CERTSinside

Free Questions for 350-201 by certsinside

Shared by Estrada on 24-05-2024

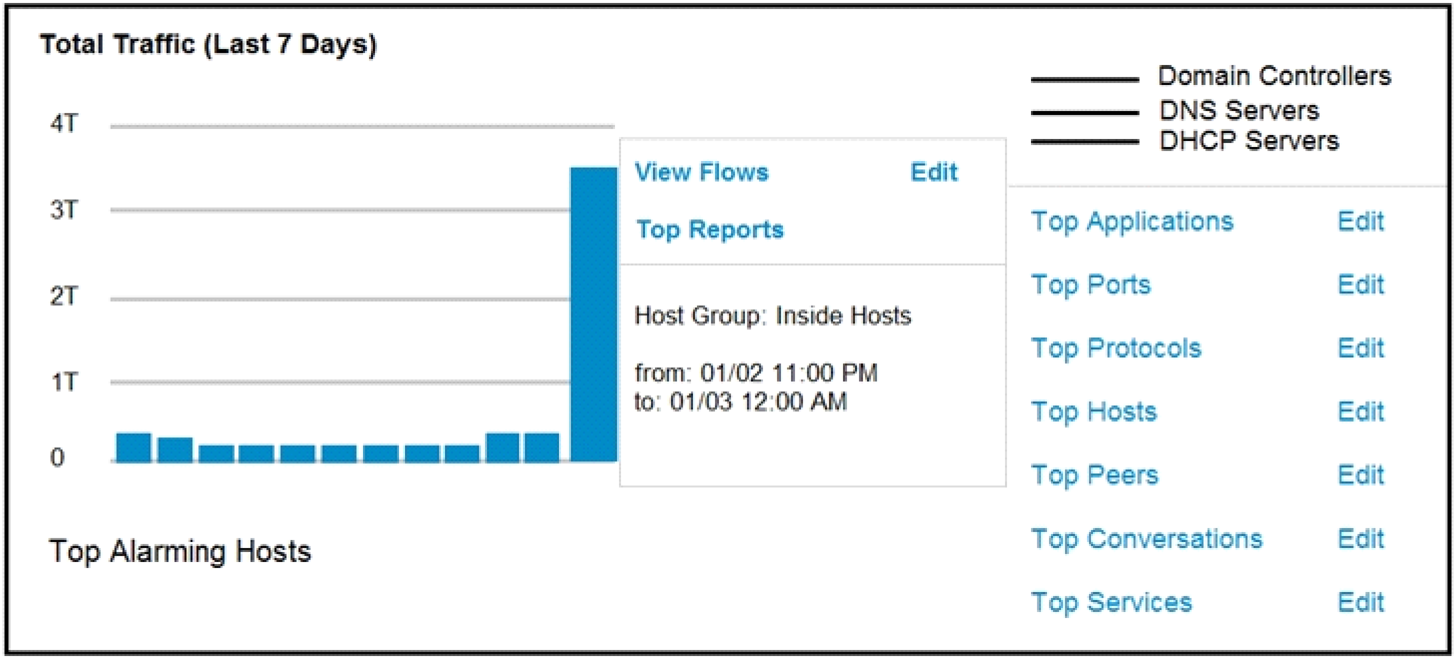
For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

Refer to the exhibit.



Host Group: Inside Hosts

from: 01/02 11:00 PM
to: 01/03 12:00 AM

An engineer notices a significant anomaly in the traffic in one of the host groups in Cisco Secure Network Analytics (Stealthwatch) and must analyze the top data transmissions. Which tool accomplishes this task?

Options:

A- Top Peers

B- Top Hosts

C- Top Conversations

D- Top Ports

Answer:

B

Question 2

Question Type: **MultipleChoice**

An engineer is developing an application that requires frequent updates to close feedback loops and enable teams to quickly apply patches. The team wants their code updates to get to market as often as possible. Which software development approach should be used to accomplish these goals?

Options:

A- continuous delivery

B- continuous integration

C- continuous deployment

D- continuous monitoring

Answer:

A

Question 3

Question Type: MultipleChoice

What is a benefit of key risk indicators?

Options:

A- clear perspective into the risk position of an organization

B- improved visibility on quantifiable information

C- improved mitigation techniques for unknown threats

D- clear procedures and processes for organizational risk

Answer:

C

Question 4

Question Type: **MultipleChoice**

An engineer is moving data from NAS servers in different departments to a combined storage database so that the data can be accessed and analyzed by the organization on-demand. Which data management process is being used?

Options:

A- data clustering

B- data regression

C- data ingestion

D- data obfuscation

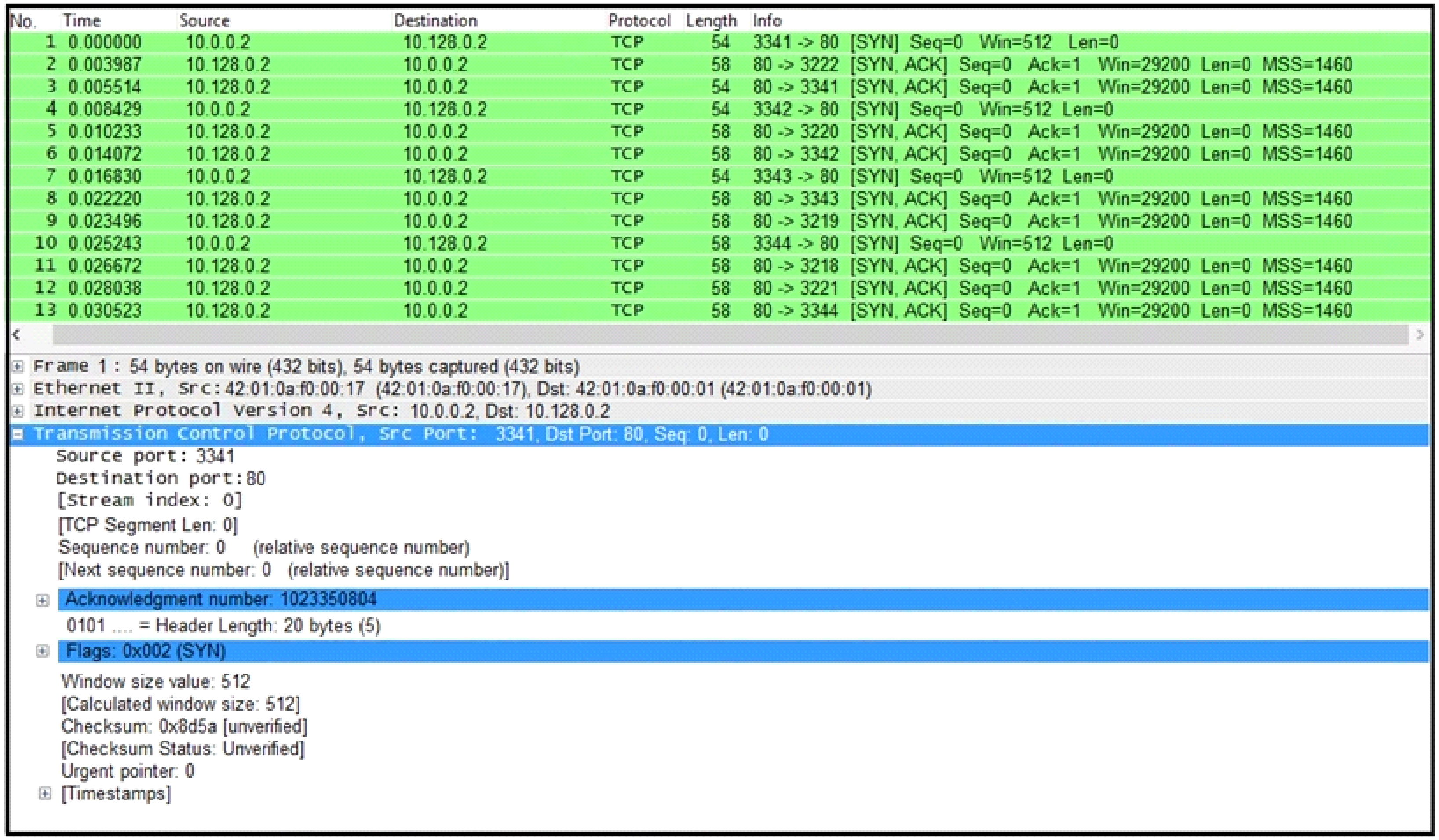
Answer:

A

Question 5

Question Type: MultipleChoice

Refer to the exhibit.



```
No.  Time      Source       Destination   Protocol Length Info
  1 0.000000   10.0.0.2     10.128.0.2    TCP      54     3341 -> 80 [SYN] Seq=0  Win=512  Len=0
  2 0.003987   10.128.0.2   10.0.0.2      TCP      58     80 -> 3222 [SYN, ACK] Seq=0  Ack=1  Win=29200 Len=0 MSS=1460
  3 0.005514   10.128.0.2   10.0.0.2      TCP      54     80 -> 3341 [SYN, ACK] Seq=0  Ack=1  Win=29200 Len=0 MSS=1460
  4 0.008429   10.0.0.2     10.128.0.2    TCP      54     3342 -> 80 [SYN] Seq=0  Win=512 Len=0
  5 0.010233   10.128.0.2   10.0.0.2      TCP      58     80 -> 3220 [SYN, ACK] Seq=0  Ack=1  Win=29200 Len=0 MSS=1460
  6 0.014072   10.128.0.2   10.0.0.2      TCP      58     80 -> 3342 [SYN, ACK] Seq=0  Ack=1  Win=29200 Len=0 MSS=1460
  7 0.016830   10.0.0.2     10.128.0.2    TCP      54     3343 -> 80 [SYN] Seq=0  Win=512 Len=0
  8 0.022220   10.128.0.2   10.0.0.2      TCP      58     80 -> 3343 [SYN, ACK] Seq=0  Ack=1  Win=29200 Len=0 MSS=1460
  9 0.023496   10.128.0.2   10.0.0.2      TCP      58     80 -> 3219 [SYN, ACK] Seq=0  Ack=1  Win=29200 Len=0 MSS=1460
 10 0.025243   10.0.0.2     10.128.0.2    TCP      58     3344 -> 80 [SYN] Seq=0  Win=512 Len=0
 11 0.026672   10.128.0.2   10.0.0.2      TCP      58     80 -> 3218 [SYN, ACK] Seq=0  Ack=1  Win=29200 Len=0 MSS=1460
 12 0.028038   10.128.0.2   10.0.0.2      TCP      58     80 -> 3221 [SYN, ACK] Seq=0  Ack=1  Win=29200 Len=0 MSS=1460
 13 0.030523   10.128.0.2   10.0.0.2      TCP      58     80 -> 3344 [SYN, ACK] Seq=0  Ack=1  Win=29200 Len=0 MSS=1460
```

```
⊞ Frame 1: 54 bytes on wire (432 bits), 54 bytes captured (432 bits)
⊞ Ethernet II, Src: 42:01:0a:f0:00:17 (42:01:0a:f0:00:17), Dst: 42:01:0a:f0:00:01 (42:01:0a:f0:00:01)
⊞ Internet Protocol Version 4, Src: 10.0.0.2, Dst: 10.128.0.2
⊟ Transmission Control Protocol, Src Port: 3341, Dst Port: 80, Seq: 0, Len: 0
     Source port: 3341
     Destination port:80
     [Stream index: 0]
     [TCP Segment Len: 0]
     Sequence number: 0    (relative sequence number)
     [Next sequence number: 0   (relative sequence number)]
   ⊞ Acknowledgment number: 1023350804
      0101 .... = Header Length: 20 bytes (5)
   ⊞ Flags: 0x002 (SYN)
      Window size value: 512
      [Calculated window size: 512]
      Checksum: 0x8d5a [unverified]
      [Checksum Status: Unverified]
      Urgent pointer: 0
   ⊞ [Timestamps]
```

What is the threat in this Wireshark traffic capture?

Options:

A- A high rate of SYN packets being sent from multiple sources toward a single destination IP

B- A flood of ACK packets coming from a single source IP to multiple destination IPs

C- A high rate of SYN packets being sent from a single source IP toward multiple destination IPs

D- A flood of SYN packets coming from a single source IP to a single destination IP

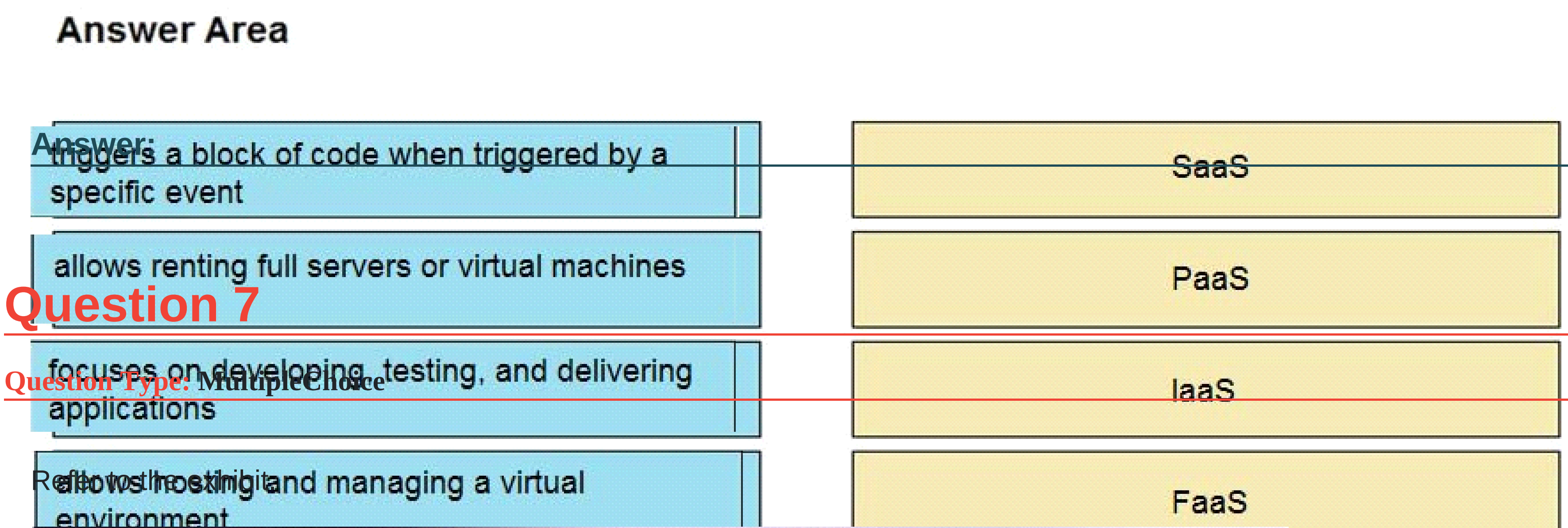
Answer:

D

Question 6

Question Type: **DragDrop**

Drag and drop the cloud computing service descriptions from the left onto the cloud service categories on the right.



Answer Area

triggers a block of code when triggered by a specific event

allows renting full servers or virtual machines

focuses on developing, testing, and delivering applications

allows hosting and managing a virtual environment

SaaS

PaaS

IaaS

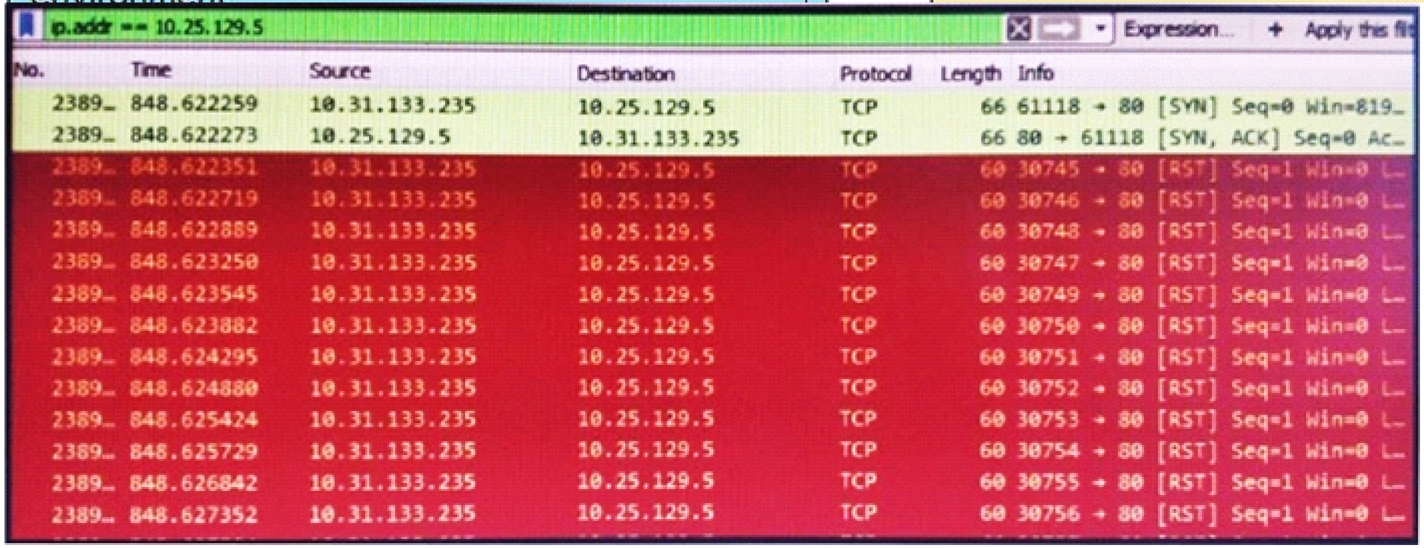
FaaS

Answer:

Question 7

Question Type: MultipleChoice

Refer to the exhibit.



```
No.    Time        Source          Destination     Protocol Length Info
2389…  848.622259  10.31.133.235   10.25.129.5     TCP      66 61118 → 80 [SYN] Seq=0 Win=819…
2389…  848.622273  10.25.129.5     10.31.133.235   TCP      66 80 → 61118 [SYN, ACK] Seq=0 Ac…
2389…  848.622351  10.31.133.235   10.25.129.5     TCP      60 30745 → 80 [RST] Seq=1 Win=0 L…
2389…  848.622719  10.31.133.235   10.25.129.5     TCP      60 30746 → 80 [RST] Seq=1 Win=0 L…
2389…  848.622889  10.31.133.235   10.25.129.5     TCP      60 30748 → 80 [RST] Seq=1 Win=0 L…
2389…  848.623250  10.31.133.235   10.25.129.5     TCP      60 30747 → 80 [RST] Seq=1 Win=0 L…
2389…  848.623545  10.31.133.235   10.25.129.5     TCP      60 30749 → 80 [RST] Seq=1 Win=0 L…
2389…  848.623882  10.31.133.235   10.25.129.5     TCP      60 30750 → 80 [RST] Seq=1 Win=0 L…
2389…  848.624295  10.31.133.235   10.25.129.5     TCP      60 30751 → 80 [RST] Seq=1 Win=0 L…
2389…  848.624880  10.31.133.235   10.25.129.5     TCP      60 30752 → 80 [RST] Seq=1 Win=0 L…
2389…  848.625424  10.31.133.235   10.25.129.5     TCP      60 30753 → 80 [RST] Seq=1 Win=0 L…
2389…  848.625729  10.31.133.235   10.25.129.5     TCP      60 30754 → 80 [RST] Seq=1 Win=0 L…
2389…  848.626842  10.31.133.235   10.25.129.5     TCP      60 30755 → 80 [RST] Seq=1 Win=0 L…
2389…  848.627352  10.31.133.235   10.25.129.5     TCP      60 30756 → 80 [RST] Seq=1 Win=0 L…
```

What is occurring in this packet capture?

Options:

A- TCP port scan

B- TCP flood

C- DNS flood

D- DNS tunneling

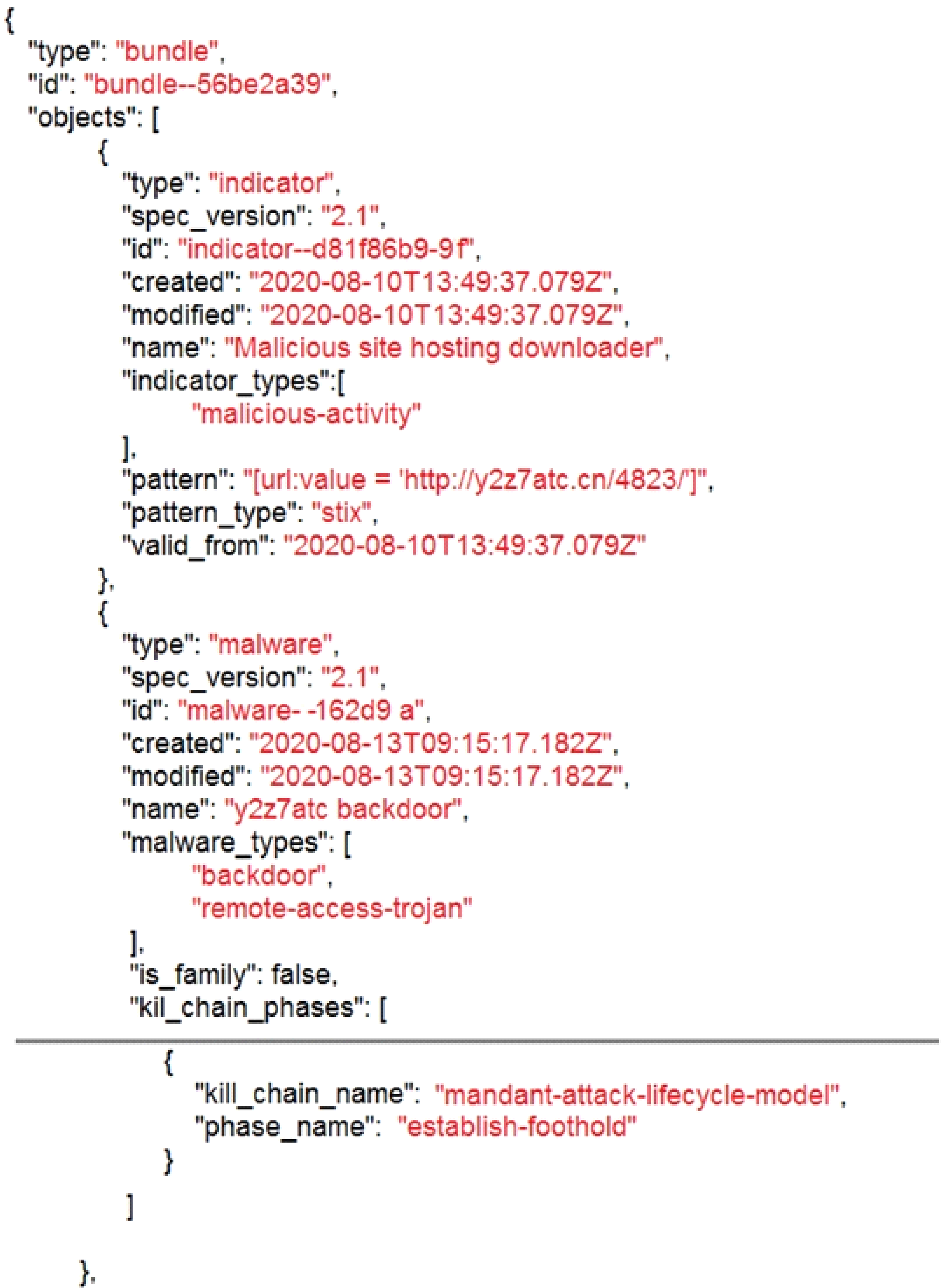
Answer:

B

Question 8

Question Type: **MultipleChoice**

Refer to the exhibit.



```
{
  "type": "bundle",
  "id": "bundle--56be2a39",
  "objects": [
         {
           "type": "indicator",
           "spec_version": "2.1",
           "id": "indicator--d81f86b9-9f",
           "created": "2020-08-10T13:49:37.079Z",
           "modified": "2020-08-10T13:49:37.079Z",
           "name": "Malicious site hosting downloader",
           "indicator_types":[
                  "malicious-activity"
           ],
           "pattern": "[url:value = 'http://y2z7atc.cn/4823/']",
           "pattern_type": "stix",
           "valid_from": "2020-08-10T13:49:37.079Z"
         },
         {
           "type": "malware",
           "spec_version": "2.1",
           "id": "malware- -162d9 a",
           "created": "2020-08-13T09:15:17.182Z",
           "modified": "2020-08-13T09:15:17.182Z",
           "name": "y2z7atc backdoor",
           "malware_types": [
                  "backdoor",
                  "remote-access-trojan"
            ],
            "is_family": false,
            "kil_chain_phases": [
                {
                   "kill_chain_name":  "mandant-attack-lifecycle-model",
                   "phase_name":  "establish-foothold"
                }
            ]

         },
```

Which indicator of compromise is represented by this STIX?

Options:

A- website redirecting traffic to ransomware server

B- website hosting malware to download files

C- web server vulnerability exploited by malware

D- cross-site scripting vulnerability to backdoor server

Answer:

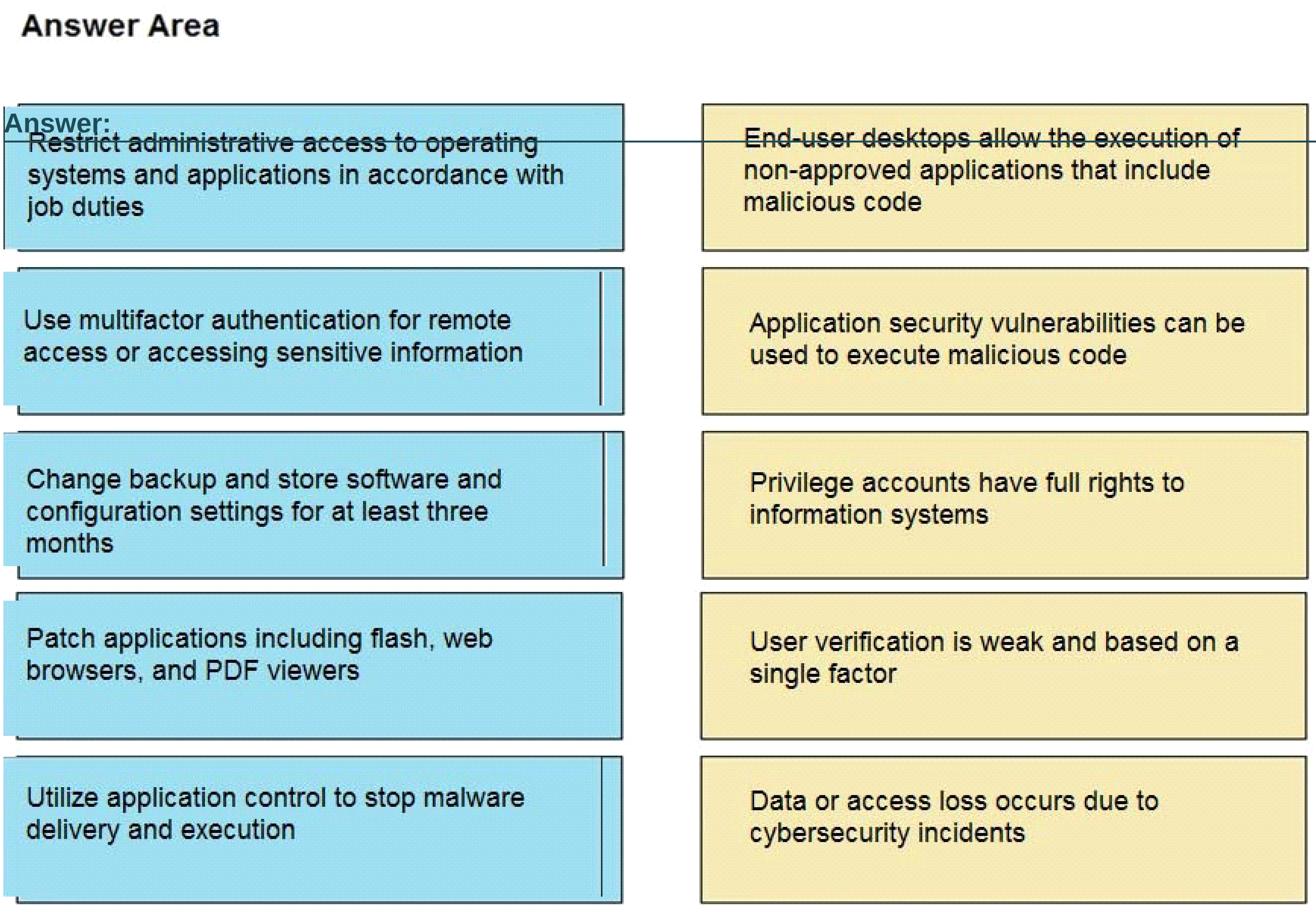
C

Question 9

Question Type: DragDrop

Drag and drop the mitigation steps from the left onto the vulnerabilities they mitigate on the right.

Answer:



Answer Area

Restrict administrative access to operating systems and applications in accordance with job duties	End-user desktops allow the execution of non-approved applications that include malicious code
Use multifactor authentication for remote access or accessing sensitive information	Application security vulnerabilities can be used to execute malicious code
Change backup and store software and configuration settings for at least three months	Privilege accounts have full rights to information systems
Patch applications including flash, web browsers, and PDF viewers	User verification is weak and based on a single factor
Utilize application control to stop malware delivery and execution	Data or access loss occurs due to cybersecurity incidents