300-215 Q&As

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

QUESTION 1

A security team detected an above-average amount of inbound tcp/135 connection attempts from unidentified senders. The security team is responding based on their incident response playbook. Which two elements are part of the eradication phase for this incident? (Choose two.)

A. anti-malware software

B. data and workload isolation

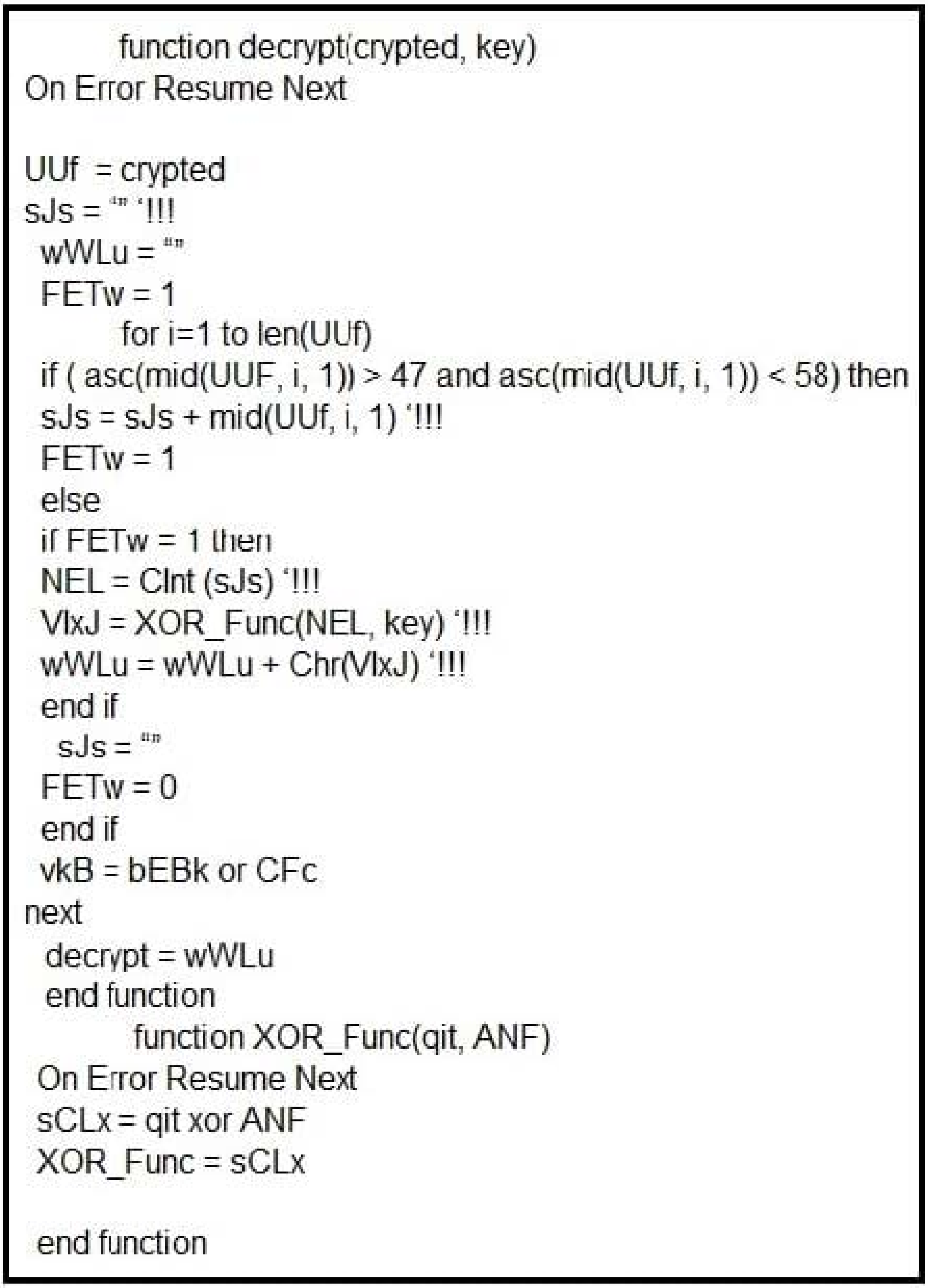
C. centralized user management

D. intrusion prevention system

E. enterprise block listing solution

Correct Answer: CD

QUESTION 2



```
        function decrypt(crypted, key)
On Error Resume Next

UUf  = crypted
sJs = "" '!!!
  wWLu = ""
  FETw = 1
        for i=1 to len(UUf)
  if ( asc(mid(UUF, i, 1)) > 47 and asc(mid(UUf, i, 1)) < 58) then
  sJs = sJs + mid(UUf, i, 1) '!!!
  FETw = 1
  else
  if FETw = 1 then
  NEL = CInt (sJs) '!!!
  VlxJ = XOR_Func(NEL, key) '!!!
  wWLu = wWLu + Chr(VlxJ) '!!!
  end if
    sJs = ""
  FETw = 0
  end if
  vkB = bEBk or CFc
next
  decrypt = wWLu
  end function
          function XOR_Func(qit, ANF)
 On Error Resume Next
 sCLx = qit xor ANF
 XOR_Func = sCLx

 end function
```

Refer to the exhibit. Which type of code created the snippet?

A. VB Script

B. Python

C. PowerShell

D. Bash Script

Correct Answer: A

QUESTION 3

What are YARA rules based upon?

A. binary patterns

B. HTML code

C. network artifacts

D. IP addresses

Correct Answer: A

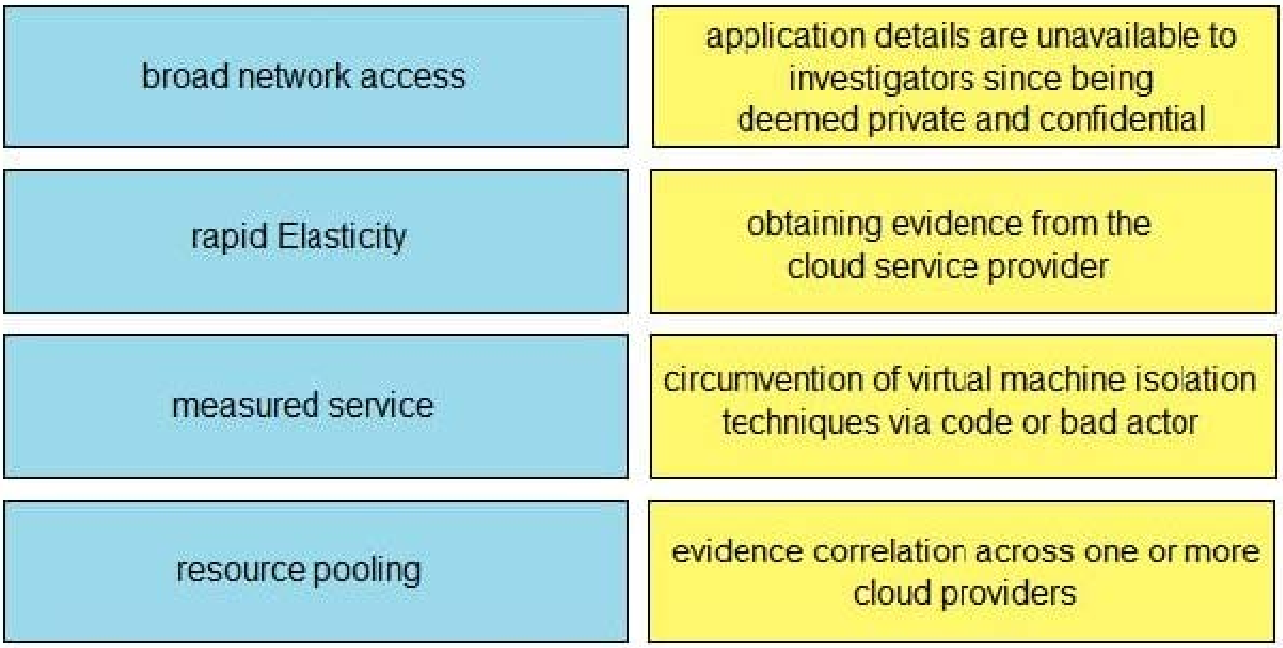
Reference: https://en.wikipedia.org/wiki/YARA#:~:text=YARA%20is%20the%20name%20of,strings%20and%20a%20boolean%20expression.

QUESTION 4

DRAG DROP

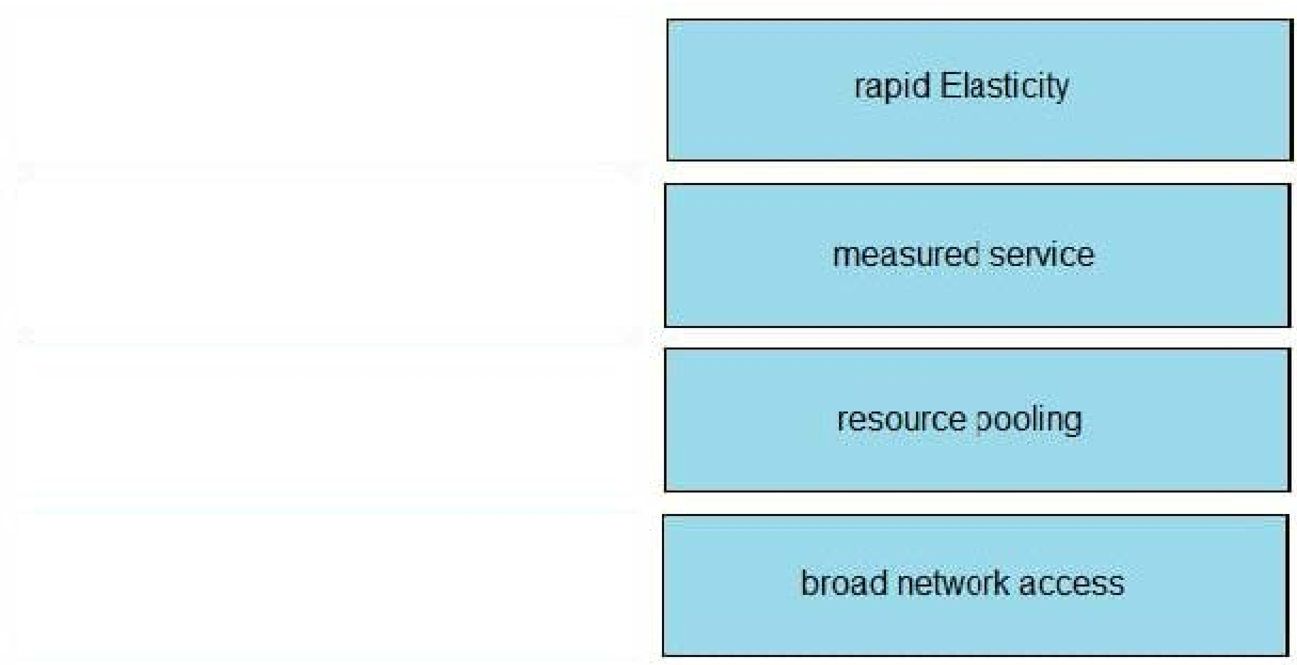
Drag and drop the cloud characteristic from the left onto the challenges presented for gathering evidence on the right.

Select and Place:



broad network access	application details are unavailable to investigators since being deemed private and confidential
rapid Elasticity	obtaining evidence from the cloud service provider
measured service	circumvention of virtual machine isolation techniques via code or bad actor
resource pooling	evidence correlation across one or more cloud providers

Correct Answer:



QUESTION 5

What is the steganography anti-forensics technique?

A. hiding a section of a malicious file in unused areas of a file

B. changing the file header of a malicious file to another file type

C. sending malicious files over a public network by encapsulation

D. concealing malicious files in ordinary or unsuspecting places

Correct Answer: A

https://blog.eccouncil.org/6-anti-forensic-techniques-that-every-cyber-investigator-dreads/