300-215$^{Q\&As}$

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

QUESTION 1

Which magic byte indicates that an analyzed file is a pdf file?

A. cGRmZmlsZQ

B. 706466666

C. 255044462d

D. 0a0ah4cg

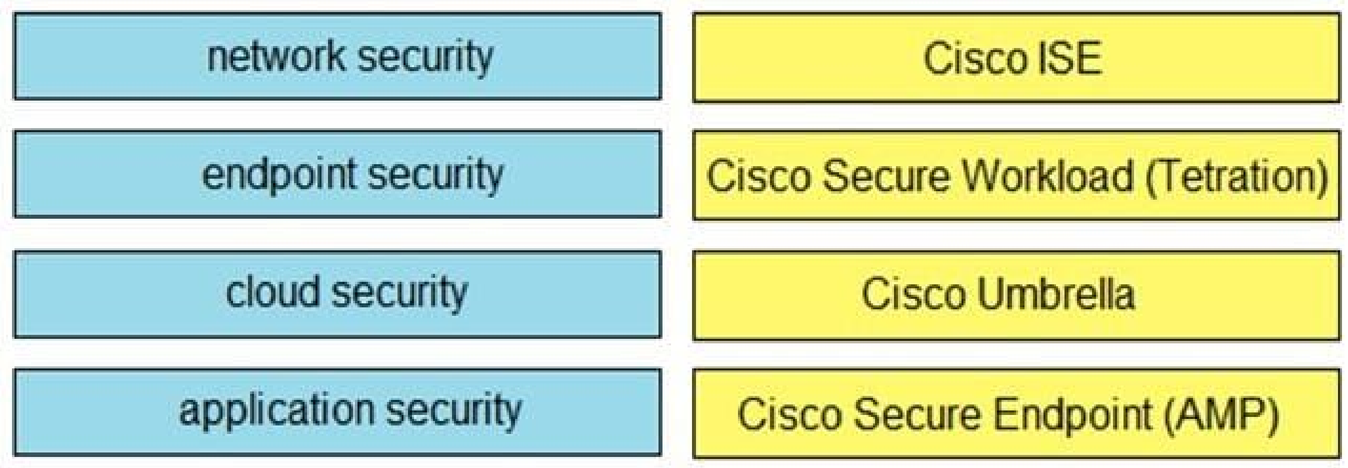
Correct Answer: C

QUESTION 2

DRAG DROP

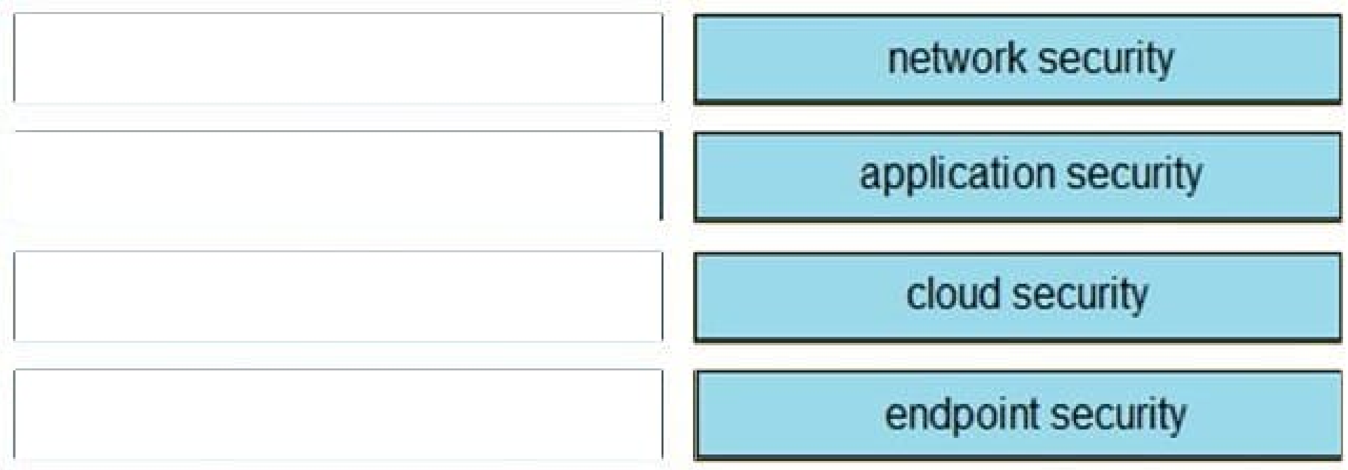
Drag and drop the capabilities on the left onto the Cisco security solutions on the right.

Select and Place:



network security	Cisco ISE
endpoint security	Cisco Secure Workload (Tetration)
cloud security	Cisco Umbrella
application security	Cisco Secure Endpoint (AMP)

Correct Answer:

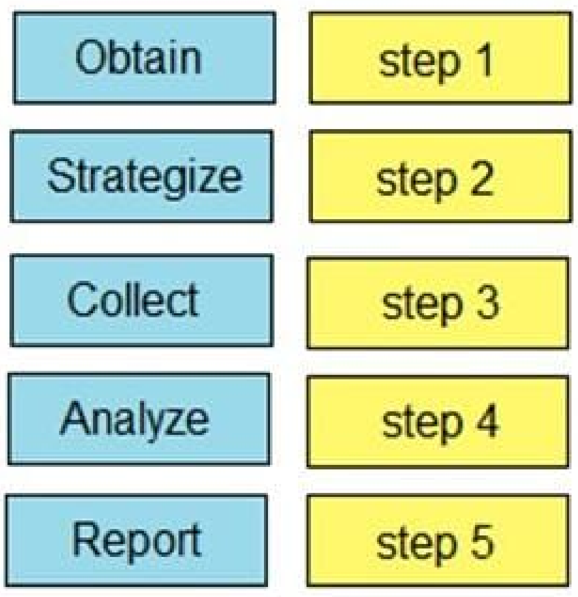


QUESTION 3

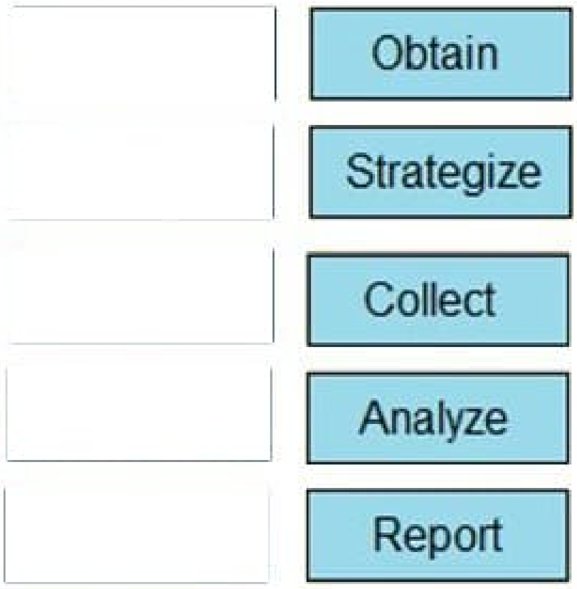
DRAG DROP

Drag and drop the steps from the left into the order to perform forensics analysis of infrastructure networks on the right.

Select and Place:



Correct Answer:



Obtain

Strategize

Collect

Analyze

Report

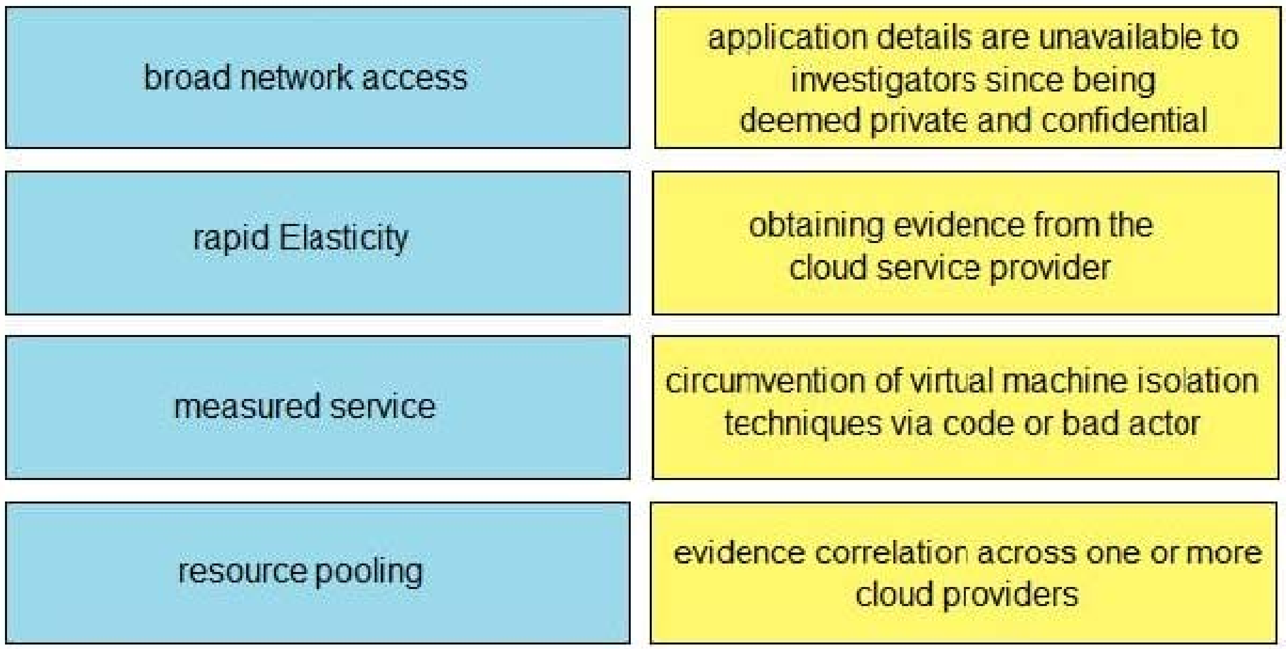
Reference: https://subscription.packtpub.com/book/networking_and_servers/9781789344523/1/ch01lvl1sec12/network-forensics-investigation-methodology

QUESTION 4

DRAG DROP

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

Select and Place:



broad network access

rapid Elasticity

measured service

resource pooling

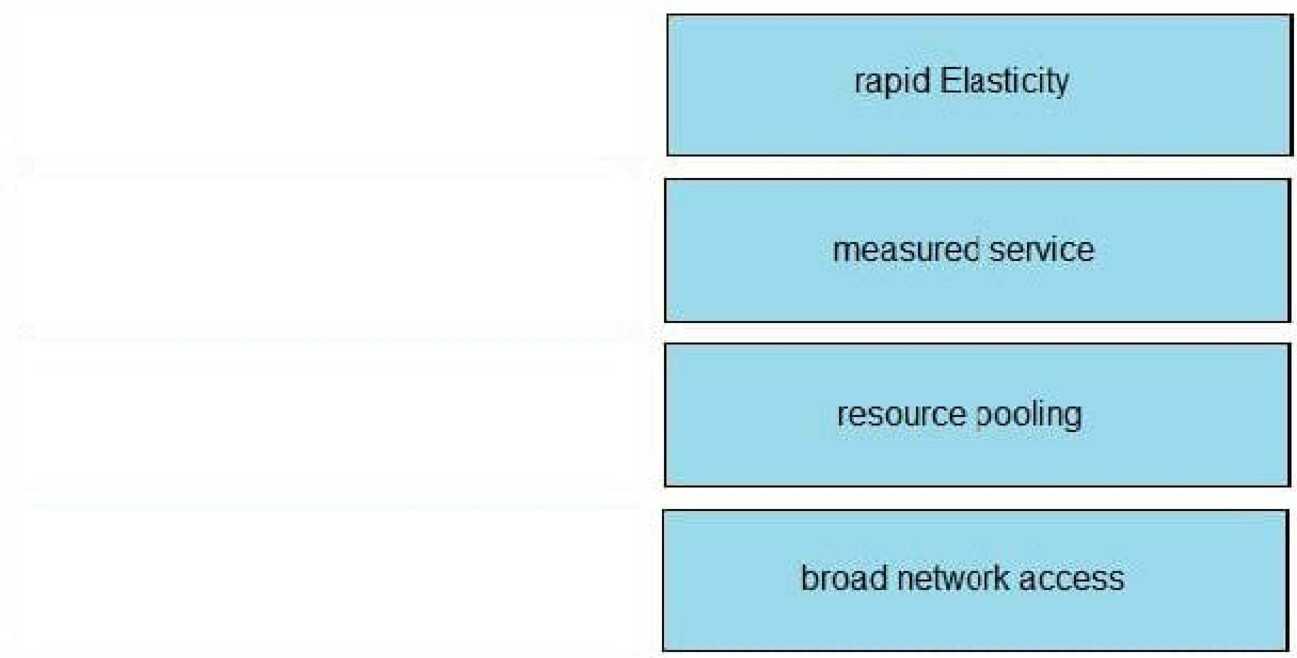
application details are unavailable to investigators since being deemed private and confidential

obtaining evidence from the cloud service provider

circumvention of virtual machine isolation techniques via code or bad actor

evidence correlation across one or more cloud providers

Correct Answer:



rapid Elasticity

measured service

resource pooling

broad network access

QUESTION 5

A security team received an alert of suspicious activity on a user\\'s Internet browser. The user\\'s anti-virus software indicated that the file attempted to create a fake recycle bin folder and connect to an external IP address. Which two actions should be taken by the security analyst with the executable file for further analysis? (Choose two.)

A. Evaluate the process activity in Cisco Umbrella.

B. Analyze the TCP/IP Streams in Cisco Secure Malware Analytics (Threat Grid).

C. Evaluate the behavioral indicators in Cisco Secure Malware Analytics (Threat Grid).

D. Analyze the Magic File type in Cisco Umbrella.

E. Network Exit Localization in Cisco Secure Malware Analytics (Threat Grid).

Correct Answer: BC