CompTIA.SY0-701.vJan-2024.by.Koanxy.37q

Number: SY0-701
Passing Score: 800
Time Limit: 120
File Version: 2.0

Exam Code: SY0-701
Exam Name: CompTIA Security+

Exam A

QUESTION 1
A company is planning to set up a SIEM system and assign an analyst to review the logs on a weekly basis. Which of the following types of controls is the company setting up?

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

Correct Answer: C
Section:
Explanation:
A detective control is a type of control that monitors and analyzes the events and activities in a system or a network, and alerts or reports when an incident or a violation occurs. A SIEM (Security Information and Event Management) system is a tool that collects, correlates, and analyzes the logs from various sources, such as firewalls, routers, servers, or applications, and provides a centralized view of the security status and incidents. An analyst who reviews the logs on a weekly basis can identify and investigate any anomalies, trends, or patterns that indicate a potential threat or a breach. A detective control can help the company to respond quickly and effectively to the incidents, and to improve its security posture and resilience.Reference=CompTIA Security+ Study Guide with over 500 Practice Test Questions: Exam SY0-701, 9th Edition, Chapter 1, page 23. CompTIA Security+ SY0-701 Exam Objectives, Domain 4.3, page 14.

QUESTION 2
An organization is building a new backup data center with cost-benefit as the primary requirement and RTO and RPO values around two days. Which of the following types of sites is the best for this scenario?

A. Real-time recovery
B. Hot
C. Cold
D. Warm

Correct Answer: C
Section:
Explanation:
A cold site is a type of backup data center that has the necessary infrastructure to support IT operations, but does not have any pre-configured hardware or software. A cold site is the cheapest option among the backup data center types, but it also has the longest recovery time objective (RTO) and recovery point objective (RPO) values. A cold site is suitable for scenarios where the cost-benefit is the primary requirement and the RTO and RPO values are not very stringent. A cold site can take up to two days or more to restore the normal operations after a disaster.Reference=CompTIA Security+ SY0-701 Certification Study Guide, page 387;Backup Types -- SY0-601 CompTIA Security+ : 2.5, video at 4:50.

QUESTION 3
A company requires hard drives to be securely wiped before sending decommissioned systems to recycling. Which of the following best describes this policy?

A. Enumeration
B. Sanitization
C. Destruction
D. Inventory

Correct Answer: B
Section:

Explanation:
Sanitization is the process of removing sensitive data from a storage device or a system before it is disposed of or reused. Sanitization can be done by using software tools or hardware devices that overwrite the data with random patterns or zeros, making it unrecoverable. Sanitization is different from destruction, which is the physical damage of the storage device to render it unusable. Sanitization is also different from enumeration, which is the identification of network resources or devices, and inventory, which is the tracking of assets and their locations. The policy of securely wiping hard drives before sending decommissioned systems to recycling is an example of sanitization, as it ensures that no confidential data can be retrieved from the recycled devices.Reference=Secure Data Destruction -- SY0-601 CompTIA Security+ : 2.7, video at 1:00;CompTIA Security+ SY0-701 Certification Study Guide, page 387.

QUESTION 4
A systems administrator works for a local hospital and needs to ensure patient data is protected and secure. Which of the following data classifications should be used to secure patient data?

A. Private
B. Critical
C. Sensitive
D. Public

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

QUESTION 5
A U.S.-based cloud-hosting provider wants to expand its data centers to new international locations. Which of the following should the hosting provider consider first?

A. Local data protection regulations
B. Risks from hackers residing in other countries
C. Impacts to existing contractual obligations
D. Time zone differences in log correlation

Correct Answer: A
Section:
Explanation:
Local data protection regulations are the first thing that a cloud-hosting provider should consider before expanding its data centers to new international locations. Data protection regulations are laws or standards that govern how personal or sensitive data is collected, stored, processed, and transferred across borders. Different countries or regions may have different data protection regulations, such as the General Data Protection Regulation (GDPR) in the European Union, the Personal Information Protection and Electronic Documents Act (PIPEDA) in Canada, or the California Consumer Privacy Act (CCPA) in the United States. A cloud-hosting provider must comply with the local data protection regulations of the countries or regions where it operates or serves customers, or else it may face legal penalties, fines, or reputational damage. Therefore, a cloud-hosting provider should research and understand the local data protection regulations of the new international locations before expanding its data centers there.Reference=CompTIA Security+ Study Guide with over 500 Practice Test Questions: Exam SY0-701, 9th Edition, Chapter 7, page 269. CompTIA Security+ SY0-701 Exam Objectives, Domain 5.1, page 14.

QUESTION 6

Which of the following would be the best way to block unknown programs from executing?

A. Access control list
B. Application allow list.
C. Host-based firewall
D. DLP solution

Correct Answer: B
Section:
Explanation:
An application allow list is a security technique that specifies which applications are permitted to run on a system or a network. An application allow list can block unknown programs from executing by only allowing the execution of programs that are explicitly authorized and verified.An application allow list can prevent malware, unauthorized software, or unwanted applications from running and compromising the security of the system or the network12.
The other options are not the best ways to block unknown programs from executing:
Access control list: This is a security technique that specifies which users or groups are granted or denied access to a resource or an object.An access control list can control the permissions and privileges of users or groups, but it does not directly block unknown programs from executing13.
Host-based firewall: This is a security device that monitors and filters the incoming and outgoing network traffic on a single host or system.A host-based firewall can block or allow network connections based on predefined rules, but it does not directly block unknown programs from executing1.
DLP solution: This is a security system that detects and prevents the unauthorized transmission or leakage of sensitive data.A DLP solution can protect the confidentiality and integrity of data, but it does not directly block unknown programs from executing1.
Reference=1: CompTIA Security+ SY0-701 Certification Study Guide, page 972: Application Whitelisting -- CompTIA Security+ SY0-701 -- 3.5, video by Professor Messer3: CompTIA Security+ SY0-701 Certification Study Guide, page 98. : CompTIA Security+ SY0-701 Certification Study Guide, page 99. : CompTIA Security+ SY0-701 Certification Study Guide, page 100.

QUESTION 7
A company hired a consultant to perform an offensive security assessment covering penetration testing and social engineering.
Which of the following teams will conduct this assessment activity?

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

Correct Answer: D
Section:
Explanation:
A red team is a group of security professionals who perform offensive security assessments covering penetration testing and social engineering. A red team simulates real-world attacks and exploits the vulnerabilities of a target organization, system, or network. A red team aims to test the effectiveness of the security controls, policies, and procedures of the target, as well as the awareness and response of the staff and the blue team. A red team can be hired as an external consultant or formed internally within the organization.Reference=CompTIA Security+ Study Guide with over 500 Practice Test Questions: Exam SY0-701, 9th Edition, Chapter 1, page 18. CompTIA Security+ (SY0-701) Certification Exam Objectives, Domain 1.8, page 4.Security Teams -- SY0-601 CompTIA Security+ : 1.8

QUESTION 8
A systems administrator is looking for a low-cost application-hosting solution that is cloud-based. Which of the following meets these requirements?

A. Serverless framework
B. Type 1 hvpervisor
C. SD-WAN
D. SDN

Correct Answer: A
Section:
Explanation:

A serverless framework is a cloud-based application-hosting solution that meets the requirements of low-cost and cloud-based. A serverless framework is a type of cloud computing service that allows developers to run applications without managing or provisioning any servers. The cloud provider handles the server-side infrastructure, such as scaling, load balancing, security, and maintenance, and charges the developer only for the resources consumed by the application. A serverless framework enables developers to focus on the application logic and functionality, and reduces the operational costs and complexity of hosting applications. Some examples of serverless frameworks are AWS Lambda, Azure Functions, and Google Cloud Functions.

A type 1 hypervisor, SD-WAN, and SDN are not cloud-based application-hosting solutions that meet the requirements of low-cost and cloud-based. A type 1 hypervisor is a software layer that runs directly on the hardware and creates multiple virtual machines that can run different operating systems and applications. A type 1 hypervisor is not a cloud-based service, but a virtualization technology that can be used to create private or hybrid clouds. A type 1 hypervisor also requires the developer to manage and provision the servers and the virtual machines, which can increase the operational costs and complexity of hosting applications. Some examples of type 1 hypervisors are VMware ESXi, Microsoft Hyper-V, and Citrix XenServer.

SD-WAN (Software-Defined Wide Area Network) is a network architecture that uses software to dynamically route traffic across multiple WAN connections, such as broadband, LTE, or MPLS. SD-WAN is not a cloud-based service, but a network optimization technology that can improve the performance, reliability, and security of WAN connections. SD-WAN can be used to connect remote sites or users to cloud-based applications, but it does not host the applications itself. Some examples of SD-WAN vendors are Cisco, VMware, and Fortinet.

SDN (Software-Defined Networking) is a network architecture that decouples the control plane from the data plane, and uses a centralized controller to programmatically manage and configure the network devices and traffic flows. SDN is not a cloud-based service, but a network automation technology that can enhance the scalability, flexibility, and efficiency of the network. SDN can be used to create virtual networks or network functions that can support cloud-based applications, but it does not host the applications itself. Some examples of SDN vendors are OpenFlow, OpenDaylight, and OpenStack.

Reference=CompTIA Security+ SY0-701 Certification Study Guide, page 264-265;Professor Messer's CompTIA SY0-701 Security+ Training Course, video 3.1 - Cloud and Virtualization, 7:40 - 10:00; [Serverless Framework]; [Type 1 Hypervisor]; [SD-WAN]; [SDN].

QUESTION 9

A security operations center determines that the malicious activity detected on a server is normal. Which of the following activities describes the act of ignoring detected activity in the future?

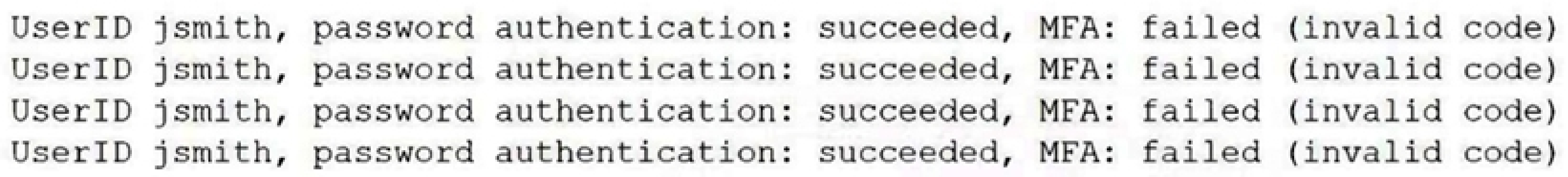
A. Tuning
B. Aggregating
C. Quarantining
D. Archiving

Correct Answer: A
Section:
Explanation:

Tuning is the activity of adjusting the configuration or parameters of a security tool or system to optimize its performance and reduce false positives or false negatives. Tuning can help to filter out the normal or benign activity that is detected by the security tool or system, and focus on the malicious or anomalous activity that requires further investigation or response. Tuning can also help to improve the efficiency and effectiveness of the security operations center by reducing the workload and alert fatigue of the analysts. Tuning is different from aggregating, which is the activity of collecting and combining data from multiple sources or sensors to provide a comprehensive view of the security posture. Tuning is also different from quarantining, which is the activity of isolating a potentially infected or compromised device or system from the rest of the network to prevent further damage or spread. Tuning is also different from archiving, which is the activity of storing and preserving historical data or records for future reference or compliance. The act of ignoring detected activity in the future that is deemed normal by the security operations center is an example of tuning, as it involves modifying the settings or rules of the security tool or system to exclude the activity from the detection scope. Therefore, this is the best answer among the given options.Reference=Security Alerting and Monitoring Concepts and Tools -- CompTIA Security+ SY0-701: 4.3, video at 7:00;CompTIA Security+ SY0-701 Certification Study Guide, page 191.

QUESTION 10

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.

Correct Answer: C
Section:
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.Reference=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

QUESTION 11
A company is concerned about weather events causing damage to the server room and downtime. Which of the following should the company consider?

A. Clustering servers

B. Geographic dispersion

C. Load balancers

D. Off-site backups

Correct Answer: B
Section:
Explanation:
Geographic dispersion is a strategy that involves distributing the servers or data centers across different geographic locations. Geographic dispersion can help the company to mitigate the risk of weather events causing damage to the server room and downtime, as well as improve the availability, performance, and resilience of the network.Geographic dispersion can also enhance the disaster recovery and business continuity capabilities of the company, as it can provide backup and failover options in case of a regional outage or disruption12.
The other options are not the best ways to address the company's concern:
Clustering servers: This is a technique that involves grouping multiple servers together to act as a single system.Clustering servers can help to improve the performance, scalability, and fault tolerance of the network, but it does not protect the servers from physical damage or downtime caused by weather events, especially if the servers are located in the same room or building3.
Load balancers: These are devices or software that distribute the network traffic or workload among multiple servers or resources.Load balancers can help to optimize the utilization, efficiency, and reliability of the network, but they do not prevent the servers from being damaged or disrupted by weather events, especially if the servers are located in the same room or building4.
Off-site backups: These are copies of data or files that are stored in a different location than the original source. Off-site backups can help to protect the data from being lost or corrupted by weather events, but they do not prevent the servers from being damaged or disrupted by weather events, nor do they ensure the availability or continuity of the network services.
Reference=1: CompTIA Security+ SY0-701 Certification Study Guide, page 972: High Availability -- CompTIA Security+ SY0-701 -- 3.4, video by Professor Messer3: CompTIA Security+ SY0-701 Certification Study Guide, page 984: CompTIA Security+ SY0-701 Certification Study Guide, page 99. : CompTIA Security+ SY0-701 Certification Study Guide, page 100.

QUESTION 12
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

Correct Answer: C
Section:
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.
Reference=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.

QUESTION 13
Which of the following security control types does an acceptable use policy best represent?

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

Correct Answer: D
Section:
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.
Reference=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

QUESTION 14
An IT manager informs the entire help desk staff that only the IT manager and the help desk lead will have access to the administrator console of the help desk software. Which of the following security techniques is the IT manager setting up?

A. Hardening
B. Employee monitoring

C. Configuration enforcement
D. Least privilege

Correct Answer: D
Section:
Explanation:
The principle of least privilege is a security concept that limits access to resources to the minimum level needed for a user, a program, or a device to perform a legitimate function. It is a cybersecurity best practice that protects high-value data and assets from compromise or insider threat. Least privilege can be applied to different abstraction layers of a computing environment, such as processes, systems, or connected devices. However, it is rarely implemented in practice.
In this scenario, the IT manager is setting up the principle of least privilege by restricting access to the administrator console of the help desk software to only two authorized users: the IT manager and the help desk lead. This way, the IT manager can prevent unauthorized or accidental changes to the software configuration, data, or functionality by other help desk staff. The other help desk staff will only have access to the normal user interface of the software, which is sufficient for them to perform their job functions.
The other options are not correct. Hardening is the process of securing a system by reducing its surface of vulnerability, such as by removing unnecessary software, changing default passwords, or disabling unnecessary services. Employee monitoring is the surveillance of workers' activity, such as by tracking web browsing, application use, keystrokes, or screenshots. Configuration enforcement is the process of ensuring that a system adheres to a predefined set of security settings, such as by applying a patch, a policy, or a template.
Reference=
https://en.wikipedia.org/wiki/Principle_of_least_privilege
https://en.wikipedia.org/wiki/Principle_of_least_privilege

QUESTION 15
Which of the following is the most likely to be used to document risks, responsible parties, and thresholds?

A. Risk tolerance
B. Risk transfer
C. Risk register
D. Risk analysis

Correct Answer: C
Section:
Explanation:
A risk register is a document that records and tracks the risks associated with a project, system, or organization. A risk register typically includes information such as the risk description, the risk owner, the risk probability, the risk impact, the risk level, the risk response strategy, and the risk status. A risk register can help identify, assess, prioritize, monitor, and control risks, as well as communicate them to relevant stakeholders. A risk register can also help document the risk tolerance and thresholds of an organization, which are the acceptable levels of risk exposure and the criteria for escalating or mitigating risks.Reference=CompTIA Security+ Certification Exam Objectives, Domain 5.1: Explain the importance of policies, plans, and procedures related to organizational security.CompTIA Security+ Study Guide (SY0-701), Chapter 5: Governance, Risk, and Compliance, page 211.CompTIA Security+ Certification Guide, Chapter 2: Risk Management, page 33.CompTIA Security+ Certification Exam SY0-701 Practice Test 1, Question 4.

QUESTION 16
Which of the following should a security administrator adhere to when setting up a new set of firewall rules?

A. Disaster recovery plan
B. Incident response procedure
C. Business continuity plan
D. Change management procedure

Correct Answer: D
Section:
Explanation:
A change management procedure is a set of steps and guidelines that a security administrator should adhere to when setting up a new set of firewall rules. A firewall is a device or software that can filter, block, or allow

network traffic based on predefined rules or policies. A firewall rule is a statement that defines the criteria and action for a firewall to apply to a packet or a connection. For example, a firewall rule can allow or deny traffic based on the source and destination IP addresses, ports, protocols, or applications. Setting up a new set of firewall rules is a type of change that can affect the security, performance, and functionality of the network. Therefore, a change management procedure is necessary to ensure that the change is planned, tested, approved, implemented, documented, and reviewed in a controlled and consistent manner. A change management procedure typically includes the following elements:
A change request that describes the purpose, scope, impact, and benefits of the change, as well as the roles and responsibilities of the change owner, implementer, and approver.
A change assessment that evaluates the feasibility, risks, costs, and dependencies of the change, as well as the alternatives and contingency plans.
A change approval that authorizes the change to proceed to the implementation stage, based on the criteria and thresholds defined by the change policy.
A change implementation that executes the change according to the plan and schedule, and verifies the results and outcomes of the change.
A change documentation that records the details and status of the change, as well as the lessons learned and best practices.
A change review that monitors and measures the performance and effectiveness of the change, and identifies any issues or gaps that need to be addressed or improved.
A change management procedure is important for a security administrator to adhere to when setting up a new set of firewall rules, as it can help to achieve the following objectives:
Enhance the security posture and compliance of the network by ensuring that the firewall rules are aligned with the security policies and standards, and that they do not introduce any vulnerabilities or conflicts.
Minimize the disruption and downtime of the network by ensuring that the firewall rules are tested and validated before deployment, and that they do not affect the availability or functionality of the network services or applications.
Improve the efficiency and quality of the network by ensuring that the firewall rules are optimized and updated according to the changing needs and demands of the network users and stakeholders, and that they do not cause any performance or compatibility issues.
Increase the accountability and transparency of the network by ensuring that the firewall rules are documented and reviewed regularly, and that they are traceable and auditable by the relevant authorities and parties.
The other options are not correct because they are not related to the process of setting up a new set of firewall rules. A disaster recovery plan 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. An incident response procedure is a set of steps and guidelines that aim to contain, analyze, eradicate, and recover from a security incident, such as a cyberattack, data breach, or malware infection. A business continuity plan is a set of strategies and actions that aim to maintain the essential functions and operations of an organization during and after a disruptive event, such as a pandemic, power outage, or civil unrest.Reference=CompTIA Security+ Study Guide (SY0-701), Chapter 7: Resilience and Recovery, page 325.Professor Messer's CompTIA SY0-701 Security+ Training Course, Section 1.3: Security Operations, video: Change Management (5:45).

QUESTION 17
A company is expanding its threat surface program and allowing individuals to security test the company's internet-facing application. The company will compensate researchers based on the vulnerabilities discovered. Which of the following best describes the program the company is setting up?

A. Open-source intelligence
B. Bug bounty
C. Red team
D. Penetration testing

Correct Answer: B
Section:
Explanation:
A bug bounty is a program that rewards security researchers for finding and reporting vulnerabilities in an application or system. Bug bounties are often used by companies to improve their security posture and incentivize ethical hacking. A bug bounty program typically defines the scope, rules, and compensation for the researchers.Reference=CompTIA Security+ Study Guide with over 500 Practice Test Questions: Exam SY0-701, 9th Edition, Chapter 1, page 10. CompTIA Security+ (SY0-701) Certification Exam Objectives, Domain 1.1, page 2.

QUESTION 18
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

Correct Answer: C
Section:

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.Reference=1: CompTIA Security+ SY0-701 Certification Study Guide, page 542: Threat Actors -- CompTIA Security+ SY0-701 -- 2.1, video by Professor Messer.

QUESTION 19
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

Correct Answer: D
Section:
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.Reference=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.

QUESTION 20
Employees in the research and development business unit receive extensive training to ensure they understand how to best protect company data. Which of the following is the type of data these employees are most likely to use in day-to-day work activities?

A. Encrypted
B. Intellectual property
C. Critical
D. Data in transit

Correct Answer: B
Section:
Explanation:
Intellectual property is a type of data that consists of ideas, inventions, designs, or other creative works that have commercial value and are protected by law. Employees in the research and development business unit are most likely to use intellectual property data in their day-to-day work activities, as they are involved in creating new products or services for the company. Intellectual property data needs to be protected from unauthorized use, disclosure, or theft, as it can give the company a competitive advantage in the market. Therefore, these employees receive extensive training to ensure they understand how to best protect this type of data.Reference=CompTIA Security+ SY0-701 Certification Study Guide, page 90;Professor Messer's CompTIA SY0-701 Security+ Training Course, video 1.2 - Security Concepts, 7:57 - 9:03.

QUESTION 21
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.

Correct Answer: A, F
Section:
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.Reference=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).

QUESTION 22
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 training.
D. Implement a phishing campaign

Correct Answer: C
Section:
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.Reference=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.

QUESTION 23
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

Correct Answer: D

Section:
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.Reference=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.

QUESTION 24
A systems administrator receives the following alert from a file integrity monitoring tool:
The hash of the cmd.exe file has changed.
The systems administrator checks the OS logs and notices that no patches were applied in the last two months. Which of the following most likely occurred?

A. The end user changed the file permissions.
B. A cryptographic collision was detected.
C. A snapshot of the file system was taken.
D. A rootkit was deployed.

Correct Answer: D
Section:
Explanation:

A rootkit is a type of malware that modifies or replaces system files or processes to hide its presence and activity. A rootkit can change the hash of the cmd.exe file, which is a command-line interpreter for Windows systems, to avoid detection by antivirus or file integrity monitoring tools. A rootkit can also grant the attacker remote access and control over the infected system, as well as perform malicious actions such as stealing data, installing backdoors, or launching attacks on other systems. A rootkit is one of the most difficult types of malware to remove, as it can persist even after rebooting or reinstalling the OS.Reference=CompTIA Security+ Study Guide with over 500 Practice Test Questions: Exam SY0-701, 9th Edition, Chapter 4, page 147. CompTIA Security+ SY0-701 Exam Objectives, Domain 1.2, page 9.

QUESTION 25
Malware spread across a company's network after an employee visited a compromised industry blog. Which of the following best describes this type of attack?

A. Impersonation
B. Disinformation
C. Watering-hole
D. Smishing

Correct Answer: C
Section:
Explanation:
A watering-hole attack is a type of cyberattack that targets groups of users by infecting websites that they commonly visit. The attackers exploit vulnerabilities to deliver a malicious payload to the organization's network. The attack aims to infect users' computers and gain access to a connected corporate network. The attackers target websites known to be popular among members of a particular organization or demographic.The attack differs from phishing and spear-phishing attacks, which typically attempt to steal data or install malware onto users' devices1
In this scenario, the compromised industry blog is the watering hole that the attackers used to spread malware across the company's network. The attackers likely chose this blog because they knew that the employees of the company were interested in its content and visited it frequently. The attackers may have injected malicious code into the blog or redirected the visitors to a spoofed website that hosted the malware. The malware then infected the employees' computers and propagated to the network.
Reference 1:Watering Hole Attacks: Stages, Examples, Risk Factors & Defense ...

QUESTION 26
A newly identified network access vulnerability has been found in the OS of legacy IoT devices. Which of the following would best mitigate this vulnerability quickly?

A. Insurance
B. Patching
C. Segmentation
D. Replacement

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

QUESTION 27
A bank insists all of its vendors must prevent data loss on stolen laptops. Which of the following strategies is the bank requiring?

A. Encryption at rest
B. Masking
C. Data classification
D. Permission restrictions

Correct Answer: A
Section:
Explanation:
Encryption at rest is a strategy that protects data stored on a device, such as a laptop, by converting it into an unreadable format that can only be accessed with a decryption key or password. Encryption at rest can prevent data loss on stolen laptops by preventing unauthorized access to the data, even if the device is physically compromised. Encryption at rest can also help comply with data privacy regulations and standards that require data protection. Masking, data classification, and permission restrictions are other strategies that can help protect data, but they may not be sufficient or applicable for data stored on laptops. Masking is a technique that obscures sensitive data elements, such as credit card numbers, with random characters or symbols, but it is usually used for data in transit or in use, not at rest. Data classification is a process that assigns labels to data based on its sensitivity and business impact, but it does not protect the data itself. Permission restrictions are rules that define who can access, modify, or delete data, but they may not prevent unauthorized access if the laptop is stolen and the security controls are bypassed.
Reference: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, page 17-18, 372-373

QUESTION 28
Which of the following would be best suited for constantly changing environments?

A. RTOS
B. Containers
C. Embedded systems
D. SCADA

Correct Answer: B
Section:
Explanation:
Containers are a method of virtualization that allows applications to run in isolated environments with their own dependencies, libraries, and configurations. Containers are best suited for constantly changing environments

because they are lightweight, portable, scalable, and easy to deploy and update.Containers can also support microservices architectures, which enable faster and more frequent delivery of software features.Reference: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, Chapter 10: Mobile Device Security, page 5121

QUESTION 29
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

Correct Answer: B
Section:
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.Reference: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, Chapter 8: Secure Protocols and Services, page 382-3831; Chapter 9: Network Security, page 441-4421

QUESTION 30
Security controls in a data center are being reviewed to ensure data is properly protected and that human life considerations are included. Which of the following best describes how the controls should be set up?

A. Remote access points should fail closed.
B. Logging controls should fail open.
C. Safety controls should fail open.
D. Logical security controls should fail closed.

Correct Answer: C
Section:
Explanation:
Safety controls are security controls that are designed to protect human life and physical assets from harm or damage. Examples of safety controls include fire alarms, sprinklers, emergency exits, backup generators, and surge protectors. Safety controls should fail open, which means that they should remain operational or allow access when a failure or error occurs. Failing open can prevent or minimize the impact of a disaster, such as a fire, flood, earthquake, or power outage, on human life and physical assets. For example, if a fire alarm fails, it should still trigger the sprinklers and unlock the emergency exits, rather than remain silent and locked. Failing open can also ensure that essential services, such as healthcare, transportation, or communication, are available during a crisis. Remote access points, logging controls, and logical security controls are other types of security controls, but they should not fail open in a data center. Remote access points are security controls that allow users or systems to access a network or a system from a remote location, such as a VPN, a web portal, or a wireless access point. Remote access points should fail closed, which means that they should deny access when a failure or error occurs. Failing closed can prevent unauthorized or malicious access to the data center's network or systems, such as by hackers, malware, or rogue devices. Logging controls are security controls that record and monitor the activities and events that occur on a network or a system, such as user actions, system errors, security incidents, or performance metrics. Logging controls should also fail closed, which means that they should stop or suspend the activities or events when a failure or error occurs. Failing closed can prevent data loss, corruption, or tampering, as well as ensure compliance with regulations and standards. Logical security controls are security controls that use software or code to protect data and systems from unauthorized or malicious access, modification, or destruction, such as encryption, authentication, authorization, or firewall. Logical security controls should also fail closed, which means that they should block or restrict access when a failure or error occurs. Failing closed can prevent data breaches, cyberattacks, or logical flaws, as well as ensure confidentiality, integrity, and availability of data and systems.
Reference: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, page 142-143, 372-373, 376-377

QUESTION 31
Which of the following should a systems administrator use to ensure an easy deployment of resources within the cloud provider?

A. Software as a service
B. Infrastructure as code
C. Internet of Things
D. Software-defined networking

Correct Answer: B
Section:
Explanation:
Infrastructure as code (IaC) is a method of using code and automation to manage and provision cloud resources, such as servers, networks, storage, and applications. IaC allows for easy deployment, scalability, consistency, and repeatability of cloud environments. IaC is also a key component of DevSecOps, which integrates security into the development and operations processes.Reference:CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, Chapter 6: Cloud and Virtualization Concepts, page 294.

QUESTION 32
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

Correct Answer: D
Section:
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.Reference:CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, Chapter 3: Securing Networks, page 132.

QUESTION 33
During the onboarding process, an employee needs to create a password for an intranet account. The password must include ten characters, numbers, and letters, and two special characters. Once the password is created, the company will grant the employee access to other company-owned websites based on the intranet profile. Which of the following access management concepts is the company most likely using to safeguard intranet accounts and grant access to multiple sites based on a user's intranet account? (Select two).

A. Federation
B. Identity proofing
C. Password complexity
D. Default password changes
E. Password manager
F. Open authentication

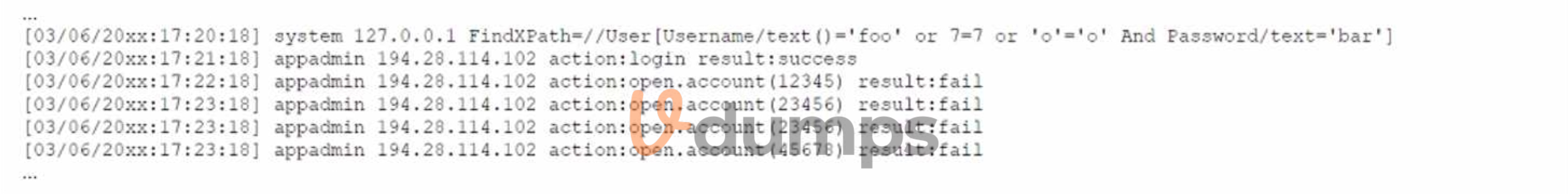
Correct Answer: A, C
Section:
Explanation:
Federation is an access management concept that allows users to authenticate once and access multiple resources or services across different domains or organizations. Federation relies on a trusted third party that stores the user's credentials and provides them to the requested resources or services without exposing them. Password complexity is a security measure that requires users to create passwords that meet certain criteria, such as length, character types, and uniqueness.Password complexity can help prevent brute-force attacks, password guessing, and credential stuffing by making passwords harder to crack or guess.Reference:CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, page 308-309 and 312-3131

QUESTION 34
A company currently uses passwords for logging in to company-owned devices and wants to add a second authentication factor Per corporate policy, users are not allowed to have smartphones at their desks Which of the following would meet these requirements?

A. Smart card
B. PIN code
C. Knowledge-based question
D. Secret key

Correct Answer: A
Section:
Explanation:
A smart card is a physical device that contains an embedded integrated circuit chip that can store and process data. A smart card can be used as a second authentication factor, in addition to a password, to verify the identity of a user who wants to log in to company-owned devices. A smart card requires a smart card reader to access the data on the chip, which adds an extra layer of security. A smart card meets the requirements of the company because it does not involve a smartphone or any other device that is not allowed at the desks

QUESTION 35
A security analyst receives a SIEM alert that someone logged in to the app admin test account, which is only used for the early detection of attacks. The security analyst then reviews the following application log:



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

Which of the following can the security analyst conclude?

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

Correct Answer: A
Section:
Explanation:
A replay attack is a type of network attack where an attacker captures and retransmits a valid data transmission, such as a login request, to gain unauthorized access or impersonate a legitimate user.
In this case, the attacker may have captured the credentials of the app admin test account and used them to log in to the application. The application log shows multiple failed login attempts from different IP addresses, which indicates a replay attack.

QUESTION 36
An organization is having difficulty correlating events from its individual AV. EDR. DLP. SWG. WAF, MDM. HIPS, and CASB systems. Which of the following is the best way to improve the situation?

A. Remove expensive systems that generate few alerts.
B. Modify the systems to alert only on critical issues.
C. Utilize a SIEM to centralize logs and dashboards.

D. Implement a new syslog/NetFlow appliance.

Correct Answer: C
Section:
Explanation:
A SIEM (Security Information and Event Management) is a system that collects, analyzes, and correlates data from multiple sources, such as AV (antivirus), EDR (endpoint detection and response), DLP (data loss prevention), SWG (secure web gateway), WAF (web application firewall), MDM (mobile device management), HIPS (host intrusion prevention system), and CASB (cloud access security broker). A SIEM can help improve the situation by providing a centralized view of the security posture, alerts, and incidents across the organization.

QUESTION 37
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

Correct Answer: D
Section:
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.