CompTIA

Exam Questions SY0-701

CompTIA Security+ Exam

About Exambible

Your Partner of IT Exam

Found in 1998

Exambible is a company specialized on providing high quality IT exam practice study materials, especially Cisco CCNA, CCDA, CCNP, CCIE, Checkpoint CCSE, CompTIA A+, Network+ certification practice exams and so on. We guarantee that the candidates will not only pass any IT exam at the first attempt but also get profound understanding about the certificates they have got. There are so many alike companies in this industry, however, Exambible has its unique advantages that other companies could not achieve.

Our Advances

* 99.9% Uptime

All examinations will be up to date.

* 24/7 Quality Support

We will provide service round the clock.

* 100% Pass Rate

Our guarantee that you will pass the exam.

* Unique Gurantee

If you do not pass the exam at the first time, we will not only arrange FULL REFUND for you, but also provide you another exam of your claim, ABSOLUTELY FREE!

NEW QUESTION 1
Which of the following agreement types defines the time frame in which a vendor needs to respond?

A. SOW
B. SLA
C. MOA
D. MOU

Answer: B

Explanation:
A service level agreement (SLA) is a type of agreement that defines the expectations and responsibilities between a service provider and a customer. It usually includes the quality, availability, and performance metrics of the service, as well as the time frame in which the provider needs to respond to service requests, incidents, or complaints. An SLA can help ensure that the customer receives the desired level of service and that the provider is accountable for meeting the agreed-upon standards.
References:
? Security+ (Plus) Certification | CompTIA IT Certifications, under “About the exam”, bullet point 3: “Operate with an awareness of applicable regulations and policies, including principles of governance, risk, and compliance.”
? CompTIA Security+ Certification Kit: Exam SY0-701, 7th Edition, Chapter 1, page 14: “Service Level Agreements (SLAs) are contracts between a service provider and a customer that specify the level of service expected from the service provider.”

NEW QUESTION 2
Which of the following is the best reason to complete an audit in a banking environment?

A. Regulatory requirement
B. Organizational change
C. Self-assessment requirement
D. Service-level requirement

Answer: A

Explanation:
A regulatory requirement is a mandate imposed by a government or an authority that must be followed by an organization or an individual. In a banking environment, audits are often required by regulators to ensure compliance with laws, standards, and policies related to security, privacy, and financial reporting. Audits help to identify and correct any gaps or weaknesses in the security posture and the internal controls of the organization. References:
? Official CompTIA Security+ Study Guide (SY0-701), page 507
? Security+ (Plus) Certification | CompTIA IT Certifications 2

NEW QUESTION 3
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.
References: 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.

NEW QUESTION 4
An administrator assists the legal and compliance team with ensuring information about customer transactions is archived for the proper time period. Which of the following data policies is the administrator carrying out?

A. Compromise
B. Retention
C. Analysis
D. Transfer
E. Inventory

Answer: B

Explanation:
A data retention policy is a set of rules that defines how long data should be stored and when it should be deleted or archived. An administrator assists the legal and compliance team with ensuring information about customer transactions is archived for the proper time period by following the data retention policy of the organization. This policy helps the organization to comply with legal and regulatory requirements, optimize storage space, and protect data privacy and security.
References
? CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, Chapter 3, Section 3.4, page 1211
? CompTIA Security+ Practice Tests: Exam SY0-701, 3rd Edition, Chapter 3, Question 15, page 832

NEW QUESTION 5

An administrator is reviewing a single server's security logs and discovers the following;

Keywords	Date and Time	Source	Event ID	Task Category
Audit Failure	09/16/2022 11:13:05 AM	Microsoft Windows security	4625	Logon
Audit Failure	09/16/2022 11:13:07 AM	Microsoft Windows security	4625	Logon
Audit Failure	09/16/2022 11:13:09 AM	Microsoft Windows security	4625	Logon
Audit Failure	09/16/2022 11:13:11 AM	Microsoft Windows security	4625	Logon
Audit Failure	09/16/2022 11:13:13 AM	Microsoft Windows security	4625	Logon
Audit Failure	09/16/2022 11:13:15 AM	Microsoft Windows security	4625	Logon
Audit Failure	09/16/2022 11:13:17 AM	Microsoft Windows security	4625	Logon
Audit Failure	09/16/2022 11:13:19 AM	Microsoft Windows security	4625	Logon
Audit Failure	09/16/2022 11:13:21 AM	Microsoft Windows security	4625	Logon
Audit Failure	09/16/2022 11:13:23 AM	Microsoft Windows security	4625	Logon
Audit Failure	09/16/2022 11:13:25 AM	Microsoft Windows security	4625	Logon
Audit Failure	09/16/2022 11:13:27 AM	Microsoft Windows security	4625	Logon

Which of the following best describes the action captured in this log file?

A. Brute-force attack
B. Privilege escalation
C. Failed password audit
D. Forgotten password by the user

Answer: A

Explanation:
A brute-force attack is a type of attack that involves systematically trying all possible combinations of passwords or keys until the correct one is found. The log file shows multiple failed login attempts in a short amount of time, which is a characteristic of a brute-force attack. The attacker is trying to guess the password of the Administrator account on the server. The log file also shows the event ID 4625, which indicates a failed logon attempt, and the status code 0xC000006A, which means the user name is correct but the password is wrong. These are indicators of compromise (IoC) that suggest a brute- force attack is taking place.
References: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, page 215-216 and 223 1

NEW QUESTION 6
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. References: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, Chapter 10: Mobile Device Security, page 512 1

NEW QUESTION 7
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. References = Non- repudiation – CompTIA Security+ SY0-701 – 1.2, CompTIA Security+ SY0-301: 6.1 – Non-repudiation, CompTIA Security+ (SY0-701) Certification Exam Objectives, Domain 1.2, page 2.

NEW QUESTION 8
Which of the following enables the use of an input field to run commands that can view or manipulate data?

A. Cross-site scripting
B. Side loading
C. Buffer overflow
D. SQL injection

Answer: D

Explanation:
= SQL injection is a type of attack that enables the use of an input field to run commands that can view or manipulate data in a database. SQL stands for Structured Query Language, which is a language used to communicate with databases. By injecting malicious SQL statements into an input field, an attacker can bypass authentication, access sensitive information, modify or delete data, or execute commands on the server.
SQL injection is one of the most common and dangerous web application
vulnerabilities. References = CompTIA Security+ Study Guide with over 500 Practice Test Questions: Exam SY0-701, 9th Edition, Chapter 5, page 195. CompTIA Security+ SY0-701 Exam Objectives, Domain 1.1, page 8.

NEW QUESTION 9
A company prevented direct access from the database administrators' workstations to the network segment that contains database servers. Which of the following should a database administrator use to access the database servers?

A. Jump server
B. RADIUS
C. HSM
D. Load balancer

Answer: A

Explanation:
A jump server is a device or virtual machine that acts as an intermediary between a user's workstation and a remote network segment. A jump server can be used to securely access servers or devices that are not directly reachable from the user's workstation, such as database servers. A jump server can also provide audit logs and access control for the remote connections. A jump server is also known as a jump box or a jump host12.
RADIUS is a protocol for authentication, authorization, and accounting of network access. RADIUS is not a device or a method to access remote servers, but rather a way to verify the identity and permissions of users or devices that request network access34. HSM is an acronym for Hardware Security Module, which is a physical device that provides secure storage and generation of cryptographic keys. HSMs are used to protect sensitive data and applications, such as digital signatures, encryption, and authentication. HSMs are not used to access remote servers, but rather to enhance the security of the data and applications that reside on them5 .
A load balancer is a device or software that distributes network traffic across multiple servers or devices, based on criteria such as availability, performance, or capacity. A load balancer can improve the scalability, reliability, and efficiency of network services, such as web servers, application servers, or database servers. A load balancer is not used to access remote servers, but rather to optimize the delivery of the services that run on them. References =
? How to access a remote server using a jump host
? Jump server
? RADIUS
? Remote Authentication Dial-In User Service (RADIUS)
? Hardware Security Module (HSM)
? [What is an HSM?]
? [Load balancing (computing)]
? [What is Load Balancing?]

NEW QUESTION 10
Which of the following provides the details about the terms of a test with a third-party penetration tester?

A. Rules of engagement
B. Supply chain analysis
C. Right to audit clause
D. Due diligence

Answer: A

Explanation:
Rules of engagement are the detailed guidelines and constraints regarding the execution of information security testing, such as penetration testing. They define the scope, objectives, methods, and boundaries of the test, as well as the roles and responsibilities of the testers and the clients. Rules of engagement help to ensure that the test is conducted in a legal, ethical, and professional manner, and that the results are accurate and reliable. Rules of engagement typically include the following elements:
? The type and scope of the test, such as black box, white box, or gray box, and the target systems, networks, applications, or data.
? The client contact details and the communication channels for reporting issues, incidents, or emergencies during the test.
? The testing team credentials and the authorized tools and techniques that they can use.
? The sensitive data handling and encryption requirements, such as how to store, transmit, or dispose of any data obtained during the test.
? The status meeting and report schedules, formats, and recipients, as well as the confidentiality and non-disclosure agreements for the test results.
? The timeline and duration of the test, and the hours of operation and testing windows.
? The professional and ethical behavior expectations for the testers, such as avoiding unnecessary damage, disruption, or disclosure of information.
Supply chain analysis, right to audit clause, and due diligence are not related to the terms of a test with a third-party penetration tester. Supply chain analysis is the process of evaluating the security and risk posture of the suppliers and partners in a business network. Right to audit clause is a provision in a contract that gives one party the right to audit another party to verify their compliance with the contract terms and conditions. Due diligence is the process of identifying and addressing the cyber risks that a potential vendor or partner brings to an organization.

References = https://www.yeahhub.com/every-penetration-tester-you-should-know-about- this-rules-of-engagement/
https://bing.com/search?q=rules+of+engagement+penetration+testing

NEW QUESTION 10
Which of the following practices would be best to prevent an insider from introducing malicious code into a company's development process?

A. Code scanning for vulnerabilities
B. Open-source component usage
C. Quality assurance testing
D. Peer review and approval

Answer: D

Explanation:
Peer review and approval is a practice that involves having other developers or experts review the code before it is deployed or released. Peer review and approval can help detect and prevent malicious code, errors, bugs, vulnerabilities, and poor quality in the development process. Peer review and approval can also enforce coding standards, best practices, and compliance requirements. Peer review and approval can be done manually or with the help of tools, such as code analysis, code review, and code
signing. References: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, Chapter 11: Secure Application Development, page 543 2

NEW QUESTION 15
A technician is opening ports on a firewall for a new system being deployed and supported by a SaaS provider. Which of the following is a risk in the new system?

A. Default credentials
B. Non-segmented network
C. Supply chain vendor
D. Vulnerable software

Answer: C

Explanation:
A supply chain vendor is a third-party entity that provides goods or services to an organization, such as a SaaS provider. A supply chain vendor can pose a risk to the new system if the vendor has poor security practices, breaches, or compromises that could affect the confidentiality, integrity, or availability of the system or its data. The organization should perform due diligence and establish a service level agreement with the vendor to mitigate this risk. The other options are not specific to the scenario of using a SaaS provider, but rather general risks that could apply to any system.

NEW QUESTION 16
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. References: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, Chapter 10: Mobile Device Security, page 507 2

NEW QUESTION 19
A security administrator needs a method to secure data in an environment that includes some form of checks so that the administrator can track any changes. Which of the following should the administrator set up to achieve this goal?

A. SPF
B. GPO
C. NAC
D. FIM

Answer: D

Explanation:
FIM stands for File Integrity Monitoring, which is a method to secure data by detecting any changes or modifications to files, directories, or registry keys. FIM can help a security administrator track any unauthorized or malicious changes to the data, as well as verify the integrity and compliance of the data. FIM can also alert the administrator of any potential breaches or incidents involving the data.
Some of the benefits of FIM are:
? It can prevent data tampering and corruption by verifying the checksums or hashes of the files.
? It can identify the source and time of the changes by logging the user and system actions.
? It can enforce security policies and standards by comparing the current state of the data with the baseline or expected state.
? It can support forensic analysis and incident response by providing evidence and audit trails of the changes.
References:
? CompTIA Security+ SY0-701 Certification Study Guide, Chapter 5: Technologies and Tools, Section 5.3: Security Tools, p. 209-210
? CompTIA Security+ SY0-701 Certification Exam Objectives, Domain 2: Technologies and Tools, Objective 2.4: Given a scenario, analyze and interpret output from security technologies, Sub-objective: File integrity monitor, p. 12

NEW QUESTION 22
Which of the following is a primary security concern for a company setting up a BYOD program?

A. End of life
B. Buffer overflow
C. VM escape
D. Jailbreaking

Answer: D

Explanation:
Jailbreaking is a primary security concern for a company setting up a BYOD (Bring Your Own Device) program. Jailbreaking is the process of removing the manufacturer's or the carrier's restrictions on a device, such as a smartphone or a tablet, to gain root access and install unauthorized or custom software. Jailbreaking can compromise the security of the device and the data stored on it, as well as expose it to malware, viruses, or hacking. Jailbreaking can also violate the warranty and the terms of service of the device, and make it incompatible with the company's security policies and standards. Therefore, a company setting up a BYOD program should prohibit jailbreaking and enforce device compliance and encryption. References = CompTIA Security+ Study Guide with over 500 Practice Test Questions: Exam SY0-701, 9th Edition, Chapter 2, page 76. CompTIA Security+ SY0-701 Exam Objectives, Domain 2.4, page 11.

NEW QUESTION 27
A hacker gained access to a system via a phishing attempt that was a direct result of a user clicking a suspicious link. The link laterally deployed ransomware, which laid dormant for multiple weeks, across the network. Which of the following would have mitigated the spread?

A. IPS
B. IDS
C. WAF
D. UAT

Answer: A

Explanation:
IPS stands for intrusion prevention system, which is a network security device that monitors and blocks malicious traffic in real time. IPS is different from IDS, which only detects and alerts on malicious traffic, but does not block it. IPS would have mitigated the spread of ransomware by preventing the hacker from accessing the system via the phishing link, or by stopping the ransomware from communicating with its command and control server or encrypting the files.

NEW QUESTION 30
An organization disabled unneeded services and placed a firewall in front of a business- critical legacy system. Which of the following best describes the actions taken by the organization?

A. Exception
B. Segmentation
C. Risk transfer
D. Compensating controls

Answer: D

Explanation:
Compensating controls are alternative security measures that are implemented when the primary controls are not feasible, cost-effective, or sufficient to mitigate the risk. In this case, the organization used compensating controls to protect the legacy system from potential attacks by disabling unneeded services and placing a firewall in front of it. This reduced the attack surface and the likelihood of exploitation.
References:
? Official CompTIA Security+ Study Guide (SY0-701), page 29
? Security Controls - CompTIA Security+ SY0-701 - 1.1 1

NEW QUESTION 33
An employee clicked a link in an email from a payment website that asked the employee to update contact information. The employee entered the log-in information but received a "page not found" error message. Which of the following types of social engineering attacks occurred?

A. Brand impersonation
B. Pretexting
C. Typosquatting
D. Phishing

Answer: D

Explanation:
Phishing is a type of social engineering attack that involves sending fraudulent emails that appear to be from legitimate sources, such as payment websites, banks, or other trusted entities. The goal of phishing is to trick the recipients into clicking on malicious links, opening malicious attachments, or providing sensitive information, such as log-in credentials, personal data, or financial details. In this scenario, the employee received an email from a payment website that asked the employee to update contact information. The email contained a link that directed the employee to a fake website that mimicked the appearance of the real one. The employee entered the log-in information, but received a "page not found" error message. This indicates that the employee fell victim to a phishing attack, and the attacker may have captured the employee's credentials for the payment website. References = Other Social Engineering Attacks – CompTIA Security+ SY0-701 – 2.2, CompTIA Security+: Social Engineering Techniques & Other Attack … - NICCS, [CompTIA Security+ Study Guide with over 500 Practice Test Questions: Exam SY0-701, 9th Edition]

NEW QUESTION 34
Which of the following threat actors is the most likely to be hired by a foreign government to attack critical systems located in other countries?

A. Hacktivist
B. Whistleblower

C. Organized crime
D. Unskilled attacker

Answer: C

Explanation:
Organized crime is a type of threat actor that is motivated by financial gain and often operates across national borders. Organized crime groups may be hired by foreign governments to conduct cyberattacks on critical systems located in other countries, such as power grids, military networks, or financial institutions. Organized crime groups have the resources, skills, and connections to carry out sophisticated and persistent attacks that can cause significant damage and disruption12. References = 1: Threat Actors - CompTIA Security+ SY0-701 - 2.1 2: CompTIA Security+ SY0-701 Certification Study Guide

NEW QUESTION 38
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. References: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, page
137 1

NEW QUESTION 43
A security engineer is implementing FDE for all laptops in an organization. Which of the following are the most important for the engineer to consider as part of the planning process? (Select two).

A. Key escrow
B. TPM presence
C. Digital signatures
D. Data tokenization
E. Public key management
F. Certificate authority linking

Answer: AB

Explanation:
? Key escrow is a method of storing encryption keys in a secure location, such as a trusted third party or a hardware security module (HSM). Key escrow is important for FDE because it allows the recovery of encrypted data in case of lost or forgotten passwords, device theft, or hardware failure. Key escrow also enables authorized access to encrypted data for legal or forensic purposes.
? TPM presence is a feature of some laptops that have a dedicated chip for storing encryption keys and other security information. TPM presence is important for FDE because it enhances the security and performance of encryption by generating and protecting the keys within the chip, rather than relying on software or external devices. TPM presence also enables features such as secure boot, remote attestation, and device authentication.

NEW QUESTION 46
After a security awareness training session, a user called the IT help desk and reported a suspicious call. The suspicious caller stated that the Chief Financial Officer wanted credit card information in order to close an invoice. Which of the following topics did the user recognize from the training?

A. Insider threat
B. Email phishing
C. Social engineering
D. Executive whaling

Answer: C

Explanation:
Social engineering is the practice of manipulating people into performing actions or divulging confidential information, often by impersonating someone else or creating a sense of urgency or trust. The suspicious caller in this scenario was trying to use social engineering to trick the user into giving away credit card information by pretending to be the CFO and asking for a payment. The user recognized this as a potential scam and reported it to the IT help desk. The other topics are not relevant to this
situation. References: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, page 19 1

NEW QUESTION 47
A security analyst reviews domain activity logs and notices the following:

```
UserID jsmith, password authentication: succeeded, MFA: failed (invalid code)
UserID jsmith, password authentication: succeeded, MFA: failed (invalid code)
UserID jsmith, password authentication: succeeded, MFA: failed (invalid code)
UserID jsmith, password authentication: succeeded, MFA: failed (invalid code)
```

Which of the following is the best explanation for what the security analyst has discovered?

A. The user jsmith's account has been locked out.

B. A keylogger is installed on [smith's workstation
C. An attacker is attempting to brute force ismith's account.
D. Ransomware has been deployed in the domain.

Answer: C

Explanation:
Brute force is a type of attack that tries to guess the password or other credentials of a user account by using a large number of possible combinations. An attacker can use automated tools or scripts to perform a brute force attack and gain unauthorized access to the account. The domain activity logs show that the user ismith has failed to log in 10 times in a row within a short period of time, which is a strong indicator of a brute force attack. The logs also show that the source IP address of the failed logins is different from the usual IP address of ismith, which suggests that the attacker is using a different device or location to launch the attack. The security analyst should take immediate action to block the attacker's IP address, reset ismith's password, and notify ismith of the incident. References = CompTIA Security+ Study Guide with over 500 Practice Test Questions: Exam SY0-701, 9th Edition, Chapter 1, page 14. CompTIA Security+ (SY0-701) Certification Exam Objectives, Domain 1.1, page 2. Threat Actors and Attributes – SY0-601 CompTIA Security+ : 1.1

NEW QUESTION 51
An administrator was notified that a user logged in remotely after hours and copied large amounts of data to a personal device.
Which of the following best describes the user's activity?

A. Penetration testing
B. Phishing campaign
C. External audit
D. Insider threat

Answer: D

Explanation:
An insider threat is a security risk that originates from within the organization, such as an employee, contractor, or business partner, who has authorized access to the organization's data and systems. An insider threat can be malicious, such as stealing, leaking, or sabotaging sensitive data, or unintentional, such as falling victim to phishing or social engineering. An insider threat can cause significant damage to the organization's reputation, finances, operations, and legal compliance. The user's activity of logging in remotely after hours and copying large amounts of data to a personal device is an example of a malicious insider threat, as it violates the organization's security policies and compromises the confidentiality and integrity of the data. References = Insider Threats – CompTIA Security+ SY0-701: 3.2, video at 0:00; CompTIA Security+ SY0-701 Certification Study Guide, page 133.

NEW QUESTION 52
A company has begun labeling all laptops with asset inventory stickers and associating them with employee IDs. Which of the following security benefits do these actions provide? (Choose two.)

A. If a security incident occurs on the device, the correct employee can be notified.
B. The security team will be able to send user awareness training to the appropriate device.
C. Users can be mapped to their devices when configuring software MFA tokens.
D. User-based firewall policies can be correctly targeted to the appropriate laptops.
E. When conducting penetration testing, the security team will be able to target the desired laptops.
F. Company data can be accounted for when the employee leaves the organization.

Answer: AF

Explanation:
Labeling all laptops with asset inventory stickers and associating them with employee IDs can provide several security benefits for a company. Two of these benefits are:
? A. If a security incident occurs on the device, the correct employee can be notified.
An asset inventory sticker is a label that contains a unique identifier for a laptop, such as a serial number, a barcode, or a QR code. By associating this identifier with an employee ID, the security team can easily track and locate the owner of the laptop in case of a security incident, such as a malware infection, a data breach, or a theft. This way, the security team can notify the correct employee about the incident, and provide them with the necessary instructions or actions to take, such as changing passwords, scanning for viruses, or reporting the loss. This can help to contain the incident, minimize the damage, and prevent further escalation.
? F. Company data can be accounted for when the employee leaves the
organization. When an employee leaves the organization, the company needs to ensure that all the company data and assets are returned or deleted from the employee's laptop. By labeling the laptop with an asset inventory sticker and
associating it with an employee ID, the company can easily identify and verify the laptop that belongs to the departing employee, and perform the appropriate data backup, wipe, or transfer procedures. This can help to protect the company data from unauthorized access, disclosure, or misuse by the former employee or any other party.
The other options are not correct because they are not related to the security benefits of labeling laptops with asset inventory stickers and associating them with employee IDs. B. The security team will be able to send user awareness training to the appropriate device. User awareness training is a type of security education that aims to improve the knowledge and behavior of users regarding security threats and best practices. The security team can send user awareness training to the appropriate device by using the email address, username, or IP address of the device, not the asset inventory sticker or the employee ID.
* C. Users can be mapped to their devices when configuring software MFA tokens. Software MFA tokens are a type of multi-factor authentication that uses a software application to generate a one-time password or a push notification for verifying the identity of a user. Users can be mapped to their devices when configuring software MFA tokens by using the device ID, phone number, or email address of the device, not the asset inventory sticker or the employee ID. D. User-based firewall policies can be correctly targeted to the appropriate laptops. User-based firewall policies are a type of firewall rules that apply to specific users or groups of users, regardless of the device or location they use to access the network. User-based firewall policies can be correctly targeted to the appropriate laptops by using the username, domain, or certificate of the user, not the asset inventory sticker or the employee ID. E. When conducting penetration testing, the security team will be able to target the desired laptops. Penetration testing is a type of security assessment that simulates a real-world attack on a network or system to identify and exploit vulnerabilities. When conducting penetration testing, the security team will be able to target the desired laptops by using the IP address, hostname, or MAC address of the laptop, not
the asset inventory sticker or the employee ID. References = CompTIA Security+ Study Guide (SY0-701), Chapter 1: General Security Concepts, page 17. Professor Messer's CompTIA SY0-701 Security+ Training Course, Section 1.4: Asset Management, video: Asset Inventory (6:12).

NEW QUESTION 53
Which of the following must be considered when designing a high-availability network? (Select two).

A. Ease of recovery
B. Ability to patch
C. Physical isolation
D. Responsiveness
E. Attack surface
F. Extensible authentication

Answer: AE

Explanation:
A high-availability network is a network that is designed to minimize downtime and ensure continuous operation of critical services and applications. To achieve this goal, a high-availability network must consider two important factors: ease of recovery and attack surface.
Ease of recovery refers to the ability of a network to quickly restore normal functionality after a failure, disruption, or disaster. A high-availability network should have mechanisms such as redundancy, failover, backup, and restore to ensure that any single point of failure does not cause a complete network outage. A high-availability network should also have procedures and policies for incident response, disaster recovery, and business continuity to minimize the impact of any network issue on the organization's operations and reputation. Attack surface refers to the exposure of a network to potential threats and vulnerabilities. A high-availability network should have measures such as encryption, authentication, authorization, firewall, intrusion detection and prevention, and patch management to protect the network from unauthorized access, data breaches, malware, denial-of-service attacks, and other cyberattacks. A high-availability network should also have processes and tools for risk assessment, threat intelligence, vulnerability scanning, and penetration testing to identify and mitigate any weaknesses or gaps in the network security. References: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, Chapter 4:
Architecture and Design, pages 164-1651. CompTIA Security+ Certification Kit: Exam SY0- 701, 7th Edition, Chapter 4: Architecture and Design, pages 164-1652.

NEW QUESTION 55
A company decided to reduce the cost of its annual cyber insurance policy by removing the coverage for ransomware attacks.
Which of the following analysis elements did the company most likely use in making this decision?

A. IMTTR
B. RTO
C. ARO
D. MTBF

Answer: C

Explanation:
ARO (Annualized Rate of Occurrence) is an analysis element that measures the frequency or likelihood of an event happening in a given year. ARO is often used in risk assessment and management, as it helps to estimate the potential loss or impact of an event. A company can use ARO to calculate the annualized loss expectancy (ALE) of an event, which is the product of ARO and the single loss expectancy (SLE). ALE represents the expected cost of an event per year, and can be used to compare with the cost of implementing a security control or purchasing an insurance policy.
The company most likely used ARO in making the decision to remove the coverage for ransomware attacks from its cyber insurance policy. The company may have estimated the ARO of ransomware attacks based on historical data, industry trends, or threat intelligence, and found that the ARO was low or negligible. The company may have also calculated the ALE of ransomware attacks, and found that the ALE was lower than the cost of the insurance policy. Therefore, the company decided to reduce the cost of its annual cyber insurance policy by removing the coverage for ransomware attacks, as it deemed the risk to be acceptable or manageable.
IMTTR (Incident Management Team Training and Readiness), RTO (Recovery Time Objective), and MTBF (Mean Time Between Failures) are not analysis elements that the company most likely used in making the decision to remove the coverage for ransomware attacks from its cyber insurance policy. IMTTR is a process of preparing and training the incident management team to respond effectively to security incidents. IMTTR does not measure the frequency or impact of an event, but rather the capability and readiness of the team. RTO is a metric that defines the maximum acceptable time for restoring a system or service after a disruption. RTO does not measure the frequency or impact of an event, but rather the availability and continuity of the system or service. MTBF is a metric that measures the average time between failures of a system or component. MTBF does not measure the frequency or impact of an event, but rather the reliability and performance of the system or component.
References = CompTIA Security+ SY0-701 Certification Study Guide, page 97-
98; Professor Messer's CompTIA SY0-701 Security+ Training Course, video 5.2 - Risk Management, 0:00 - 3:00.

NEW QUESTION 57
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.

NEW QUESTION 58
Which of the following factors are the most important to address when formulating a training curriculum plan for a security awareness program? (Select two).

A. Channels by which the organization communicates with customers
B. The reporting mechanisms for ethics violations
C. Threat vectors based on the industry in which the organization operates
D. Secure software development training for all personnel
E. Cadence and duration of training events

F. Retraining requirements for individuals who fail phishing simulations

Answer: CE

Explanation:
A training curriculum plan for a security awareness program should address the following factors:
? The threat vectors based on the industry in which the organization operates. This will help the employees to understand the specific risks and challenges that their organization faces, and how to protect themselves and the organization from cyberattacks. For example, a healthcare organization may face different threat vectors than a financial organization, such as ransomware, data breaches, or medical device hacking1.
? The cadence and duration of training events. This will help the employees to retain
the information and skills they learn, and to keep up with the changing security landscape. The training events should be frequent enough to reinforce the key concepts and behaviors, but not too long or too short to lose the attention or interest of the employees. For example, a security awareness program may include monthly newsletters, quarterly webinars, annual workshops, or periodic quizzes2.
References: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, Chapter 2, page 34; CompTIA Security+ Certification Kit: Exam SY0-701, 7th Edition, Chapter 2, page 55.

NEW QUESTION 59
Users at a company are reporting they are unable to access the URL for a new retail website because it is flagged as gambling and is being blocked.
Which of the following changes would allow users to access the site?

A. Creating a firewall rule to allow HTTPS traffic
B. Configuring the IPS to allow shopping
C. Tuning the DLP rule that detects credit card data
D. Updating the categorization in the content filter

Answer: D

Explanation:
A content filter is a device or software that blocks or allows access to web content based on predefined rules or categories. In this case, the new retail website is mistakenly categorized as gambling by the content filter, which prevents users from accessing it. To resolve this issue, the content filter's categorization needs to be updated to reflect the correct category of the website, such as shopping or retail. This will allow the content filter to allow access to the website instead of blocking it.
References: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, Chapter 3: Technologies and Tools, page 1221. CompTIA Security+ Certification Kit: Exam SY0-701, 7th Edition, Chapter 3: Technologies and Tools, page 1222.

NEW QUESTION 64
A healthcare organization wants to provide a web application that allows individuals to digitally report health emergencies.
Which of the following is the most important consideration during development?

A. Scalability
B. Availability
C. Cost
D. Ease of deployment

Answer: B

Explanation:
Availability is the ability of a system or service to be accessible and usable when needed. For a web application that allows individuals to digitally report health emergencies, availability is the most important consideration during development, because any downtime or delay could have serious consequences for the health and safety of the users. The web application should be designed to handle high traffic, prevent denial-of- service attacks, and have backup and recovery plans in case of failures2.
References: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, Chapter 2, page 41.

NEW QUESTION 69
A company is developing a business continuity strategy and needs to determine how many staff members would be required to sustain the business in the case of a disruption. Which of the following best describes this step?

A. Capacity planning
B. Redundancy
C. Geographic dispersion
D. Tablet exercise

Answer: A

Explanation:
Capacity planning is the process of determining the resources needed to meet the current and future demands of an organization. Capacity planning can help a company develop a business continuity strategy by estimating how many staff members would be required to sustain the business in the case of a disruption, such as a natural disaster, a cyberattack, or a pandemic. Capacity planning can also help a company optimize the use of its resources, reduce costs, and improve performance. References = CompTIA Security+ Study Guide with over 500 Practice Test Questions: Exam SY0-701, 9th Edition, Chapter 4, page 184. CompTIA Security+ (SY0-701) Certification Exam Objectives, Domain 4.1, page 14. Business Continuity – SY0-601 CompTIA Security+ : 4.1

NEW QUESTION 72
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. References = 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 – SY0-601 CompTIA Security+ : 3.2

NEW QUESTION 76
A technician wants to improve the situational and environmental awareness of existing users as they transition from remote to in-office work. Which of the following is the best option?

A. Send out periodic security reminders.
B. Update the content of new hire documentation.
C. Modify the content of recurring trainin
D. D Implement a phishing campaign

Answer: C

Explanation:
Recurring training is a type of security awareness training that is conducted periodically to refresh and update the knowledge and skills of the users. Recurring training can help improve the situational and environmental awareness of existing users as they transition from remote to in-office work, as it can cover the latest threats, best practices, and policies that are relevant to their work environment. Modifying the content of recurring training can ensure that the users are aware of the current security landscape and the expectations of their roles. References = CompTIA Security+ Study Guide with over 500 Practice Test Questions: Exam SY0-701, 9th Edition, Chapter 5, page 232. CompTIA Security+ (SY0-701) Certification Exam Objectives, Domain 5.1, page 18.

NEW QUESTION 78
A newly appointed board member with cybersecurity knowledge wants the board of directors to receive a quarterly report detailing the number of incidents that impacted the organization. The systems administrator is creating a way to present the data to the board of directors. Which of the following should the systems administrator use?

A. Packet captures
B. Vulnerability scans
C. Metadata
D. Dashboard

Answer: D

Explanation:
A dashboard is a graphical user interface that provides a visual representation of key performance indicators, metrics, and trends related to security events and incidents. A dashboard can help the board of directors to understand the number and impact of incidents that affected the organization in a given period, as well as the status and effectiveness of the security controls and processes. A dashboard can also allow the board of directors to drill down into specific details or filter the data by various criteria12.
A packet capture is a method of capturing and analyzing the network traffic that passes through a device or a network segment. A packet capture can provide detailed information about the source, destination, protocol, and content of each packet, but it is not a suitable way to present a summary of incidents to the board of directors13.
A vulnerability scan is a process of identifying and assessing the weaknesses and exposures in a system or a network that could be exploited by attackers. A vulnerability scan can help the organization to prioritize and remediate the risks and improve the security posture, but it is not a relevant way to report the number of incidents that occurred in a quarter14.
Metadata is data that describes other data, such as its format, origin, structure, or context. Metadata can provide useful information about the characteristics and properties of data, but it is not a meaningful way to communicate the impact and frequency of incidents to the board of directors. References = 1: CompTIA Security+ SY0-701 Certification Study Guide, page 3722: SIEM Dashboards – SY0-601 CompTIA Security+ : 4.3, video by Professor Messer3: CompTIA Security+ SY0-701 Certification Study Guide, page 3464: CompTIA Security+ SY0-701 Certification Study Guide, page 362. : CompTIA Security+ SY0-701 Certification Study Guide, page 97.

NEW QUESTION 81
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
References:
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

NEW QUESTION 86
A security analyst scans a company's public network and discovers a host is running a remote desktop that can be used to access the production network. Which of the following changes should the security analyst recommend?

A. Changing the remote desktop port to a non-standard number
B. Setting up a VPN and placing the jump server inside the firewall
C. Using a proxy for web connections from the remote desktop server
D. Connecting the remote server to the domain and increasing the password length

Answer: B

Explanation:
A VPN is a virtual private network that creates a secure tunnel between two or more devices over a public network. A VPN can encrypt and authenticate the data, as well as hide the IP addresses and locations of the devices. A jump server is a server that acts as an intermediary between a user and a target server, such as a production server. A jump server can provide an additional layer of security and access control, as well as logging and auditing capabilities. A firewall is a device or software that filters and blocks unwanted network traffic based on predefined rules. A firewall can protect the internal network from external threats and limit the exposure of sensitive services and ports. A security analyst should recommend setting up a VPN and placing the jump server inside the firewall to improve the security of the remote desktop access to the production network. This way, the remote desktop service will not be exposed to the public network, and only authorized users with VPN credentials can access the jump server and then the production
server. References: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, Chapter 8: Secure Protocols and Services, page 382-383 1; Chapter 9: Network Security, page 441-442 1

NEW QUESTION 88
Which of the following scenarios describes a possible business email compromise attack?

A. An employee receives a gift card request in an email that has an executive's name in the display field of the email.
B. Employees who open an email attachment receive messages demanding payment in order to access files.
C. A service desk employee receives an email from the HR director asking for log-in credentials to a cloud administrator account.
D. An employee receives an email with a link to a phishing site that is designed to look like the company's email portal.

Answer: A

Explanation:
A business email compromise (BEC) attack is a type of phishing attack that targets employees who have access to company funds or sensitive information. The attacker impersonates a trusted person, such as an executive, a vendor, or a client, and requests a fraudulent payment, a wire transfer, or confidential data. The attacker often uses social engineering techniques, such as urgency, pressure, or familiarity, to convince the victim to comply with the request12.
In this scenario, option A describes a possible BEC attack, where an employee receives a gift card request in an email that has an executive's name in the display field of the email. The email may look like it is coming from the executive, but the actual email address may be spoofed or compromised. The attacker may claim that the gift cards are needed for a business purpose, such as rewarding employees or clients, and ask the employee to purchase them and send the codes. This is a common tactic used by BEC attackers to steal money from unsuspecting victims34.
Option B describes a possible ransomware attack, where malicious software encrypts the files on a device and demands a ransom for the decryption key. Option C describes a possible credential harvesting attack, where an attacker tries to obtain the login information of a privileged account by posing as a legitimate authority. Option D describes a possible phishing attack, where an attacker tries to lure the victim to a fake website that mimics the company's email portal and capture their credentials. These are all types of cyberattacks, but they are not examples of BEC attacks. References = 1: Business Email Compromise - CompTIA Security+ SY0-701 - 2.2 2: CompTIA Security+ SY0-701 Certification Study Guide 3: Business Email Compromise: The 12 Billion Dollar Scam 4: TOTAL: CompTIA Security+ Cert (SY0-701) | Udemy

NEW QUESTION 90
During a security incident, the security operations team identified sustained network traffic from a malicious IP address: 10.1.4.9. A security analyst is creating an inbound firewall rule to block the IP address from accessing the organization's network. Which of the following fulfills this request?

A. access-list inbound deny ig source 0.0.0.0/0 destination 10.1.4.9/32
B. access-list inbound deny ig source 10.1.4.9/32 destination 0.0.0.0/0
C. access-list inbound permit ig source 10.1.4.9/32 destination 0.0.0.0/0
D. access-list inbound permit ig source 0.0.0.0/0 destination 10.1.4.9/32

Answer: B

Explanation:
A firewall rule is a set of criteria that determines whether to allow or deny a packet to pass through the firewall. A firewall rule consists of several elements, such as the action, the protocol, the source address, the destination address, and the port number. The syntax of a firewall rule may vary depending on the type and vendor of the firewall, but the basic logic is the same. In this question, the security analyst is creating an inbound firewall rule to block the IP address 10.1.4.9 from accessing the organization's network. This means that the action should be deny, the protocol should be any (or ig for IP), the source address should be 10.1.4.9/32 (which means a single IP address), the destination address should be 0.0.0.0/0 (which means any IP address), and the port number should be any. Therefore, the correct firewall rule is:
access-list inbound deny ig source 10.1.4.9/32 destination 0.0.0.0/0
This rule will match any packet that has the source IP address of 10.1.4.9 and drop it. The other options are incorrect because they either have the wrong action, the wrong source address, or the wrong destination address. For example, option A has the source and destination addresses reversed, which means that it will block any packet that has the destination IP address of 10.1.4.9, which is not the intended goal. Option C has the wrong action, which is permit, which means that it will allow the packet to pass through the firewall, which is also not the intended goal. Option D has the same problem as option A, with the source and destination addresses reversed.
References = Firewall Rules – CompTIA Security+ SY0-401: 1.2, Firewalls – SY0-601 CompTIA Security+ : 3.3, Firewalls – CompTIA Security+ SY0-501, Understanding Firewall Rules – CompTIA Network+ N10-005: 5.5, Configuring Windows Firewall – CompTIA A+ 220-1102 – 1.6.

NEW QUESTION 94
An enterprise has been experiencing attacks focused on exploiting vulnerabilities in older browser versions with well-known exploits. Which of the following

security solutions should be configured to best provide the ability to monitor and block these known signature-based attacks?

A. ACL
B. DLP
C. IDS
D. IPS

Answer: D

Explanation:
An intrusion prevention system (IPS) is a security device that monitors network traffic and blocks or modifies malicious packets based on predefined rules or signatures. An IPS can prevent attacks that exploit known vulnerabilities in older browser versions by detecting and dropping the malicious packets before they reach the target system. An IPS can also perform other functions, such as rate limiting, encryption, or redirection. References: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, Chapter 3: Securing Networks, page 132.

NEW QUESTION 96
A client demands at least 99.99% uptime from a service provider's hosted security services. Which of the following documents includes the information the service provider should return to the client?

A. MOA
B. SOW
C. MOU
D. SLA

Answer: D

Explanation:
A service level agreement (SLA) is a document that defines the level of service expected by a customer from a service provider, indicating the metrics by which that service is measured, and the remedies or penalties, if any, should the agreed-upon levels not be achieved. An SLA can specify the minimum uptime or availability of a service, such as 99.99%, and the consequences for failing to meet that standard. A memorandum of agreement (MOA), a statement of work (SOW), and a memorandum of understanding (MOU) are other types of documents that can be used to establish a relationship between parties, but they do not typically include the details of service levels and performance metrics that an SLA does. References: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, page 16-17

NEW QUESTION 98
While troubleshooting a firewall configuration, a technician determines that a “deny any” policy should be added to the bottom of the ACL. The technician updates the policy, but the new policy causes several company servers to become unreachable.
Which of the following actions would prevent this issue?

A. Documenting the new policy in a change request and submitting the request to change management
B. Testing the policy in a non-production environment before enabling the policy in the production network
C. Disabling any intrusion prevention signatures on the 'deny any* policy prior to enablingthe new policy
D. Including an 'allow any1 policy above the 'deny any* policy

Answer: B

Explanation:
A firewall policy is a set of rules that defines what traffic is allowed or denied on a network. A firewall policy should be carefully designed and tested before being implemented, as a misconfigured policy can cause network disruptions or security breaches. A common best practice is to test the policy in a non-production environment, such as a lab or a simulation, before enabling the policy in the production network. This way, the technician can verify the functionality and performance of the policy, and identify and resolve any issues or conflicts, without affecting the live network. Testing the policy in a non-production environment would prevent the issue of the ‘deny any’ policy causing several company servers to become unreachable, as the technician would be able to detect and correct the problem before applying the policy to the production network. Documenting the new policy in a change request and submitting the request to change management is a good practice, but it would not prevent the issue by itself. Change management is a process that ensures that any changes to the network are authorized, documented, and communicated, but it does not guarantee that the changes are error-free or functional. The technician still needs to test the policy before implementing it.
Disabling any intrusion prevention signatures on the ‘deny any’ policy prior to enabling the new policy would not prevent the issue, and it could reduce the security of the network. Intrusion prevention signatures are patterns that identify malicious or unwanted traffic, and allow the firewall to block or alert on such traffic. Disabling these signatures would make the firewall less effective in detecting and preventing attacks, and it would not affect the reachability of the company servers.
Including an ‘allow any’ policy above the ‘deny any’ policy would not prevent the issue, and it would render the ‘deny any’ policy useless. A firewall policy is processed from top to bottom, and the first matching rule is applied. An ‘allow any’ policy would match any traffic and allow it to pass through the firewall, regardless of the source, destination, or protocol. This would negate the purpose of the ‘deny any’ policy, which is to block any traffic that does not match any of the previous rules. Moreover, an ‘allow any’ policy would create a security risk, as it would allow any unauthorized or malicious traffic to enter or exit the network.
References = CompTIA Security+ SY0-701 Certification Study Guide, page 204- 205; Professor Messer’s CompTIA SY0-701 Security+ Training Course, video 2.1 - Network Security Devices, 8:00 - 10:00.

NEW QUESTION 100
An attacker posing as the Chief Executive Officer calls an employee and instructs the employee to buy gift cards. Which of the following techniques is the attacker using?

A. Smishing
B. Disinformation
C. Impersonating
D. Whaling

Answer: D

Explanation:
Whaling is a type of phishing attack that targets high-profile individuals, such as executives, celebrities, or politicians. The attacker impersonates someone with

authority or influence and tries to trick the victim into performing an action, such as transferring money, revealing sensitive information, or clicking on a malicious link. Whaling is also called CEO fraud or business email compromise2.
References: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, Chapter 3, page 97.

NEW QUESTION 104
Which of the following tools can assist with detecting an employee who has accidentally emailed a file containing a customer's PII?

A. SCAP
B. Net Flow
C. Antivirus
D. DLP

Answer: D

Explanation:
DLP stands for Data Loss Prevention, which is a tool that can assist with detecting and preventing the unauthorized transmission or leakage of sensitive data, such as a customer's PII (Personally Identifiable Information). DLP can monitor, filter, and block data in motion (such as emails), data at rest (such as files), and data in use (such as applications). DLP can also alert the sender, the recipient, or the administrator of the data breach, and apply remediation actions, such as encryption, quarantine, or deletion. DLP can help an organization comply with data protection regulations, such as GDPR, HIPAA, or PCI DSS, and protect its reputation and assets. References = CompTIA Security+ Study Guide with over 500 Practice Test Questions: Exam SY0-701, 9th Edition, Chapter 2, page 78. CompTIA Security+ SY0-701 Exam Objectives, Domain 2.5, page 11.

NEW QUESTION 107
A Chief Information Security Officer (CISO) wants to explicitly raise awareness about the increase of ransomware-as-a-service in a report to the management team. Which of the following best describes the threat actor in the CISO's report?

A. Insider threat
B. Hacktivist
C. Nation-state
D. Organized crime

Answer: D

Explanation:
Ransomware-as-a-service is a type of cybercrime where hackers sell or rent ransomware tools or services to other criminals who use them to launch attacks and extort money from victims. This is a typical example of organized crime, which is a group of criminals who work together to conduct illegal activities for profit. Organized crime is different from other types of threat actors, such as insider threats, hacktivists, or nation-states, who may have different motives, methods, or targets. References: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, page 17 1

NEW QUESTION 110
A systems administrator is creating a script that would save time and prevent human error when performing account creation for a large number of end users. Which of the following would be a good use case for this task?

A. Off-the-shelf software
B. Orchestration
C. Baseline
D. Policy enforcement

Answer: B

Explanation:
Orchestration is the process of automating multiple tasks across different systems and applications. It can help save time and reduce human error by executing predefined workflows and scripts. In this case, the systems administrator can use orchestration to create accounts for a large number of end users without having to manually enter their information and assign permissions. References: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, page 457 1

NEW QUESTION 115
Which of the following is used to validate a certificate when it is presented to a user?

A. OCSP
B. CSR
C. CA
D. CRC

Answer: A

Explanation:
OCSP stands for Online Certificate Status Protocol. It is a protocol that allows applications to check the revocation status of a certificate in real-time. It works by sending a query to an OCSP responder, which is a server that maintains a database of revoked certificates. The OCSP responder returns a response that indicates whether the certificate is valid, revoked, or unknown. OCSP is faster and more efficient than downloading and parsing Certificate Revocation Lists (CRLs), which are large files that contain the serial numbers of all revoked certificates issued by a Certificate Authority (CA). References: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, page 337 1

NEW QUESTION 119
Which of the following automation use cases would best enhance the security posture of an organization by rapidly updating permissions when employees leave a company?

A. Provisioning resources
B. Disabling access

C. Reviewing change approvals
D. Escalating permission requests

Answer: B

Explanation:
Disabling access is an automation use case that would best enhance the security posture of an organization by rapidly updating permissions when employees leave a company. Disabling access is the process of revoking or suspending the access rights of a user account, such as login credentials, email, VPN, cloud services, etc. Disabling access can prevent unauthorized or malicious use of the account by former employees or attackers who may have compromised the account. Disabling access can also reduce the attack surface and the risk of data breaches or leaks. Disabling access can be automated by using scripts, tools, or workflows that can trigger the action based on predefined events, such as employee termination, resignation, or transfer. Automation can ensure that the access is disabled in a timely, consistent, and efficient manner, without relying on manual intervention or human error.
References: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, Chapter 5: Identity and Access Management, page 2131. CompTIA Security+ Certification Kit: Exam SY0-701, 7th Edition, Chapter 5: Identity and Access Management, page 2132.

NEW QUESTION 120
Which of the following is the phase in the incident response process when a security analyst reviews roles and responsibilities?

A. Preparation
B. Recovery
C. Lessons learned
D. Analysis

Answer: A

Explanation:
Preparation is the phase in the incident response process when a security analyst reviews roles and responsibilities, as well as the policies and procedures for handling incidents. Preparation also involves gathering and maintaining the necessary tools, resources, and contacts for responding to incidents. Preparation can help a security analyst to be ready and proactive when an incident occurs, as well as to reduce the impact and duration of the incident.
Some of the activities that a security analyst performs during the preparation phase are:
? Defining the roles and responsibilities of the incident response team members, such as the incident manager, the incident coordinator, the technical lead, the communications lead, and the legal advisor.
? Establishing the incident response plan, which outlines the objectives, scope, authority, and procedures for responding to incidents, as well as the escalation and reporting mechanisms.
? Developing the incident response policy, which defines the types and categories of incidents, the severity levels, the notification and reporting requirements, and the roles and responsibilities of the stakeholders.
? Creating the incident response playbook, which provides the step-by-step guidance and checklists for handling specific types of incidents, such as denial-of-service, ransomware, phishing, or data breach.
? Acquiring and testing the incident response tools, such as network and host-based scanners, malware analysis tools, forensic tools, backup and recovery tools, and communication and collaboration tools.
? Identifying and securing the incident response resources, such as the incident response team, the incident response location, the evidence storage, and the external support.
? Building and maintaining the incident response contacts, such as the internal and external stakeholders, the law enforcement agencies, the regulatory bodies, and the media.
References:
? CompTIA Security+ SY0-701 Certification Study Guide, Chapter 6: Architecture and Design, Section 6.4: Secure Systems Design, p. 279-280
? CompTIA Security+ SY0-701 Certification Exam Objectives, Domain 3: Architecture and Design, Objective 3.5: Given a scenario, implement secure network architecture concepts, Sub-objective: Incident response, p. 16

NEW QUESTION 121
A security administrator would like to protect data on employees' laptops. Which of the following encryption techniques should the security administrator use?

A. Partition
B. Asymmetric
C. Full disk
D. Database

Answer: C

Explanation:
Full disk encryption (FDE) is a technique that encrypts all the data on a hard drive, including the operating system, applications, and files. FDE protects the data from unauthorized access in case the laptop is lost, stolen, or disposed of without proper sanitization. FDE requires the user to enter a password, a PIN, a smart card, or a biometric factor to unlock the drive and boot the system. FDE can be implemented by using software solutions, such as BitLocker, FileVault, or VeraCrypt, or by using hardware solutions, such as self-encrypting drives (SEDs) or Trusted Platform Modules (TPMs). FDE is a recommended encryption technique for laptops and other mobile devices that store sensitive data.
Partition encryption is a technique that encrypts only a specific partition or volume on a hard drive, leaving the rest of the drive unencrypted. Partition encryption is less secure than FDE, as it does not protect the entire drive and may leave traces of data on unencrypted areas. Partition encryption is also less convenient than FDE, as it requires the user to mount and unmount the encrypted partition manually.
Asymmetric encryption is a technique that uses a pair of keys, one public and one private, to encrypt and decrypt data. Asymmetric encryption is mainly used for securing communication, such as email, web, or VPN, rather than for encrypting data at rest. Asymmetric encryption is also slower and more computationally intensive than symmetric encryption, which is the type of encryption used by FDE and partition encryption.
Database encryption is a technique that encrypts data stored in a database, such as tables, columns, rows, or cells. Database encryption can be done at the application level, the database level, or the file system level. Database encryption is useful for protecting data from unauthorized access by database administrators, hackers, or malware, but it does not protect the data from physical theft or loss of the device that hosts the database. References = Data Encryption – CompTIA Security+ SY0-401: 4.4, CompTIA Security+Cheat Sheet and PDF | Zero To Mastery, CompTIA Security+ SY0-601 Certification Course - Cybr, Application Hardening – SY0-601 CompTIA Security+ : 3.2.

NEW QUESTION 122
A security manager created new documentation to use in response to various types of security incidents. Which of the following is the next step the manager should take?

A. Set the maximum data retention policy.
B. Securely store the documents on an air-gapped network.
C. Review the documents' data classification policy.
D. Conduct a tabletop exercise with the team.

Answer: D

Explanation:
A tabletop exercise is a simulated scenario that tests the effectiveness of a security incident response plan. It involves gathering the relevant stakeholders and walking through the steps of the plan, identifying any gaps or issues that need to be addressed. A tabletop exercise is a good way to validate the documentation created by the security manager and ensure that the team is prepared for various types of security incidents. References: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, Chapter 6: Risk Management, page 2841. CompTIA Security+ Certification Kit: Exam SY0-701, 7th Edition, Chapter 6: Risk Management, page 2842.

NEW QUESTION 124
An enterprise is trying to limit outbound DNS traffic originating from its internal network. Outbound DNS requests will only be allowed from one device with the IP address 10.50.10.25. Which of the following firewall ACLs will accomplish this goal?

A. Access list outbound permit 0.0.0.0 0 0.0.0.0/0 port 53 Access list outbound deny 10.50.10.25 32 0.0.0.0/0 port 53
B. Access list outbound permit 0.0.0.0/0 10.50.10.25 32 port 53 Access list outbound deny 0.0.0.0 0 0.0.0.0/0 port 53
C. Access list outbound permit 0.0.0.0 0 0.0.0.0/0 port 53 Access list outbound deny 0.0.0.0/0 10.50.10.25 32 port 53
D. Access list outbound permit 10.50.10.25 32 0.0.0.0/0 port 53 Access list outbound deny 0.0.0.0.0.0.0.0/0 port 53

Answer: D

Explanation:
The correct answer is D because it allows only the device with the IP address 10.50.10.25 to send outbound DNS requests on port 53, and denies all other devices from doing so. The other options are incorrect because they either allow all devices to send outbound DNS requests (A and C), or they allow no devices to send outbound DNS requests (B). References = You can learn more about firewall ACLs and DNS in the following resources:
? CompTIA Security+ SY0-701 Certification Study Guide, Chapter 4: Network Security1
? Professor Messer's CompTIA SY0-701 Security+ Training Course, Section 3.2: Firewall Rules2
? TOTAL: CompTIA Security+ Cert (SY0-701) | Udemy, Section 6: Network Security, Lecture 28: Firewall Rules3

NEW QUESTION 129
A security administrator is deploying a DLP solution to prevent the exfiltration of sensitive customer data. Which of the following should the administrator do first?

A. Block access to cloud storage websites.
B. Create a rule to block outgoing email attachments.
C. Apply classifications to the data.
D. Remove all user permissions from shares on the file server.

Answer: C

Explanation:
Data classification is the process of assigning labels or tags to data based on its sensitivity, value, and risk. Data classification is the first step in a data loss prevention (DLP) solution, as it helps to identify what data needs to be protected and how. By applying classifications to the data, the security administrator can define appropriate policies and rules for the DLP solution to prevent the exfiltration of sensitive customer data. References: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, Chapter 8: Data Protection, page 323. CompTIA Security+ Practice Tests: Exam SY0-701, 3rd Edition, Chapter 8: Data Protection, page 327.

NEW QUESTION 134
A technician needs to apply a high-priority patch to a production system. Which of the following steps should be taken first?

A. Air gap the system.
B. Move the system to a different network segment.
C. Create a change control request.
D. Apply the patch to the system.

Answer: C

Explanation:
= A change control request is a document that describes the proposed change to a system, the reason for the change, the expected impact, the approval process, the testing plan, the implementation plan, the rollback plan, and the communication plan. A change control request is a best practice for applying any patch to a production system, especially a high-priority one, as it ensures that the change is authorized, documented, tested, and communicated. A change control request also minimizes the risk of unintended consequences, such as system downtime, data loss, or security breaches. References = CompTIA Security+ Study Guide with over 500 Practice Test Questions: Exam SY0-701, 9th Edition, Chapter 6, page 235. CompTIA Security+ SY0-701 Exam Objectives, Domain 4.1, page 13.

NEW QUESTION 136
A company is discarding a classified storage array and hires an outside vendor to complete the disposal. Which of the following should the company request from the vendor?

A. Certification
B. Inventory list
C. Classification
D. Proof of ownership

Answer: A

Explanation:

The company should request a certification from the vendor that confirms the storage array has been disposed of securely and in compliance with the company's policies and standards. A certification provides evidence that the vendor has followed the proper procedures and methods to destroy the classified data and prevent unauthorized access or recovery. A certification may also include details such as the date, time, location, and method of disposal, as well as the names and signatures of the personnel
involved. References: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, Chapter 3, page 1441

NEW QUESTION 138
A systems administrator wants to prevent users from being able to access data based on their responsibilities. The administrator also wants to apply the required access structure via a simplified format. Which of the following should the administrator apply to the site recovery resource group?

A. RBAC
B. ACL
C. SAML
D. GPO

Answer: A

Explanation:
RBAC stands for Role-Based Access Control, which is a method of restricting access to data and resources based on the roles or responsibilities of users. RBAC simplifies the management of permissions by assigning roles to users and granting access rights to roles, rather than to individual users. RBAC can help enforce the principle of least privilege and reduce the risk of unauthorized access or data leakage. The other options are not as suitable for the scenario as RBAC, as they either do not prevent access based on responsibilities, or do not apply a simplified format. References: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, page 133 1

NEW QUESTION 141
An organization is leveraging a VPN between its headquarters and a branch location.
Which of the following is the VPN protecting?

A. Data in use
B. Data in transit
C. Geographic restrictions
D. Data sovereignty

Answer: B

Explanation:
Data in transit is data that is moving from one location to another, such as over a network or through the air. Data in transit is vulnerable to interception, modification, or theft by malicious actors. A VPN (virtual private network) is a technology that protects data in transit by creating a secure tunnel between two endpoints and encrypting the data that passes through it2.
References: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, Chapter 4, page 145.

NEW QUESTION 145
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. References = 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.

NEW QUESTION 150
An administrator discovers that some files on a database server were recently encrypted. The administrator sees from the security logs that the data was last accessed by a domain user. Which of the following best describes the type of attack that occurred?

A. Insider threat
B. Social engineering
C. Watering-hole
D. Unauthorized attacker

Answer: A

Explanation:
An insider threat is a type of attack that originates from someone who has legitimate access to an organization's network, systems, or data. In this case, the domain user who encrypted the files on the database server is an example of an insider threat, as they abused their access privileges to cause harm to the organization. Insider threats can be motivated by various factors, such as financial gain, revenge, espionage, or sabotage. References: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, Chapter 1: General Security Concepts, page 251. CompTIA Security+ Certification Kit: Exam SY0- 701, 7th Edition, Chapter 1: General Security Concepts, page 252.

NEW QUESTION 152
Which of the following is used to add extra complexity before using a one-way data transformation algorithm?

A. Key stretching
B. Data masking
C. Steganography
D. Salting

Answer: D

Explanation:
Salting is the process of adding extra random data to a password or other data before applying a one-way data transformation algorithm, such as a hash function. Salting increases the complexity and randomness of the input data, making it harder for attackers to guess or crack the original data using precomputed tables or brute force methods. Salting also helps prevent identical passwords from producing identical hash values, which could reveal the passwords to attackers who have access to the hashed data. Salting is commonly used to protect passwords stored in databases or transmitted over networks. References =
? Passwords technical overview
? Encryption, hashing, salting – what's the difference?
? Salt (cryptography)

NEW QUESTION 157
Which of the following vulnerabilities is associated with installing software outside of a manufacturer's approved software repository?

A. Jailbreaking
B. Memory injection
C. Resource reuse
D. Side loading

Answer: D

Explanation:
Side loading is the process of installing software outside of a manufacturer's approved software repository. This can expose the device to potential vulnerabilities, such as malware, spyware, or unauthorized access. Side loading can also bypass security controls and policies that are enforced by the manufacturer or the organization. Side loading is often done by users who want to access applications or features that are not available or allowed on their devices. References = Sideloading - CompTIA Security + Video Training | Interface Technical Training, Security+ (Plus) Certification | CompTIA IT Certifications, Load Balancers – CompTIA Security+ SY0-501 – 2.1, CompTIA Security+ SY0-601 Certification Study Guide.

NEW QUESTION 159
Which of the following threat actors is the most likely to use large financial resources to attack critical systems located in other countries?

A. Insider
B. Unskilled attacker
C. Nation-state
D. Hacktivist

Answer: C

Explanation:
A nation-state is a threat actor that is sponsored by a government or a political entity to conduct cyberattacks against other countries or organizations. Nation-states have large financial resources, advanced technical skills, and strategic objectives that may target critical systems such as military, energy, or infrastructure. Nation-states are often motivated by espionage, sabotage, or warfare12. References = 1: CompTIA Security+ SY0-701 Certification Study Guide, page 542: Threat Actors – CompTIA
Security+ SY0-701 – 2.1, video by Professor Messer.

NEW QUESTION 161
An organization would like to store customer data on a separate part of the network that is not accessible to users on the main corporate network. Which of the following should the administrator use to accomplish this goal?

A. Segmentation
B. Isolation
C. Patching
D. Encryption

Answer: A

Explanation:
Segmentation is a network design technique that divides the network into smaller and isolated segments based on logical or physical boundaries. Segmentation can help improve network security by limiting the scope of an attack, reducing the attack surface, and enforcing access control policies. Segmentation can also enhance network performance, scalability, and manageability. To accomplish the goal of storing customer data on a separate part of the network, the administrator can use segmentation technologies such as subnetting, VLANs, firewalls, routers, or switches. References: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, page 308-309 1

NEW QUESTION 165
An administrator finds that all user workstations and servers are displaying a message that is associated with files containing an extension of .ryk. Which of the following types of infections is present on the systems?

A. Virus
B. Trojan
C. Spyware

D. Ransomware

Answer: D

Explanation:
Ransomware is a type of malware that encrypts the victim's files and demands a ransom for the decryption key. The ransomware usually displays a message on the infected system with instructions on how to pay the ransom and recover the files. The .ryk extension is associated with a ransomware variant called Ryuk, which targets large organizations and demands high ransoms1.
References: CompTIA Security+ Certification Kit: Exam SY0-701, 7th Edition, Chapter 1, page 17.

NEW QUESTION 168
Which of the following security control types does an acceptable use policy best represent?

A. Detective
B. Compensating
C. Corrective
D. Preventive

Answer: D

Explanation:
An acceptable use policy (AUP) is a set of rules that govern how users can access and use a corporate network or the internet. The AUP helps companies minimize their exposure to cyber security threats and limit other risks. The AUP also serves as a notice to users about what they are not allowed to do and protects the company against misuse of their network. Users usually have to acknowledge that they understand and agree to the rules before accessing the network1.
An AUP best represents a preventive security control type, because it aims to deter or stop potential security incidents from occurring in the first place. A preventive control is proactive and anticipates possible threats and vulnerabilities, and implements measures to prevent them from exploiting or harming the system or the data. A preventive control can be physical, technical, or administrative in nature2.
Some examples of preventive controls are:
? Locks, fences, or guards that prevent unauthorized physical access to a facility or a device
? Firewalls, antivirus software, or encryption that prevent unauthorized logical access to a network or a system
? Policies, procedures, or training that prevent unauthorized or inappropriate actions or behaviors by users or employees
An AUP is an example of an administrative preventive control, because it defines the policies and procedures that users must follow to ensure the security and proper use of the network and the IT resources. An AUP can prevent users from engaging in activities that could compromise the security, performance, or availability of the network or the system, such as:
? Downloading or installing unauthorized or malicious software
? Accessing or sharing sensitive or confidential information without authorization or encryption
? Using the network or the system for personal, illegal, or unethical purposes
? Bypassing or disabling security controls or mechanisms
? Connecting unsecured or unapproved devices to the network
By enforcing an AUP, a company can prevent or reduce the likelihood of security breaches, data loss, legal liability, or reputational damage caused by user actions or inactions3.
References = 1: How to Create an Acceptable Use Policy - CoreTech, 2: [Security Control Types: Preventive, Detective, Corrective, and Compensating], 3: Why You Need A
Corporate Acceptable Use Policy - CompTIA

NEW QUESTION 169
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. References = 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.

NEW QUESTION 170
A user is attempting to patch a critical system, but the patch fails to transfer. Which of the following access controls is most likely inhibiting the transfer?

A. Attribute-based
B. Time of day
C. Role-based
D. Least privilege

Answer: D

Explanation:
The least privilege principle states that users and processes should only have the minimum level of access required to perform their tasks. This helps to prevent unauthorized or unnecessary actions that could compromise security. In this case, the patch transfer might be failing because the user or process does not have the appropriate permissions to access the critical system or the network resources needed for the transfer. Applying the least privilege principle can help to avoid this issue by granting the user or process the necessary access rights for the patching activity. References: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, page 931

NEW QUESTION 171
Which of the following is required for an organization to properly manage its restore process in the event of system failure?

A. IRP
B. DRP
C. RPO
D. SDLC

Answer: B

Explanation:
A disaster recovery plan (DRP) is a set of policies and procedures that aim to restore the normal operations of an organization in the event of a system failure, natural disaster, or other emergency. A DRP typically includes the following elements:
? A risk assessment that identifies the potential threats and impacts to the organization's critical assets and processes.
? A business impact analysis that prioritizes the recovery of the most essential functions and data.
? A recovery strategy that defines the roles and responsibilities of the recovery team, the resources and tools needed, and the steps to follow to restore the system.
? A testing and maintenance plan that ensures the DRP is updated and validated regularly. A DRP is required for an organization to properly manage its restore process in the event of system failure, as it provides a clear and structured framework for recovering from a disaster and minimizing the downtime and data loss.
References = CompTIA Security+ Study Guide (SY0-701), Chapter 7: Resilience and Recovery, page 325.

NEW QUESTION 174
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
References:
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, Chapter 4: Identity and Access Management, page 179

NEW QUESTION 178
A company is developing a critical system for the government and storing project information on a fileshare. Which of the following describes how this data will most likely be classified? (Select two).

A. Private
B. Confidential
C. Public
D. Operational
E. Urgent
F. Restricted

Answer: BF

Explanation:
Data classification is the process of assigning labels to data based on its sensitivity and business impact. Different organizations and sectors may have different data classification schemes, but a common one is the following1:
? Public: Data that can be freely disclosed to anyone without any harm or risk.
? Private: Data that is intended for internal use only and may cause some harm or risk if disclosed.
? Confidential: Data that is intended for authorized use only and may cause significant harm or risk if disclosed.
? Restricted: Data that is intended for very limited use only and may cause severe harm or risk if disclosed.
In this scenario, the company is developing a critical system for the government and storing project information on a fileshare. This data is likely to be classified as confidential and restricted, because it is not meant for public or private use, and it may cause serious damage to national security or public safety if disclosed. The government may also have specific requirements or regulations for handling such data, such as encryption, access control, and auditing2. References: 1: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, page 16-17 2: Data Classification Practices: Final Project Description Released

NEW QUESTION 180
A systems administrator set up a perimeter firewall but continues to notice suspicious connections between internal endpoints. Which of the following should be set up in order to mitigate the threat posed by the suspicious activity?

A. Host-based firewall

B. Web application firewall
C. Access control list
D. Application allow list

Answer: A

Explanation:
A host-based firewall is a software application that runs on an individual endpoint and filters the incoming and outgoing network traffic based on a set of rules. A host-based firewall can help to mitigate the threat posed by suspicious connections between internal endpoints by blocking or allowing the traffic based on the source, destination, port, protocol, or application. A host-based firewall is different from a web application firewall, which is a type of firewall that protects web applications from common web-based attacks, such as SQL injection, cross-site scripting, and session hijacking. A host-based firewall is also different from an access control list, which is a list of rules that control the access to network resources, such as files, folders, printers, or routers. A host- based firewall is also different from an application allow list, which is a list of applications that are authorized to run on an endpoint, preventing unauthorized or malicious applications from executing. References: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, page 254

NEW QUESTION 185
.....

Relate Links

100% Pass Your SY0-701 Exam with Exambible Prep Materials

https://www.exambible.com/SY0-701-exam/

Contact us

We are proud of our high-quality customer service, which serves you around the clock 24/7.

Viste - https://www.exambible.com/