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.pass4itsure.com/300-215.html

100% Passing Guarantee
100% Money Back Assurance

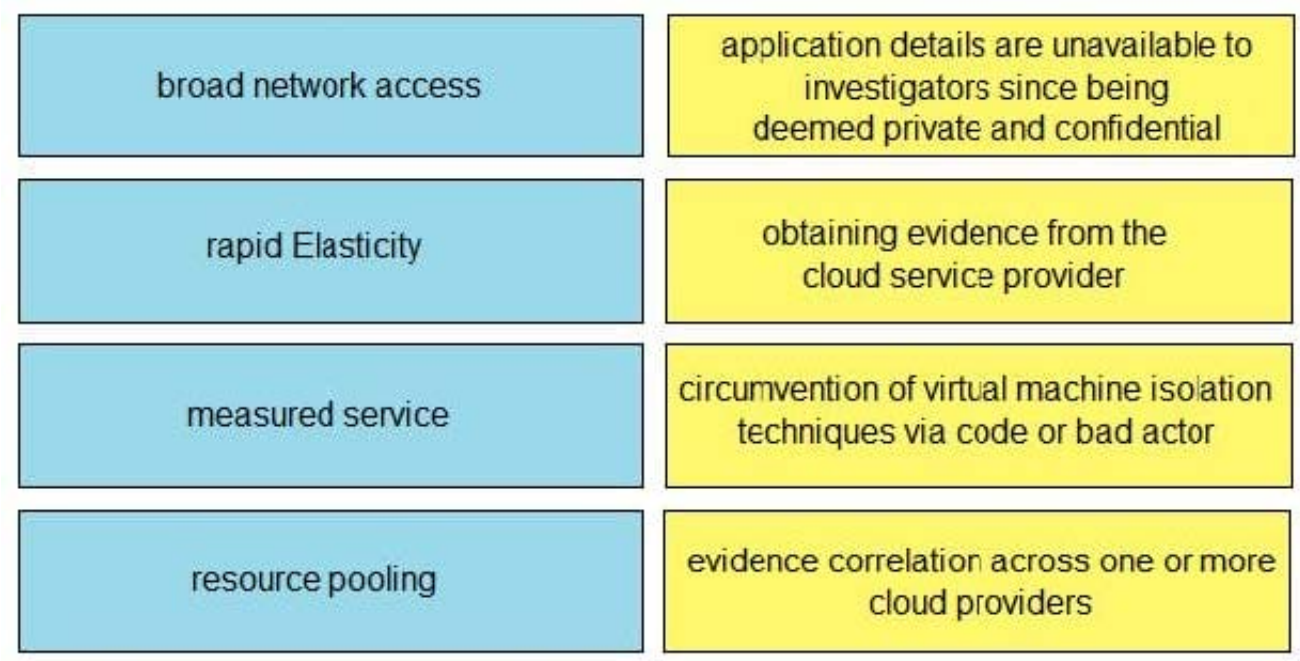
Following Questions and Answers are all new published by Cisco Official Exam Center

QUESTION 1

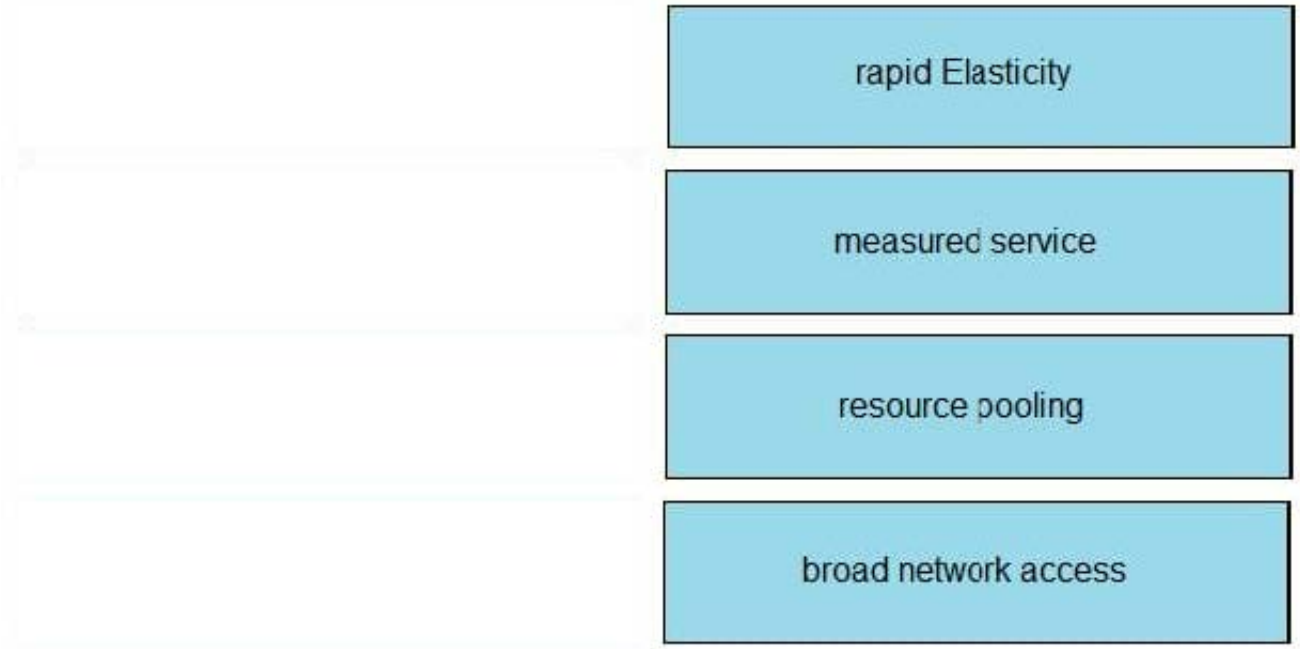
DRAG DROP

Drag and drop the cloud characteristic from the left onto the challenges presented for gathering evidence on the right.

Select and Place:



Correct Answer:



QUESTION 2

Refer to the exhibit. According to the Wireshark output, what are two indicators of compromise for detecting an Emotet malware download? (Choose two.)

A. Domain name:iraniansk.com

B. Server: nginx

C. Hash value: 5f31ab113af08=1597090577

D. filename= "Fy.exe"

E. Content-Type: application/octet-stream

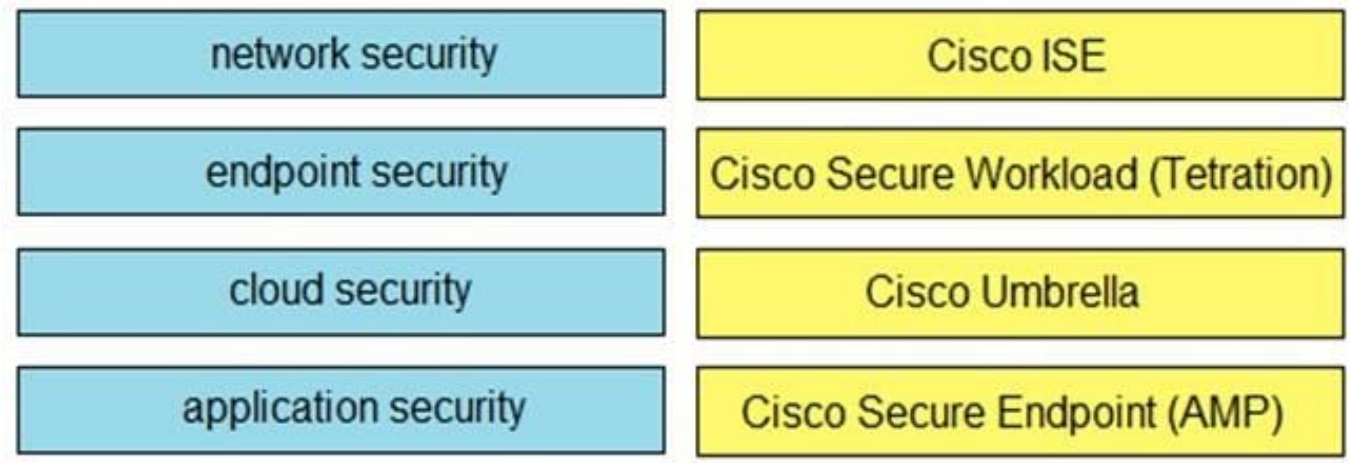
Correct Answer: CE

QUESTION 3

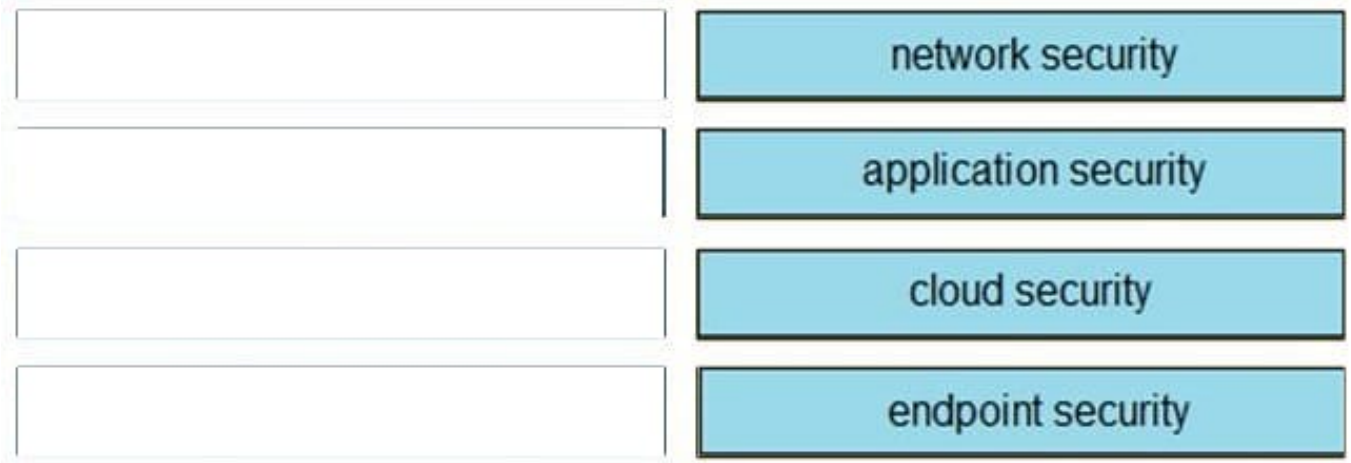
DRAG DROP

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

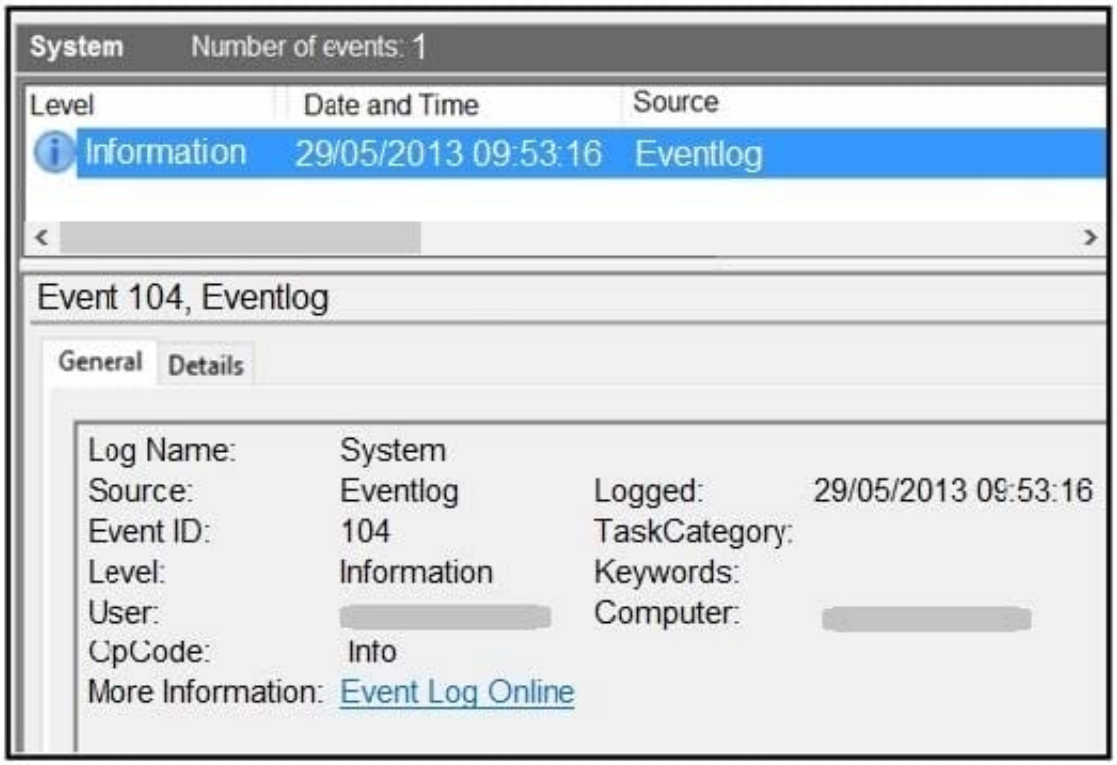
Select and Place:



Correct Answer:



QUESTION 4



Refer to the exhibit. An employee notices unexpected changes and setting modifications on their workstation and creates an incident ticket. A support specialist checks processes and services but does not identify anything suspicious. The ticket was escalated to an analyst who reviewed this event log and also discovered that the workstation had multiple large data dumps on network shares. What should be determined from this information?

A. data obfuscation

B. reconnaissance attack

C. brute-force attack

D. log tampering

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