examunion

Certified IT Exam Material Authority

Accurate study guides, High passing rate!

We offer free update service for one year!

http://www.examunion.com

Exam : **CS0-002**

Title : CompTIA Cybersecurity Analyst (CySA+) Certification Exam

Version : DEMO

1.An analyst receives an alert from the continuous-monitoring solution about unauthorized changes to the firmware versions on several field devices. The asset owners confirm that no firmware version updates were performed by authorized technicians, and customers have not reported any performance issues or outages.
Which Of the following actions would be BEST for the analyst to recommend to the asset owners to secure the devices from further exploitation?
A. Change the passwords on the devices.
B. Implement BIOS passwords.
C. Remove the assets from the production network for analysis.
D. Report the findings to the threat intel community.
Answer: C
Explanation:
If were referring to other devices, yes - Implement BIOS passwords before they are compromised. But the ones that were already compromised, they need to be removed from the system to avoid further exploitation. Plus, if you put a password on there, the attacker may now have your password.
Remove the assets from the production network for analysis. If the analyst receives an alert about unauthorized changes to the firmware versions on several field devices, the best action to recommend to the asset owners is to remove the assets from the production network for analysis. This would prevent further exploitation of the devices by isolating them from potential attackers and allow the analyst to investigate the source and nature of the unauthorized changes. Changing the passwords on the devices, implementing BIOS passwords, or reporting the findings to the threat intel community are other possible actions, but they are not as effective or urgent as removing the assets from the production network for analysis.
Reference: https://www.sans.org/reading-room/whitepapers/incident/incident-handlers-handbook-33901

2.As part of the senior leadership team's ongoing nsk management activities the Chief Information Security Officer has tasked a security analyst with coordinating the right training and testing methodology to respond to new business initiatives or significant changes to existing ones The management team wants to examine a new business process that would use existing infrastructure to process and store sensitive data**.**
Which of the following would be appropnate for the security analyst to coordinate?
A. A black-box penetration testing engagement
B. A tabletop exercise
C. Threat modeling
D. A business impact analysis
Answer: C
Explanation:
Threat modeling is a process that helps identify and analyze the potential threats and vulnerabilities of a system or process. It can help evaluate the security risks and mitigation strategies of a new business process that would use existing infrastructure to process and store sensitive data. A black-box penetration testing engagement, a tabletop exercise, or a business impact analysis are other methods that can be used to assess the security or resilience of a system or process, but they are not as appropriate as threat modeling for coordinating the right training and testing methodology to respond to new business initiatives or significant changes to existing ones.

Reference: https://owasp.org/www-community/Application_Threat_Modeling

3.Which of the following is an advantage of SOAR over SIEM?
A. SOAR is much less expensive.
B. SOAR reduces the amount of human intervention required.
C. SOAR can aggregate data from many sources.
D. SOAR uses more robust encryption protocols.
Answer: B
Explanation:
SOAR (Security Orchestration, Automation, and Response) reduces the amount of human intervention required, which is an advantage over SIEM (Security Information and Event Management). SIEM is a tool that collects, analyzes, and correlates data from various sources, such as logs, alerts, and events, to provide security monitoring and incident detection. SIEM can help security teams identify and prioritize potential threats, but it still requires manual intervention to investigate and respond to incidents2. SOAR is a tool that builds on SIEM by automating and orchestrating various security tasks and workflows, such as incident response, threat hunting, and threat intelligence. SOAR can help security teams reduce manual effort, improve efficiency, and accelerate incident resolution3.

4.A financial organization has offices located globally. Per the organization’s policies and procedures, all executives who conduct Business overseas must have their mobile devices checked for malicious software or evidence of tempering upon their return. The information security department oversees the process, and no executive has had a device compromised. The Chief information Security Officer wants to Implement an additional safeguard to protect the organization's data.
Which of the following controls would work BEST to protect the privacy of the data if a device is stolen?
A. Implement a mobile device wiping solution for use if a device is lost or stolen.
B. Install a DLP solution to track data now
C. Install an encryption solution on all mobile devices.
D. Train employees to report a lost or stolen laptop to the security department immediately
Answer: A
Explanation:
A mobile device wiping solution is a security feature that allows an organization to remotely erase or delete all data on a mobile device if it is lost or stolen2 A mobile device wiping solution can help protect the privacy of the data on a device and prevent unauthorized access or disclosure of sensitive information. A mobile device wiping solution can be implemented using built-in features of some mobile operating systems, third-party applications, or mobile device management (MDM) software.
Reference: 2 What Is Mobile Device Wiping? | Shred-it UK

5.Which of the following are considered PII by themselves? (Select TWO).
A. Government ID
B. Job title
C. Employment start date
D. Birth certificate
E. Employer address
F. Mother's maiden name

Answer: A,D

Explanation:

PII (Personally Identifiable Information) is any information that can be used to identify, contact, or locate a specific individual, either by itself or when combined with other information1. PII by itself is information that can uniquely identify an individual without any additional information. Examples of PII by itself are:

☞ Government ID. A government ID is a number or code that is issued by a government authority to an individual for identification purposes. Examples of government IDs are social security numbers, passport numbers, driver's license numbers, etc. A government ID can uniquely identify an individual without any additional information.

☞ Birth certificate. A birth certificate is a document that records the birth of an individual and contains information such as name, date of birth, place of birth, parents' names, etc. A birth certificate can uniquely identify an individual without any additional information.

Other examples of PII by itself are biometric data, DNA profile, fingerprints, etc. Examples of information that are not PII by themselves are:

☞ Job title. A job title is a name or description of a position or role in an organization. A job title does not uniquely identify an individual without any additional information, as many individuals can have the same job title.

☞ Employment start date. An employment start date is the date when an individual began working for an organization. An employment start date does not uniquely identify an individual without any additional information, as many individuals can have the same employment start date.

☞ Employer address. An employer address is the location of an organization where an individual works. An employer address does not uniquely identify an individual without any additional information, as many individuals can work at the same employer address.

☞ Mother's maiden name. A mother's maiden name is the surname that a woman had before she married. A mother's maiden name does not uniquely identify an individual without any additional information, as many individuals can have the same mother's maiden name.

Other examples of information that are not PII by themselves are gender, race, ethnicity, age, etc.

Reference: 1: https://www.techopedia.com/definition/23889/personally-identifiable-information-pii