Free Questions for SY0-601

Shared by Barr on 12-12-2023

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

A company uses specially configured workstations for any work that requires administrator privileges to its Tier 0 and Tier 1 systems The company follows a strict process to harden systems immediately upon delivery Even with these strict security measures in place an incident occurred from one of the workstations The root cause appears to be that the SoC was tampered with or replaced Which of the following most likely occurred?

Options:

A- Fileless malware
B- A downgrade attack
C- A supply-chain attack
D- A logic bomb
E- Misconfigured BIOS

Answer:

C

Explanation:

A supply-chain attack is a type of cyberattack that targets a trusted third-party vendor who offers services or products vital to the supply chain. A supply-chain attack can occur in software or hardware. In this case, the most likely scenario is that the SoC (system on chip) was compromised by a malicious actor before it was delivered to the company, either by tampering with or replacing it with a malicious version.This would allow the attacker to gain access to the company's systems through the specially configured workstations

Question 2

Question Type: MultipleChoice

A company wants to improve its access standards to prevent threat actors from togging in to the corporate network with compromised credentials in addition to MF

Options:

A- the Chief Information Security Officer wants an additional layer of protection enabled based on certain criteria Which of the following is the best way to provide additional protection?
A- Conditional access policies
B- Kerbaos access ticketing
C- Terminal access controller
D- Enabled key vaults

Answer:

A, A

Question 3

Question Type: MultipleChoice

The IT department's on-site developer has been with the team for many years. Each lime an application is released; the security team is able to identify multiple vulnerabilities Which of the Mowing would best help the team ensure the application is ready to be released to production?

Options:

A- Limit the use of third-party libraries.
B- Prevent data exposure queries.
C- Obfuscate the source code
D- Submit the application to OA before releasing it.

Answer:

D

Explanation:

Submitting the application to QA before releasing it would best help the team ensure the application is ready to be released to production. QA stands for quality assurance, which is a process of testing and verifying that a software product meets the specified requirements and standards. QA can help identify and fix any bugs, errors, vulnerabilities, or performance issues before the software is deployed to the end users. QA can also ensure that the software meets the security objectives and complies with the best practices and regulations.

Question 4

Question Type: MultipleChoice

An organization has hired a red team to simulate attacks on its security pos-ture, which Of following will the blue team do after detecting an IOC?

Options:

A- Reimage the impacted workstations.
B- Activate runbooks for incident response.
C- Conduct forensics on the compromised system,
D- Conduct passive reconnaissance to gather information

Answer:

B

Explanation:

A runbook is a set of predefined procedures and steps that guide an incident response team through the process of handling a security incident.It can help the blue team respond quickly and effectively to an indicator of compromise (IOC) by following the best practices and predefined actions for containment, eradication, recovery and lessons learned.

Question 5

Question Type: MultipleChoice

An organization implemented cloud-managed IP cameras to monitor building entry points and sensitive areas. The service provider enables direct TCP'IP connection to stream live video footage from each camer

a. The organization wants to ensure this stream is encrypted and authenticated Which of the following protocols should be implemented to best meet this objective?

Options:

A- SSH

B- SRTP
C- S/MIME
D- PPTP

Answer:

B

Question 6

Question Type: MultipleChoice

A threat actor used a sophisticated attack to breach a well-known ride-sharing. company. The threat actor posted on social media that this action was in response to the company's treatment of its drivers Which of the following best describes tm type of throat actor?

Options:

A- Nation-slate
B- Hacktivist
C- Organized crime
D- Shadow IT

Answer:

B

Explanation:

A threat actor who used a sophisticated attack to breach a well-known ride-sharing company and posted on social media that this action was in response to the company's treatment of its drivers is most likely a hacktivist.A hacktivist is a person who uses hacking skills to promote a social or political cause, such as human rights, environmentalism, or anti-corporatism5.

Question 7

Question Type: MultipleChoice

The manager who is responsible for a data set has asked a security engineer to apply encryption to the data on a hard disk. The security engineer is an example of a:

Options:

A- data controller
B- data owner.
C- data custodian.
D- data processor

Answer:

C

Explanation:

The security engineer is an example of a data custodian. A data custodian is a person who is responsible for implementing and maintaining the security controls for the data, such as encryption, backup, access control, etc. A data custodian acts on behalf of the data owner, who is the person who has the authority and accountability for the data. A data controller is a person who determines the purposes and means of processing the data, such as a company or an organization.A data processor is a person who processes the data on behalf of the data controller, such as a service provider or a vendor1.

Question 8

Question Type: MultipleChoice

A user's login credentials were recently compromised During the investigation, the security analyst determined the user input credentials into a pop-up window when prompted to confirm the username and password However the trusted website does not use a pop-up for entering user colonials Which of the following attacks occurred?

Options:

A- Cross-site scripting
B- SOL injection
C- DNS poisoning
D- Certificate forgery

Answer:

D

Explanation:

The user input credentials into a pop-up window that was not part of the trusted website. This suggests that the attacker was able to forge a certificate and present a fake website that looked like the legitimate one.This is a type of attack known as certificate forgery, which exploits the trust relationship between users and websites that use SSL/TLS encryption2.

Question 9

Question Type: MultipleChoice

A Chief Security Officer (CSO) is concerned that cloud-based services are not adequately protected from advanced threats and malware. The CSO believes there is a high risk that a data breach could occur in the near future due to the lack of detective and preventive controls Which of the following should be implemented to best address the CSO's concerns? (Select two).

Options:

A- AWAF
B- A CASB
C- An NG-SWG
D- Segmentation
E- Encryption
F- Containenzation

Answer:

B, E

Explanation:

A CASB (Cloud Access Security Broker) and encryption are two solutions that can address the CSO's concerns about cloud-based services security. A CASB is a software tool or service that acts as an intermediary between users and cloud service providers, enforcing security policies and providing visibility and control over cloud activities.A CASB can help detect and prevent advanced threats and malware by applying data loss prevention, threat protection, anomaly detection, and encryption capabilities to cloud data and traffic456Encryption is a process of transforming data into an unreadable format using a secret key or algorithm, making it

inaccessible to unauthorized parties. Encryption can help protect cloud data from breaches by ensuring that only authorized users with the correct key can decrypt and access the data.Encryption can be applied to data at rest (stored in the cloud) or data in transit (moving between the cloud and users)789Reference:CompTIA Security+ SY0-601 Certification Study Guide, Chapter 8: Implementing Secure Protocols, page 360;What is a Cloud Access Security Broker (CASB)? | McAfee;Cloud Access Security Brokers (CASBs) - Gartner IT Glossary;What is Cloud Access Security Broker (CASB)? - Definition from WhatIs.com;What is Encryption? | Malwarebytes;Encryption - Wikipedia;What is Encryption? How Does Encryption Work? | Kaspersky

P2P exams

P2P exams

To Get Premium Files for SY0-601 Visit
https://www.p2pexams.com/products/sy0-601

For More Free Questions Visit
https://www.p2pexams.com/comptia/pdf/sy0-601

