NO.1 A recent malware outbreak across a subnet included successful rootkit installations on many PCs, ensuring persistence by rendering remediation efforts ineffective. Which of the following would BEST detect the presence of a rootkit in the future?

A. EDR

B. FDE

C. NIDS

D. DLP

Answer: A

NO.2 An application developer accidentally uploaded a company's code-signing certificate private key to a public web server. The company is concerned about malicious use of its certificate. Which of the following should the company do FIRST?

A. Delete the private key from the repository-.

B. Verify the public key is not exposed as well.

C. Update the DLP solution to check for private keys.

D. Revoke the code-signing certificate.

Answer: D

NO.3 An organization needs to implement more stringent controls over administrator/root credentials and service accounts. Requirements for the project include:

Check-in/checkout of credentials
The ability to use but not know the password
Automated password changes
Logging of access to credentials
Which of the following solutions would meet the requirements?

A. OAuth 2.0

B. Secure Enclave

C. An OpenID Connect authentication system

D. A privileged access management system

Answer: C

NO.4 After consulting with the Chief Risk Officer (CRO). a manager decides to acquire cybersecurity insurance for the company Which of the following risk management strategies is the manager adopting?

A. Risk avoidance

B. Risk mitigation

C. Risk transference

D. Risk acceptance

Answer: C

NO.5 A company is adopting a BYOD policy and is looking for a comprehensive solution to protect company information on user devices. Which of the following solutions would BEST support the policy?

A. Remote wipe

B. Mobile device management
C. Full-device encryption
D. Biometrics
Answer: B

NO.6 The SOC is reviewing process and procedures after a recent incident. The review indicates it took more than 30 minutes to determine that quarantining an infected host was the best course of action. The allowed the malware to spread to additional hosts before it was contained. Which of the following would be BEST to improve the incident response process?
A. Updating the playbooks with better decision points
B. Implementing manual quarantining of infected hosts
C. Dividing the network into trusted and untrusted zones
D. Providing additional end-user training on acceptable use
Answer: A

NO.7 A user recent an SMS on a mobile phone that asked for bank delays. Which of the following social-engineering techniques was used in this case?
A. SPIM
B. Smishing
C. Vishing
D. Spear phishing
Answer: B

NO.8 A Chief Information Security Officer (CISO) is evaluating the dangers involved in deploying a new ERP system for the company. The CISO categorizes the system, selects the controls that apply to the system, implements the controls, and then assesses the success of the controls before authorizing the system. Which of the following is the CISO using to evaluate the environment for this new ERP system?
A. ISO 27002
B. NIST Risk Management Framework
C. The Diamond Model of Intrusion Analysis
D. CIS Critical Security Controls
Answer: A
Explanation:
ISO/IEC 27002
ISO/IEC 27002 is an information security standard published by the International Organization for Standardization and by the International Electrotechnical Commission, titled Information technology - Security techniques - Code of practice for information security controls.

NO.9 An engineer needs to deploy a security measure to identify and prevent data tampering within the enterprise. Which of the following will accomplish this goal?
A. Antivirus
B. IPS
C. FIM

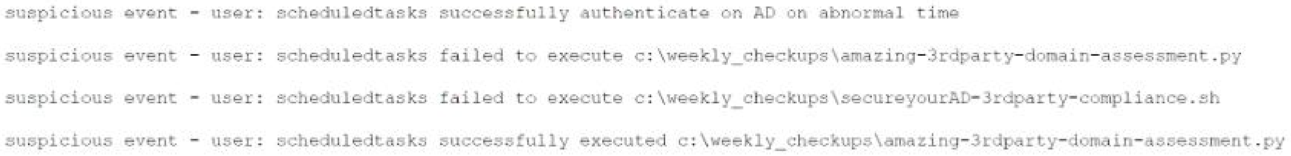
D. FTP

Answer: C

Explanation:

Data tampering prevention can include simple security measures such as the encryption of data, and can include lengths such as using file integrity monitoring (FIM) systems for better security.
https://www.cypressdatadefense.com/blog/data-tampering-prevention/

NO.10 A junior security analyst is conducting an analysis after passwords were changed on multiple accounts without users' interaction. The SIEM have multiple login entries with the following text:



```
suspicious event - user: scheduledtasks successfully authenticate on AD on abnormal time

suspicious event - user: scheduledtasks failed to execute c:\weekly_checkups\amazing-3rdparty-domain-assessment.py

suspicious event - user: scheduledtasks failed to execute c:\weekly_checkups\secureyourAD-3rdparty-compliance.sh

suspicious event - user: scheduledtasks successfully executed c:\weekly_checkups\amazing-3rdparty-domain-assessment.py
```

Which of the following is the MOST likely attack conducted on the environment?

A. Malicious script

B. Privilege escalation

C. Domain hijacking

D. DNS poisoning

Answer: A

NO.11 A database administrator needs to ensure all passwords are stored in a secure manner, so the administrate adds randomly generated data to each password before string. Which of the following techniques BEST explains this action?

A. Predictability

B. Hashing

C. Salting

D. Key stretching

Answer: C

NO.12 A recent audit uncovered a key finding regarding the use of a specific encryption standard in a web application that is used to communicate with business customers. Due to the technical limitations of its customers the company is unable to upgrade the encryption standard. Which of the following types of controls should be used to reduce the risk created by this scenario?

A. Physical

B. Detective

C. Compensating

D. Preventive

Answer: C

NO.13 An organization wants to implement a biometric system with the highest likelihood that an unauthorized user will be denied access. Which of the following should the organization use to compare biometric solutions?

A. CER

B. Difficulty of use

C. FRR
D. Cost
E. FAR
Answer: C

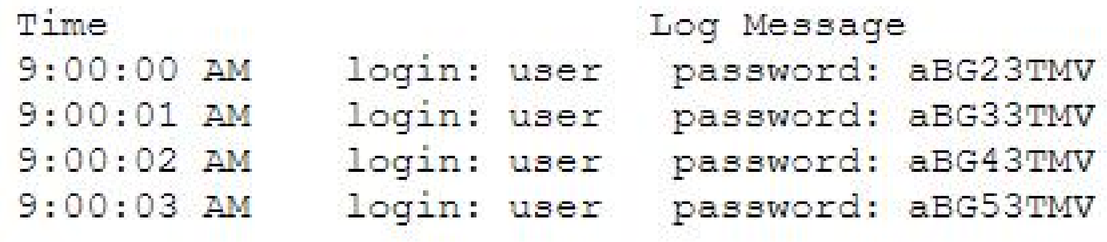
NO.14 An organization wants to integrate its incident response processes into a workflow with automated decision points and actions based on predefined playbooks. Which of the following should the organization implement?
A. SIEM
B. SOAR
C. EDR
D. CASB
Answer: B
Explanation:
Why is SOAR used? To synchronize tools, accelerate response times, reduce alert fatigue, and compensate for the skill shortage gap. To collaborate with other analysts during investigations. To analyze workload, organize an analyst's tasks, and allow teams to respond using their own processes.
EDR
The Endpoint Detection and Response Solutions (EDR) market is defined as solutions that record and store endpoint-system-level behaviors, use various data analytics techniques to detect suspicious system behavior, provide contextual information, block malicious activity, and provide remediation suggestions to restore ...

NO.15 A company provides mobile devices to its users to permit access to email and enterprise applications. The company recently started allowing users to select from several different vendors and device models. When configuring the MDM, which of the following is a key security implication of this heterogeneous device approach?
A. The most common set of MDM configurations will become the effective set of enterprise mobile security controls.
B. MDMs typically will not support heterogeneous deployment environments, so multiple MDMs will need to be installed and configured.
C. All devices will need to support SCEP-based enrollment; therefore, the heterogeneity of the chosen architecture may unnecessarily expose private keys to adversaries.
D. Certain devices are inherently less secure than others, so compensatory controls will be needed to address the delta between device vendors.
Answer: D

NO.16 An attack relies on an end user visiting a website the end user would typically visit, however, the site is compromised and uses vulnerabilities in the end users browser to deploy malicious software. Which of the blowing types of attack does this describe?
A. Watering hole
B. Whaling
C. Smishing
D. Phishing

Answer: A

NO.17 A user's account is constantly being locked out. Upon further review, a security analyst found the following in the SIEM



```
Time                                    Log Message
9:00:00 AM    login: user   password: aBG23TMV
9:00:01 AM    login: user   password: aBG33TMV
9:00:02 AM    login: user   password: aBG43TMV
9:00:03 AM    login: user   password: aBG53TMV
```

Which of the following describes what is occurring?

A. An attacker is utilizing a password-spraying attack against the account.

B. An attacker is utilizing a rainbow table attack against the account.

C. An attacker is utilizing a brute-force attack against the account.

D. An attacker is utilizing a dictionary attack against the account.

Answer: A

NO.18 A recent security audit revealed that a popular website with IP address 172.16.1.5 also has an FTP service that employees were using to store sensitive corporate dat a. The organization's outbound firewall processes rules top-down. Which of the following would permit HTTP and HTTPS, while denying all other services for this host?

A. access-rule permit tcp destination 172.16.1.5 port 80
access-rule permit tcp destination 172.16-1-5 port 443
access-rule deny ip destination 172.16.1.5

B. access-rule permit tcp destination 172.16.1.5 port 22
access-rule permit tcp destination 172.16.1.5 port 443
access-rule deny tcp destination 172.16.1.5 port 80

C. access-rule permit tcp destination 172.16.1.5 port 21
access-rule permit tcp destination 172.16.1.5 port 80
access-rule deny ip destination 172.16.1.5

D. access-rule permit tcp destination 172.16.1.5 port 80
access-rule permit tcp destination 172.16.1.5 port 443
access-rule deny tcp destination 172.16.1.5 port 21

Answer: D

NO.19 A security analyst needs to perform periodic vulnerably scans on production systems. Which of the following scan types would produce the BEST vulnerability scan report?

A. Credentialed

B. Port

C. Intrusive

D. Host discovery

Answer: A

NO.20 An engineer is setting up a VDI environment for a factory location, and the business wants to deploy a low-cost solution to enable users on the shop floor to log in to the VDI environment directly. Which of the following should the engineer select to meet these requirements?

A. Workstations

B. Containers

C. Thin clients

D. Laptops

Answer: C