Free Questions for CS0-002 by braindumpscollection

Shared by Maddox on 12-12-2023

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: **MultipleChoice**

An analyst is performing a BIA and needs to consider measures and metrics. Which of the following would help the analyst achieve this objective? (Select two).

Options:

A- Time to reimage the server

B- Minimum data backup volume

C- Disaster recovery plan for non-critical services

D- Maximum downtime before impact is unacceptable

E- Time required to inform stakeholders about outage

F- Total time accepted for business process outage

Answer:

D, F

Explanation:

The objective of a BIA is to determine the potential impacts of various disruptions on the business processes and functions, and to establish the recovery priorities and objectives for each process and function. To achieve this objective, the analyst needs to consider various measures and metrics that can quantify the impacts and the recovery requirements. Some of the common measures and metrics that are used in a BIA are:

Maximum downtime before impact is unacceptable: This metric defines the maximum amount of time that a business process or function can be disrupted without causing significant or irreversible damage to the organization's reputation, operations, finances, or legal obligations. This metric is also known as the maximum tolerable downtime (MTD) or maximum tolerable period of disruption (MTPD).It helps to determine the recovery time objective (RTO), which is the target time for restoring the process or function to an acceptable level of service after a disruption1.

Total time accepted for business process outage: This metric defines the total amount of time that a business process or function can be out of service within a given period, such as a day, a week, or a month.This metric is also known as the recovery point objective (RPO), which is the maximum amount of data loss or corruption that can be tolerated after a disruption1. It helps to determine the backup frequency and retention policy for the data and systems that support the process or function.

Time required to inform stakeholders about outage: This metric defines the time frame for communicating with the internal and external stakeholders who are affected by or involved in the disruption and recovery of a business process or function.This metric helps to establish the crisis communication plan and protocol, which specifies who, what, when, where, why, and how to communicate during and after a disruption2. It also helps to manage the expectations and perceptions of the stakeholders and to maintain their trust and confidence in the organization.

Time to reimage the server: This metric defines the time needed to restore a server to its original or desired state after a disruption. This metric helps to estimate the resources and efforts required for recovering the server and its applications.It also helps to evaluate the feasibility and effectiveness of different recovery strategies, such as restoring from backup, rebuilding from scratch, or replacing with a spare3.

Minimum data backup volume: This metric defines the minimum amount of data that needs to be backed up regularly to ensure the continuity and integrity of a business process or function. This metric helps to optimize the backup process and reduce the storage costs and bandwidth consumption.It also helps to identify the critical data elements and sources that are essential for the process or function4.

Question 2

Question Type: MultipleChoice

A Chief Information Security Officer has requested a security measure be put in place to redirect certain traffic on the network. Which of the following would best resolve this issue?

Options:

A- Sinkholing

B- Blocklisting

C- Geoblocking

D- Sandboxing

Answer:

A

Explanation:

Sinkholing is a technique for manipulating data flow in a network; you redirect traffic from its intended destination to a server of your choosing.It can be used maliciously, to steer legitimate traffic away from its intended recipient, but security professionals more commonly use sinkholing as a tool for research and reacting to attacks1.

For example, sinkholing can be used to redirect traffic from a botnet or a malware-infected host to a server under the control of the defender, where the traffic can be analyzed, blocked, or neutralized.This can help identify and isolate compromised devices, prevent command-and-control communication, and disrupt malicious activities2.

The other options are not the best solutions for the following reasons:

Blocklisting is a technique for preventing access to or communication with certain IP addresses, domains, or applications that are known or suspected to be malicious. Blocklisting can be implemented using firewalls, routers, proxies, or software tools. Blocklisting can protect a network from unwanted or harmful traffic, but it does not redirect the traffic to a different destination.

Geoblocking is a technique for restricting access to or communication with certain IP addresses, domains, or applications based on their geographic location. Geoblocking can be implemented using firewalls, routers, proxies, or software tools. Geoblocking can protect a network from unauthorized or undesirable traffic from specific regions or countries, but it does not redirect the traffic to a different destination.

Sandboxing is a technique for isolating and executing potentially malicious code or applications in a separate and secure environment. Sandboxing can be implemented using virtual machines, containers, or software tools. Sandboxing can protect a network from malware infection or damage, but it does not redirect the network traffic to a different destination.

Question 3

Question Type: MultipleChoice

An organization is performing a risk assessment to prioritize resources for mitigation and remediation based on impact. Which of the following metrics, in addition to the CVSS for each CVE, would best enable the organization to prioritize its efforts?

Options:

A- OS type

B- OS or application versions

C- Patch availability

D- System architecture

E- Mission criticality

Answer:

C

Explanation:

A risk assessment is a process of identifying, analyzing, and evaluating the potential threats and vulnerabilities that may affect an organization's assets, operations, or objectives.A risk assessment matrix is a tool that can help prioritize the risks based on their likelihood and impact1.

The CVSS (Common Vulnerability Scoring System) is a standard framework for rating the severity of vulnerabilities in software systems.The CVSS provides a numerical score from 0 to 10, as well as a qualitative rating from Low to Critical, based on the characteristics and consequences of the vulnerability2.

However, the CVSS score alone may not be sufficient to determine the priority of mitigation and remediation actions for each vulnerability. Other factors that may influence the decision include:

Patch availability: This metric indicates whether there is a fix or update available for the vulnerability from the vendor or developer. Patch availability can affect the urgency and feasibility of remediation, as well as the risk exposure and potential damage of exploitation.For example, a vulnerability with a high CVSS score but with a readily available patch may be less critical than a vulnerability with a lower CVSS score but with no patch available3.

Mission criticality: This metric reflects the importance and value of the asset or system affected by the vulnerability to the organization's mission, goals, or functions. Mission criticality can affect the impact and priority of remediation, as well as the risk tolerance and acceptance level of the organization.For example, a vulnerability with a high CVSS score but affecting a non-essential system may be less critical than a vulnerability with a lower CVSS score but affecting a core system4.

OS type: This metric indicates the operating system (OS) of the asset or system affected by the vulnerability. OS type can affect the likelihood and complexity of exploitation, as well as the availability and compatibility of patches or mitigations.For example, a vulnerability with a high CVSS score but affecting an uncommon or unsupported OS may be less critical than a vulnerability with a lower CVSS score but affecting a widely used or supported OS3.

OS or application versions: This metric indicates the specific version of the OS or application affected by the vulnerability. OS or application versions can affect the applicability and relevance of the vulnerability, as well as the availability and compatibility of patches or mitigations.For example, a vulnerability with a high CVSS score but affecting an outdated or obsolete version may be less critical than a vulnerability with a lower CVSS score but affecting a current or popular version3.

System architecture: This metric indicates the design and configuration of the asset or system affected by the vulnerability. System architecture can affect the exposure and accessibility of the vulnerability, as well as the effectiveness and efficiency of patches or mitigations.For example, a vulnerability with a high CVSS score but affecting an isolated or segmented system may be less critical than a vulnerability with a lower CVSS score but affecting an interconnected or integrated system3.

Therefore, to best enable the organization to prioritize its efforts based on impact, patch availability is one of the most important metrics to consider in addition to the CVSS score for each CVE (Common Vulnerabilities and Exposures). Patch availability can directly influence the risk level and remediation strategy for each vulnerability.

Question 4

Question Type: MultipleChoice

A company is building a new fabrication plant and designing its production lines based on the products it manufactures and the networks to support them. The security engineer has the following requirements:

* Each production line must be secured using a single posture.

* Each production line must only communicate with the other lines in a least privilege method.

* Access to each production line from the rest of the network must be strictly controlled.

To best provide the protection that meets these requirements, each product line should be:

Options:

A- logically segmented and firewalled to control inbound and outbound connectivity.

B- air gapped and firewalled to manage connectivity.

C- air gapped but connected to one another by data diodes.

D- logically segmented and then air gapped to specifically limit traffic.

Answer:

A

Explanation:

Logical segmentation is a technique that divides a network into smaller, isolated segments based on logical criteria, such as function, role, or application. Logical segmentation can be implemented using various technologies, such as VLANs, subnets, virtual firewalls, or software-defined networking (SDN).Logical segmentation can enhance the security of a network by reducing the attack surface, limiting the lateral movement of threats, enforcing the principle of least privilege, and facilitating the monitoring and auditing of network traffic12.

Firewall is a device or software that filters and controls the incoming and outgoing network traffic based on predefined rules or policies. Firewall can be deployed at the network perimeter or within the network to create internal zones or segments.Firewall can protect a network from unauthorized access, malicious attacks, or data exfiltration by allowing or blocking traffic based on the source, destination, port, protocol, or application3.

To best provide the protection that meets the requirements of the security engineer, each product line should be logically segmented and firewalled to control inbound and outbound connectivity. This way, each product line can be secured using a single posture that is consistent and manageable. Each product line can also communicate with the other lines in a least privilege method by allowing only the necessary traffic and blocking the rest. Access to each product line from the rest of the network can be strictly controlled by applying firewall rules that restrict or limit the traffic based on the business needs.

Question 5

Question Type: **MultipleChoice**

A company wants to ensure a third party does not take intellectual property and build a competing product. Which of the following is a non-technical data and privacy control that would best protect the company?

Options:

A- Data encryption

B- A non-disclosure agreement

C- Purpose limitation

D- Digital rights management

Answer:

B

Explanation:

A non-disclosure agreement (NDA) is a legally binding contract that establishes a confidential relationship between two or more parties and prevents them from sharing or using certain information that is deemed sensitive, proprietary, or valuable1.An NDA can be used to protect intellectual property (IP) such as trade secrets, inventions, designs, or business plans from being disclosed to competitors or the public2.

A company that wants to ensure a third party does not take its IP and build a competing product can use an NDA to restrict the access, use, and disclosure of its IP by the third party.For example, if the company hires a contractor to develop a software application, the company can require the contractor to sign an NDA that prohibits the contractor from copying, modifying, selling, or revealing the source code or any other details of the application to anyone else3. The NDA can also specify the duration, scope, and consequences of the confidentiality obligation.

Question 6

Question Type: MultipleChoice

A security analyst needs to recommend the best approach to test a new application that simulates abnormal user behavior to find software bugs. Which of the following would best accomplish this task?

Options:

A- A static analysis to find libraries with flaws handling user inputs

B- A dynamic analysis using a dictionary to simulate user inputs

C- Reverse engineering to circumvent software protections

D- Fuzzing tools with polymorphic methods

Answer:

D

Explanation:

Fuzzing is a technique that involves sending random, malformed, or unexpected inputs to an application to trigger errors, crashes, or vulnerabilities.Fuzzing can be used to test the robustness and security of software, especially when the source code is not available or the input format is complex1.Fuzzing can also simulate abnormal user behavior, such as entering invalid data, clicking on random buttons, or sending malicious requests2.

Fuzzing tools are software programs that automate the process of generating and sending inputs to the application under test.There are different types of fuzzing tools, such as black-box fuzzers, white-box fuzzers, and grey-box fuzzers, depending on the level of information and feedback they have about the application1. Some examples of fuzzing tools areAFL,Peach, and [Sulley].

Polymorphic methods are techniques that allow fuzzing tools to modify or mutate the inputs in different ways, such as changing the length, value, type, or structure of the data. Polymorphic methods can increase the diversity and effectiveness of the inputs and help discover more bugs or vulnerabilities in the application .

Therefore, using fuzzing tools with polymorphic methods would be the best approach to test a new application that simulates abnormal user behavior to find software bugs. This approach would generate a large number of inputs that cover various scenarios and edge cases and expose any flaws or weaknesses in the application's functionality or security.

Question 7

Question Type: MultipleChoice

A user receives a potentially malicious attachment that contains spelling errors and a PDF document. A security analyst reviews the email and decides to download the attachment to a Linux sandbox for review. Which of the following commands would most likely indicate if the email is malicious?

Options:

A- sha256sum ~/Desktop/fi1e.pdf

B- /bin/;s -1 ~/Desktop/fi1e.pdf

C- strings ~/Desktop/fi1e.pdf | grep -i "<script"

D- cat < ~/Desktop/file.pdf | grep ---i .exe

Answer:

C

Explanation:

This command would most likely indicate if the email attachment is malicious, as it would display any JavaScript code embedded in the PDF file.JavaScript code can be used by attackers to execute malicious commands or scripts on the victim's system when the PDF file is opened1.The strings command extracts the printable characters from a binary file, such as a PDF file, and the grep -i "<script" option searches for the presence of JavaScript code in a case-insensitive manner2.

Question 8

Question Type: **MultipleChoice**

During a risk assessment, a senior manager inquires about what the cost would be if a unique occurrence would impact the availability of a critical service. The service generates $1 ,000 in revenue for the organization. The impact of the attack would affect 20% of the server's capacity to perform jobs. The organization expects that five out of twenty attacks would succeed during the year. Which of the following is the calculated single loss expectancy?

Options:

A- $200

B- $800

C- $5,000

D- $20,000

Answer:

A

Explanation:

The single loss expectancy (SLE) is a measure of the monetary loss associated with a single occurrence of a risk. The SLE can be calculated by multiplying the asset value (AV) by the exposure factor (EF), which is the percentage of loss that the asset would suffer if the risk occurred. In this case, the asset value is the revenue generated by the service, which is $1,000. The exposure factor is the impact of the attack on the server's capacity, which is 20%.Therefore, the SLE is $1,000 x 0.2 = $2001.

Question 9

Question Type: **MultipleChoice**

Which of the following is the best method to ensure secure boot UEFI features are enabled to prevent boot malware?

Options:

A- Enable secure boot in the hardware and reload the operating system.

B- Reconfigure the system's MBR and enable NTFS.

C- Set I-JEFI to legacy mode and enable security features.

D- Convert the legacy partition table to UEFI and repair the operating system.

B) Reconfigure the system's MBR and enable NTFS is not correct. MBR stands for Master Boot Record, and it is a legacy partitioning scheme that stores information about the partitions and the boot loader on a disk. NTFS stands for New Technology File System, and it is a file system that supports features such as encryption, compression, and access control. Reconfiguring the system's MBR and enabling NTFS would not enable secure boot UEFI features, as they are not related to UEFI or secure boot.Moreover, MBR is incompatible with UEFI, as UEFI requires a different partitioning scheme called GPT (GUID Partition Table)3.

C) Set UEFI to legacy mode and enable security features is not correct. Legacy mode is a compatibility mode that allows UEFI systems to boot using legacy BIOS methods. Legacy mode disables some of the features and benefits of UEFI, such as secure boot, faster boot time, or larger disk support. Setting UEFI to legacy mode would not enable secure boot UEFI features, but rather disable them.

D) Convert the legacy partition table to UEFI and repair the operating system is not correct. Converting the legacy partition table to UEFI means changing the partitioning scheme from MBR to GPT, which is required for UEFI systems to boot. However, this alone would not enable secure boot UEFI features, as it also depends on the firmware settings and the operating system support. Repairing the operating system may or may not fix any issues caused by converting the partition table, but it would not necessarily enable secure boot either.

1:What Is Secure Boot?2:How to Enable Secure Boot3:MBR vs GPT: Which One Is Better for You?: [UEFI vs Legacy BIOS -- The Ultimate Comparison Guide]

Answer:

A

Explanation:

The correct answer is A. Enable secure boot in the hardware and reload the operating system. Secure boot is a feature of UEFI that ensures that only trusted and authorized code can execute during the boot process.Secure boot can prevent boot malware, such as rootkits or bootkits, from compromising the system before the operating system loads1. To enable secure boot, the hardware must support UEFI and have a firmware that implements the secure boot protocol. The operating system must also support UEFI and have a digital signature that matches the keys stored in the firmware. If the operating system was installed in legacy mode or does not have a valid signature, it may not boot with secure boot enabled.Therefore, it may be necessary to reload the operating system after enabling secure boot in the hardware2.

Question 10

Question Type: MultipleChoice

An intrusion detection analyst reported an inbound connection originating from an unknown IP address recorded on the VPN server for multiple internal hosts. During an investigation, a security analyst determines there were no identifiers associated with the hosts. Which of the following should the security analyst enforce to obtain the best information?

Options:

A- Update the organization's IP table.

B- Enable user access logging.

C- Shut down all VPN connections.

D- Create rules for the Active Directory.

Answer:

B

Explanation:

User access logging (UAL) is a feature on Windows Server operating systems that records the details of remote access and management activities performed by users on the server.UAL can provide information such as the user name, the source IP address, the destination host name, the protocol used, and the time and duration of the connection1. Enabling user access logging on the VPN server can help the security analyst to obtain the best information to identify and investigate the inbound connection originating from an unknown IP address.

Question 11

Question Type: **MultipleChoice**

An analyst needs to understand how an attacker compromised a server. Which of the following procedures will best deliver the information that is necessary to reconstruct the steps taken by the attacker?

Options:

A- Scan the affected system with an anti-malware tool and check for vulnerabilities with a vulnerability scanner.

B- Extract the server's system timeline, verifying hashes and network connections during a certain time frame.

C- Clone the entire system and deploy it in a network segment built for tests and investigations while monitoring the system during a certain time frame.

D- Clone the server's hard disk and extract all the binary files, comparing hash signatures with malware databases.

Answer:

B

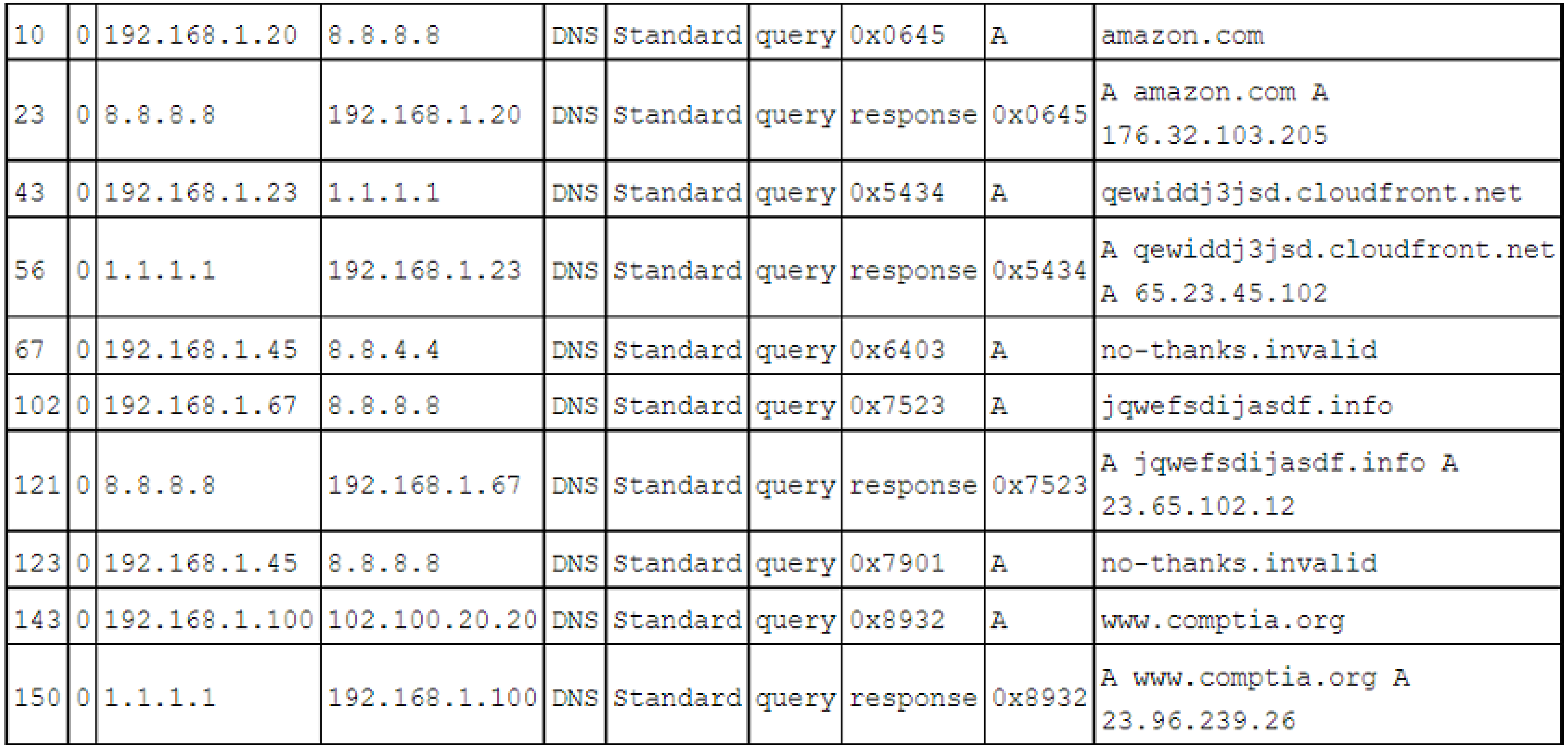
Explanation:

The correct answer is B. Extract the server's system timeline, verifying hashes and network connections during a certain time frame. A system timeline is a chronological record of the events and activities that occurred on a system, such as file creation, modification, or deletion, process execution, registry changes, or network connections. A system timeline can help an analyst to understand how an attacker compromised a server by showing the sequence of actions and artifacts left by the attacker. An analyst can also verify the hashes of the files and processes involved in the compromise and compare them with known malware signatures or databases.Additionally, an analyst can check the network connections made by the server during the compromise and identify the source and destination IP addresses, ports, and protocols used by the attacker1.

Question 12

Question Type: **MultipleChoice**

A cybersecurity analyst inspects DNS logs on a regular basis to identify possible IOCs that are not triggered by known signatures. The analyst reviews the following log snippet:



10	0	192.168.1.20	8.8.8.8	DNS	Standard	query	0x0645	A	amazon.com
23	0	8.8.8.8	192.168.1.20	DNS	Standard	query	response	0x0645	A amazon.com A 176.32.103.205
43	0	192.168.1.23	1.1.1.1	DNS	Standard	query	0x5434	A	qewiddj3jsd.cloudfront.net
56	0	1.1.1.1	192.168.1.23	DNS	Standard	query	response	0x5434	A qewiddj3jsd.cloudfront.net A 65.23.45.102
67	0	192.168.1.45	8.8.4.4	DNS	Standard	query	0x6403	A	no-thanks.invalid
102	0	192.168.1.67	8.8.8.8	DNS	Standard	query	0x7523	A	jqwefsdijasdf.info
121	0	8.8.8.8	192.168.1.67	DNS	Standard	query	response	0x7523	A jqwefsdijasdf.info A 23.65.102.12
123	0	192.168.1.45	8.8.8.8	DNS	Standard	query	0x7901	A	no-thanks.invalid
143	0	192.168.1.100	102.100.20.20	DNS	Standard	query	0x8932	A	www.comptia.org
150	0	1.1.1.1	192.168.1.100	DNS	Standard	query	response	0x8932	A www.comptia.org A 23.96.239.26

Which of the following should the analyst do next based on the information reviewed?

Options:

A- The analyst should disable DNS recursion.

B- The analyst should block requests to no---thanks. invalid.

C- The analyst should disconnect host 192.168.1.67.

D- The analyst should sinkhole 102.100.20.20.

E- The analyst should disallow queries to the 8.8.8.8 resolver.

A) The analyst should disable DNS recursion is not correct.DNS recursion is a process where a DNS server queries other DNS servers on behalf of a client until it finds the authoritative answer for a domain name2. Disabling DNS recursion would prevent the DNS server from resolving any domain names that are not in its cache or zone files, which would affect the normal functionality of the network and the internet access of the clients.

C) The analyst should disconnect host 192.168.1.67 is not correct. Disconnecting host 192.168.1.67 would stop the communication with the malicious domain, but it would also disrupt the legitimate activities of the host and its user. Moreover, disconnecting the host would not remove the malware or root cause of the compromise, and it would not prevent the host from reconnecting to the malicious domain once it is online again.

D) The analyst should sinkhole 102.100.20.20 is not correct.Sinkholing is a technique that redirects malicious or unwanted traffic to a controlled destination, such as a fake or isolated server3. Sinkholing 102.100.20.20 would prevent the communication with the malicious domain, but it would also require access and control over the public resolver 8.8.8.8, which is not owned or managed by the analyst or the company.

E) The analyst should disallow queries to the 8.8.8.8 resolver is not correct. Disallowing queries to the 8.8.8.8 resolver would prevent the communication with the malicious domain, but it would also affect the resolution of other legitimate domain names that are not in the local DNS server's cache or zone files.

1:DNS Tunneling: how DNS can be (ab)used by malicious actors2:What Is DNS Recursion?3:What Is a Sinkhole Attack?

Answer:

B

Explanation:

The correct answer is B. The analyst should block requests to no-thanks.invalid. The log snippet shows a DNS query from host 192.168.1.67 to the public resolver 8.8.8.8 for the domain name no-thanks.invalid, which is resolved to the IP address 102.100.20.20.This is a possible indicator of compromise (IOC), as no-thanks.invalid is a known malicious domain that is used by attackers to exfiltrate data or execute commands on compromised hosts1. The analyst should block requests to this domain to prevent further communication with the attacker's server and investigate the host 192.168.1.67 for signs of infection.