vSphere/6.7/com.vmware.vsphere.monitoring.doc/GUID-832A2618-6B11-4A28-9672-93296DA931D0.html>

QUESTION 4

An employee receives an email from a "trusted" person containing a hyperlink that is malvertising. The employee clicks the link and the malware downloads. An information analyst observes an alert at the SIEM and engages the cybersecurity team to conduct an analysis of this incident in accordance with the incident response plan. Which event detail should be included in this root cause analysis?

- A. phishing email sent to the victim
- B. alarm raised by the SIEM
- C. information from the email header
- D. alert identified by the cybersecurity team

Correct Answer: B

QUESTION 5

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

[Latest 300-215 Dumps](#)

[300-215 Practice Test](#)

[300-215 Exam Questions](#)