VCEplus.com

SY0-601

Number: SY0-601
Passing Score: 800
Time Limit: 120 min
File Version: 1

SY0-601

Website: https://vceplus.com - https://vceplus.co
VCE to PDF Converter: https://vceplus.com/vce-to-pdf/
Facebook: https://www.facebook.com/VCE.For.All.VN/
Twitter : https://twitter.com/VCE_Plus

https://vceplus.com/

VCEplus.com

Exam A

QUESTION 1
Which of the following will MOST likely adversely impact the operations of unpatched traditional programmable-logic controllers, running a back-end LAMP server and OT systems with human-management interfaces that are accessible over the Internet via a web interface? (Choose two.)

https://vceplus.com/

A. Cross-site scripting
B. Data exfiltration
C. Poor system logging
D. Weak encryption
E. SQL injection
F. Server-side request forgery

VCEplus.com

Correct Answer: DF
Section: (none)
Explanation

Explanation/Reference:

QUESTION 2
A Chief Security Office's (CSO's) key priorities are to improve preparation, response, and recovery practices to minimize system downtime and enhance organizational resilience to ransomware attacks. Which of the following would BEST meet the CSO's objectives?

A. Use email-filtering software and centralized account management, patch high-risk systems, and restrict administration privileges on fileshares.
B. Purchase cyber insurance from a reputable provider to reduce expenses during an incident.

VCEplus.com

C. Invest in end-user awareness training to change the long-term culture and behavior of staff and executives, reducing the organization's susceptibility to phishing attacks.
D. Implement application whitelisting and centralized event-log management, and perform regular testing and validation of full backups. **Correct Answer:** D

Section: (none)
Explanation

Explanation/Reference:

QUESTION 3
A network engineer has been asked to investigate why several wireless barcode scanners and wireless computers in a warehouse have intermittent connectivity to the shipping server. The barcode scanners and computers are all on forklift trucks and move around the warehouse during their regular use. Which of the following should the engineer do to determine the issue? (Choose two.)

A. Perform a site survey
B. Deploy an FTK Imager
C. Create a heat map
D. Scan for rogue access points
E. Upgrade the security protocols
F. Install a captive portal

VCEplus.com

Correct Answer: AC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 4
A security administrator suspects an employee has been emailing proprietary information to a competitor. Company policy requires the administrator to capture an exact copy of the employee's hard disk. Which of the following should the administrator use?

A. `dd`
B. `chmod`
C. `dnsenum`
D. `logger`

VCEplus.com

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
QUESTION 5
Which of the following is MOST likely to outline the roles and responsibilities of data controllers and data processors?

A. SSAE SOC 2
B. PCI DSS
C. GDPR
D. ISO 31000

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

VCEplus.com

QUESTION 6
Phishing and spear-phishing attacks have been occurring more frequently against a company's staff. Which of the following would MOST likely help mitigate this issue?

A. DNSSEC and DMARC
B. DNS query logging
C. Exact mail exchanger records in the DNS
D. The addition of DNS conditional forwarders

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 7
On which of the following is the live acquisition of data for forensic analysis MOST dependent? (Choose two.)

CEplus.com

A. Data accessibility
B. Legal hold
C. Cryptographic or hash algorithm
D. Data retention legislation
E. Value and volatility of data
F. Right-to-audit clauses

Correct Answer: EF
Section: (none)
Explanation

Explanation/Reference:

QUESTION 8
Which of the following incident response steps involves actions to protect critical systems while maintaining business operations?

CEplus.com

A. Investigation
B. Containment
C. Recovery
D. Lessons learned

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 9
A network engineer needs to build a solution that will allow guests at the company's headquarters to access the Internet via WiFi. This solution should not allow access to the internal corporate network, but it should require guests to sign off on the acceptable use policy before accessing the Internet. Which of the following should the engineer employ to meet these requirements?

A. Implement open PSK on the APs
B. Deploy a WAF
C. Configure WIPS on the APs

VCEplus.com

D. Install a captive portal

Correct Answer: D
Section: (none)
Explanation
Explanation/Reference:

QUESTION 10
A network administrator needs to build out a new datacenter, with a focus on resiliency and uptime. Which of the following would BEST meet this objective? (Choose two.)

A. Dual power supply
B. Off-site backups
C. Automatic OS upgrades
D. NIC teaming
E. Scheduled penetration testing
F. Network-attached storage

VCEplus.com

Correct Answer: AB
Section: (none)
Explanation

Explanation/Reference:

QUESTION 11
A researcher has been analyzing large data sets for the last ten months. The researcher works with colleagues from other institutions and typically connects via SSH to retrieve additional data. Historically, this setup has worked without issue, but the researcher recently started getting the following message:

```
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
@   WARNING:  REMOTE HOST IDENTIFICATION HAS CHANGED!   @
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
IT IS POSSIBLE THAT SOMEONE IS DOING SOMETHING NASTY!
The fingerprint for the RSA key sent by the remote host is
SHA256:cBqYjal6ToV3jEIJHUSKtjjVziqnVd4Cz+1fhTM6+k4.
Please contact your system administrator.
RSA host key for 18.231.33.78 has changed and you have requested strict checking.
Host key verification failed.
```

VCEplus.com

Which of the following network attacks is the researcher MOST likely experiencing?

A. MAC cloning
B. Evil twin
C. Man-in-the-middle
D. ARP poisoning
Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 12
Several employees return to work the day after attending an industry trade show. That same day, the security manager notices several malware alerts coming from each of the employee's workstations. The security manager investigates but finds no signs of an attack on the perimeter firewall or the NIDS. Which of the following is MOST likely causing the malware alerts?

A. A worm that has propagated itself across the intranet, which was initiated by presentation media
B. A fileless virus that is contained on a vCard that is attempting to execute an attack
C. A Trojan that has passed through and executed malicious code on the hosts
D. A USB flash drive that is trying to run malicious code but is being blocked by the host firewall

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 13
A financial organization has adopted a new secure, encrypted document-sharing application to help with its customer loan process. Some important PII needs to be shared across this new platform, but it is getting blocked by the DLP systems. Which of the following actions will BEST allow the PII to be shared with the secure application without compromising the organization's security posture?

A. Configure the DLP policies to allow all PII
B. Configure the firewall to allow all ports that are used by this application
C. Configure the antivirus software to allow the application

CEplus.com

D. Configure the DLP policies to whitelist this application with the specific PII
E. Configure the application to encrypt the PII

Correct Answer: D
Section: (none)
Explanation
Explanation/Reference:

QUESTION 14
An auditor is performing an assessment of a security appliance with an embedded OS that was vulnerable during the last two assessments. Which of the following BEST explains the appliance's vulnerable state?

A. The system was configured with weak default security settings.
B. The device uses weak encryption ciphers.
C. The vendor has not supplied a patch for the appliance.
D. The appliance requires administrative credentials for the assessment.

CEplus.com

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 15
A company's bank has reported that multiple corporate credit cards have been stolen over the past several weeks. The bank has provided the names of the affected cardholders to the company's forensics team to assist in the cyber-incident investigation.

An incident responder learns the following information:
▪ The timeline of stolen card numbers corresponds closely with affected users making Internet-based purchases from diverse websites via enterprise desktop PCs.
▪ All purchase connections were encrypted, and the company uses an SSL inspection proxy for the inspection of encrypted traffic of the hardwired network. ▪ Purchases made with corporate cards over the corporate guest WiFi network, where no SSL inspection occurs, were unaffected.

Which of the following is the MOST likely root cause?

A. HTTPS sessions are being downgraded to insecure cipher suites
B. The SSL inspection proxy is feeding events to a compromised SIEM

VCEplus.com

C. The payment providers are insecurely processing credit card charges
D. The adversary has not yet established a presence on the guest WiFi network

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
QUESTION 16
A pharmaceutical sales representative logs on to a laptop and connects to the public WiFi to check emails and update reports. Which of the following would be BEST to prevent other devices on the network from directly accessing the laptop? (Choose two.)

A. Trusted Platform Module
B. A host-based firewall
C. A DLP solution
D. Full disk encryption
E. A VPN
F. Antivirus software

VCEplus.com

Correct Answer: AB
Section: (none)
Explanation

Explanation/Reference:

QUESTION 17
A company is implementing MFA for all applications that store sensitive data. The IT manager wants MFA to be non-disruptive and user friendly. Which of the following technologies should the IT manager use when implementing MFA?

A. One-time passwords
B. Email tokens
C. Push notifications
D. Hardware authentication

Correct Answer: C

VCEplus.com

Section: (none)
Explanation

Explanation/Reference:

QUESTION 18
The CSIRT is reviewing the lessons learned from a recent incident. A worm was able to spread unhindered throughout the network and infect a large number of computers and servers. Which of the following recommendations would be BEST to mitigate the impacts of a similar incident in the future?
A. Install a NIDS device at the boundary.
B. Segment the network with firewalls.
C. Update all antivirus signatures daily.
D. Implement application blacklisting.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

VCEplus.com

QUESTION 19
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. Mobile device management
B. Full-device encryption
C. Remote wipe
D. Biometrics

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 20

VCEplus.com

A development team employs a practice of bringing all the code changes from multiple team members into the same development project through automation. A tool is utilized to validate the code and track source code through version control. Which of the following BEST describes this process?

A. Continuous delivery
B. Continuous integrationC. Continuous validation
D. Continuous monitoring

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 21
A cybersecurity administrator needs to add disk redundancy for a critical server. The solution must have a two-drive failure for better fault tolerance. Which of the following RAID levels should the administrator select?

VCEplus.com

A. 0
B. 1
C. 5
D. 6

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 22
Which of the following BEST explains the reason why a server administrator would place a document named password.txt on the desktop of an administrator account on a server?

A. The document is a honeyfile and is meant to attract the attention of a cyberintruder.
B. The document is a backup file if the system needs to be recovered.
C. The document is a standard file that the OS needs to verify the login credentials.
D. The document is a keylogger that stores all keystrokes should the account be compromised.

VCEplus.com

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 23
A small company that does not have security staff wants to improve its security posture. Which of the following would BEST assist the company?
A. MSSP
B. SOAR
C. IaaS
D. PaaS

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

VCEplus.com

QUESTION 24
A cybersecurity manager has scheduled biannual meetings with the IT team and department leaders to discuss how they would respond to hypothetical cyberattacks. During these meetings, the manager presents a scenario and injects additional information throughout the session to replicate what might occur in a dynamic cybersecurity event involving the company, its facilities, its data, and its staff. Which of the following describes what the manager is doing?

A. Developing an incident response plan
B. Building a disaster recovery plan
C. Conducting a tabletop exercise
D. Running a simulation exercise

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

VCEplus.com

QUESTION 25
A RAT that was used to compromise an organization's banking credentials was found on a user's computer. The RAT evaded antivirus detection. It was installed by a user who has local administrator rights to the system as part of a remote management tool set. Which of the following recommendations would BEST prevent this from reoccurring?

A. Create a new acceptable use policy.
B. Segment the network into trusted and untrusted zones.
C. Enforce application whitelisting.
D. Implement DLP at the network boundary.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 26
A network administrator has been asked to install an IDS to improve the security posture of an organization. Which of the following control types is an IDS?

VCEplus.com

A. Corrective
B. Physical
C. Detective
D. Administrative

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 27
A startup company is using multiple SaaS and IaaS platforms to stand up a corporate infrastructure and build out a customer-facing web application. Which of the following solutions would be BEST to provide security, manageability, and visibility into the platforms?

A. SIEM
B. DLP
C. CASB

VCEplus.com

D. SWG

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 28
A root cause analysis reveals that a web application outage was caused by one of the company's developers uploading a newer version of the third-party libraries that were shared among several applications. Which of the following implementations would be BEST to prevent the issue from reoccurring?

A. CASB
B. SWG
C. Containerization
D. Automated failover

VCEplus.com

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 29
A company has drafted an insider-threat policy that prohibits the use of external storage devices. Which of the following would BEST protect the company from data exfiltration via removable media?

A. Monitoring large data transfer transactions in the firewall logs
B. Developing mandatory training to educate employees about the removable media policy
C. Implementing a group policy to block user access to system files
D. Blocking removable-media devices and write capabilities using a host-based security tool

Correct Answer: D
Section: (none)
Explanation

VCEplus.com

Explanation/Reference:

QUESTION 30
A security analyst receives a SIEM alert that someone logged in to the appadmin test account, which is only used for the early detection of attacks. The security analyst then reviews the following application log:

```
...
[03/06/20xx:17:20:18] system 127.0.0.1 FindXPath=//User[Username/text()='foo' or 7=7 or 'o'='o' And Password/text='bar']
[03/06/20xx:17:21:18] appadmin 194.28.114.102 action:login result:success
[03/06/20xx:17:22:18] appadmin 194.28.114.102 action:open.account(12345) result:fail
[03/06/20xx:17:23:18] appadmin 194.28.114.102 action:open.account(23456) result:fail
[03/06/20xx:17:23:18] appadmin 194.28.114.102 action:open.account(23456) result:fail
[03/06/20xx:17:23:18] appadmin 194.28.114.102 action:open.account(45678) result:fail
```

Which of the following can the security analyst conclude?

A. A replay attack is being conducted against the application.
B. An injection attack is being conducted against a user authentication system.
C. A service account password may have been changed, resulting in continuous failed logins within the application.
D. A credentialed vulnerability scanner attack is testing several CVEs against the application.

Correct Answer: C
Section: (none)
Explanation

VCEplus.com

Explanation/Reference:

QUESTION 31
In which of the following situations would it be BEST to use a detective control type for mitigation?

A. A company implemented a network load balancer to ensure 99.999% availability of its web application.
B. A company designed a backup solution to increase the chances of restoring services in case of a natural disaster.
C. A company purchased an application-level firewall to isolate traffic between the accounting department and the information technology department.
D. A company purchased an IPS system, but after reviewing the requirements, the appliance was supposed to monitor, not block, any traffic.
E. A company purchased liability insurance for flood protection on all capital assets.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

VCEplus.com

QUESTION 32
The IT department's on-site developer has been with the team for many years. Each time an application is released, the security team is able to identify multiple vulnerabilities. Which of the following would BEST help the team ensure the application is ready to be released to production?

A. Limit the use of third-party libraries.
B. Prevent data exposure queries.
C. Obfuscate the source code.
D. Submit the application to QA before releasing it.
Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 33
In which of the following common use cases would steganography be employed?

VCEplus.com

A. Obfuscation
B. Integrity
C. Non-repudiation
D. Blockchain

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 34
To secure an application after a large data breach, an e-commerce site will be resetting all users' credentials. Which of the following will BEST ensure the site's users are not compromised after the reset?

A. A password reuse policy
B. Account lockout after three failed attempts
C. Encrypted credentials in transit
D. A geofencing policy based on login history

VCEplus.com

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 35
In which of the following risk management strategies would cybersecurity insurance be used?
A. Transference
B. Avoidance
C. Acceptance
D. Mitigation

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

VCEplus.com

QUESTION 36
A security analyst is using a recently released security advisory to review historical logs, looking for the specific activity that was outlined in the advisory. Which of the following is the analyst doing?

A. A packet capture
B. A user behavior analysis
C. Threat hunting
D. Credentialed vulnerability scanning

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 37

VCEplus.com

Which of the following would MOST likely support the integrity of a voting machine?

A. Asymmetric encryption
B. Blockchain
C. Transport Layer Security
D. Perfect forward secrecy

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 38
A Chief Information Security Officer (CISO) needs to create a policy set that meets international standards for data privacy and sharing. Which of the following should the CISO read and understand before writing the policies?

VCEplus.com

A. PCI DSS
B. GDPR
C. NIST
D. ISO 31000

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 39
A commercial cyber-threat intelligence organization observes IoCs across a variety of unrelated customers. Prior to releasing specific threat intelligence to other paid subscribers, the organization is MOST likely obligated by contracts to:

A. perform attribution to specific APTs and nation-state actors.
B. anonymize any PII that is observed within the IoC data.
C. add metadata to track the utilization of threat intelligence reports.
D. assist companies with impact assessments based on the observed data.

CEplus.com

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 40
Which of the following is the purpose of a risk register?
A. To define the level or risk using probability and likelihood
B. To register the risk with the required regulatory agencies
C. To identify the risk, the risk owner, and the risk measures
D. To formally log the type of risk mitigation strategy the organization is using

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

CEplus.com

QUESTION 41
The Chief Financial Officer (CFO) of an insurance company received an email from Ann, the company's Chief Executive Officer (CEO), requesting a transfer of $10,000 to an account. The email states Ann is on vacation and has lost her purse, containing cash and credit cards. Which of the following social-engineering techniques is the attacker using?

A. Phishing
B. Whaling
C. Typo squatting
D. Pharming

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

VCEplus.com

QUESTION 42
An organization wants to implement a third factor to an existing multifactor authentication. The organization already uses a smart card and password. Which of the following would meet the organization's needs for a third factor?

A. Date of birth
B. Fingerprints
C. PIN
D. TPM

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 43
A user contacts the help desk to report the following:

- Two days ago, a pop-up browser window prompted the user for a name and password after connecting to the corporate wireless SSID. This had never happened before, but the user entered the information as requested.
- The user was able to access the Internet but had trouble accessing the department share until the next day. ▪

The user is now getting notifications from the bank about unauthorized transactions.

Which of the following attack vectors was MOST likely used in this scenario?

A. Rogue access point
B. Evil twin
C. DNS poisoning
D. ARP poisoning

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

VCEplus.com

QUESTION 44
A host was infected with malware. During the incident response, Joe, a user, reported that he did not receive any emails with links, but he had been browsing the Internet all day. Which of the following would MOST likely show where the malware originated?

A. The DNS logs
B. The web server logs
C. The SIP traffic logs
D. The SNMP logs

Correct Answer: A
Section: (none)
Explanation
Explanation/Reference:

QUESTION 45
Joe, an employee, receives an email stating he won the lottery. The email includes a link that requests a name, mobile phone number, address, and date of birth be provided to confirm Joe's identity before sending him the prize. Which of the following BEST describes this type of email?

VCEplus.com

A. Spear phishing
B. Whaling
C. Phishing
D. Vishing

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 46
Which of the following refers to applications and systems that are used within an organization without consent or approval?

A. Shadow IT
B. OSINT
C. Dark web
D. Insider threats

VCEplus.com

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 47
A manufacturer creates designs for very high security products that are required to be protected and controlled by the government regulations. These designs are not accessible by corporate networks or the Internet. Which of the following is the BEST solution to protect these designs?

A. An air gap
B. A Faraday cage
C. A shielded cable
D. A demilitarized zone

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

VCEplus.com

QUESTION 48
A company processes highly sensitive data and senior management wants to protect the sensitive data by utilizing classification labels. Which of the following access control schemes would be BEST for the company to implement?

A. Discretionary
B. Rule-based
C. Role-based
D. Mandatory

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

CEplus.com

QUESTION 49
Which of the following policies would help an organization identify and mitigate potential single points of failure in the company's IT/security operations?

A. Least privilege
B. Awareness training
C. Separation of duties
D. Mandatory vacation

Correct Answer: C
Section: (none)
Explanation
Explanation/Reference:

QUESTION 50
Which of the following would be the BEST method for creating a detailed diagram of wireless access points and hotspots?

A. Footprinting
B. White-box testing
C. A drone/UAV
D. Pivoting

CEplus.com

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 51
A user enters a password to log in to a workstation and is then prompted to enter an authentication code. Which of the following MFA factors or attributes are being utilized in the authentication process? (Choose two.)

A. Something you know
B. Something you have
C. Somewhere you are
D. Someone you know
E. Something you are

VCEplus.com

F. Something you can do

Correct Answer: AB
Section: (none)
Explanation

Explanation/Reference:

QUESTION 52
When selecting a technical solution for identity management, an architect chooses to go from an in-house solution to a third-party SaaS provider. Which of the following risk management strategies is this an example of?
A. Transference
B. Avoidance
C. Acceptance
D. Mitigation

Correct Answer: A
Section: (none)
Explanation

VCEplus.com

Explanation/Reference:

QUESTION 53
A website developer is working on a new e-commerce website and has asked an information security expert for the most appropriate way to store credit card numbers to create an easy reordering process. Which of the following methods would BEST accomplish this goal?

A. Salting the magnetic strip information
B. Encrypting the credit card information in transit
C. Hashing the credit card numbers upon entry
D. Tokenizing the credit cards in the database

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

VCEplus.com

QUESTION 54
A company recently experienced a data breach and the source was determined to be an executive who was charging a phone in a public area. Which of the following would MOST likely have prevented this breach?

A. A firewall
B. A device pin
C. A USB data blocker
D. Biometrics

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 55
A network administrator would like to configure a site-to-site VPN utilizing IPsec. The administrator wants the tunnel to be established with data integrity, encryption, authentication, and anti-replay functions. Which of the following should the administrator use when configuring the VPN?

VCEplus.com

A. AH
B. EDR
C. ESP
D. DNSSEC

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 56
Users have been issued smart cards that provide physical access to a building. The cards also contain tokens that can be used to access information systems. Users can log in to any thin client located throughout the building and see the same desktop each time. Which of the following technologies are being utilized to provide these capabilities? (Choose two.)

A. COPE

VCEplus.com

B. VDI
C. GPS
D. TOTP
E. RFID
F. BYOD

Correct Answer: BE
Section: (none)
Explanation

Explanation/Reference:
QUESTION 57
The Chief Security Officer (CSO) at a major hospital wants to implement SSO to help improve security in the environment and protect patient data, particularly at shared terminals. The Chief Risk Officer (CRO) is concerned that training and guidance have not been provided to frontline staff, and a risk analysis has not been performed. Which of the following is the MOST likely cause of the CRO's concerns?

A. SSO would simplify username and password management, making it easier for hackers to guess accounts.
B. SSO would reduce password fatigue, but staff would still need to remember more complex passwords.
C. SSO would reduce the password complexity for frontline staff.
D. SSO would reduce the resilience and availability of systems if the identity provider goes offline.

VCEplus.com

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 58
A cybersecurity administrator has a reduced team and needs to operate an on-premises network and security infrastructure efficiently. To help with the situation, the administrator decides to hire a service provider. Which of the following should the administrator use?

A. SDP
B. AAA
C. IaaS
D. MSSP
E. Microservices

VCEplus.com

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 59
A security analyst is investigating an incident that was first reported as an issue connecting to network shares and the Internet. While reviewing logs and tool output, the analyst sees the following:

IP address	Physical address
10.0.0.1	00-18-21-ad-24-bc
10.0.0.114	01-31-a3-cd-23-ab
10.0.0.115	00-18-21-ad-24-bc
10.0.0.116	00-19-08-ba-07-da
10.0.0.117	01-12-21-ca-11-ad

Which of the following attacks has occurred?

VCEplus.com

A. IP conflict
B. Pass-the-hash
C. MAC flooding
D. Directory traversal
E. ARP poisoning

Correct Answer: E
Section: (none)
Explanation

Explanation/Reference:

QUESTION 60
An organization suffered an outage, and a critical system took 90 minutes to come back online. Though there was no data loss during the outage, the expectation was that the critical system would be available again within 60 minutes. Which of the following is the 60-minute expectation an example of?

A. MTBF
B. RPO

VCEplus.com

C. MTTR
D. RTO

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 61
An organization is concerned that its hosted web servers are not running the most updated version of the software. Which of the following would work BEST to help identify potential vulnerabilities?

A. `hping3 -S comptia.org -p 80`
B. `nc -l -v comptia.org -p 80`
C. `nmap comptia.org -p 80 -sV`
D. `nslookup -port=80 comptia.org`

VCEplus.com

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 62
A retail executive recently accepted a job with a major competitor. The following week, a security analyst reviews the security logs and identifies successful logon attempts to access the departed executive's accounts. Which of the following security practices would have addressed the issue?

A. A non-disclosure agreement
B. Least privilege
C. An acceptable use policy
D. Offboarding

Correct Answer: D

VCEplus.com

Section: (none)
Explanation

Explanation/Reference:

QUESTION 63
A security analyst is performing a forensic investigation involving compromised account credentials. Using the Event Viewer, the analyst was able to detect the following message: “Special privileges assigned to new logon.” Several of these messages did not have a valid logon associated with the user before these privileges were assigned. Which of the following attacks is MOST likely being detected?

A. Pass-the-hash
B. Buffer overflow
C. Cross-site scripting
D. Session replay

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

VCEplus.com

QUESTION 64
A systems administrator needs to implement an access control scheme that will allow an object’s access policy to be determined by its owner. Which of the following access control schemes BEST fits the requirements?

A. Role-based access control
B. Discretionary access control
C. Mandatory access control
D. Attribute-based access control

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

VCEplus.com

QUESTION 65
A company has limited storage space available and an online presence that cannot be down for more than four hours. Which of the following backup methodologies should the company implement to allow for the FASTEST database restore time in the event of a failure, while being mindful of the limited available storage space?

A. Implement full tape backups every Sunday at 8:00 p.m. and perform nightly tape rotations.
B. Implement differential backups every Sunday at 8:00 p.m. and nightly incremental backups at 8:00 p.m.
C. Implement nightly full backups every Sunday at 8:00 p.m.
D. Implement full backups every Sunday at 8:00 p.m. and nightly differential backups at 8:00 p.m.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
QUESTION 66
An organization has a growing workforce that is mostly driven by additions to the sales department. Each newly hired salesperson relies on a mobile device to conduct business. The Chief Information Officer (CIO) is wondering if the organization may need to scale down just as quickly as it scaled up. The CIO is also concerned about the organization's security and customer privacy. Which of the following would be BEST to address the CIO's concerns?

A. Disallow new hires from using mobile devices for six months.
B. Select four devices for the sales department to use in a CYOD model. C. Implement BYOD for the sales department while leveraging the MDM.
D. Deploy mobile devices using the COPE methodology.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 67
A public relations team will be taking a group of guests on a tour through the facility of a large e-commerce company. The day before the tour, the company sends out an email to employees to ensure all whiteboards are cleaned and all desks are cleared. The company is MOST likely trying to protect against:

A. loss of proprietary information.
B. damage to the company's reputation.

VCEplus.com

C. social engineering.
D. credential exposure.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 68
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:

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

VCEplus.com

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 69
A network engineer is troubleshooting wireless network connectivity issues that were reported by users. The issues are occurring only in the section of the building that is closest to the parking lot. Users are intermittently experiencing slow speeds when accessing websites and are unable to connect to network drives. The issues appear to increase when laptop users return to their desks after using their devices in other areas of the building. There have also been reports of users being required to enter their credentials on web pages in order to gain access to them. Which of the following is the MOST likely cause of this issue?

A. An external access point is engaging in an evil-twin attack.
B. The signal on the WAP needs to be increased in that section of the building.
C. The certificates have expired on the devices and need to be reinstalled.
D. The users in that section of the building are on a VLAN that is being blocked by the firewall.

Correct Answer: A

VCEplus.com

Section: (none)
Explanation

Explanation/Reference:

QUESTION 70
A company's Chief Information Officer (CIO) is meeting with the Chief Information Security Officer (CISO) to plan some activities to enhance the skill levels of the company's developers. Which of the following would be MOST suitable for training the developers?

A. A capture-the-flag competition
B. A phishing simulation
C. Physical security training
D. Basic awareness training

Correct Answer: D
Section: (none)
Explanation
Explanation/Reference:

VCEplus.com

QUESTION 71
Under GDPR, which of the following is MOST responsible for the protection of privacy and website user rights?

A. The data protection officer
B. The data processor
C. The data owner
D. The data controller

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 72

VCEplus.com

A global pandemic is forcing a private organization to close some business units and reduce staffing at others. Which of the following would be BEST to help the organization's executives determine their next course of action?

A. An incident response plan
B. A communications plan
C. A disaster recovery plan
D. A business continuity plan

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 73
Which of the following describes the ability of code to target a hypervisor from inside a guest OS?

VCEplus.com

A. Fog computing
B. VM escape
C. Software-defined networking
D. Image forgery
E. Container breakout

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 74
Which of the following ISO standards is certified for privacy?

A. ISO 9001
B. ISO 27002
C. ISO 27701
D. ISO 31000

VCEplus.com

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 75
A document that appears to be malicious has been discovered in an email that was sent to a company's Chief Financial Officer (CFO). Which of the following would be BEST to allow a security analyst to gather information and confirm it is a malicious document without executing any code it may contain?

A. Open the document on an air-gapped network.
B. View the document's metadata for origin clues.
C. Search for matching file hashes on malware websites.
D. Detonate the document in an analysis sandbox.

Correct Answer: C
Section: (none)
Explanation
Explanation/Reference:

VCEplus.com

QUESTION 76
Which of the following is a team of people dedicated to testing the effectiveness of organizational security programs by emulating the techniques of potential attackers?

A. Red team
B. White team
C. Blue team
D. Purple team

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

VCEplus.com

QUESTION 77
A security analyst needs to be proactive in understanding the types of attacks that could potentially target the company's executives. Which of the following intelligence sources should the security analyst review?

A. Vulnerability feeds
B. Trusted automated exchange of indicator information
C. Structured threat information expression
D. Industry information-sharing and collaboration groups

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 78
An organization has hired a security analyst to perform a penetration test. The analyst captures 1Gb worth of inbound network traffic to the server and transfers the pcap back to the machine for analysis. Which of the following tools should the analyst use to further review the pcap?

VCEplus.com

A. Nmap
B. cURL
C. Netcat
D. Wireshark

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 79
A company uses wireless for all laptops and keeps a very detailed record of its assets, along with a comprehensive list of devices that are authorized to be on the wireless network. The Chief Information Officer (CIO) is concerned about a script kiddie potentially using an unauthorized device to brute force the wireless PSK and obtain access to the internal network. Which of the following should the company implement to BEST prevent this from occurring?

A. A BPDU guard

VCEplus.com

B. WPA-EAP
C. IP filtering
D. A WIDS

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 80
A vulnerability assessment report will include the CVSS score of the discovered vulnerabilities because the score allows the organization to better:

A. validate the vulnerability exists in the organization's network through penetration testing.
B. research the appropriate mitigation techniques in a vulnerability database.
C. find the software patches that are required to mitigate a vulnerability.
D. prioritize remediation of vulnerabilities based on the possible impact.

VCEplus.com

Correct Answer: D
Section: (none)
Explanation
Explanation/Reference:

QUESTION 81
A security engineer is reviewing log files after a third party discovered usernames and passwords for the organization's accounts. The engineer sees there was a change in the IP address for a vendor website one week earlier. This change lasted eight hours. Which of the following attacks was MOST likely used?

A. Man-in-the-middle
B. Spear phishingC. Evil twin
D. DNS poisoning

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

VCEplus.com

QUESTION 82
A large industrial system's smart generator monitors the system status and sends alerts to third-party maintenance personnel when critical failures occur. While reviewing the network logs, the company's security manager notices the generator's IP is sending packets to an internal file server's IP. Which of the following mitigations would be BEST for the security manager to implement while maintaining alerting capabilities?

A. Segmentation
B. Firewall whitelisting
C. Containment
D. Isolation

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 83
A software developer needs to perform code-execution testing, black-box testing, and non-functional testing on a new product before its general release. Which of the following BEST describes the tasks the developer is conducting?

VCEplus.com

A. Verification
B. Validation
C. Normalization
D. Staging

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 84
A security analyst is configuring a large number of new company-issued laptops. The analyst received the following requirements:

- The devices will be used internationally by staff who travel extensively.
- Occasional personal use is acceptable due to the travel requirements.
- Users must be able to install and configure sanctioned programs and productivity suites.

VCEplus.com

- The devices must be encrypted.
- The devices must be capable of operating in low-bandwidth environments.

Which of the following would provide the GREATEST benefit to the security posture of the devices?

A. Configuring an always-on VPN
B. Implementing application whitelisting
C. Requiring web traffic to pass through the on-premises content filter
D. Setting the antivirus DAT update schedule to weekly

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 85
Company engineers regularly participate in a public Internet forum with other engineers throughout the industry. Which of the following tactics would an attacker MOST likely use in this scenario?
A. Watering-hole attack
B. Credential harvesting
C. Hybrid warfare
D. Pharming

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 86
Which of the following will provide the BEST physical security countermeasures to stop intruders? (Choose two.)

A. Alarms
B. Signage
C. Lighting

CEplus.com

D. Mantraps
E. Fencing
F. Sensors

Correct Answer: EF
Section: (none)
Explanation

Explanation/Reference:

QUESTION 87
A security analyst is looking for a solution to help communicate to the leadership team the severity levels of the organization's vulnerabilities. Which of the following would BEST meet this need?

A. CVE
B. SIEM
C. SOAR
D. CVSS

CEplus.com

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 88
The Chief Executive Officer (CEO) of an organization would like staff members to have the flexibility to work from home anytime during business hours, including during a pandemic or crisis. However, the CEO is concerned that some staff members may take advantage of the flexibility and work from high-risk countries while on holiday or outsource work to a third-party organization in another country. The Chief Information Officer (CIO) believes the company can implement some basic controls to mitigate the majority of the risk. Which of the following would be BEST to mitigate the CEO's concerns? (Choose two.)

A. Geolocation
B. Time-of-day restrictions
C. Certificates
D. Tokens
E. Geotagging

VCEplus.com

F. Role-based access controls

Correct Answer: AB
Section: (none)
Explanation

Explanation/Reference:

QUESTION 89
The SOC is reviewing processes 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. This 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. Dividing the network into trusted and untrusted zones
C. Providing additional end-user training on acceptable use
D. Implementing manual quarantining of infected hosts

VCEplus.com

Correct Answer: A
Section: (none)
Explanation
Explanation/Reference:

QUESTION 90
A network administrator is setting up wireless access points in all the conference rooms and wants to authenticate devices using PKI. Which of the following should the administrator configure?

A. A captive portal
B. PSK
C. 802.1X
D. WPS

Correct Answer: C
Section: (none)
Explanation

VCEplus.com

Explanation/Reference:

QUESTION 91
Which of the following are the MOST likely vectors for the unauthorized or unintentional inclusion of vulnerable code in a software company's final software releases? (Choose two.)

A. Unsecure protocols
B. Use of penetration-testing utilities
C. Weak passwords
D. Included third-party libraries
E. Vendors/supply chain
F. Outdated anti-malware software

Correct Answer: AC
Section: (none)
Explanation

Explanation/Reference:

VCEplus.com

QUESTION 92
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. Preventive
D. Compensating

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

VCEplus.com

QUESTION 93
An organization just experienced a major cyberattack incident. The attack was well coordinated, sophisticated, and highly skilled. Which of the following targeted the organization?

A. Shadow IT
B. An insider threat
C. A hacktivist
D. An advanced persistent threat

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 94
An enterprise has hired an outside security firm to conduct penetration testing on its network and applications. The firm has been given all the developer's documentation about the internal architecture. Which of the following BEST represents the type of testing that will occur?

VCEplus.com

A. Bug bounty
B. White-box
C. Black-box
D. Gray-box
Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 95
A security engineer has enabled two-factor authentication on all workstations. Which of the following approaches are the MOST secure? (Choose two.)

A. Password and security question
B. Password and CAPTCHA
C. Password and smart card
D. Password and fingerprint

VCEplus.com

E. Password and one-time token
F. Password and voice

Correct Answer: CD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 96
A Chief Information Security Officer (CISO) is concerned about the organization's ability to continue business operations in the event of a prolonged DDoS attack on its local datacenter that consumes database resources. Which of the following will the CISO MOST likely recommend to mitigate this risk?

A. Upgrade the bandwidth available into the datacenter.
B. Implement a hot-site failover location.
C. Switch to a complete SaaS offering to customers.
D. Implement a challenge response test on all end-user queries.

VCEplus.com

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
QUESTION 97
Which of the following will MOST likely cause machine learning and AI-enabled systems to operate with unintended consequences?

A. Stored procedures
B. Buffer overflows
C. Data bias
D. Code reuse

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

https://vceplus.com/

www.vceplus.com - Free Questions & Answers - Online Courses - Convert VCE to PDF - VCEplus.com