Itfreedumps provides the latest online questions for all IT certifications, such as IBM, Microsoft, CompTIA, Huawei, and so on.

Hot exams are available below.

AZ-204 Developing Solutions for Microsoft Azure

820-605 Cisco Customer Success Manager

MS-203 Microsoft 365 Messaging

HPE2-T37 Using HPE OneView

300-415 Implementing Cisco SD-WAN Solutions (ENSDWI)

DP-203 Data Engineering on Microsoft Azure

500-220 Engineering Cisco Meraki Solutions v1.0

NACE-CIP1-001 Coating Inspector Level 1

NACE-CIP2-001 Coating Inspector Level 2

200-301 Implementing and Administering Cisco Solutions

Share some SY0-701 exam online questions below.

1.A certificate authority needs to post information about expired certificates.
Which of the following would accomplish this task?
A. TPM
B. CRL
C. PKI

D. CSR
Answer: B
Explanation:
A Certificate Revocation List (CRL) is a digitally signed list maintained by a Certificate Authority (CA) that contains revoked or expired certificates. This prevents clients from trusting compromised or outdated certificates.
TPM (A) is a hardware security module, unrelated to certificate revocation.
PKI (C) is the overall system managing digital certificates, but it does not store revocation lists.
CSR (D) is a request to obtain a certificate, not to revoke one.
Reference: CompTIA Security+ SY0-701 Official Study Guide, Security Architecture domain.

2.A network administrator wants to ensure that network traffic is highly secure while in transit.
Which of the following actions best describes the actions the network administrator should take?
A. Ensure that NAC is enforced on all network segments, and confirm that firewalls have updated policies to block unauthorized traffic.
B. Ensure only TLS and other encrypted protocols are selected for use on the network, and only permit authorized traffic via secure protocols.
C. Configure the perimeter IPS to block inbound HTTPS directory traversal traffic, and verify that signatures are updated on a daily basis.
D. Ensure the EDR software monitors for unauthorized applications that could be used by threat actors, and configure alerts for the security team.
Answer: B

3.Which of the following is a preventive physical security control?
A. Video surveillance system
B. Bollards
C. Alarm system
D. Motion sensors
Answer: B

4.A software development manager wants to ensure the authenticity of the code created by the company.
Which of the following options is the most appropriate?
A. Testing input validation on the user input fields
B. Performing code signing on company-developed software
C. Performing static code analysis on the software
D. Ensuring secure cookies are use
Answer: B
Explanation:
Code signing is a technique that uses cryptography to verify the authenticity and integrity of the code created by the company. Code signing involves applying a digital signature to the code using a private key that only the company possesses. The digital signature can be verified by anyone who has the corresponding public key, which can be distributed through a trusted certificate authority. Code signing can prevent unauthorized modifications, tampering, or malware injection into the code, and it can also assure the users that the code is from a legitimate source.
Reference = CompTIA Security+ Study Guide with over 500 Practice Test Questions: Exam SY0-701, 9th Edition, Chapter 2, page 74. CompTIA Security+ (SY0-701) Certification Exam Objectives, Domain 3.2, page 11. Application Security C SY0-601 CompTIA Security+: 3.2

5.Which of the following would be most useful in determining whether the long-term cost to transfer a risk is less than the impact of the risk?
A. ARO
B. RTO
C. RPO
D. ALE
E. SLE
Answer: D
Explanation:
The Annual Loss Expectancy (ALE) is most useful in determining whether the long-term cost to transfer a risk is less than the impact of the risk. ALE is calculated by multiplying the Single Loss Expectancy (SLE) by the Annualized Rate of Occurrence (ARO), which provides an estimate of the annual expected loss due to a specific risk, making it valuable for long-term financial planning and risk management decisions.
Reference: CompTIA Security+ SY0-701 course content and official CompTIA study resources.

6.Which of the following is a reason why a forensic specialist would create a plan to preserve data after an modem and prioritize the sequence for performing forensic analysis?
A. Order of volatility
B. Preservation of event logs
C. Chain of custody
D. Compliance with legal hold
Answer: A
Explanation:
When conducting a forensic analysis after an incident, it's essential to prioritize the data collection process based on the "order of volatility." This principle dictates that more volatile data (e.g., data in memory, network connections) should be captured before less volatile data (e.g., disk drives, logs). The idea is to preserve the most transient and potentially valuable evidence first, as it is more likely to be lost or altered quickly.
Reference =
CompTIA Security+ SY0-701 Course Content: Domain 04 Security Operations.
CompTIA Security+ SY0-601 Study Guide: Chapter on Digital Forensics.

7.After a security incident, a systems administrator asks the company to buy a NAC platform. Which of the following attack surfaces is the systems administrator trying to protect?
A. Bluetooth
B. Wired
C. NFC
D. SCADA
Answer: B
Explanation:
A NAC (network access control) platform is a technology that enforces security policies on devices that attempt to access a network. A NAC platform can verify the identity, role, and compliance of the devices, and grant or deny access based on predefined rules. A NAC platform can protect both wired and wireless networks, but in this scenario, the systems administrator is trying to protect the wired attack surface, which is the set of vulnerabilities that can be exploited through a physical connection to the network12.
Reference: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, Chapter 5, page 189; CompTIA Security+ Certification Kit: Exam SY0-701, 7th Edition, Chapter 5, page 237.

8.Which of the following is the best way to secure an on-site data center against intrusion from an insider?
A. Bollards
B. Access badge
C. Motion sensor
D. Video surveillance
Answer: B

9.A company wants to get alerts when others are researching and doing reconnaissance on the company One approach would be to host a part of the Infrastructure online with known vulnerabilities that would appear to be company assets.
Which of the following describes this approach?
A. Watering hole
B. Bug bounty
C. DNS sinkhole
D. Honeypot
Answer: D
Explanation:
A honeypot is a security mechanism set up to attract and detect potential attackers by simulating vulnerable assets. By hosting a part of the infrastructure online with known vulnerabilities that appear to be company assets, the company can observe and analyze the behavior of attackers conducting reconnaissance. This approach allows the company to get alerts and gather intelligence on potential threats.
Reference = CompTIA Security+ SY0-701 study materials, particularly on threat detection techniques such as honeypots.

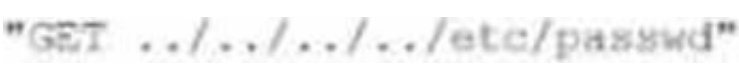
10.A security administrator needs to reduce the attack surface in the company's data centers.
Which of the following should the security administrator do to complete this task?
A. Implement a honeynet.
B. Define Group Policy on the servers.
C. Configure the servers for high availability.
D. Upgrade end-of-support operating systems.
Answer: D
Explanation:
Upgrading end-of-support operating systems is one of the most effective ways to reduce the attack surface. Unsupported OS versions no longer receive security patches, making them prime targets for attackers. Removing outdated software ensures that known vulnerabilities cannot be exploited. A (honeynet) is used for threat analysis, not reducing the attack surface.
B (Group Policy) helps enforce security policies but does not address outdated vulnerabilities.
C (High availability) focuses on uptime, not security risk reduction.
Reference: CompTIA Security+ SY0-701 Official Study Guide, Security Architecture domain.

11.An employee who was working remotely lost a mobile device containing company data.
Which of the following provides the best solution to prevent future data loss?
A. MDM
B. DLP
C. FDE

D. EDR
Answer: A

12.Which of the following must be considered when designing a high-availability network? (Choose two).
A. Ease of recovery
B. Ability to patch
C. Physical isolation
D. Responsiveness
E. Attack surface
F. Extensible authentication
Answer: A, E
Explanation:
A high-availability network is a network that is designed to minimize downtime and ensure continuous operation even in the event of a failure or disruption.
A high-availability network must consider the following factors12:
Ease of recovery: This refers to the ability of the network to restore normal functionality quickly and efficiently after a failure or disruption. Ease of recovery can be achieved by implementing backup and restore procedures, redundancy and failover mechanisms, fault tolerance and resilience, and disaster recovery plans.
Attack surface: This refers to the amount of exposure and vulnerability of the network to potential threats and attacks. Attack surface can be reduced by implementing security controls such as firewalls, encryption, authentication, access control, segmentation, and hardening. The other options are not directly related to high-availability network design:
Ability to patch: This refers to the process of updating and fixing software components to address security issues, bugs, or performance improvements. Ability to patch is important for maintaining the security and functionality of the network, but it is not a specific factor for high-availability network design.
Physical isolation: This refers to the separation of network components or devices from other networks or physical environments. Physical isolation can enhance the security and performance of the network, but it can also reduce the availability and accessibility of the network resources.
Responsiveness: This refers to the speed and quality of the network's performance and service delivery. Responsiveness can be measured by metrics such as latency, throughput, jitter, and packet loss. Responsiveness is important for ensuring customer satisfaction and user experience, but it is not a specific factor for high-availability network design.
Extensible authentication: This refers to the ability of the network to support multiple and flexible authentication methods and protocols. Extensible authentication can improve the security and convenience of the network, but it is not a specific factor for high-availability network design.
Reference = 1: CompTIA Security+ SY0-701 Certification Study Guide, page 972: High Availability C CompTIA Security+ SY0-701 C 3.4, video by Professor Messer.

13.A security administrator observed the following in a web server log while investigating an incident:



Which of the following attacks did the security administrator most likely see?
A. Privilege escalation
B. Credential replay
C. Brute force

D. Directory traversal
Answer: D

14.While considering the organization's cloud-adoption strategy, the Chief Information Security Officer sets a goal to outsource patching of firmware, operating systems, and applications to the chosen cloud vendor.
Which of the following best meets this goal?
A. Community cloud
B. PaaS
C. Containerization
D. Private cloud
E. SaaS
F. laaS
Answer: E
Explanation:
Software as a Service (SaaS) is the cloud model that best meets the goal of outsourcing the management, including patching, of firmware, operating systems, and applications to the cloud vendor. In a SaaS environment, the cloud provider is responsible for maintaining and updating the entire software stack, allowing the organization to focus on using the software rather than managing its infrastructure.
Reference = CompTIA Security+ SY0-701 study materials, particularly the domains related to cloud security models.

15.A network manager wants to protect the company's VPN by implementing multifactor authentication that uses:
. Something you know
. Something you have
. Something you are
Which of the following would accomplish the manager's goal?
A. Domain name, PKI, GeolP lookup
B. VPN IP address, company ID, facial structure
C. Password, authentication token, thumbprint
D. Company URL, TLS certificate, home address
Answer: C
Explanation:
The correct answer is C. Password, authentication token, thumbprint. This combination of authentication factors satisfies the manager’s goal of implementing multifactor authentication that uses something you know, something you have, and something you are.
Something you know is a type of authentication factor that relies on the user’s knowledge of a secret or personal information, such as a password, a PIN, or a security question. A password is a common example of something you know that can be used to access a VPN12
Something you have is a type of authentication factor that relies on the user’s possession of a physical object or device, such as a smart card, a token, or a smartphone. An authentication token is a common example of something you have that can be used to generate a one-time password (OTP) or a code that can be used to access a VPN12
Something you are is a type of authentication factor that relies on the user’s biometric characteristics, such as a fingerprint, a face, or an iris. A thumbprint is a common example of something you are that can be used to scan and verify the user’s identity to access a VPN12
Reference: 1: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, Chapter 4: Identity and Access Management, page 177 2: CompTIA Security+ Certification Kit: Exam SY0-701, 7th Edition,

16.A security analyst learns that an attack vector, used as part of a recent incident, was a well-known IoT device exploit. The analyst needs to review logs to identify the time of the initial exploit.
Which of the following logs should the analyst review first?
A. Endpoint
B. Application
C. Firewall
D. NAC
Answer: C
Explanation:
Detailed Firewall logs provide details of all network traffic, including connections to and from IoT devices. They are typically the first source of evidence for identifying the time of an exploit.
Reference: CompTIA Security+ SY0-701 Study Guide, Domain 4: Security Operations, Section: "Log Analysis for Incident Response".

17.Which of the following is a reason environmental variables are a concern when reviewing potential system vulnerabilities?
A. The contents of environmental variables could affect the scope and impact of an exploited vulnerability.
B. In-memory environmental variable values can be overwritten and used by attackers to insert malicious code.
C. Environmental variables define cryptographic standards for the system and could create vulnerabilities if deprecated algorithms are used.
D. Environmental variables will determine when updates are run and could mitigate the likelihood of vulnerability exploitation.
Answer: A
Explanation:
Environmental variables store configuration settings, paths, and other system-related information that applications and processes use. If an attacker gains access to these variables, they could manipulate them to alter application behavior, gain unauthorized access, or escalate privileges.
For example, an attacker could modify the PATH variable to execute malicious programs instead of legitimate ones. This can significantly increase the scope and impact of an exploited vulnerability, making it a major security concern.
Reference: CompTIA Security+ SY0-701 Official Study Guide, Security Architecture domain.

18.Which of the following steps in the risk management process involves establishing the scope and potential risks involved with a project?
A. Risk mitigation
B. Risk identification
C. Risk treatment
D. Risk monitoring and review
Answer: B
Explanation:
Risk identification is the first step in the risk management process, where potential threats and vulnerabilities are analyzed to understand their impact on an organization. This includes identifying assets, evaluating threats, and assessing potential vulnerabilities. Risk mitigation: Reducing risk by implementing controls.
Risk treatment: Determining how to handle identified risks.

Risk monitoring and review: Ongoing evaluation of risk controls.
Reference: CompTIA Security+ SY0-701 Official Study Guide, Security Program Management and Oversight domain.

19.A company implemented an MDM policy 10 mitigate risks after repealed instances of employees losing company-provided mobile phones. In several cases. The lost phones were used maliciously to perform social engineering attacks against other employees.
Which of the following MDM features should be configured to best address this issue? (Select two).
A. Screen locks
B. Remote wipe
C. Full device encryption
D. Push notifications
E. Application management
F. Geolocation
Answer: A,B
Explanation:
Integrating each SaaS solution with an Identity Provider (IdP) is the most effective way to address the security issue. This approach allows for Single Sign-On (SSO) capabilities, where users can access multiple SaaS applications with a single set of credentials while maintaining strong password policies across all services. It simplifies the user experience and ensures consistent security enforcement across different SaaS platforms.
Reference =
CompTIA Security+ SY0-701 Course Content: Domain 05 Security Program Management and Oversight.
CompTIA Security+ SY0-601 Study Guide: Chapter on Identity and Access Management.

20.Which of the following aspects of the data management life cycle is most directly impacted by local and international regulations?
A. Destruction
B. Certification
C. Retention
D. Sanitization
Answer: C
Explanation:
Detailed
Retention policies dictate how long data must be stored to comply with local and international regulations. Non-compliance can result in legal and financial penalties.
Reference: CompTIA Security+ SY0-701 Study Guide, Domain 5: Security Program Management, Section: "Data Retention and Legal Requirements".

21.A systems administrator is working on a solution with the following requirements:
• Provide a secure zone.
• Enforce a company-wide access control policy.
• Reduce the scope of threats.
Which of the following is the systems administrator setting up?
A. Zero Trust
B. AAA
C. Non-repudiation
D. CIA

Answer: A
Explanation:
Zero Trust is a security model that assumes no trust for any entity inside or outside the network perimeter and requires continuous verification of identity and permissions. Zero Trust can provide a secure zone by isolating and protecting sensitive data and resources from unauthorized access. Zero Trust can also enforce a company-wide access control policy by applying the principle of least privilege and granular segmentation for users, devices, and applications. Zero Trust can reduce the scope of threats by preventing lateral movement and minimizing the attack surface.
Reference: 5: This source explains the concept and benefits of Zero Trust security and how it differs from traditional security models.
8: This source provides an overview of Zero Trust identity security and how it can help verify the identity and integrity of users and devices.

22.An attacker submits a request containing unexpected characters in an attempt to gain unauthorized access to information within the underlying systems.
Which of the following best describes this attack?
A. Side loading
B. Target of evaluation
C. Resource reuse
D. SQL injection
Answer: D

23.Which of the following are cases in which an engineer should recommend the decommissioning of a network device? (Select two).
A. The device has been moved from a production environment to a test environment.
B. The device is configured to use cleartext passwords.
C. The device is moved to an isolated segment on the enterprise network.
D. The device is moved to a different location in the enterprise.
E. The device's encryption level cannot meet organizational standards.
F. The device is unable to receive authorized updates.
Answer: E
Explanation:
An engineer should recommend the decommissioning of a network device when the device poses a security risk or a compliance violation to the enterprise environment. A device that cannot meet the encryption standards or receive authorized updates is vulnerable to attacks and breaches, and may expose sensitive data or compromise network integrity. Therefore, such a device should be removed from the network and replaced with a more secure and updated one.
Reference
CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, Chapter 2, Section 2.2, page 671
CompTIA Security+ Practice Tests: Exam SY0-701, 3rd Edition, Chapter 2, Question 16, page 512

24.Which of the following roles, according to the shared responsibility model, is responsible for securing the company’s database in an IaaS model for a cloud environment?
A. Client
B. Third-party vendor
C. Cloud provider
D. DBA
Answer: A
Explanation:

According to the shared responsibility model, the client and the cloud provider have different roles and responsibilities for securing the cloud environment, depending on the service model. In an IaaS (Infrastructure as a Service) model, the cloud provider is responsible for securing the physical infrastructure, such as the servers, storage, and network devices, while the client is responsible for securing the operating systems, applications, and data that run on the cloud infrastructure. Therefore, the client is responsible for securing the company's database in an IaaS model for a cloud environment, as the database is an application that stores data. The client can use various security controls, such as encryption, access control, backup, and auditing, to protect the database from unauthorized access, modification, or loss. The third-party vendor and the DBA (Database Administrator) are not roles defined by the shared responsibility model, but they may be involved in the implementation or management of the database security.
Reference = CompTIA Security+ SY0-701 Certification Study Guide, page 263-264; Professor Messer's CompTIA SY0-701 Security+ Training Course, video 3.1 - Cloud and Virtualization, 5:00 - 7:40.

25.Which of the following explains how to determine the global regulations that data is subject to regardless of the country where the data is stored?
A. Geographic dispersion
B. Data sovereignty
C. Geographic restrictions
D. Data segmentation
Answer: B

26.A company wants to improve the availability of its application with a solution that requires minimal effort in the event a server needs to be replaced or added.
Which of the following would be the best solution to meet these objectives?
A. Load balancing
B. Fault tolerance
C. Proxy servers
D. Replication
Answer: A
Explanation:
Detailed Load balancing improves application availability by distributing traffic across multiple servers. If one server fails, traffic is automatically routed to other available servers with minimal intervention.
Reference: CompTIA Security+ SY0-701 Study Guide, Domain 3: Security Architecture, Section: "High Availability Solutions".

27.A systems administrator works for a local hospital and needs to ensure patient data is protected and secure.
Which of the following data classifications should be used to secure patient data?
A. Private
B. Critical
C. Sensitive
D. Public
Answer: C
Explanation:
Data classification is a process of categorizing data based on its level of sensitivity, value, and impact to the organization if compromised. Data classification helps to determine the appropriate security controls and policies to protect the data from unauthorized access, disclosure, or modification.

Different organizations may use different data classification schemes, but a common one is the four-tier model, which consists of the following categories: public, private, sensitive, and critical.
Public data is data that is intended for public access and disclosure, and has no impact to the organization if compromised. Examples of public data include marketing materials, press releases, and public web pages.
Private data is data that is intended for internal use only, and has a low to moderate impact to the organization if compromised. Examples of private data include employee records, financial reports, and internal policies.
Sensitive data is data that is intended for authorized use only, and has a high impact to the organization if compromised. Examples of sensitive data include personal information, health records, and intellectual property.
Critical data is data that is essential for the organization's operations and survival, and has a severe impact to the organization if compromised. Examples of critical data include encryption keys, disaster recovery plans, and system backups.
Patient data is a type of sensitive data, as it contains personal and health information that is protected by law and ethical standards. Patient data should be used only by authorized personnel for legitimate purposes, and should be secured from unauthorized access, disclosure, or modification. Therefore, the systems administrator should use the sensitive data classification to secure patient data.
Reference = CompTIA Security+ SY0-701 Certification Study Guide, page 90-91; Professor Messer's CompTIA SY0-701 Security+ Training Course, video 5.5 - Data Classifications, 0:00 - 4:30.

28.An organization needs to monitor its users' activities to prevent insider threats.
Which of the following solutions would help the organization achieve this goal?
A. Behavioral analytics
B. Access control lists
C. Identity and access management
D. Network intrusion detection system
Answer: A
Explanation:
Detailed Behavioral analytics tools monitor user actions and detect anomalies that may indicate insider threats, such as unauthorized access or unusual data exfiltration activities. These tools establish baselines for normal behavior and flag deviations.
Reference: CompTIA Security+ SY0-701 Study Guide, Domain 4: Security Operations, Section: "Behavioral Analytics and Monitoring".

29.After a company was compromised, customers initiated a lawsuit. The company's attorneys have requested that the security team initiate a legal hold in response to the lawsuit.
Which of the following describes the action the security team will most likely be required to take?
A. Retain the emails between the security team and affected customers for 30 days.
B. Retain any communications related to the security breach until further notice.
C. Retain any communications between security members during the breach response.
D. Retain all emails from the company to affected customers for an indefinite period of time.
Answer: B
Explanation:
A legal hold (also known as a litigation hold) is a notification sent from an organization's legal team to employees instructing them not to delete electronically stored information (ESI) or discard paper documents that may be relevant to a new or imminent legal case. A legal hold is intended to preserve evidence and prevent spoliation, which is the intentional or negligent destruction of evidence that could harm a party's case. A legal hold can be triggered by various events, such as a lawsuit, a regulatory investigation, or a subpoena12

In this scenario, the company’s attorneys have requested that the security team initiate a legal hold in response to the lawsuit filed by the customers after the company was compromised. This means that the security team will most likely be required to retain any communications related to the security breach until further notice. This could include emails, instant messages, reports, logs, memos, or any other documents that could be relevant to the lawsuit. The security team should also inform the relevant custodians (the employees who have access to or control over the ESI) of their preservation obligations and monitor their compliance. The security team should also document the legal hold process and its scope, as well as take steps to protect the ESI from alteration, deletion, or loss34 Reference: 1: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, Chapter 6: Risk Management, page 303 2: CompTIA Security+ Certification Kit: Exam SY0-701, 7th Edition, Chapter 6: Risk Management, page 305 3: Legal Hold (Litigation Hold) - The Basics of E-Discovery - Exterro 5 4: The Legal Implications and Consequences of a Data Breach 6

30.HOTSPOT
Select the appropriate attack and remediation from each drop-down list to label the corresponding attack with its remediation.

INSTRUCTIONS
Not all attacks and remediation actions will be used.
If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.

Attack Description	Target	Attack Identified	BEST Preventative or Remediation Action
An attacker sends multiple SYN packets from multiple sources.	Web server	Botnet RAT Logic Bomb Backdoor Virus Spyware Worm Adware Ransomware Keylogger Phishing	Enable DDoS protection Patch vulnerable systems Disable vulnerable services Change the default system password Update the cryptographic algorithms Change the default application password Implement 2FA using push notification Conduct a code review Implement application fuzzing Implement a host-based IPS Disable remote access services
The attack establishes a connection, which allows remote commands to be executed.	User	Botnet RAT Logic Bomb Backdoor Virus Spyware Worm Adware Ransomware Keylogger Phishing	Enable DDoS protection Patch vulnerable systems Disable vulnerable services Change the default system password Update the cryptographic algorithms Change the default application password Implement 2FA using push notification Conduct a code review Implement application fuzzing Implement a host-based IPS Disable remote access services
The attack is self propagating and compromises a SQL database using well-known credentials as it moves through the network.	Database server	Botnet RAT Logic Bomb Backdoor Virus Spyware Worm Adware Ransomware Keylogger Phishing	Enable DDoS protection Patch vulnerable systems Disable vulnerable services Change the default system password Update the cryptographic algorithms Change the default application password Implement 2FA using push notification Conduct a code review Implement application fuzzing Implement a host-based IPS Disable remote access services
The attacker uses hardware to remotely monitor a user's input activity to harvest credentials.	Executive	Botnet RAT Logic Bomb Backdoor Virus Spyware Worm Adware Ransomware Keylogger Phishing	Enable DDoS protection Patch vulnerable systems Disable vulnerable services Change the default system password Update the cryptographic algorithms Change the default application password Implement 2FA using push notification Conduct a code review Implement application fuzzing Implement a host-based IPS Disable remote access services
The attacker embeds hidden access in an internally developed application that bypasses account login.	Application	Botnet RAT Logic Bomb Backdoor Virus Spyware Worm Adware Ransomware Keylogger Phishing	Enable DDoS protection Patch vulnerable systems Disable vulnerable services Change the default system password Update the cryptographic algorithms Change the default application password Implement 2FA using push notification Conduct a code review Implement application fuzzing Implement a host-based IPS Disable remote access services

Answer:

Attack Description	Target	Attack Identified	BEST Preventative or Remediation Action
An attacker sends multiple SYN packets from multiple sources.	Web server	Botnet	Enable DDoS protection
The attack establishes a connection, which allows remote commands to be executed.	User	RAT	Implement a host-based IPS
The attack is self propagating and compromises a SQL database using well-known credentials as it moves through the network.	Database server	Worm	Change the default application password
The attacker uses hardware to remotely monitor a user's input activity to harvest credentials.	Executive	Keylogger	Disable vulnerable services
The attacker embeds hidden access in an internally developed application that bypasses account login.	Application	Backdoor	Implement 2FA using push notification

Attack Identified options: Botnet, RAT, Logic Bomb, Backdoor, Virus, Spyware, Worm, Adware, Ransomware, Keylogger, Phishing

BEST Preventative or Remediation Action options: Enable DDoS protection, Patch vulnerable systems, Disable vulnerable services, Change the default system password, Update the cryptographic algorithms, Change the default application password, Implement 2FA using push notification, Conduct a code review, Implement application fuzzing, Implement a host-based IPS, Disable remote access services

Explanation:
Web server Botnet Enable DDoS protection User
RAT Implement a host-based IPS Database server
Worm Change the default application password
Executive KeyloggerDisable vulnerable services
Application Backdoor Implement 2FA using push notification
A screenshot of a computer program Description automatically generated with low confidence

31.A company is implementing a policy to allow employees to use their personal equipment for work. However, the company wants to ensure that only company-approved applications can be installed. Which of the following addresses this concern?
A. MDM
B. Containerization
C. DLP
D. FIM
Answer: A
Explanation:
Comprehensive and Detailed In-Depth
Mobile Device Management (MDM) is a security solution that allows organizations to enforce policies on employee-owned or company-issued mobile devices. It can restrict the installation of unauthorized applications, ensuring that only company-approved apps are used. Containerization isolates work applications from personal applications but does not enforce app restrictions.
Data Loss Prevention (DLP) focuses on preventing sensitive data leaks rather than managing app installations.
File Integrity Monitoring (FIM) tracks changes to files and system configurations but does not control app installations.
Therefore, MDM is the best solution for restricting unauthorized applications on personal devices.

32.Which of the following describes the category of data that is most impacted when it is lost?
A. Confidential
B. Public
C. Private
D. Critical
Answer: D

33.Which of the following actions could a security engineer take to ensure workstations and servers are properly monitored for unauthorized changes and software?
A. Configure all systems to log scheduled tasks.
B. Collect and monitor all traffic exiting the network.
C. Block traffic based on known malicious signatures.
D. Install endpoint management software on all systems.
Answer: D
Explanation:
Endpoint management software is a tool that allows security engineers to monitor and control the configuration, security, and performance of workstations and servers from a central console. Endpoint management software can help detect and prevent unauthorized changes and software installations, enforce policies and compliance, and provide reports and alerts on the status of the endpoints. The other options are not as effective or comprehensive as endpoint management software for this purpose.

Reference: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, page 137 1

34.A newly identified network access vulnerability has been found in the OS of legacy loT devices. Which of the following would best mitigate this vulnerability quickly?
A. Insurance
B. Patching
C. Segmentation
D. Replacement
Answer: C
Explanation:
Segmentation is a technique that divides a network into smaller subnetworks or segments, each with its own security policies and controls. Segmentation can help mitigate network access vulnerabilities in legacy loT devices by isolating them from other devices and systems, reducing their attack surface and limiting the potential impact of a breach. Segmentation can also improve network performance and efficiency by reducing congestion and traffic. Patching, insurance, and replacement are other possible strategies to deal with network access vulnerabilities, but they may not be feasible or effective in the short term. Patching may not be available or compatible for legacy loT devices, insurance may not cover the costs or damages of a cyberattack, and replacement may be expensive and time-consuming.
Reference: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, page 142-143

35.An organization recently updated its security policy to include the following statement:
Regular expressions are included in source code to remove special characters such as $, |, ;. &, `, and ? from variables set by forms in a web application.
Which of the following best explains the security technique the organization adopted by making this addition to the policy?
A. Identify embedded keys
B. Code debugging
C. Input validation
D. Static code analysis
Answer: C
Explanation:
Input validation is a security technique that checks the user input for any malicious or unexpected data before processing it by the application. Input validation can prevent various types of attacks, such as injection, cross-site scripting, buffer overflow, and command execution, that exploit the vulnerabilities in the application code. Input validation can be performed on both the client-side and the server-side, using methods such as whitelisting, blacklisting, filtering, sanitizing, escaping, and encoding. By including regular expressions in the source code to remove special characters from the variables set by the forms in the web application, the organization adopted input validation as a security technique. Regular expressions are patterns that match a specific set of characters or strings, and can be used to filter out any unwanted or harmful input. Special characters, such as $, |, ;, &, `, and ?, can be used by attackers to inject commands or scripts into the application, and cause damage or data theft. By removing these characters from the input, the organization can reduce the risk of such attacks.
Identify embedded keys, code debugging, and static code analysis are not the security techniques that the organization adopted by making this addition to the policy. Identify embedded keys is a process of finding and removing any hard-coded keys or credentials from the source code, as these can pose a security risk if exposed or compromised. Code debugging is a process of finding and fixing any errors or bugs in the source code, which can affect the functionality or performance of the application. Static code analysis is a process of analyzing the source code without executing it, to

identify any vulnerabilities, flaws, or coding standards violations. These techniques are not related to the use of regular expressions to remove special characters from the input.
Reference = CompTIA Security+ SY0-701 Certification Study Guide, page 375-376; Professor Messer's CompTIA SY0-701 Security+ Training Course, video 4.1 - Vulnerability Scanning, 8:00 - 9:08; Application Security C SY0-601 CompTIA Security+: 3.2, 0:00 - 2:00.

36.An organization experiences a cybersecurity incident involving a command-and-control server. Which of the following logs should be analyzed to identify the impacted host? (Select two).
A. Application
B. Authentication
C. DHCP
D. Network
E. Firewall
F. Database
Answer: C,E
Explanation:
To identify the impacted host in a command-and-control (C2) server incident, the following logs should be analyzed:
DHCP logs: These logs record IP address assignments. By reviewing DHCP logs, an organization can determine which host was assigned a specific IP address during the time of the attack.
Firewall logs: Firewall logs will show traffic patterns, including connections to external C2 servers. Analyzing these logs helps to identify the IP address and port numbers of the communicating host.
Application, Authentication, and Database logs are less relevant in this context because they focus on internal processes and authentication events rather than network traffic involved in a C2 attack.

37.Which of the following is a type of vulnerability that refers to the unauthorized installation of applications on a device through means other than the official application store?
A. Cross-site scripting
B. Buffer overflow
C. Jailbreaking
D. Side loading
Answer: D
Explanation:
Side loading refers to the process of installing applications on a device from outside the official app store, which can introduce security vulnerabilities by bypassing standard app validation processes.Reference: Security+ SY0-701 Course Content, Security+ SY0-601 Book.

38.Which of the following examples would be best mitigated by input sanitization?
A. <script>alert ("Warning!") ,-</script>
B. nmap - 10.11.1.130
C. Email message: "Click this link to get your free gift card."
D. Browser message: "Your connection is not private."
Answer: A
Explanation:
This example of a script injection attack would be best mitigated by input sanitization. Input sanitization involves cleaning or filtering user inputs to ensure that they do not contain harmful data, such as malicious scripts. This prevents attackers from executing script-based attacks (e.g., Cross-Site Scripting or XSS).
Nmap command is unrelated to input sanitization, as it is a network scanning tool.

Email phishing attempts require different mitigations, such as user training.
Browser warnings about insecure connections involve encryption protocols, not input validation

39.Which of the following should a security operations center use to improve its incident response procedure?
A. Playbooks
B. Frameworks
C. Baselines
D. Benchmarks
Answer: A
Explanation:
A playbook is a documented set of procedures that outlines the step-by-step response to specific types of cybersecurity incidents. Security Operations Centers (SOCs) use playbooks to improve consistency, efficiency, and accuracy during incident response. Playbooks help ensure that the correct procedures are followed based on the type of incident, ensuring swift and effective remediation. Frameworks provide general guidelines for implementing security but are not specific enough for incident response procedures.
Baselines represent normal system behavior and are used for anomaly detection, not incident response guidance.
Benchmarks are performance standards and are not directly related to incident response.

40.A security analyst receives alerts about an internal system sending a large amount of unusual DNS queries to systems on the internet over short periods of time during non-business hours.
Which of the following is most likely occurring?
A. A worm is propagating across the network.
B. Data is being exfiltrated.
C. A logic bomb is deleting data.
D. Ransomware is encrypting files.
Answer: B
Explanation:
Data exfiltration is a technique that attackers use to steal sensitive data from a target system or network by transmitting it through DNS queries and responses. This method is often used in advanced persistent threat (APT) attacks, in which attackers seek to persistently evade detection in the target environment. A large amount of unusual DNS queries to systems on the internet over short periods of time during non-business hours is a strong indicator of data exfiltration. A worm, a logic bomb, and ransomware would not use DNS queries to communicate with their command and control servers or perform their malicious actions.
Reference: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, page 487; Introduction to DNS Data Exfiltration; Identifying a DNS Exfiltration Attack That Wasn’t Real ? This Time

41.An administrator must replace an expired SSL certificate.
Which of the following does the administrator need to create the new SSL certificate?
A. CSR
B. OCSP
C. Key
D. CRL
Answer: A
Explanation:
A Certificate Signing Request (CSR) is a request sent to a certificate authority (CA) to issue an SSL

certificate. The CSR contains information like the public key, which will be part of the certificate.
Reference: Security+ SY0-701 Course Content, Security+ SY0-601 Book.

42.Which of the following incident response activities ensures evidence is properly handied?
A. E-discovery
B. Chain of custody
C. Legal hold
D. Preservation
Answer: B
Explanation:
Chain of custody is the process of documenting and preserving the integrity of evidence collected during an incident response. It involves recording the details of each person who handled the evidence, the time and date of each transfer, and the location where the evidence was stored. Chain of custody ensures that the evidence is admissible in legal proceedings and can be traced back to its source. E-discovery, legal hold, and preservation are related concepts, but they do not ensure evidence is properly handled.
Reference: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, page 487; NIST SP 800-61: 3.2. Evidence Gathering and Handling

43.A small business uses kiosks on the sales floor to display product information for customers. A security team discovers the kiosks use end-of-life operating systems.
Which of the following is the security team most likely to document as a security implication of the current architecture?
A. Patch availability
B. Product software compatibility
C. Ease of recovery
D. Cost of replacement
Answer: A
Explanation:
End-of-life operating systems are those that are no longer supported by the vendor or manufacturer, meaning they do not receive any security updates or patches. This makes them vulnerable to exploits and attacks that take advantage of known or unknown flaws in the software. Patch availability is the security implication of using end-of-life operating systems, as it affects the ability to fix or prevent security issues. Other factors, such as product software compatibility, ease of recovery, or cost of replacement, are not directly related to security, but rather to functionality, availability, or budget.
Reference: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, page 29 1

44.A systems administrator is concerned users are accessing emails through a duplicate site that is not run by the company.
Which of the following is used in this scenario?
A. Impersonation
B. Replication
C. Phishing
D. Smishing
Answer: A

45.During the onboarding process, an employee needs to create a password for an intranet account. The password must include ten characters, numbers, and letters, and two special characters. Once

the password is created, the company will grant the employee access to other company-owned websites based on the intranet profile.
Which of the following access management concepts is the company most likely using to safeguard intranet accounts and grant access to multiple sites based on a user's intranet account? (Select two).
A. Federation
B. Identity proofing
C. Password complexity
D. Default password changes
E. Password manager
F. Open authentication
Answer: A,C
Explanation:
Federation is an access management concept that allows users to authenticate once and access multiple resources or services across different domains or organizations. Federation relies on a trusted third party that stores the user's credentials and provides them to the requested resources or services without exposing them. Password complexity is a security measure that requires users to create passwords that meet certain criteria, such as length, character types, and uniqueness. Password complexity can help prevent brute-force attacks, password guessing, and credential stuffing by making passwords harder to crack or guess.
Reference: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, page 308-309 and 312-313
1

46.Which of the following methods to secure credit card data is best to use when a requirement is to see only the last four numbers on a credit card?
A. Encryption
B. Hashing
C. Masking
D. Tokenization
Answer: C
Explanation:
Masking is a method to secure credit card data that involves replacing some or all of the digits with symbols, such as asterisks, dashes, or Xs, while leaving some of the original digits visible. Masking is best to use when a requirement is to see only the last four numbers on a credit card, as it can prevent unauthorized access to the full card number, while still allowing identification and verification of the cardholder. Masking does not alter the original data, unlike encryption, hashing, or tokenization, which use algorithms to transform the data into different formats.
Reference: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, Chapter 2: Compliance and Operational Security, page 721. CompTIA Security+ Certification Kit: Exam SY0-701, 7th Edition, Chapter 2: Compliance and Operational Security, page 722.

47.Which of the following describes an executive team that is meeting in a board room and testing the company's incident response plan?
A. Continuity of operations
B. Capacity planning
C. Tabletop exercise
D. Parallel processing
Answer: C
Explanation:
A tabletop exercise involves the executive team or key stakeholders discussing and testing the company's incident response plan in a simulated environment. These exercises are low-stress,

discussion-based, and help to validate the plan's effectiveness by walking through different scenarios without disrupting actual operations. It is an essential part of testing business continuity and incident response strategies.
Continuity of operations refers to the ability of an organization to continue functioning during and after a disaster but doesn't specifically involve simulations like tabletop exercises.
Capacity planning is related to ensuring the infrastructure can handle growth, not incident response testing.
Parallel processing refers to running multiple processes simultaneously, which is unrelated to testing an incident response plan.

48.One of a company's vendors sent an analyst a security bulletin that recommends a BIOS update.
Which of the following vulnerability types is being addressed by the patch?
A. Virtualization
B. Firmware
C. Application
D. Operating system
Answer: B
Explanation:
Firmware is a type of software that is embedded in hardware devices, such as BIOS, routers, printers, or cameras. Firmware controls the basic functions and operations of the device, and can be updated or patched to fix bugs, improve performance, or enhance security. Firmware vulnerabilities are flaws or weaknesses in the firmware code that can be exploited by attackers to gain unauthorized access, modify settings, or cause damage to the device or the network. A BIOS update is a patch that addresses a firmware vulnerability in the basic input/output system of a computer, which is responsible for booting the operating system and managing the communication between the hardware and the software. The other options are not types of vulnerabilities, but rather categories of software or technology.

49.During a recent log review, an analyst discovers evidence of successful injection attacks.
Which of the following will best address this issue?
A. Authentication
B. Secure cookies
C. Static code analysis
D. Input validation
Answer: D
Explanation:
Input validation is the primary defense against injection attacks, such as SQL injection or command injection. It ensures that user-supplied data is properly sanitized before processing, preventing attackers from injecting malicious code.
Authentication (A) helps verify user identity but does not prevent injection attacks.
Secure cookies (B) improve session security but do not address injection vulnerabilities.
Static code analysis (C) helps identify vulnerabilities in source code but does not actively prevent attacks in real-time.
Reference: CompTIA Security+ SY0-701 Official Study Guide, Threats, Vulnerabilities, and Mitigations domain.

50.A legal department must maintain a backup from all devices that have been shredded and recycled by a third party.
Which of the following best describes this requirement?

A. Data retention
B. Certification
C. Sanitation
D. Destruction
Answer: A

51.A security analyst discovers that a large number of employee credentials had been stolen and were being sold on the dark web. The analyst investigates and discovers that some hourly employee credentials were compromised, but salaried employee credentials were not affected.
Most employees clocked in and out while they were Inside the building using one of the kiosks connected to the network. However, some clocked out and recorded their time after leaving to go home. Only those who clocked in and out while Inside the building had credentials stolen. Each of the kiosks are on different floors, and there are multiple routers, since the business segments environments for certain business functions.
Hourly employees are required to use a website called acmetimekeeping.com to clock in and out. This website is accessible from the internet.
Which of the following Is the most likely reason for this compromise?
A. A brute-force attack was used against the time-keeping website to scan for common passwords.
B. A malicious actor compromised the time-keeping website with malicious code using an unpatched vulnerability on the site, stealing the credentials.
C. The internal DNS servers were poisoned and were redirecting acmetimkeeping.com to malicious domain that intercepted the credentials and then passed them through to the real site
D. ARP poisoning affected the machines in the building and caused the kiosks lo send a copy of all the submitted credentials to a machine.machine.
Answer: B
Explanation:
The scenario suggests that only the employees who used the kiosks inside the building had their credentials compromised. Since the time-keeping website is accessible from the internet, it is possible that a malicious actor exploited an unpatched vulnerability in the site, allowing them to inject malicious code that captured the credentials of those who logged in from the kiosks. This is a common attack vector for stealing credentials from web applications.
Reference =
CompTIA Security+ SY0-701 Course Content: The course discusses web application vulnerabilities and how attackers can exploit them to steal credentials.

52.Which of the following would best explain why a security analyst is running daily vulnerability scans on all corporate endpoints?
A. To track the status of patch installations
B. To find shadow IT cloud deployments
C. To continuously monitor hardware inventory
D. To hunt for active attackers in the network
Answer: A
Explanation:
Detailed
Daily vulnerability scans help identify missing patches or updates across endpoints, allowing security teams to ensure compliance with patch management policies.
Reference: CompTIA Security+ SY0-701 Study Guide, Domain 4: Security Operations, Section: "Vulnerability Management".

53.A Chief Information Security Officer wants to monitor the company's servers for SQLi attacks and allow for comprehensive investigations if an attack occurs. The company uses SSL decryption to allow traffic monitoring.
Which of the following strategies would best accomplish this goal?
A. Logging all NetFlow traffic into a SIEM
B. Deploying network traffic sensors on the same subnet as the servers
C. Logging endpoint and OS-specific security logs
D. Enabling full packet capture for traffic entering and exiting the servers
Answer: D
Explanation:
Full packet capture is a technique that records all network traffic passing through a device, such as a router or firewall. It allows for detailed analysis and investigation of network events, such as SQLi attacks, by providing the complete content and context of the packets. Full packet capture can help identify the source, destination, payload, and timing of an SQLi attack, as well as the impact on the server and database. Logging NetFlow traffic, network traffic sensors, and endpoint and OS-specific security logs can provide some information about network activity, but they do not capture the full content of the packets, which may limit the scope and depth of the investigation.
Reference: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, page 372-373

54.Which of the following security concepts is being followed when implementing a product that offers protection against DDoS attacks?
A. Availability
B. Non-repudiation
C. Integrity
D. Confidentiality
Answer: C

55.In which of the following scenarios is tokenization the best privacy technique 10 use?
A. Providing pseudo-anonymization tor social media user accounts
B. Serving as a second factor for authentication requests
C. Enabling established customers to safely store credit card Information
D. Masking personal information inside databases by segmenting data
Answer: C
Explanation:
Tokenization is a process that replaces sensitive data, such as credit card information, with a non-sensitive equivalent (token) that can be used in place of the actual data. This technique is particularly useful in securely storing payment information because the token can be safely stored and transmitted without exposing the original credit card number.
Reference =
CompTIA Security+ SY0-701 Course Content: Domain 03 Security Architecture.
CompTIA Security+ SY0-601 Study Guide: Chapter on Cryptography and Data Protection.

56.Which of the following would be best suited for constantly changing environments?
A. RTOS
B. Containers
C. Embedded systems
D. SCADA
Answer: B
Explanation:

Containers are a method of virtualization that allows applications to run in isolated environments with their own dependencies, libraries, and configurations. Containers are best suited for constantly changing environments because they are lightweight, portable, scalable, and easy to deploy and update. Containers can also support microservices architectures, which enable faster and more frequent delivery of software features.
Reference: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, Chapter 10: Mobile Device Security, page 512 1

57.Which of the following control types is AUP an example of?
A. Physical
B. Managerial
C. Technical
D. Operational
Answer: B
Explanation:
An Acceptable Use Policy (AUP) is an example of a managerial control. Managerial controls are policies and procedures that govern an organization's operations, ensuring security through directives and rules. The AUP defines acceptable behavior and usage of company resources, setting guidelines for employees.
Physical controls refer to security measures like locks, fences, or security guards.
Technical controls involve security mechanisms such as firewalls or encryption.
Operational controls are procedures for maintaining security, such as backup and recovery plans.

58.Which of the following allows for the attribution of messages to individuals?
A. Adaptive identity
B. Non-repudiation
C. Authentication
D. Access logs
Answer: B
Explanation:
Non-repudiation is the ability to prove that a message or document was sent or signed by a particular person, and that the person cannot deny sending or signing it. Non-repudiation can be achieved by using cryptographic techniques, such as hashing and digital signatures, that can verify the authenticity and integrity of the message or document. Non-repudiation can be useful for legal, financial, or contractual purposes, as it can provide evidence of the origin and content of the message or document.
Reference = Non-repudiation C CompTIA Security+ SY0-701 C 1.2, CompTIA Security+ SY0-301: 6.1 C Non-repudiation, CompTIA Security+ (SY0-701) Certification Exam Objectives, Domain 1.2, page 2.

59.A security administrator is reissuing a former employee's laptop.
Which of the following is the best combination of data handling activities for the administrator to perform? (Select two).
A. Data retention
B. Certification
C. Tokenization
D. Classification
E. Sanitization
F. Enumeration

Answer: C, E

60.A systems administrator receives the following alert from a file integrity monitoring tool:
The hash of the cmd.exe file has changed.
The systems administrator checks the OS logs and notices that no patches were applied in the last two months.
Which of the following most likely occurred?
A. The end user changed the file permissions.
B. A cryptographic collision was detected.
C. A snapshot of the file system was taken.
D. A rootkit was deployed.
Answer: D
Explanation:
A rootkit is a type of malware that modifies or replaces system files or processes to hide its presence and activity. A rootkit can change the hash of the cmd.exe file, which is a command-line interpreter for Windows systems, to avoid detection by antivirus or file integrity monitoring tools. A rootkit can also grant the attacker remote access and control over the infected system, as well as perform malicious actions such as stealing data, installing backdoors, or launching attacks on other systems. A rootkit is one of the most difficult types of malware to remove, as it can persist even after rebooting or reinstalling the OS.
Reference = CompTIA Security+ Study Guide with over 500 Practice Test Questions: Exam SY0-701, 9th Edition, Chapter 4, page 147. CompTIA Security+ SY0-701 Exam Objectives, Domain 1.2, page 9.

61.A penetration tester begins an engagement by performing port and service scans against the client environment according to the rules of engagement.
Which of the following reconnaissance types is the tester performing?
A. Active
B. Passive
C. Defensive
D. Offensive
Answer: A
Explanation:
Active reconnaissance is a type of reconnaissance that involves sending packets or requests to a target and analyzing the responses. Active reconnaissance can reveal information such as open ports, services, operating systems, and vulnerabilities. However, active reconnaissance is also more likely to be detected by the target or its security devices, such as firewalls or intrusion detection systems. Port and service scans are examples of active reconnaissance techniques, as they involve probing the target for specific information.
Reference = CompTIA Security+ Certification Exam Objectives, Domain 1.1: Given a scenario, conduct reconnaissance using appropriate techniques and
tools. CompTIA Security+ Study Guide (SY0-701), Chapter 2: Reconnaissance and Intelligence Gathering, page 47. CompTIA Security+ Certification Exam SY0-701 Practice Test 1, Question 1.

62.For which of the following reasons would a systems administrator leverage a 3DES hash from an installer file that is posted on a vendor's website?
A. To test the integrity of the file
B. To validate the authenticity of the file
C. To activate the license for the file

D. To calculate the checksum of the file
Answer: A

63.A company is considering an expansion of access controls for an application that contractors and internal employees use to reduce costs.
Which of the following risk elements should the implementation team understand before granting access to the application?
A. Threshold
B. Appetite
C. Avoidance
D. Register
Answer: B
Explanation:
Risk appetite refers to the level of risk an organization is willing to accept before implementing security measures. When expanding access controls, the company must assess how much risk is acceptable in terms of data exposure, unauthorized access, and compliance obligations.
Reference: CompTIA Security+ SY0-701 Official Study Guide, Risk Management domain.

64.A systems administrator is looking for a low-cost application-hosting solution that is cloud-based.
Which of the following meets these requirements?
A. Serverless framework
B. Type 1 hvpervisor
C. SD-WAN
D. SDN
Answer: A
Explanation:
A serverless framework is a cloud-based application-hosting solution that meets the requirements of low-cost and cloud-based. A serverless framework is a type of cloud computing service that allows developers to run applications without managing or provisioning any servers. The cloud provider handles the server-side infrastructure, such as scaling, load balancing, security, and maintenance, and charges the developer only for the resources consumed by the application. A serverless framework enables developers to focus on the application logic and functionality, and reduces the operational costs and complexity of hosting applications. Some examples of serverless frameworks are AWS Lambda, Azure Functions, and Google Cloud Functions.
A type 1 hypervisor, SD-WAN, and SDN are not cloud-based application-hosting solutions that meet the requirements of low-cost and cloud-based. A type 1 hypervisor is a software layer that runs directly on the hardware and creates multiple virtual machines that can run different operating systems and applications. A type 1 hypervisor is not a cloud-based service, but a virtualization technology that can be used to create private or hybrid clouds. A type 1 hypervisor also requires the developer to manage and provision the servers and the virtual machines, which can increase the operational costs and complexity of hosting applications. Some examples of type 1 hypervisors are VMware ESXi, Microsoft Hyper-V, and Citrix XenServer.
SD-WAN (Software-Defined Wide Area Network) is a network architecture that uses software to dynamically route traffic across multiple WAN connections, such as broadband, LTE, or MPLS. SD-WAN is not a cloud-based service, but a network optimization technology that can improve the performance, reliability, and security of WAN connections. SD-WAN can be used to connect remote sites or users to cloud-based applications, but it does not host the applications itself. Some examples of SD-WAN vendors are Cisco, VMware, and Fortinet.
SDN (Software-Defined Networking) is a network architecture that decouples the control plane from the data plane, and uses a centralized controller to programmatically manage and configure the

network devices and traffic flows. SDN is not a cloud-based service, but a network automation technology that can enhance the scalability, flexibility, and efficiency of the network. SDN can be used to create virtual networks or network functions that can support cloud-based applications, but it does not host the applications itself. Some examples of SDN vendors are OpenFlow, OpenDaylight, and OpenStack.
Reference = CompTIA Security+ SY0-701 Certification Study Guide, page 264-265; Professor Messer's CompTIA SY0-701 Security+ Training Course, video 3.1 - Cloud and Virtualization, 7:40 - 10:00; [Serverless Framework]; [Type 1 Hypervisor]; [SD-WAN]; [SDN].

65.A security consultant is working with a client that wants to physically isolate its secure systems. Which of the following best describes this architecture?
A. SDN
B. Air gapped
C. Containerized
D. Highly available
Answer: B

66.A security analyst finds a rogue device during a monthly audit of current endpoint assets that are connected to the network. The corporate network utilizes 002.1X for access control. To be allowed on the network, a device must have a Known hardware address, and a valid user name and password must be entered in a captive portal.
The following is the audit report:

IP address	MAC	Host	Account
10.10.04.42	BE-AC-11-F1-E4-44	PC-NY	user1
10.10.04.30	EB-AC-11-82-42-F3	PC-CA	user3
10.10.04.59	20-BB-5A-11-52-29	PC-PA	user2
10.10.04.50	20-BB-5A-F0-E9-D1	PC-TX	user4
10.10.04.22	EB-AC-11-82-42-F3	WIN10	user3
10.10.04.26	BB-20-11-21-A2-73	PC-NJ	admin

Which of the following is the most likely way a rogue device was allowed to connect?
A. A user performed a MAC cloning attack with a personal device.
B. A DMCP failure caused an incorrect IP address to be distributed
C. An administrator bypassed the security controls for testing.
D. DNS hijacking let an attacker intercept the captive portal traffic.
Answer: A
Explanation:
The most likely way a rogue device was able to connect to the network is through a MAC cloning attack. In this attack, a personal device copies the MAC address of an authorized device, bypassing the 802.1X access control that relies on known hardware addresses for network access. The matching MAC addresses in the audit report suggest that this technique was used to gain unauthorized network access.
Reference =
CompTIA Security+ SY0-701 Course Content: Domain 03 Security Architecture.
CompTIA Security+ SY0-601 Study Guide: Chapter on Network Security and MAC Address Spoofing.

67.Which of the following should an internal auditor check for first when conducting an audit of the organization's risk management program?
A. Policies and procedures
B. Asset management
C. Vulnerability assessment
D. Business impact analysts
Answer: A

68.A systems administrator receives an alert that a company's internal file server is very slow and is only working intermittently.
The systems administrator reviews the server management software and finds the following information about the server:

ServerName	#Connections	CPU%	MEM%	Read/s	Writes/s
FileSev01	12	99.6%	97%	50KB/s	100KB/s

Which of the following indicators most likely triggered this alert?
A. Concurrent session usage
B. Network saturation
C. Account lockout
D. Resource consumption
Answer: D

69.A company is adding a clause to its AUP that states employees are not allowed to modify the operating system on mobile devices.
Which of the following vulnerabilities is the organization addressing?
A. Cross-site scripting
B. Buffer overflow
C. Jailbreaking
D. Side loading
Answer: C
Explanation:
Jailbreaking is the process of removing the restrictions imposed by the manufacturer or carrier on a mobile device, such as an iPhone or iPad. Jailbreaking allows users to install unauthorized applications, modify system settings, and access root privileges. However, jailbreaking also exposes the device to potential security risks, such as malware, spyware, unauthorized access, data loss, and voided warranty. Therefore, an organization may prohibit employees from jailbreaking their mobile devices to prevent these vulnerabilities and protect the corporate data and network.
Reference: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, Chapter 10: Mobile Device Security, page 507 2

70.An organization has a new regulatory requirement to implement corrective controls on a financial system.
Which of the following is the most likely reason for the new requirement?
A. To defend against insider threats altering banking details
B. To ensure that errors are not passed to other systems
C. To allow for business insurance to be purchased
D. To prevent unauthorized changes to financial data

Answer: D
Explanation:
Detailed
Corrective controls, such as auditing and versioning, help prevent unauthorized changes to financial data, ensuring data integrity and compliance with regulations.
Reference: CompTIA Security+ SY0-701 Study Guide, Domain 5: Security Program Management, Section: "Controls for Financial Systems".

71.A company relies on open-source software libraries to build the software used by its customers. Which of the following vulnerability types would be the most difficult to remediate due to the company's reliance on open-source libraries?
A. Buffer overflow
B. SQL injection
C. Cross-site scripting
D. Zero day
Answer: D
Explanation:
Zero-day vulnerabilities are unknown flaws in software, making them harder to patch, especially when using open-source libraries without dedicated support teams. ==========

72.A company is concerned about the theft of client data from decommissioned laptops.
Which of the following is the most cost-effective method to decrease this risk?
A. Wiping
B. Recycling
C. Shredding
D. Deletion
Answer: A
Explanation:
Wiping involves securely erasing data by overwriting the hard drive, ensuring the information is unrecoverable. It is cost-effective compared to physical destruction methods like shredding.

73.Which of the following is a possible consequence of a VM escape?
A. Malicious instructions can be inserted into memory and give the attacker elevated permissions.
B. An attacker can access the hypervisor and compromise other VMs.
C. Unencrypted data can be read by a user in a separate environment.
D. Users can install software that is not on the manufacturer's approved list.
Answer: B
Explanation:
Detailed A VM escape occurs when an attacker breaks out of a virtual machine's isolation to access the hypervisor. This compromise can allow control of the hypervisor and all other VMs on the host, posing significant security risks.
Reference: CompTIA Security+ SY0-701 Study Guide, Domain 3: Security Architecture, Section: "Virtualization Risks and Mitigation".

74.An organization would like to calculate the time needed to resolve a hardware issue with a server. Which of the following risk management processes describes this example?
A. Recovery point objective
B. Mean time between failures

C. Recovery time objective
D. Mean time to repair
Answer: D

75.A security analyst is evaluating a SaaS application that the human resources department would like to implement. The analyst requests a SOC 2 report from the SaaS vendor.
Which of the following processes is the analyst most likely conducting?
A. Internal audit
B. Penetration testing
C. Attestation
D. Due diligence
Answer: D

76.A new employee logs in to the email system for the first time and notices a message from human resources about onboarding. The employee hovers over a few of the links within the email and discovers that the links do not correspond to links associated with the company.
Which of the following attack vectors is most likely being used?
A. Business email
B. Social engineering
C. Unsecured network
D. Default credentials
Answer: B
Explanation:
The employee notices that the links in the email do not correspond to the company's official URLs, indicating that this is likely a social engineering attack. Social engineering involves manipulating individuals into divulging confidential information or performing actions that may compromise security. Phishing emails, like the one described, often contain fraudulent links to trick the recipient into providing sensitive information or downloading malware.
Business email refers to business email compromise (BEC), which typically involves impersonating a high-level executive to defraud the company.
Unsecured network is unrelated to the email content.
Default credentials do not apply here, as the issue is with suspicious links, not login credentials.

77.Security controls in a data center are being reviewed to ensure data is properly protected and that human life considerations are included.
Which of the following best describes how the controls should be set up?
A. Remote access points should fail closed.
B. Logging controls should fail open.
C. Safety controls should fail open.
D. Logical security controls should fail closed.
Answer: C
Explanation:
Safety controls are security controls that are designed to protect human life and physical assets from harm or damage. Examples of safety controls include fire alarms, sprinklers, emergency exits, backup generators, and surge protectors. Safety controls should fail open, which means that they should remain operational or allow access when a failure or error occurs. Failing open can prevent or minimize the impact of a disaster, such as a fire, flood, earthquake, or power outage, on human life and physical assets. For example, if a fire alarm fails, it should still trigger the sprinklers and unlock the emergency exits, rather than remain silent and locked. Failing open can also ensure that essential

services, such as healthcare, transportation, or communication, are available during a crisis. Remote access points, logging controls, and logical security controls are other types of security controls, but they should not fail open in a data center. Remote access points are security controls that allow users or systems to access a network or a system from a remote location, such as a VPN, a web portal, or a wireless access point. Remote access points should fail closed, which means that they should deny access when a failure or error occurs. Failing closed can prevent unauthorized or malicious access to the data center's network or systems, such as by hackers, malware, or rogue devices. Logging controls are security controls that record and monitor the activities and events that occur on a network or a system, such as user actions, system errors, security incidents, or performance metrics. Logging controls should also fail closed, which means that they should stop or suspend the activities or events when a failure or error occurs. Failing closed can prevent data loss, corruption, or tampering, as well as ensure compliance with regulations and standards. Logical security controls are security controls that use software or code to protect data and systems from unauthorized or malicious access, modification, or destruction, such as encryption, authentication, authorization, or firewall. Logical security controls should also fail closed, which means that they should block or restrict access when a failure or error occurs. Failing closed can prevent data breaches, cyberattacks, or logical flaws, as well as ensure confidentiality, integrity, and availability of data and systems.
Reference: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, page 142-143, 372-373, 376-377