Free Questions for 350-201 by actualtestdumps

Shared by West on 22-07-2024

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

A customer is using a central device to manage network devices over SNMPv2. A remote attacker caused a denial of service condition and can trigger this vulnerability by issuing a GET request for the ciscoFlashMIB OID on an affected device. Which should be disabled to resolve the issue?

Options:

A- SNMPv2

B- TCP small services

C- port UDP 161 and 162

D- UDP small services

Answer:

A

Question 2

Question Type: MultipleChoice

An audit is assessing a small business that is selling automotive parts and diagnostic services. Due to increased customer demands, the company recently started to accept credit card payments and acquired a POS terminal. Which compliance regulations must the audit apply to the company?

Options:

A- HIPAA

B- FISMA

C- COBIT

D- PCI DSS

Answer:

D

Question 3

Question Type: MultipleChoice

Refer to the exhibit.

```
try
{
   using (MemoryStream memoryStream = new MemoryStream())
   {
         memoryStream.Position = 32L;
         using (AesCryptoServiceProvider aesCryptoServiceProvider = new AesCryptoServiceProvider())
         {
            aesCryptoServiceProvider.KeySize = 128;
            aesCryptoServiceProvider.BlockSize = 128;
            aesCryptoServiceProvider.Mode = CipherMode.CBC;
            aesCryptoServiceProvider.Padding = PaddingMode.PKCS7;
            aesCryptoServiceProvider.Key = key;
            aesCryptoServiceProvider.GenerateIV();
            using (CryptoStream cryptoSream = new CryptoStream(memoryStream, aesCryptoServiceProvider.CreateEncryptor(), CryptoStreamMode.Write))
            {
                  memoryStream.Write(aesCryptoServiceProvider.IV, 0, aesCryptoServiceProvider.IV.Length);
                  cryptoStream.Write(input, 0, input.Length);
                  cryptoStream.FlushFinalBlock();
                  using (HMACSHA256 hMACSHA = new HMACSHA256(bytes))
                  {
                     byte[] array = hMACSHA.ComputeHash(memoryStream.ToArray(), 32, memoryStream.ToArray().Length - 32);
                     memoryStream.Position = 0L;
                     memoryStream.Write(array, 0, array.Length);
                  }
            }
         }
         result = memoryStream.ToArray();
   }
}
catch
{
}
```

An engineer is performing a static analysis on a malware and knows that it is capturing keys and webcam events on a company server. What is the indicator of compromise?

Options:

A- The malware is performing comprehensive fingerprinting of the host, including a processor, motherboard manufacturer, and connected removable storage.

B- The malware is a ransomware querying for installed anti-virus products and operating systems to encrypt and render unreadable until payment is made for file decryption.

C- The malware has moved to harvesting cookies and stored account information from major browsers and configuring a reverse proxy for intercepting network activity.

D- The malware contains an encryption and decryption routine to hide URLs/IP addresses and is storing the output of loggers and webcam captures in locally encrypted files for retrieval.

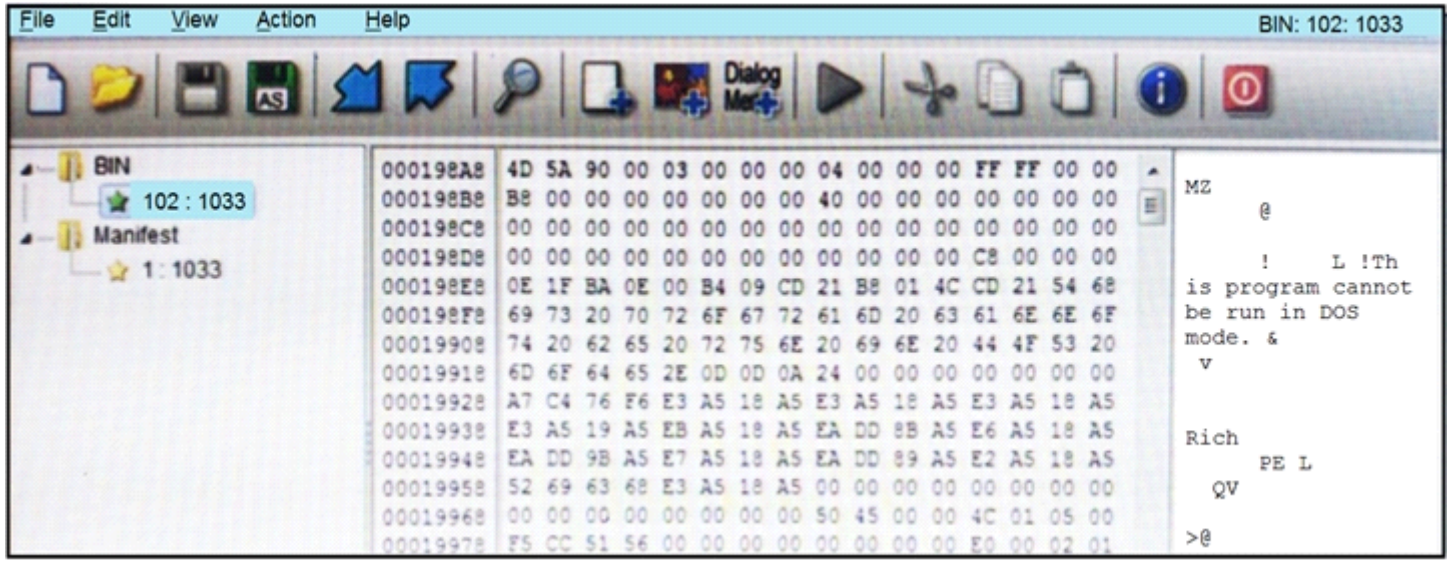
Answer:

B

Question 4

Question Type: MultipleChoice

Refer to the exhibit.



An engineer is reverse engineering a suspicious file by examining its resources. What does this file indicate?

Options:

A- a DOS MZ executable format

B- a MS-DOS executable archive

C- an archived malware

D- a Windows executable file

Answer:

D

Question 5

Question Type: MultipleChoice

How is a SIEM tool used?

Options:

A- To collect security data from authentication failures and cyber attacks and forward it for analysis

B- To search and compare security data against acceptance standards and generate reports for analysis

C- To compare security alerts against configured scenarios and trigger system responses

D- To collect and analyze security data from network devices and servers and produce alerts

Answer:

D

Question 6

Question Type: MultipleChoice

An employee who often travels abroad logs in from a first-seen country during non-working hours. The SIEM tool generates an alert that the user is forwarding an increased amount of emails to an external mail domain and then logs out. The investigation concludes that the external domain belongs to a competitor. Which two behaviors triggered UEBA? (Choose two.)

Options:

A- domain belongs to a competitor

B- log in during non-working hours

C- email forwarding to an external domain

D- log in from a first-seen country

E- increased number of sent mails

Answer:

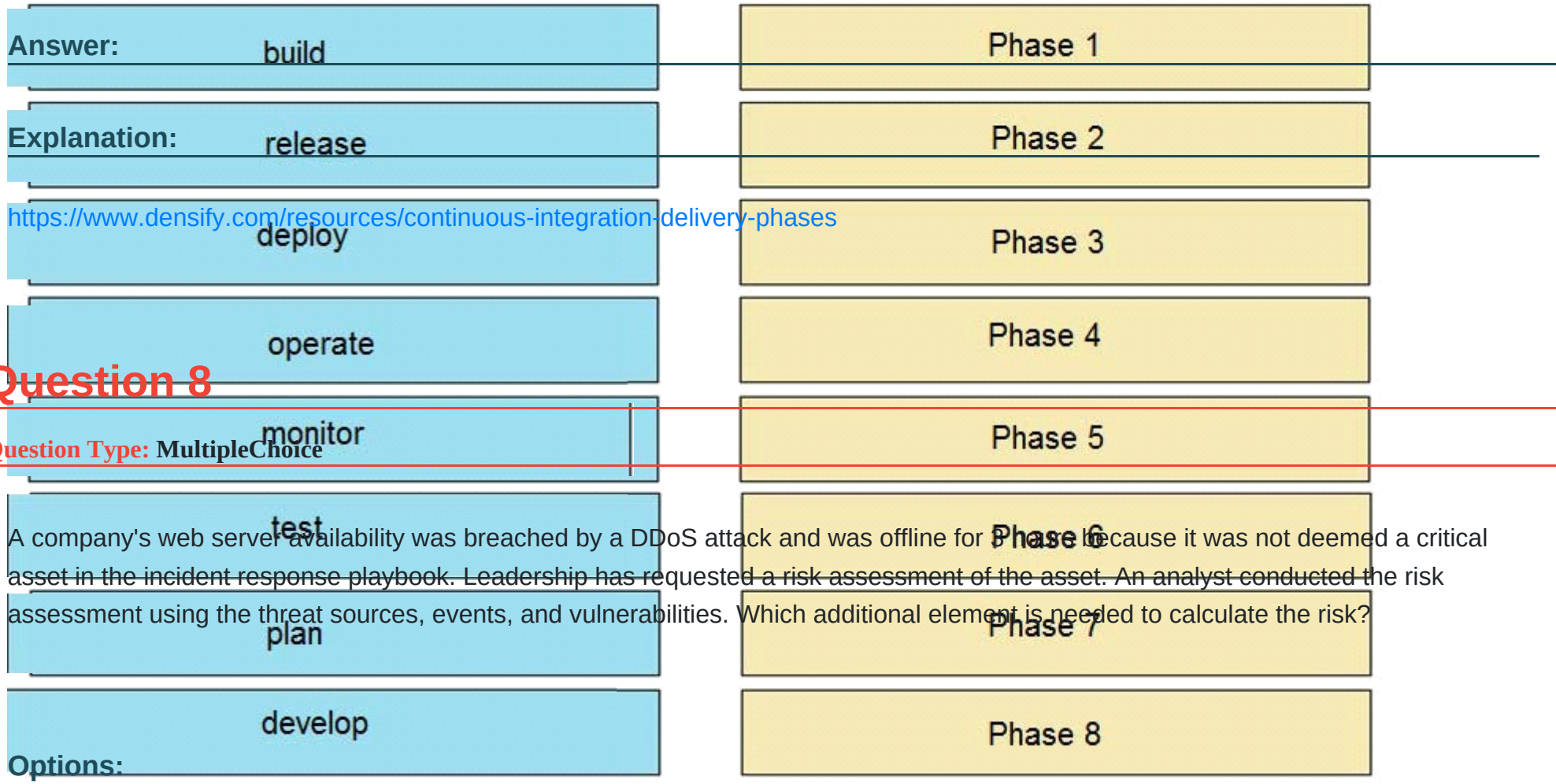
A, B

Question 7

Question Type: DragDrop

Drag and drop the components from the left onto the phases of the CI/CD pipeline on the right.

Answer Area



Answer:

Explanation:

https://www.densify.com/resources/continuous-integration-delivery-phases

Question 8

Question Type: MultipleChoice

A company's web server availability was breached by a DDoS attack and was offline for 3 hours because it was not deemed a critical asset in the incident response playbook. Leadership has requested a risk assessment of the asset. An analyst conducted the risk assessment using the threat sources, events, and vulnerabilities. Which additional element is needed to calculate the risk?

Options:

A- assessment scope

B- event severity and likelihood

C- incident response playbook

D- risk model framework

Answer:

D

Question 9

Question Type: DragDrop

Drag and drop the telemetry-related considerations from the left onto their cloud service models on the right.

Answer Area

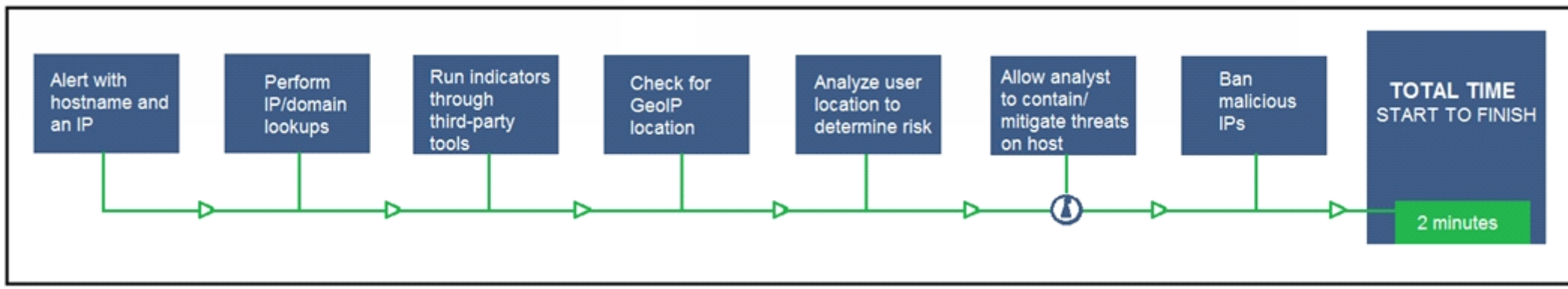
Answer:

Logs, alerts, and events for application performance monitoring and application health are configurable by the customer	SaaS
The customer controls limited application configuration settings and obtaining logs for security monitoring may be limited	PaaS

Question 10

Question Type: MultipleChoice

Refer to the exhibit.



An engineer configured this SOAR solution workflow to identify account theft threats and privilege escalation, evaluate risk, and respond by resolving the threat. This solution is handling more threats than Security analysts have time to analyze. Without this analysis, the team cannot be proactive and anticipate attacks. Which action will accomplish this goal?

Options:

A- Exclude the step "BAN malicious IP" to allow analysts to conduct and track the remediation

B- Include a step "Take a Snapshot" to capture the endpoint state to contain the threat for analysis

C- Exclude the step "Check for GeoIP location" to allow analysts to analyze the location and the associated risk based on asset criticality

D- Include a step "Reporting" to alert the security department of threats identified by the SOAR reporting engine

Answer:

A

Question 11

Question Type: **MultipleChoice**

What is a principle of Infrastructure as Code?

Options:

A- System maintenance is delegated to software systems

B- Comprehensive initial designs support robust systems

C- Scripts and manual configurations work together to ensure repeatable routines

D- System downtime is grouped and scheduled across the infrastructure

Answer:

B

Question 12

Question Type: MultipleChoice

What is the HTTP response code when the REST API information requested by the authenticated user cannot be found?

Options:

A- 401

B- 402

C- 403

D- 404

Answer:

A