CompTIA

Exam Questions SY0-601

CompTIA Security+ Exam

NEW QUESTION 1
- (Exam Topic 1)
A company is implementing BYOD and wants to ensure all users have access to the same cloud-based services. Which of the following would BEST allow the company to meet this requirement?

A. laaS
B. PasS
C. MaaS
D. SaaS

Answer: D

NEW QUESTION 2
- (Exam Topic 1)
A company recently experienced a significant data loss when proprietary Information was leaked to a
competitor. The company took special precautions by using proper labels; however, email filter logs do not have any record of the incident. An Investigation confirmed the corporate network was not breached, but documents were downloaded from an employee's COPE tablet and passed to the competitor via cloud storage. Which of the following is the BEST mitigation strategy to prevent this from happening in the future?

A. User training
B. CASB
C. MDM
D. EDR

Answer: D

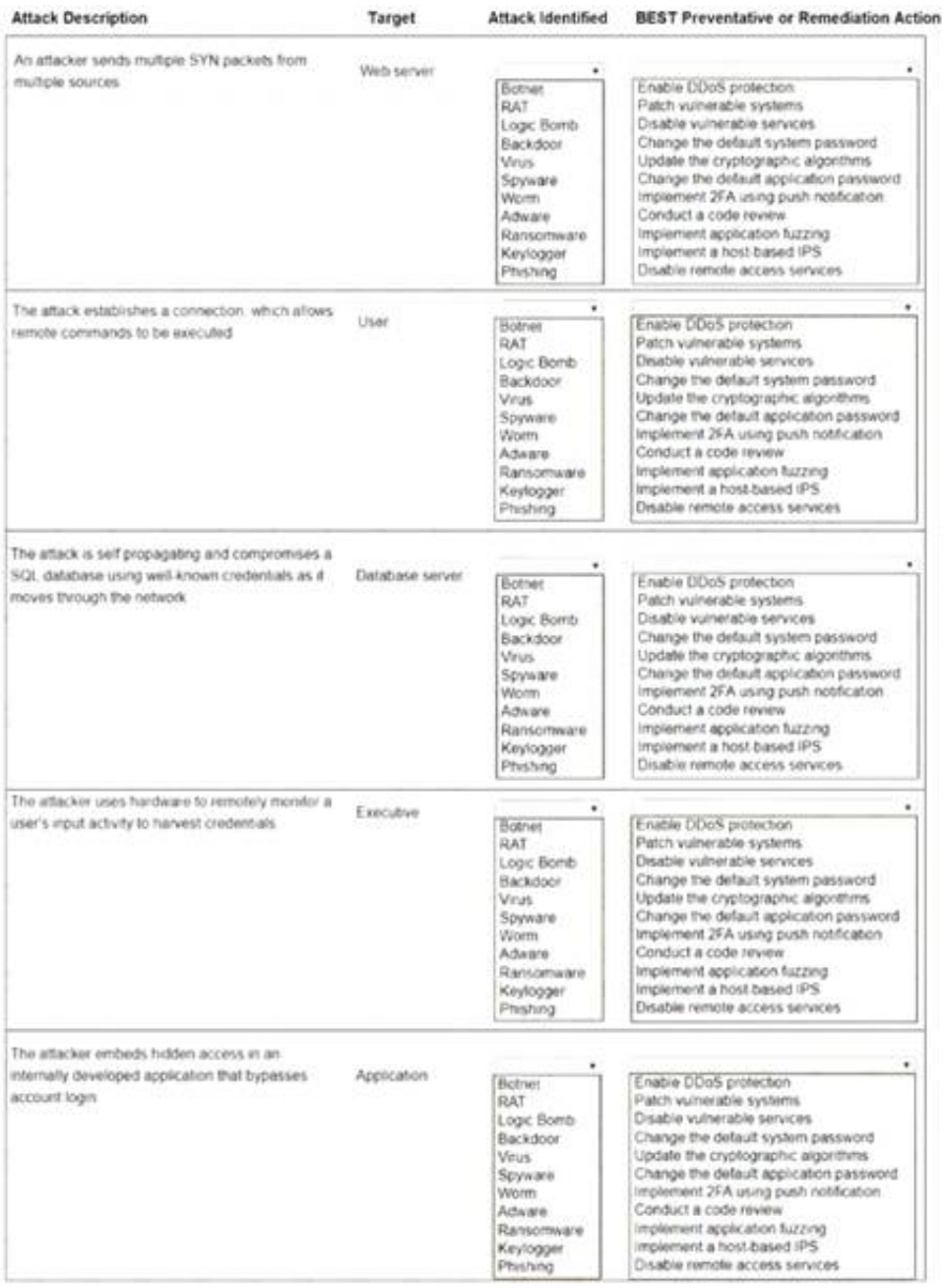
NEW QUESTION 3
- (Exam Topic 1)
Which of the following would BEST provide detective and corrective controls for thermal regulation?

A. A smoke detector
B. A fire alarm
C. An HVAC system
D. A fire suppression system
E. Guards

Answer: C

Explanation:
What are the functions of an HVAC system?
An HVAC system is designed to control the environment in which it works. It achieves this by controlling the temperature (THERMAL) of a room through heating and cooling. It also controls the humidity level in that environment by controlling the movement and distribution of air inside the room. So it provides detective and corrective controls for THERMAL regulation.

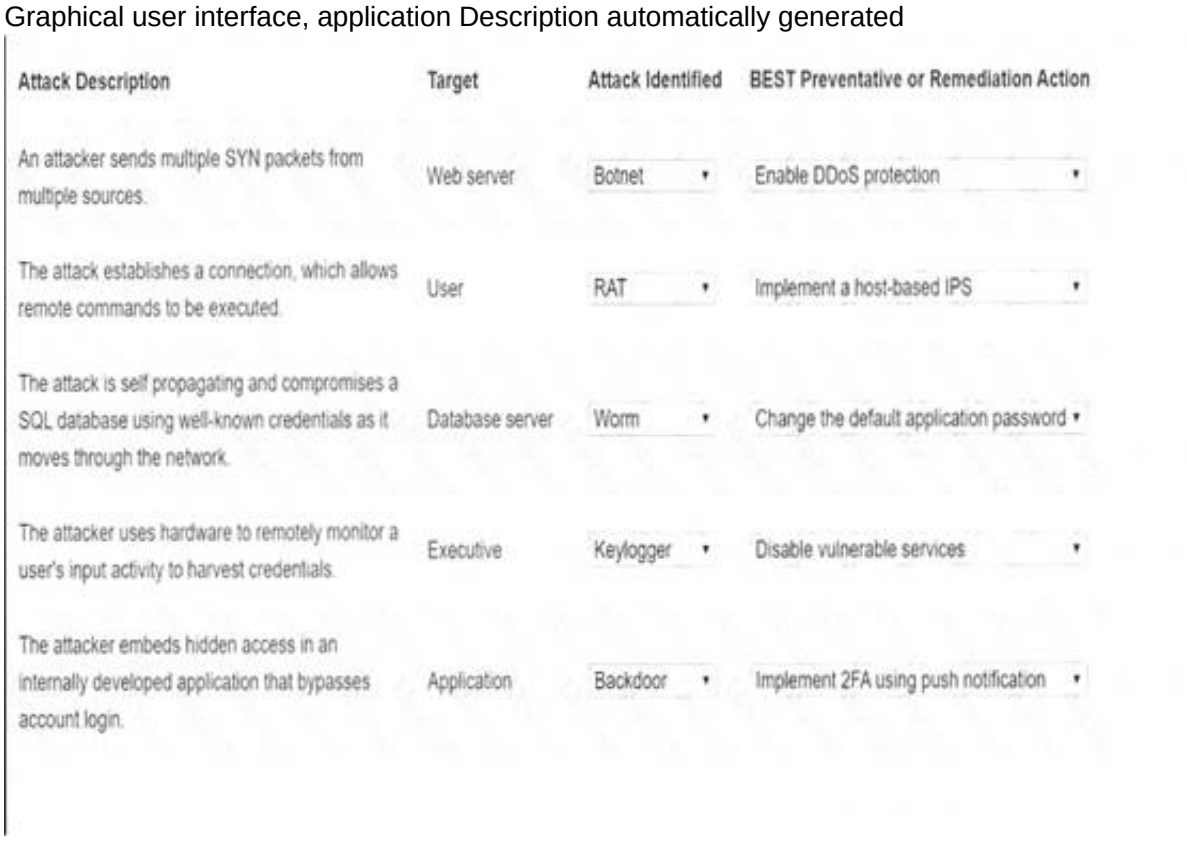
NEW QUESTION 4
- (Exam Topic 1)
Select the appropriate attack and remediation from each drop-down list to label the corresponding attack with its remediation.
INSTRUCTIONS
Not all attacks and remediation actions will be used.
If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.



A. Mastered
B. Not Mastered

Answer: A

Explanation:
Web serverBotnet Enable DDoS protectionUser RAT Implement a host-based IPSDatabase server Worm Change the default application passwordExecutive KeyloggerDisable vulnerable servicesApplication Backdoor Implement 2FA using push notification
Graphical user interface, application Description automatically generated



NEW QUESTION 5
- (Exam Topic 1)
The Chief Information Secunty Officer (CISO) requested a report on potential areas of improvement following a security incident. Which of the following incident response processes is the CISO requesting?

A. Lessons learned
B. Preparation
C. Detection
D. Containment

E. Root cause analysis

Answer: A

NEW QUESTION 6
- (Exam Topic 1)
Certain users are reporting their accounts are being used to send unauthorized emails and conduct suspicious activities After further investigation, a security analyst notices the following
• All users share workstations throughout the day
• Endpoint protection was disabled on several workstations throughout the network.
• Travel times on logins from the affected users are impossible
• Sensitive data is being uploaded to external sites
• All usee account passwords were forced lo be reset and the issue continued Which of the following attacks is being used to compromise the user accounts?

A. Brute-force
B. Keylogger
C. Dictionary
D. Rainbow

Answer: C

NEW QUESTION 7
- (Exam Topic 1)
Which of the following would BEST provide a systems administrator with the ability to more efficiently identify systems and manage permissions and policies based on location, role, and service level?

A. Standard naming conventions
B. Domain services
C. Baseline configurations
D. Diagrams

Answer: C

NEW QUESTION 8
- (Exam Topic 1)
A security analyst was called to investigate a file received directly from a hardware manufacturer. The analyst is trying to determine whether odified in transit before installation on the user's computer. Which of the following can be used to safely assess the file?

A. Check the hash of the installation file
B. Match the file names
C. Verify the URL download location
D. Verify the code-signing certificate

Answer: A

Explanation:
The hardware manufacturer will post the hash of the file publicly, and anyone who receives a copy of that file will be able to run a checksum on the file themselves, and compare them to the official manufacturer-provided checksum. Hashing is almost always the correct answer in these type of questions. You'll see a lot of Github repositories using hashed checksums as well for verification, and I recently just installed Java onto my new computer. Java provided me with a hashed checksum for the setup executable.

NEW QUESTION 9
- (Exam Topic 1)
A business operations manager is concerned that a PC that is critical to business operations will have a costly hardware failure soon. The manager is looking for options to continue business operations without incurring large costs. Which of the following would mitigate the manager's concerns?

A. Implement a full system upgrade
B. Perform a physical-to-virtual migration
C. Install uninterruptible power supplies
D. Purchase cybersecurity insurance

Answer: B

NEW QUESTION 10
- (Exam Topic 1)
Which of the following would detect intrusions at the perimeter of an airport?

A. Signage
B. Fencing
C. Motion sensors
D. Lighting
E. Bollards

Answer: C

NEW QUESTION 10
- (Exam Topic 1)

A security incident has been resolved Which of the following BEST describes the importance of the final phase of the incident response plan?

A. It examines and documents how well the team responded discovers what caused the incident, and determines how the incident can be avoided in the future
B. It returns the affected systems back into production once systems have been fully patched, data restored and vulnerabilities addressed
C. It identifies the incident and the scope of the breach how it affects the production environment, and the ingress point
D. It contains the affected systems and disconnects them from the network, preventing further spread of the attack or breach

Answer: A

NEW QUESTION 13
- (Exam Topic 1)
An organization is migrating several SaaS applications that support SSO. The security manager wants to ensure the migration is completed securely. Which of the following should the organization consider before implementation? (Select TWO).

A. The back-end directory source
B. The identity federation protocol
C. The hashing method
D. The encryption method
E. The registration authority
F. The certificate authority

Answer: CF

NEW QUESTION 15
- (Exam Topic 1)
A security analyst is investigating some users who are being redirected to a fake website that resembles www.comptia.org. The following output was found on the naming server of the organization:

Name	Type	Data
www	A	192.168.1.10
server1	A	10.10.10.10
server2	A	10.10.10.11
file	A	10.10.10.12

Which of the following attacks has taken place?

A. Domain reputation
B. Domain hijacking
C. Disassociation
D. DNS poisoning

Answer: D

NEW QUESTION 18
- (Exam Topic 1)
An organization is building backup server rooms in geographically diverse locations The Chief Information Security Officer implemented a requirement on the project that states the new hardware cannot be susceptible to the same vulnerabilities in the existing server room Which of the following should the systems engineer consider?

A. Purchasing hardware from different vendors
B. Migrating workloads to public cloud infrastructure
C. Implementing a robust patch management solution
D. Designing new detective security controls

Answer: A

NEW QUESTION 23
- (Exam Topic 1)
Which of the following tools is effective in preventing a user from accessing unauthorized removable media?

A. USB data blocker
B. Faraday cage
C. Proximity reader
D. Cable lock

Answer: B

NEW QUESTION 27
- (Exam Topic 1)
Which of the following would be the BEST way to analyze diskless malware that has infected a VDI?

A. Shut down the VDI and copy off the event logs.
B. Take a memory snapshot of the running system.
C. Use NetFlow to identify command-and-control IPs.
D. Run a full on-demand scan of the root volume.

Answer: B

NEW QUESTION 30
- (Exam Topic 1)
A large bank with two geographically dispersed data centers is concerned about major power disruptions at both locations Every day each location expenences very bnef outages that last for a few seconds However dunng the summer a high risk of intentional brownouts that last up to an hour exists particularly at one of the locations near an jndustnal smelter. Which of the following is the BEST solution to reduce the risk of data loss?

A. Dual supply
B. Generator
C. PDU
D. Daily backups

Answer: B

NEW QUESTION 32
- (Exam Topic 1)
A customer service representative reported an unusual text message that was sent to the help desk. The message contained an unrecognized invoice number with a large balance due and a link to click for more details. Which of the following BEST descnbes this technique?

A. Vishing
B. Whaling
C. Phishing
D. Smishing

Answer: D

NEW QUESTION 34
- (Exam Topic 1)
An organization discovered files with proprietary financial data have been deleted. The files have been recovered from backup but every time the Chief Financial Officer logs in to the file server, the same files are deleted again No other users are experiencing this issue. Which of the following types of malware is MOST likely causing this behavior?

A. Logic bomb
B. Crypto malware
C. Spyware
D. Remote access Trojan

Answer: A

Explanation:
Logic bomb: a set of instructions secretly incorporated into a program so that if a particular condition is satisfied they will be carried out, usually with harmful effects.

NEW QUESTION 35
- (Exam Topic 1)
Which biometric error would allow an unauthorized user to access a system?

A. False acceptance
B. False entrance
C. False rejection
D. False denial

Answer: C

NEW QUESTION 39
- (Exam Topic 1)
Which of the following risk management strategies would an organization use to maintain a legacy system with known risks for operational purposes?

A. Acceptance
B. Transference
C. Avoidance
D. Mitigation

Answer: A

NEW QUESTION 40
- (Exam Topic 1)
While reviewing an alert that shows a malicious request on one web application, a cybersecurity analyst is alerted to a subsequent token reuse moments later on a different service using the same single sign-on method. Which of the following would BEST detect a malicious actor?

A. Utilizing SIEM correlation engines
B. Deploying Netflow at the network border
C. Disabling session tokens for all sites
D. Deploying a WAF for the web server

Answer: A

Explanation:

The initial compromise was a malicious request on a web server. Moments later the token created with SSO was used on another service, the question does not specify what type of service. Deploying a WAF on the web server will detect the attacker but only on that server. If the attacker issues the same malicious request to get another SSO token correlating that event with using that SSO token in other services would allows to detect the malicious activity.

NEW QUESTION 43
- (Exam Topic 1)
During a recent incident an external attacker was able to exploit an SMB vulnerability over the internet. Which of the following action items should a security analyst perform FIRST to prevent this from occurring again?

A. Check for any recent SMB CVEs
B. Install AV on the affected server
C. Block unneeded TCP 445 connections
D. Deploy a NIDS in the affected subnet

Answer: C

NEW QUESTION 44
- (Exam Topic 1)
The Chief Compliance Officer from a bank has approved a background check policy for all new hires Which of the following is the policy MOST likely protecting against?

A. Preventing any current employees' siblings from working at the bank to prevent nepotism
B. Hiring an employee who has been convicted of theft to adhere to industry compliance
C. Filtenng applicants who have added false information to resumes so they appear better qualified
D. Ensuring no new hires have worked at other banks that may be trying to steal customer information

Answer: B

NEW QUESTION 48
- (Exam Topic 1)
An IT manager is estimating the mobile device budget for the upcoming year Over the last five years, the number of devices that were replaced due to loss damage or theft steadily increased by 10%. Which of the following would BEST describe the estimated number of devices to be replaced next year?

A. ALE
B. ARO
C. RPO
D. SLE

Answer: A

NEW QUESTION 53
- (Exam Topic 1)
A software company adopted the following processes before releasing software to production;
• Peer review
• Static code scanning
• Signing
A considerable number of vulnerabilities are still being detected when code is executed on production Which of the following security tools can improve vulnerability detection on this environment?

A. File integrity monitonng for the source code
B. Dynamic code analysis tool
C. Encrypted code repository
D. Endpoint detection and response solution

Answer: A

NEW QUESTION 55
- (Exam Topic 1)
An organization wants to participate in threat intelligence information sharing with peer groups. Which of the following would MOST likely meet the organizations requirement?

A. Perform OSINT investigations
B. Subscribe to threat intelligence feeds
C. Submit RFCs
D. Implement a TAXII server

Answer: B

NEW QUESTION 60
- (Exam Topic 1)
Which of the following control types is focused primarily on reducing risk before an incident occurs?

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

Answer: D

NEW QUESTION 64
- (Exam Topic 1)
Data exftitration analysis indicates that an attacker managed to download system configuration notes from a web server. The web-server logs have been deleted, but analysts have determined that the system configuration notes were stored in the database administrator's folder on the web server Which of the following attacks explains what occurred? (Select TWO)

A. Pass-the- hash
B. Directory traversal
C. SQL injection
D. Privilege escalation
E. Cross-site scnpting
F. Request forgery

Answer: AD

NEW QUESTION 68
- (Exam Topic 1)
Which of the following statements BEST describes zero-day exploits'?

A. When a zero-day exploit is discovered, the system cannot be protected by any means
B. Zero-day exploits have their own scoring category in CVSS
C. A zero-day exploit is initially undetectable and no patch for it exists
D. Discovering zero-day exploits is always performed via bug bounty programs

Answer: C

NEW QUESTION 73
- (Exam Topic 1)
A company wants to restrict emailing of PHI documents. The company is implementing a DLP solution In order to reslnct PHI documents which of the following should be performed FIRST?

A. Retention
B. Governance
C. Classification
D. Change management

Answer: C

NEW QUESTION 76
- (Exam Topic 1)
During a recent penetration test, the tester discovers large amounts of data were exfiltrated over the course of 12 months via the internet. The penetration tester stops the test to inform the client of the findings Which of the following should be the client's NEXT step to mitigate the issue"

A. Conduct a full vulnerability scan to identify possible vulnerabilities
B. Perform containment on the critical servers and resources
C. Review the firewall and identify the source of the active connection
D. Disconnect the entire infrastructure from the internet

Answer: D

NEW QUESTION 80
- (Exam Topic 1)
A company is auditing the manner in which its European customers' personal information is handled Which of the following should the company consult?

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

Answer: A

NEW QUESTION 84
- (Exam Topic 1)
Which of the following is the GREATEST security concern when outsourcing code development to third-party contractors for an internet-facing application?

A. Intellectual property theft
B. Elevated privileges
C. Unknown backdoor
D. Quality assurance

Answer: C

NEW QUESTION 85

- (Exam Topic 1)
Which of the following would be indicative of a hidden audio file found inside of a piece of source code?

A. Steganography
B. Homomotphic encryption
C. Cipher surte
D. Blockchain

Answer: A

Explanation:
Steganography is the technique of hiding secret data within an ordinary, non-secret, file or message in order to avoid detection; the secret data is then extracted at its destination. The use of steganography can be combined with encryption as an extra step for hiding or protecting data. The word steganography is derived from the Greek words steganos (meaning hidden or covered) and the Greek root graph (meaning to write).

NEW QUESTION 86
- (Exam Topic 1)
A security analyst is working on a project to implement a solution that monitors network communications and provides alerts when abnormal behavior is detected Which of the following is the security analyst MOST likely implementing?

A. Vulnerability scans
B. User behavior analysis
C. Security orchestration, automation, and response
D. Threat hunting

Answer: C

Explanation:
SOAR solutions automatically aggregate and validate data from various sources, including threat intelligence, security information and event management (SIEM), and user and entity behavior analytics (UEBA) tools. It helps make security operations centers (SOCs) intelligence-driven, providing the context needed to make informed decisions and accelerate detection and response.

NEW QUESTION 87
- (Exam Topic 1)
A security analyst is receiving numerous alerts reporting that the response time of an internet-facing application has been degraded However, the internal network performance was not degraded. Which of the following MOST likely explains this behavior?

A. DNS poisoning
B. MAC flooding
C. DDoS attack
D. ARP poisoning

Answer: C

NEW QUESTION 92
- (Exam Topic 1)
Which of the following control Types would be BEST to use in an accounting department to reduce losses from fraudulent transactions?

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

Answer: C

Explanation:
Corrective controls are implemented after detective controls to rectify the problem and (ideally) prevent it from happening again.

NEW QUESTION 95
- (Exam Topic 1)
A junior security analyst iss conducting an analysis after passwords were changed on multiple accounts without users' interaction. The SIEM have multiple logtn entnes with the following text:

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

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

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

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

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

A. Malicious script
B. Privilege escalation
C. Doman hijacking
D. DNS poisoning

Answer: A

NEW QUESTION 98
- (Exam Topic 1)
During a trial, a judge determined evidence gathered from a hard drive was not admissible. Which of the following BEST explains this reasoning?

A. The forensic investigator forgot to run a checksum on the disk image after creation
B. The chain of custody form did not note time zone offsets between transportation regions
C. The computer was turned of
D. and a RAM image could not be taken at the same time
E. The hard drive was not properly kept in an antistatic bag when rt was moved

Answer: A

NEW QUESTION 100
- (Exam Topic 1)
An engineer recently deployed a group of 100 web servers in a cloud environment. Per the security policy, all web-server ports except 443 should be disabled. Which of the following can be used to accomplish this task?

A. Application allow list
B. SWG
C. Host-based firewall
D. VPN

Answer: B

NEW QUESTION 101
- (Exam Topic 1)
Which of the following documents provides expectations at a technical level for quality, availability, and responsibilities?

A. EOL
B. SLA
C. MOU
D. EOSL

Answer: B

NEW QUESTION 102
- (Exam Topic 1)
The Chief Information Security Officer wants to prevent exfiltration of sensitive information from employee cell phones when using public USB power charging stations. Which of the following would be the BEST solution to Implement?

A. DLP
B. USB data blocker
C. USB OTG
D. Disabling USB ports

Answer: A

Explanation:
USB data blockers are good, but they're reliant on the employee actually using them. A DLP solution such as MobileIron forces compliance, by locking corporate resources behind a secure application. For example: Users any mobile device policy, such as BYOD, CYOD, and COPE. If they want to access their corporate email on their phone. They will need to sign into the MobileIron application, in order to be granted visibility to their corporate email account. Since the emails are being read/sent through the MobileIron application. Safeguards can be applied even on an outside network-mobile level. If an employee attempts to send a customers social security number, the MobileIron will either block it, alert it, or both, contingent on how the company setup the MobileIron service to work.

NEW QUESTION 107
- (Exam Topic 1)
The Chief Information Security Officer (CISO) has requested that a third-party vendor provide supporting documents that show proper controls are in place to protect customer data. Which of the following would be BEST for the third-party vendor to provide to the CISO?

A. GDPR compliance attestation
B. Cloud Security Alliance materials
C. SOC 2 Type 2 report
D. NIST RMF workbooks

Answer: C

Explanation:
https://www.itgovernance.co.uk/soc-reporting

NEW QUESTION 110
- (Exam Topic 1)
An administrator is experiencing issues when trying to upload a support file to a vendor A pop-up message reveals that a payment card number was found in the file, and the file upload was Mocked. Which of the following controls is most likely causing this issue and should be checked FIRST?

A. DLP
B. Firewall rule
C. Content filter
D. MDM

E. Application allow list

Answer: A

NEW QUESTION 111
- (Exam Topic 1)
A security policy states that common words should not be used as passwords. A security auditor was able to perform a dictionary attack against corporate credentials Which of the following controls was being violated?

A. Password complexity
B. Password history
C. Password reuse
D. Password length

Answer: B

NEW QUESTION 116
- (Exam Topic 1)
As part of a security compliance assessment, an auditor performs automated vulnerability scans. In addition, which of the following should the auditor do to complete the assessment?

A. User behavior analysis
B. Packet captures
C. Configuration reviews
D. Log analysis

Answer: D

Explanation:
A vulnerability scanner is essentially doing that. It scans every part of your network configuration that it can, and determines if known vulnerabilities are known at any point of that.

NEW QUESTION 120
- (Exam Topic 1)
A user enters a username and a password at the login screen for a web portal. A few seconds later the following message appears on the screen: Please use a combination of numbers, special characters, and letters in the password field. Which of the following concepts does this message describe?

A. Password complexity
B. Password reuse
C. Password history
D. Password age

Answer: A

NEW QUESTION 123
- (Exam Topic 1)
Which of the following is the MOST relevant security check to be performed before embedding third-parry libraries in developed code?

A. Check to see if the third party has resources to create dedicated development and staging environments.
B. Verify the number of companies that downloaded the third-party code and the number of contributions on the code repository.
C. Assess existing vulnerabilities affecting the third-parry code and the remediation efficiency of the libraries' developers.
D. Read multiple penetration-testing reports for environments running software that reused the library.

Answer: D

NEW QUESTION 128
- (Exam Topic 1) A
user is attempting to navigate to a website from inside the company network using a desktop. When the user types in the URL. https://www.site.com, the user is presented with a certificate mismatch warning from the browser. The user does not receive a warning when visiting http://www.anothersite.com. Which of the following describes this attack?

A. On-path
B. Domain hijacking
C. DNS poisoning
D. Evil twin

Answer: C

NEW QUESTION 130
- (Exam Topic 1)
A security analyst needs to be able to search and correlate logs from multiple sources in a single tool Which of the following would BEST allow a security analyst to have this ability?

A. SOAR
B. SIEM
C. Log collectors
D. Network-attached storage

Answer: B

Explanation:
SIEM event correlation is an essential part of any SIEM solution. It aggregates and analyzes log data from across your network applications, systems, and devices, making it possible to discover security threats and malicious patterns of behaviors that otherwise go unnoticed and can lead to compromise or data loss.

NEW QUESTION 131
- (Exam Topic 1)
Which of the following organizations sets frameworks and controls for optimal security configuration on systems?

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

Answer: D

NEW QUESTION 133
- (Exam Topic 1)
Which of the following is the MOST effective control against zero-day vulnerabilities?

A. Network segmentation
B. Patch management
C. Intrusion prevention system
D. Multiple vulnerability scanners

Answer: A

NEW QUESTION 138
- (Exam Topic 1)
The SOC for a large MSSP is meeting to discuss the lessons learned from a recent incident that took much too long to resolve This type of incident has become more common in recent weeks and is consuming large amounts of the analysts' time due to manual tasks being performed Which of the following solutions should the SOC consider to BEST improve its response time?

A. Configure a NIDS appliance using a Switched Port Analyzer
B. Collect OSINT and catalog the artifacts in a central repository
C. Implement a SOAR with customizable playbooks
D. Install a SIEM with community-driven threat intelligence

Answer: C

Explanation:
SOAR (Security Orchestration, Automation, and Response) Can use either playbook or runbook. It assists in collecting threat related data from a range of sources and automate responses to low level threats. (frees up some of the CSIRT time)

NEW QUESTION 139
- (Exam Topic 1)
A security analyst has been asked by the Chief Information Security Officer to
• develop a secure method of providing centralized management of infrastructure
• reduce the need to constantly replace aging end user machines
• provide a consistent user desktop expenence
Which of the following BEST meets these requirements?

A. BYOD
B. Mobile device management
C. VDI
D. Containers ation

Answer: C

NEW QUESTION 143
- (Exam Topic 1)
A security analyst was asked to evaluate a potential attack that occurred on a publicly accessible section of the company's website The malicious actor posted an entry in an attempt to trick users into cltckmg the following:

```
https://www.c0mptia.com/contact-us/%3Fname%3D%3Cscript%3Ealert(document.cookie)%3C%2Fscript%3E
```

Which of the following was MOST likely observed?

A. DLL injection
B. Session replay
C. SOLI
D. XSS

Answer: B

NEW QUESTION 146
- (Exam Topic 1)

Two organizations plan to collaborate on the evaluation of new SIEM solutions for their respective companies. A combined effort from both organizations' SOC teams would speed up the effort. Which of the following can be written to document this agreement?

A. MOU
B. ISA
C. SLA
D. NDA

Answer: A

Explanation:
A document that regulates security-relevant aspects of an intended connection between an agency and an external system. It regulates the security interface between any two systems operating under two different distinct authorities. It includes a variety of descriptive, technical, procedural, and planning information. It is usually preceded by a formal MOA/MOU that defines high- level roles and responsibilities in management of a cross-domain connection.
https://csrc.nist.gov/glossary/term/interconnection_security_agreement

NEW QUESTION 148
- (Exam Topic 1)
A database administrator wants to grant access to an application that will be reading and writing data to a database. The database is shared by other applications also used by the finance department Which of the following account types Is MOST appropriate for this purpose?

A. Service
B. Shared
C. eneric
D. Admin

Answer: A

NEW QUESTION 149
- (Exam Topic 1)
Which of the following will increase cryptographic security?

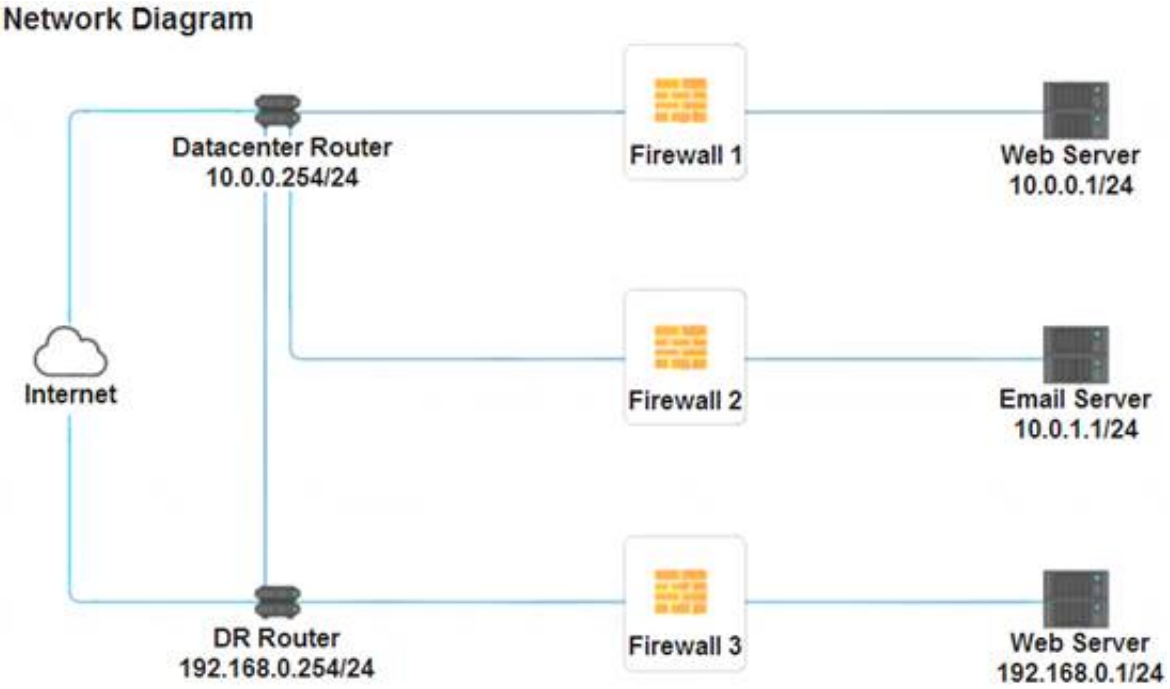
A. High data entropy
B. Algorithms that require less computing power
C. Longer key longevity
D. Hashing

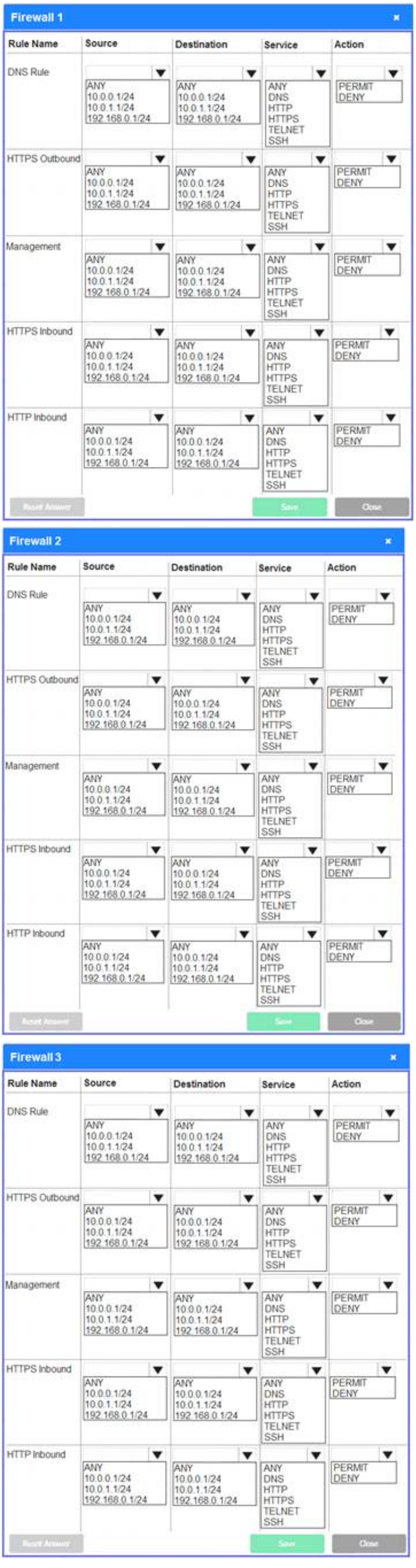
Answer: C

NEW QUESTION 150
- (Exam Topic 1)
A company recently added a DR site and is redesigning the network. Users at the DR site are having issues browsing websites.
INSTRUCTIONS
Click on each firewall to do the following:
- Deny cleartext web traffic.
- Ensure secure management protocols are used. Please Resolve issues at the DR site.

The ruleset order cannot be modified due to outside constraints.
If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.

Network Diagram

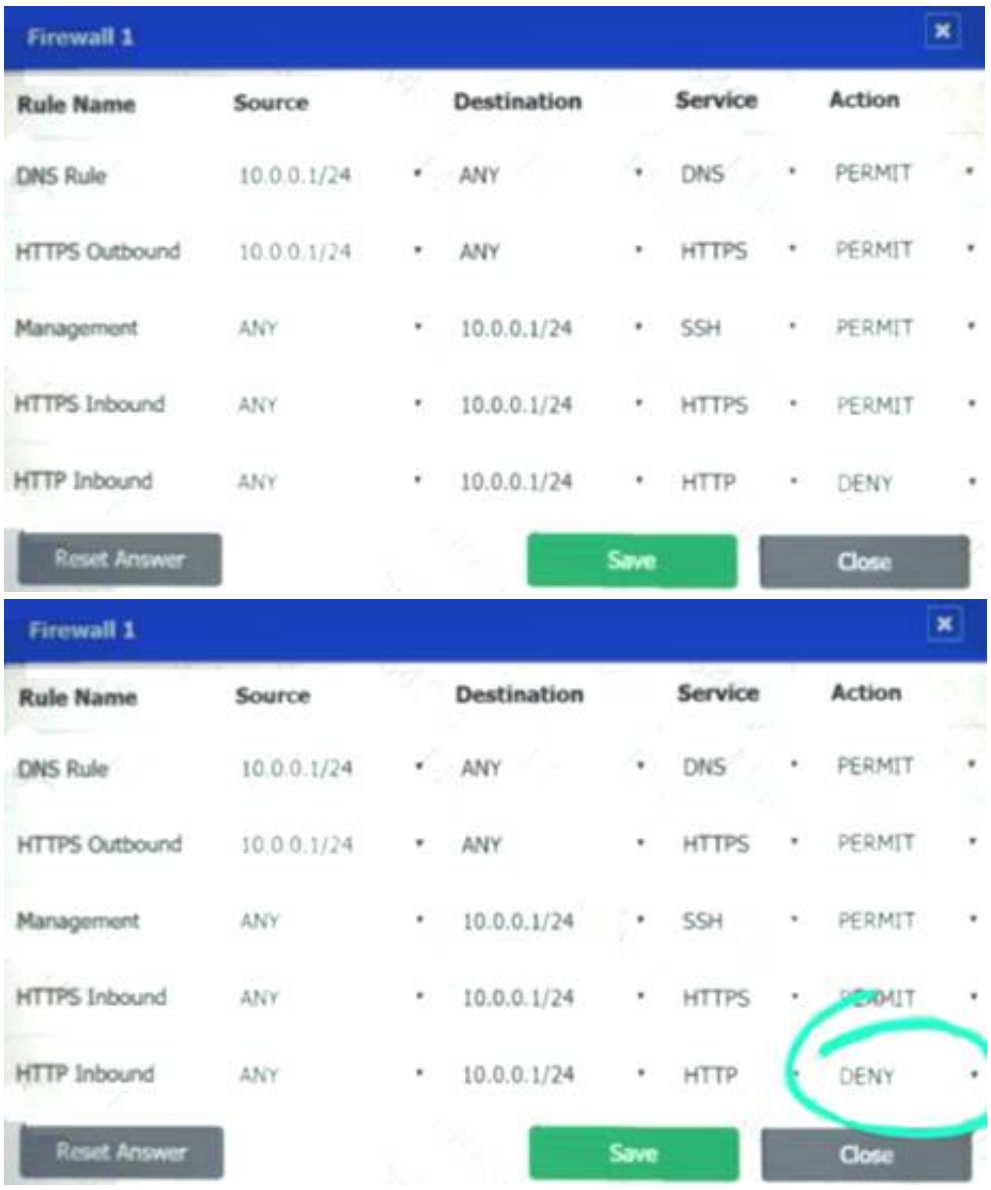



Firewall 1
Rule Name
Source
Destination
Service
Action
DNS Rule
HTTPS Outbound
Management
HTTPS Inbound
HTTP Inbound
ANY
10.0.0.1/24
10.0.1.1/24
192.168.0.1/24
ANY
DNS
HTTP
HTTPS
TELNET
SSH
PERMIT
DENY
Reset Answer
Save
Close
Firewall 2
Rule Name
Source
Destination
Service
Action
DNS Rule
HTTPS Outbound
Management
HTTPS Inbound
HTTP Inbound
ANY
10.0.0.1/24
10.0.1.1/24
192.168.0.1/24
ANY
DNS
HTTP
HTTPS
TELNET
SSH
PERMIT
DENY
Reset Answer
Save
Close
Firewall 3
Rule Name
Source
Destination
Service
Action
DNS Rule
HTTPS Outbound
Management
HTTPS Inbound
HTTP Inbound
ANY
10.0.0.1/24
10.0.1.1/24
192.168.0.1/24
ANY
DNS
HTTP
HTTPS
TELNET
SSH
PERMIT
DENY
Reset Answer
Save
Close

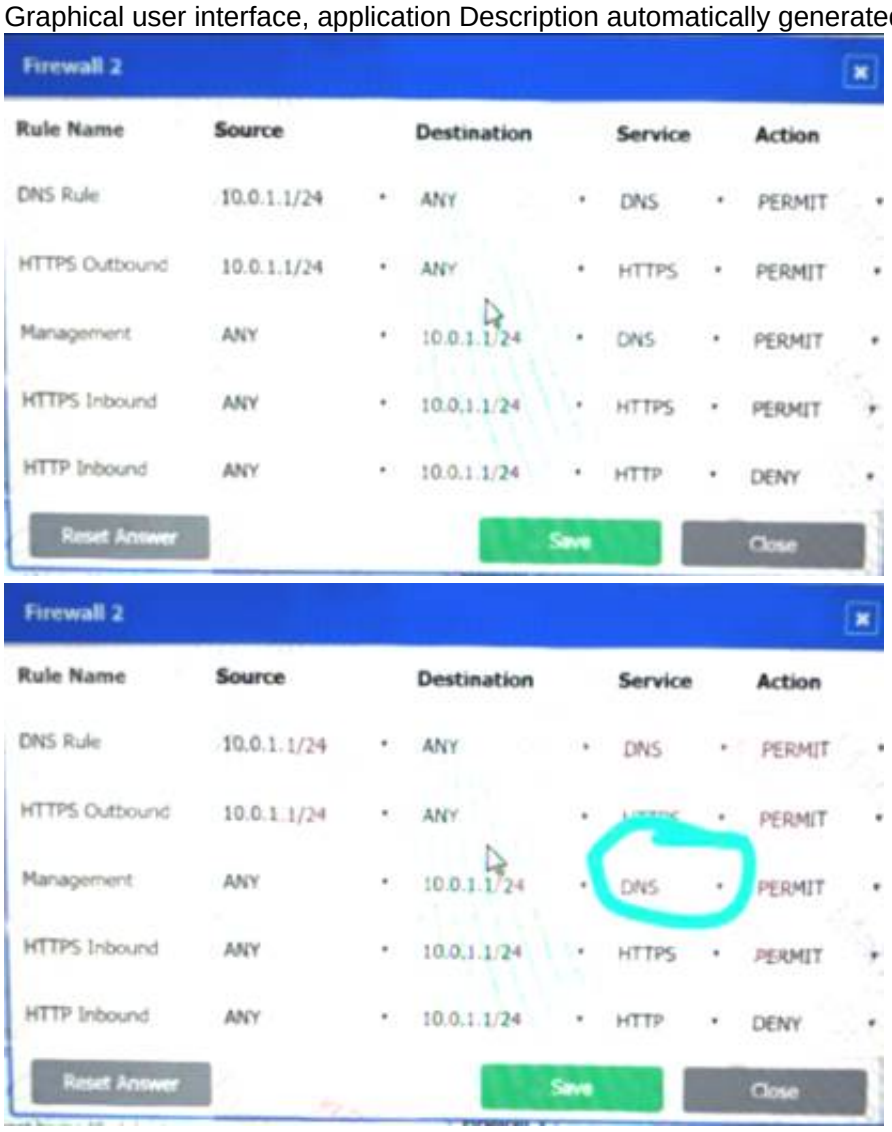
A. Mastered
B. Not Mastered

Answer: A

Explanation:
Firewall 1:



DNS Rule – ANY --> ANY --> DNS --> PERMIT
HTTPS Outbound – 10.0.0.1/24 --> ANY --> HTTPS --> PERMIT Management – ANY --> ANY --> SSH --> PERMIT
HTTPS Inbound – ANY --> ANY --> HTTPS --> PERMIT HTTP Inbound – ANY --> ANY --> HTTP --> DENY
Firewall 2: No changes should be made to this firewall
Graphical user interface, application Description automatically generated



Firewall 3:
DNS Rule – ANY --> ANY --> DNS --> PERMIT
HTTPS Outbound – 192.168.0.1/24 --> ANY --> HTTPS --> PERMIT Management – ANY --> ANY --> SSH --> PERMIT
HTTPS Inbound – ANY --> ANY --> HTTPS --> PERMIT HTTP Inbound – ANY --> ANY --> HTTP --> DENY
Graphical user interface, application Description automatically generated

NEW QUESTION 152
- (Exam Topic 1)
A security analyst is evaluating solutions to deploy an additional layer of protection for a web application The goal is to allow only encrypted communications without relying on network devices Which of the following can be implemented?

A. HTTP security header
B. DNSSEC implementation
C. SRTP
D. S/MIME

Answer: C

NEW QUESTION 153
- (Exam Topic 1)
An engineer wants to inspect traffic to a cluster of web servers in a cloud environment. Which of the following solutions should the engineer implement?

A. Proxy server
B. WAF
C. Load balancer
D. VPN

Answer: B

NEW QUESTION 156
- (Exam Topic 1)
A security forensics analyst is examining a virtual server. The analyst wants to preserve the present state of the virtual server, including memory contents Which of the following backup types should be used?

A. Snapshot
B. Differential
C. Cloud
D. Full
E. Incremental

Answer: A

NEW QUESTION 159
- (Exam Topic 1)
An organization wants to implement a biometric system with the highest likelihood that an unauthorized user will be denied access. Which of the following should the organization use to compare biometric solutions?

A. FRR
B. Difficulty of use
C. Cost
D. FAR

E. CER

Answer: A

NEW QUESTION 160
- (Exam Topic 1)
A report delivered to the Chief Information Security Officer (CISO) shows that some user credentials could be exfilltrated. The report also indicates that users tend to choose the same credentials on different systems and applications. Which of the following policies should the CISO use to prevent someone from using the exfilltrated credentials?

A. MFA
B. Lockout
C. Time-based logins
D. Password history

Answer: B

NEW QUESTION 165
- (Exam Topic 1)
Which of the following employee roles is responsible for protecting an organization's collected personal information?

A. CTO
B. DPO
C. CEO
D. DBA

Answer: B

Explanation:
Many companies also have a data protection officer or DPO. This is a higher-level manager who is responsible for the organization's overall data privacy policies.
https://www.professormesser.com/security-plus/sy0-601/sy0-601-video/data-roles-and-responsibilities/#:~:text=

NEW QUESTION 168
- (Exam Topic 1)
A company is providing security awareness training regarding the importance of not forwarding social media messages from unverified sources. Which of the following risks would this training help to prevent?

A. Hoaxes
B. SPIMs
C. Identity fraud
D. Credential harvesting

Answer: A

Explanation:
Hoax
A hoax is a falsehood deliberately fabricated to masquerade as the truth. It is distinguishable from errors in observation or judgment, rumors, urban legends, pseudo sciences, and April Fools' Day events that are passed along in good faith by believers or as jokes.
Identity theft
Identity theft occurs when someone uses another person's personal identifying information, like their name, identifying number, or credit card number, without their permission, to commit fraud or other crimes. The term identity theft was coined in 1964. Identity fraud (also known as identity theft or crime) involves someone using another individual's personal information without consent, often to obtain a benefit.
Credential Harvesting
Credential Harvesting (or Account Harvesting) is the use of MITM attacks, DNS poisoning, phishing, and other vectors to amass large numbers of credentials (username / password combinations) for reuse.

NEW QUESTION 169
- (Exam Topic 1)
Which of the following components can be used to consolidate and forward inbound Internet traffic to multiple cloud environments though a single firewall?

A. Transit gateway
B. Cloud hot site
C. Edge computing
D. DNS sinkhole

Answer: A

NEW QUESTION 174
- (Exam Topic 1)
An organization has activated an incident response plan due to a malware outbreak on its network The organization has brought in a forensics team that has identified an internet-facing Windows server as the likely point of initial compromise The malware family that was detected is known to be distributed by manually logging on to servers and running the malicious code Which of the following actions would be BEST to prevent reinfection from the initial infection vector?

A. Prevent connections over TFTP from the internal network
B. Create a firewall rule that blocks port 22 from the internet to the server
C. Disable file shanng over port 445 to the server
D. Block port 3389 inbound from untrusted networks

Answer: A

NEW QUESTION 179
- (Exam Topic 1)
A SOC operator is analyzing a log file that contains the following entries:

```
[06-Apr-2021-18:00:06] GET /index.php/../../../../../../etc/passwd
[06-Apr-2021-18:01:07] GET /index.php/../../../../../../etc/shadow
[06-Apr-2021-18:01:26] GET /index.php/../../../../../../../../../../etc/passwd
[06-Apr-2021-18:02:16] GET /index.php?var1=;cat /etc/passwd;&var2=7865tgydk
[06-Apr-2021-18:02:56] GET /index.php?var1=;cat /etc/shadow;&var2=7865tgydk
```

A. SQL injection and improper input-handling attempts
B. Cross-site scripting and resource exhaustion attempts
C. Command injection and directory traversal attempts
D. Error handling and privilege escalation attempts

Answer: C

NEW QUESTION 182
- (Exam Topic 1)
A security analyst wants to fingerpnnt a web server Which of the following tools will the security analyst MOST likely use to accomplish this task?

A. nmap -p1-65S35 192.168.0.10
B. dig 192.168.0.10
C. cur1 --htad http://192.168.0.10
D. ping 192.168.0.10

Answer: C

Explanation:
HTTP/1.1 301 Moved Permanently Server: cloudflare
Date: Thu, 01 Sep 2022 22:36:50 GMT
Content-Type: text/html Content-Length: 167 Connection: keep-alive Location: https://1.1.1.1/
CF-RAY: 74417cb04d6b9a50-MFE

NEW QUESTION 185
- (Exam Topic 1)
A tax organization is working on a solution to validate the online submission of documents The solution should be earned on a portable USB device that should be inserted on any computer that is transmitting a transaction securely. Which of the following is the BEST certificate for these requirements?

A. User certificate
B. Self-signed certificate
C. Computer certificate
D. Root certificate

Answer: D

NEW QUESTION 187
- (Exam Topic 1)
Which of the following is the BEST example of a cost-effective physical control to enforce a USB removable media restriction policy?

A. Putting security/antitamper tape over USB ports logging the port numbers and regularly inspecting the ports
B. Implementing a GPO that will restrict access to authorized USB removable media and regularly verifying that it is enforced
C. Placing systems into locked key-controlled containers with no access to the USB ports
D. Installing an endpoint agent to detect connectivity of USB and removable media

Answer: B

NEW QUESTION 188
- (Exam Topic 1)
Which of the following describes the continuous delivery software development methodology?

A. Waterfall
B. Spiral
C. V-shaped
D. Agile

Answer: D

NEW QUESTION 192
- (Exam Topic 2)
A security analyst is tasked with defining the “something you are“ factor of the company’s MFA settings. Which of the following is BEST to use to complete the configuration?

A. Gait analysis

B. Vein
C. Soft token
D. HMAC-based, one-time password

Answer: A

NEW QUESTION 197
- (Exam Topic 2)
A security engineer is building a file transfer solution to send files to a business partner. The users would like to drop off the files in a specific directory and have the server send to the business partner. The connection to the business partner is over the internet and needs to be secure. Which of the following can be used?

A. S/MIME
B. LDAPS
C. SSH
D. SRTP

Answer: B

NEW QUESTION 201
- (Exam Topic 2)
A security analyst is reviewing application logs to determine the source of a breach and locates the following log:

```
https://www.comptia.com/login.php?id='%20or%20'1'1='1
```

Which Of the following has been observed?

A. DLL Injection
B. API attack
C. SQLI
D. XSS

Answer: C

NEW QUESTION 205
- (Exam Topic 2)
A company is moving its retail website to a public cloud provider. The company wants to tokenize credit card data but not allow the cloud provider to see the stored credit card information. Which of the following would BEST meet these objectives?

A. WAF
B. CASB
C. VPN
D. TLS

Answer: B

NEW QUESTION 206
- (Exam Topic 2)
Which of the following are the BEST ways to implement remote home access to a company's intranet systems if establishing an always-on VPN is not an option? (Select Two)

A. Install VPN concentrations at home offices
B. Create NAT on the firewall for intranet systems
C. Establish SSH access to a jump server
D. Implement a SSO solution
E. Enable MFA for intranet systems
F. Configure SNMPv3 server and clients.

Answer: AE

NEW QUESTION 207
- (Exam Topic 2)
An administrator is configuring a firewall rule set for a subnet to only access DHCP, web pages, and SFTP, and to specifically block FTP. Which of the following would BEST accomplish this goal?

A.
```
[Permission Source Destination Port]
Allow: Any Any 80
Allow: Any Any 443
Allow: Any Any 67
Allow: Any Any 68
Allow: Any Any 22
Deny: Any Any 21
Deny: Any Any
```

B.
```
[Permission Source Destination Port]
Allow: Any Any 80
Allow: Any Any 443
Allow: Any Any 67
Allow: Any Any 68
Deny: Any Any 22
Allow: Any Any 21
Deny: Any Any
```

C.
```
[Permission Source Destination Port]
Allow: Any Any 80
Allow: Any Any 443
Allow: Any Any 22
Deny: Any Any 67
Deny: Any Any 68
Deny: Any Any 21
Allow: Any Any
```

D.
```
[Permission Source Destination Port]
Allow: Any Any 80
Allow: Any Any 443
Deny: Any Any 67
Allow: Any Any 68
Allow: Any Any 22
Allow: Any Any 21
Allow: Any Any
```

A. Option A
B. Option B
C. Option C
D. Option D

Answer: A

NEW QUESTION 210
- (Exam Topic 2)
Which of the following should an organization consider implementing In the event executives need to speak to the media after a publicized data breach?

A. Incident response plan
B. Business continuity plan
C. Communication plan
D. Disaster recovery plan

Answer: D

NEW QUESTION 215
- (Exam Topic 2)
An untrusted SSL certificate was discovered during the most recent vulnerability scan. A security analyst determines the certificate is signed properly and is a valid wildcard. This same certificate is installed on other company servers without issue. Which of the following is the MOST likely reason for this finding?

A. The required intermediate certificate is not loaded as part of the certificate chain.
B. The certificate is on the CRL and is no longer valid.
C. The corporate CA has expired on every server, causing the certificate to fail verification.
D. The scanner is incorrectly configured to not trust this certificate when detected on the server.

Answer: A

NEW QUESTION 217
- (Exam Topic 2)
In a phishing attack, the perpetrator is pretending to be someone in a position of power in an effort to influence the target to click or follow the desired response. Which of the following principles is being used?

A. Authority
B. Intimidation
C. Consensus
D. Scarcity

Answer: B

NEW QUESTION 221
- (Exam Topic 2)
A company wants to simplify the certificate management process. The company has a single domain with several dozen subdomains, all of which are publicly accessible on the internet. Which of the following BEST describes the type of certificate the company should implement?

A. Subject alternative name

B. Wildcard
C. Self-signed
D. Domain validation

Answer: B

Explanation:
Wildcard SSL certificates are for a single domain and all its subdomains. A subdomain is under the umbrella of the main domain. Usually subdomains will have an address that begins with something other than 'www.'
For example, www.cloudflare.com has a number of subdomains, including blog.cloudflare.com, support.cloudflare.com, and developers.cloudflare.com. Each is a subdomain under the main cloudflare.com domain.
Wildcard SSL Certificate
A single Wildcard SSL certificate can apply to all of these subdomains. Any subdomain will be listed in the SSL certificate. Users can see a list of subdomains covered by a particular certificate by clicking on the padlock in the URL bar of their browser, then clicking on "Certificate" (in Chrome) to view the certificate's details.
https://www.cloudflare.com/learning/ssl/types-of-ssl-certificates/

NEW QUESTION 226
- (Exam Topic 2)
Which of the following explains why RTO is included in a BIA?

A. It identifies the amount of allowable downtime for an application or system,
B. It prioritizes risks so the organization can allocate resources appropriately,
C. It monetizes the loss of an asset and determines a break-even point for risk mitigation.
D. It informs the backup approach so that the organization can recover data to a known time.

Answer: A

NEW QUESTION 228
- (Exam Topic 2)
A SOC operator is receiving continuous alerts from multiple Linux systems indicating that unsuccessful SSH attempts to a functional user ID have been attempted on each one of them in a short period of time. Which of the following BEST explains this behavior?

A. Rainbow table attack
B. Password spraying
C. Logic bomb
D. Malware bot

Answer: B

Explanation:
Password Spraying is a variant of what is known as a brute force attack. In a traditional brute force attack, the perpetrator attempts to gain unauthorized access to a single account by guessing the password "repeatedly" in a very short period of time.

NEW QUESTION 232
- (Exam Topic 2)
Users are presented with a banner upon each login to a workstation. The banner mentions that users are not entitled to any reasonable expectation of privacy and access is for authorized personnel only.
In order to proceed past that banner. users must click the OK button. Which of the following is this an example of?

A. AUP
B. NDA
C. SLA
D. MOU

Answer: A

NEW QUESTION 235
- (Exam Topic 2)
Which of the following uses SAML for authentication?

A. TOTP
B. Federation
C. Kerberos
D. HOTP

Answer: B

NEW QUESTION 240
- (Exam Topic 2)
A security analyst is receiving several alerts per user and is trying to determine If various logins are malicious. The security analyst would like to create a baseline of normal operations and reduce noise. Which of the following actions should the security analyst perform?

A. Adjust the data flow from authentication sources to the SIEM.
B. Disable email alerting and review the SIEM directly.
C. Adjust the sensitivity levels of the SIEM correlation engine.
D. Utilize behavioral analysis to enable the SIEM's learning mode.

Answer: D

NEW QUESTION 245
- (Exam Topic 2)
A Chief Security Officer is looking for a solution that can reduce the occurrence of customers receiving errors from back-end infrastructure when systems go offline unexpectedly. The security architect would like the solution to help maintain session persistence. Which of the following would BEST meet the requirements?

A. Reverse proxy
B. NIC teaming
C. Load balancer
D. Forward proxy

Answer: B

NEW QUESTION 246
- (Exam Topic 2)
A systems analyst is responsible for generating a new digital forensics chain-of-custody form. Which of the following should the analyst include in this documentation? (Select TWO).

A. The order of volatility
B. A CRC32 checksum
C. The provenance of the artifacts
D. The vendor's name
E. The date time
F. A warning banner

Answer: AE

NEW QUESTION 249
- (Exam Topic 2)
A user forwarded a suspicious email to the security team, Upon investigation, a malicious URL was discovered. Which of the following should be done FIRST to prevent other users from accessing the malicious URL?

A. Configure the web content filter for the web address.
B. Report the website to threat intelligence partners
C. Set me SIEM to alert for any activity to the web address.
D. Send out a corporate communication to warn all users Of the malicious email.

Answer: A

NEW QUESTION 251
- (Exam Topic 2)
Server administrator want to configure a cloud solution so that computing memory and processor usage is maximized most efficiently acress a number of virtual servers. They also need to avoid potential
denial-of-service situations caused by availiability. Which of the following should administrator configure to
maximize system availability while efficiently utilizing available computing power?

A. Dynamic resource allocation
B. High availability
C. Segmentation
D. Container security

Answer: C

NEW QUESTION 256
- (Exam Topic 2)
A company is under investigation for possible fraud. As part of the investigation. the authorities need to review all emails and ensure data is not deleted.
Which of the following should the company implement to assist in the investigation?

A. Legal hold
B. Chain of custody
C. Data loss prevention
D. Content filter

Answer: A

NEW QUESTION 258
- (Exam Topic 2)
A cyber-security administrator is using an enterprise firewall. The administrator created some rules, but now Seems to be unresponsive. All connections being dropped by the firewall. Which of the following would be the BEST option to remove the rules?

A. # iptables -t mangle -x
B. # iptables -f
C. # iptables -z
D. # iptables -p input -j drop

Answer: A

NEW QUESTION 262
- (Exam Topic 2)
Which of the following is an example of risk avoidance?

A. Installing security updates directly in production to expedite vulnerability fixes
B. Buying insurance to prepare for financial loss associated with exploits
C. Not installing new software to prevent compatibility errors
D. Not taking preventive measures to stop the theft of equipment

Answer: C

NEW QUESTION 267
- (Exam Topic 2)
The Chief Information Security Officer (CISO) of a bank recently updated the incident response policy. The CISO is concerned that members of the incident response team do not understand their roles. The bank wants to test the policy but with the least amount of resources or impact. Which of the following BEST meets the requirements?

A. Warm site failover
B. Tabletop walk-through
C. Parallel path testing
D. Full outage simulation

Answer: B

NEW QUESTION 271
- (Exam Topic 2)
An audit Identified Pll being utilized In the development environment of a critical application. The Chief Privacy Officer (CPO) Is adamant that this data must be removed; however, the developers are concerned that without real data they cannot perform functionality tests and search for specific data. Which of the following should a security professional implement to BEST satisfy both the CPO's and the development team's requirements?

A. Data anonymlzallon
B. Data encryption
C. Data masking
D. Data tokenization

Answer: C

Explanation:
Data masking can mean that all or part of the contents of a field are redacted, by substituting all character strings with "x" for example. A field might be partially redacted to preserve metadata for analysis purposes. For example, in a telephone number, the dialing prefix might be retained, but the subscriber number redacted.
Data masking can also use techniques to preserve the original format of the field. Data masking is an irreversible deidentification technique

NEW QUESTION 272
- (Exam Topic 2)
An analyst receives multiple alerts for beaconing activity for a host on the network, After analyzing the activity, the analyst observes the following activity:
• A user enters comptia.org into a web browser.
• The website that appears is not the comptia.org site.
• The website is a malicious site from the attacker.
• Users in a different office are not having this issue. Which of the following types of attacks was observed?

A. On-path attack
B. DNS poisoning
C. Locator (URL) redirection
D. Domain hijacking

Answer: C

NEW QUESTION 277
- (Exam Topic 2)
Which of the following is the BEST action to foster a consistent and auditable incident response process?

A. Incent new hires to constantly update the document with external knowledge.
B. Publish the document in a central repository that is easily accessible to the organization.
C. Restrict eligibility to comment on the process to subject matter experts of each IT silo.
D. Rotate CIRT members to foster a shared responsibility model in the organization.

Answer: B

NEW QUESTION 282
- (Exam Topic 2)
Which of the following is a policy that provides a greater depth of knowldge across an organization?

A. Asset manahement policy
B. Separation of duties policy
C. Acceptable use policy
D. Job Rotation policy

Answer: C

NEW QUESTION 285
- (Exam Topic 2)
An attacker has determined the best way to impact operations is to infiltrate third-party software vendors. Which of the following vectors is being exploited?

A. Social media
B. Cloud
C. Supply chain
D. Social engineering

Answer: D

NEW QUESTION 288
- (Exam Topic 2)
During an incident response process involving a laptop, a host was identified as the entry point for malware. The management team would like to have the laptop restored and given back to the user. The cybersecurity analyst would like to continue investigating the intrusion on the host. Which of the following would allow the analyst to continue the investigation and also return the laptop to the user as soon as possible?

A. dd
B. memdump
C. tcpdump
D. head

Answer: A

NEW QUESTION 290
- (Exam Topic 2)
The new Chief Information Security Officer at a company has asked the security team to implement stronger user account policies. The new policies require:
• Users to choose a password unique to their last ten passwords
• Users to not log in from certain high-risk countries
Which of the following should the security team implement? (Select TWO).

A. Password complexity
B. Password history
C. Geolocation
D. Geofencing
E. Geotagging
F. Password reuse

Answer: AB

NEW QUESTION 291
- (Exam Topic 2)
A security engineer is concerned about using an agent on devices that relies completely on defined known-bad signatures. The security engineer wants to implement a tool with multiple components including the ability to track, analyze, and monitor devices without reliance on definitions alone. Which of the following solutions BEST fits this use case?

A. EDR
B. DLP
C. NGFW
D. HIPS

Answer: A

Explanation:
The acronym EDR stands for Endpoint Detection and Response and is also known as EDTR. It is an endpoint security solution that is responsible for continuous monitoring of endpoints. This permanent monitoring enables the technology to detect and respond to cyber threats such as malware or ransomware at an early stage. The basis for this is always the analysis of context-related information, which can be used to make corrective proposals for recovery.

NEW QUESTION 296
- (Exam Topic 2)
Which of the following is the FIRST environment in which proper, secure coding should be practiced?

A. Stage
B. Development
C. Production
D. Test

Answer: B

Explanation:
The developer has to start writing secure code from beginning itself. Which will then be tested, staged and finally production

NEW QUESTION 298
- (Exam Topic 2)

A vulnerability has been discovered and a known patch to address the vulnerability does not exist. Which of the following controls works BEST until a proper fix is released?

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

Answer: A

NEW QUESTION 303
- (Exam Topic 2)
Which of the following control types fixes a previously identified issue and mitigates a risk?

A. Detective
B. Corrective
C. Preventative
D. Finalized

Answer: B

NEW QUESTION 308
- (Exam Topic 2)
Which of the following documents provides guidance regarding the recommended deployment of network security systems from the manufacturer?

A. Cloud control matrix
B. Reference architecture
C. NIST RMF
D. CIS Top 20

Answer: C

NEW QUESTION 309
- (Exam Topic 2)
Which of the following describes a social engineering technique that seeks to exploit a person's sense of urgency?

A. A phishing email stating a cash settlement has been awarded but will expire soon
B. A smishing message stating a package is scheduled for pickup
C. A vishing call that requests a donation be made to a local charity
D. A SPIM notification claiming to be undercover law enforcement investigating a cybercrime

Answer: A

Explanation:
Phishing
As one of the most popular social engineering attack types, phishing scams are email and text message campaigns aimed at creating a sense of urgency, curiosity or fear in victims. It then prods them into revealing sensitive information, clicking on links to malicious websites, or opening attachments that contain malware.
https://www.imperva.com/learn/application-security/social-engineering-attack/#:~:text=Phishing,curiosity%20o

NEW QUESTION 314
- (Exam Topic 3)
A root cause analysis reveals that a web application outage was caused by one of the company's developers uploading a newer version of the third-party libraries that were shared among several applications. Which of the following implementations would be BEST to prevent the issue from reoccurring?

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

Answer: C

Explanation:
Containerization is defined as a form of operating system virtualization, through which applications are run in isolated user spaces called containers, all using the same shared operating system (OS).

NEW QUESTION 318
- (Exam Topic 3)
A security analyst reviews the datacenter access logs for a fingerprint scanner and notices an abundance of errors that correlate with users' reports of issues accessing the facility. Which of the following MOST likely the cause of the cause of the access issues?

A. False rejection
B. Cross-over error rate
C. Efficacy rale
D. Attestation

Answer: A

Explanation:

where a legitimate user is not recognized. This is also referred to as a Type I error or false non-match rate (FNMR). FRR is measured as a percentage.

NEW QUESTION 323
- (Exam Topic 3)
A company has drafted an insider-threat policy that prohibits the use of external storage devices. Which of the following would BEST protect the company from data exfiltration via removable media?

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

Answer: D

NEW QUESTION 326
- (Exam Topic 3)
Which of the following are the MOST likely vectors for the unauthorized inclusion of vulnerable code in a software company's final software releases? (Select TWO.)

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

Answer: DE

NEW QUESTION 329
- (Exam Topic 3)
A security analyst is using a recently released security advisory to review historical logs, looking for the specific activity that was outlined in the advisory. Which of the following is the analyst doing?

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

Answer: C

NEW QUESTION 334
- (Exam Topic 3)
An organization's RPO for a critical system is two hours. The system is used Monday through Friday, from 9:00 am to 5:00 pm. Currently, the organization performs a full backup every Saturday that takes four hours to complete. Which of the following additional backup implementations would be the BEST way for the analyst to meet the business requirements?

A. Incremental backups Monday through Friday at 6:00 p.m and differential backups hourly
B. Full backups Monday through Friday at 6:00 p.m and incremental backups hourly.
C. incremental backups Monday through Friday at 6:00 p.m and full backups hourly.
D. Full backups Monday through Friday at 6:00 p.m and differential backups hourly.

Answer: A

NEW QUESTION 336
- (Exam Topic 3)
A security administrator checks the table of a network switch, which shows the following output: Which of the following is happening to this switch?

A. MAC Flooding
B. DNS poisoning
C. MAC cloning
D. ARP poisoning

Answer: A

NEW QUESTION 341
- (Exam Topic 3)
A network administrator would like to configure a site-to-site VPN utilizing iPSec. The administrator wants the tunnel to be established with data integrity encryption, authentication and anti- replay functions Which of the following should the administrator use when configuring the VPN?

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

Answer: C

Explanation:

https://www.hypr.com/encapsulating-security-payload-esp/
Encapsulating Security Payload (ESP) is a member of the Internet Protocol Security (IPsec) set of protocols that encrypt and authenticate the packets of data between computers using a Virtual Private Network (VPN). The focus and layer on which ESP operates makes it possible for VPNs to function securely.

NEW QUESTION 344
- (Exam Topic 3)
Which of the following technical controls is BEST suited for the detection and prevention of buffer overflows on hosts?

A. DLP
B. HIDS
C. EDR
D. NIPS

Answer: C

NEW QUESTION 346
- (Exam Topic 3)
A security analyst is performing a packet capture on a series of SOAP HTTP requests for a security
assessment. The analyst redirects the output to a file After the capture is complete, the analyst needs to review the first transactions quickly and then search the entire series of requests for a particular string Which of the following would be BEST to use to accomplish the task? (Select TWO).

A. head
B. Tcpdump
C. grep
D. rail
E. curl
F. openssi
G. dd

Answer: AC

Explanation:
A - "analyst needs to review the first transactions quickly"
C - "search the entire series of requests for a particular string"

NEW QUESTION 351
- (Exam Topic 3)
Which of the following BEST describes a security exploit for which a vendor patch is not readily available?

A. Integer overflow
B. Zero-day
C. End of life
D. Race condition

Answer: B

NEW QUESTION 356
- (Exam Topic 3)
An organization is repairing the damage after an incident, Which of the following controls és being implemented?

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

Answer: C

NEW QUESTION 361
- (Exam Topic 3)
A company is designing the layout of a new datacenter so it will have an optimal environmental temperature Which of the following must be included? (Select TWO)

A. An air gap
B. A cold aisle
C. Removable doors
D. A hot aisle
E. An loT thermostat
F. A humidity monitor

Answer: EF

NEW QUESTION 363
- (Exam Topic 3)
A Chief Security Office's (CSO's) key priorities are to improve preparation, response, and recovery practices to minimize system downtime and enhance organizational resilience to ransomware attacks. Which of the following would BEST meet the CSO's objectives?

A. Use email-filtering software and centralized account management, patch high-risk systems, and restrict administration privileges on fileshares.

B. Purchase cyber insurance from a reputable provider to reduce expenses during an incident.
C. Invest in end-user awareness training to change the long-term culture and behavior of staff and executives, reducing the organization's susceptibility to phishing attacks.
D. Implement application whitelisting and centralized event-log management, and perform regular testing and validation of full backups.

Answer: B

NEW QUESTION 367
- (Exam Topic 3)
A company provides mobile devices to its users to permit access to email and enterprise applications. The company recently started allowing users to select from several different vendors and device models. When configuring the MDM, which of the following is a key security implication of this heterogeneous device approach?

A. The most common set of MDM configurations will become the effective set of enterprise mobile security controls.
B. All devices will need to support SCEP-based enrollment; therefore, the heterogeneity of the chosen architecture may unnecessarily expose private keys to adversaries.
C. Certain devices are inherently less secure than others, so compensatory controls will be needed to address the delta between device vendors.
D. MDMs typically will not support heterogeneous deployment environments, so multiple MDMs will need to be installed and configured.

Answer: C

NEW QUESTION 370
- (Exam Topic 3)
A startup company is using multiple SaaS and IaaS platforms to stand up a corporate infrastructure and build out a customer-facing web application. Which of the following solutions would be BEST to provide security, manageability, and visibility into the platforms?

A. SIEM
B. DLP
C. CASB
D. SWG

Answer: C

NEW QUESTION 373
- (Exam Topic 3)
A network engineer at a company with a web server is building a new web environment with the following requirements:
* Only one web server at a time can service requests.
* If the primary web server fails, a failover needs to occur to ensure the secondary web server becomes the primary.
Which of the following load-balancing options BEST fits the requirements?

A. Cookie-based
B. Active-passive
C. Persistence
D. Round robin

Answer: A

NEW QUESTION 378
- (Exam Topic 3)
A network administrator is setting up wireless access points in all the conference rooms and wants to authenticate device using PKI. Which of the following should the administrator configure?

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

Answer: C

NEW QUESTION 383
- (Exam Topic 3)
A security engi is cor that the gy tor on endpoints ts too heavily dependent on previously defined attacks. The engineer would like a tool to monitor for changes to key Mes and network traffic on the device. Which of the following tools BEST addresses both detection and prevention?

A. NIDS
B. HIPS
C. AV
D. NGFW

Answer: A

NEW QUESTION 384
- (Exam Topic 3)
An organization wants to implement a third factor to an existing multifactor authentication. The organization already uses a smart card and password. Which of the following would meet the organization’s needs for a third factor?

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

Answer: B

NEW QUESTION 385
- (Exam Topic 3)
An organization has been experiencing outages during holiday sales and needs to ensure availability of its point-of-sale systems The IT administrator has been asked to improve both server-data fault tolerance and site availability under high consumer load Which of the following are the BEST options to accomplish this objective'? (Select TWO)

A. Load balancing
B. Incremental backups
C. UPS
D. RAID
E. Dual power supply
F. NIC teaming

Answer: AD

NEW QUESTION 386
- (Exam Topic 3)
A user recent an SMS on a mobile phone that asked for bank delays. Which of the following social-engineering techniques was used in this case?

A. SPIM
B. Vishing
C. Spear phishing
D. Smishing

Answer: D

NEW QUESTION 390
- (Exam Topic 3)
Against the recommendation of the IT security analyst, a company set all user passwords on a server as “P@)55wOrD". Upon review of the /etc/pesswa file, an attacker found the following:

```
alice:a8df3b6c4fd75f061743ifd248f3519idf8d237f
bob:2d250c5b2976b03d757f324ebd59340df96aa05e
chris:ea981ec3285421d014108089f3f3f597ce0f4150
```

hich of the following BEST explains why the encrypted passwords do not match?

A. Perfect forward secrecy
B. Key stretching
C. Salting
D. Hashing

Answer: C

NEW QUESTION 394
- (Exam Topic 3)
hich of the following is the BEST method for ensuring non-repudiation?

A. SSO
B. Digital certificate
C. Token
D. SSH key

Answer: B

NEW QUESTION 395
- (Exam Topic 3)
A company's Chief Information Security Officer (CISO) recently warned the security manager that the company’s Chief Executive Officer (CEO) is planning to publish a controversial option article in a national newspaper, which may result in new cyberattacks Which of the following would be BEST for the security manager to use in a threat mode?

A. Hacktivists
B. White-hat hackers
C. Script kiddies
D. Insider threats

Answer: A

NEW QUESTION 399

- (Exam Topic 3)
A company's Chief Information Office (CIO) is meeting with the Chief Information Security Officer (CISO) to plan some activities to enhance the skill levels of the company's developers. Which of the following would be MOST suitable for training the developers'?

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

Answer: B

NEW QUESTION 402
- (Exam Topic 3)
A security analyst sees the following log output while reviewing web logs:

```
[02/Feb2019:03:39:21 -0000] 23.35.212.99 12.59.34.88 - "GET /uri/input.action?query=%2f..%2f..%2f..%2fetc%2fpasswrd HTTP/1.0" 80 200 200
[02/Feb2019:03:39:85 -0000] 23.35.212.99 12.59.34.88 - "GET /uri/input.action?query=/../../../etc/password HTTP/1.0" 80 200 200
```

Which of the following mitigation strategies would be BEST to prevent this attack from being successful?

A. Secure cookies
B. Input validation
C. Code signing
D. Stored procedures

Answer: B

NEW QUESTION 405
- (Exam Topic 3)
A company recently experienced a data breach and the source was determined to be an executive who was charging a phone in a public area. Which of the following would MOST likely have prevented this breach?

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

Answer: C

Explanation:
https://www.promorx.com/blogs/blog/how-does-a-usb-data-blocker-work Connecting via the data port of your mobile device, the Data Blockers creates a barrier between your mobile device and the charging station. Your phone will draw power as usual, allowing you to use it normally and charge it at the same time, but this clever piece of equipment will prevent any data exchange.
“Malicious USB charging cables and plugs are also a widespread problem. As with card skimming, a device may be placed over a public charging port at airports and other transit locations. A USB data blocker can provide mitigation against these juice- jacking attacks by preventing any sort of data transfer when the smartphone or laptop is connected to a charge point ”

NEW QUESTION 410
- (Exam Topic 3)
A recently discovered zero-day exploit utilizes an unknown vulnerability in the SMB network protocol to rapidly infect computers. Once infected, computers are encrypted and held for ransom. Which of the following would BEST prevent this attack from reoccurring?

A. Configure the perimeter firewall to deny inbound external connections to SMB ports.
B. Ensure endpoint detection and response systems are alerting on suspicious SMB connections.
C. Deny unauthenticated users access to shared network folders.
D. Verify computers are set to install monthly operating system, updates automatically.

Answer: A

NEW QUESTION 414
- (Exam Topic 3)
A company recently transitioned to a strictly BYOD culture due to the cost of replacing lost or damaged corporate-owned mobile devices. Which of the following technologies would be BEST to balance the BYOD culture while also protecting the company’s data?

A. Containerization
B. Geofencing
C. Full-disk encryption
D. Remote wipe

Answer: C

NEW QUESTION 416
- (Exam Topic 3)
An engineer wants to access sensitive data from a corporate-owned mobile device. Personal data is not allowed on the device. Which of the following MDM configurations must be considered when the engineer travels for business?

A. Screen locks
B. Application management

C. Geofencing
D. Containerization

Answer: D

NEW QUESTION 417
- (Exam Topic 3)
A consultant is configuring a vulnerability scanner for a large, global organization in multiple countries. The consultant will be using a service account to scan systems with administrative privileges on a weekly basis, but there is a concern that hackers could gain access to account to the account and pivot through the global network. Which of the following would be BEST to help mitigate this concern?

A. Create consultant accounts for each region, each configured with push MFA notifications.
B. Create one global administrator account and enforce Kerberos authentication
C. Create different accounts for each regio
D. limit their logon times, and alert on risky logins
E. Create a guest account for each regio
F. remember the last ten passwords, and block password reuse

Answer: C

Explanation:
https://www.crowdstrike.com/blog/service-accounts-performing-interactive-logins/

NEW QUESTION 419
- (Exam Topic 3)
Which of the following is a detective and deterrent control against physical intrusions?

A. Alock
B. An alarm
C. A fence
D. Asign

Answer: B

NEW QUESTION 420
- (Exam Topic 3)
Which of the following types of controls is a CCTV camera that is not being monitored?

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

Answer: B

NEW QUESTION 423
- (Exam Topic 3)
A security analyst is reviewing a new website that will soon be made publicly available. The analyst sees the following in the URL:
http://dev-site.comptia.org/home/show.php?sessionID=77276554&loc=us
The analyst then sends an internal user a link to the new website for testing purposes, and when the user clicks the link, the analyst is able to browse the website with the following URL:
http://dev-site.comptia.org/home/show.php?sessionID=98988475&loc=us Which of the following application attacks is being tested?

A. Pass-the-hash
B. Session replay
C. Object deference
D. Cross-site request forgery

Answer: B

NEW QUESTION 426
- (Exam Topic 3)
After a ransomware attack a forensics company needs to review a cryptocurrency transaction between the victim and the attacker. Which of the following will the company MOST likely review to trace this transaction?

A. The public ledger
B. The NetFlow data
C. A checksum
D. The event log

Answer: A

Explanation:
https://www.investopedia.com/tech/what-cryptocurrency-public-ledger/

NEW QUESTION 431

- (Exam Topic 3)
A security engineer needs to Implement the following requirements:
• All Layer 2 switches should leverage Active Directory tor authentication.
• All Layer 2 switches should use local fallback authentication If Active Directory Is offline.
• All Layer 2 switches are not the same and are manufactured by several vendors.
Which of the following actions should the engineer take to meet these requirements? (Select TWO). Implement RADIUS.

A. Configure AAA on the switch with local login as secondary
B. Configure port security on the switch with the secondary login method.
C. Implement TACACS+
D. Enable the local firewall on the Active Directory server.
E. Implement a DHCP server

Answer: AB

NEW QUESTION 432
- (Exam Topic 3)
Phishing and spear-phishing attacks have been occurring more frequently against a company's staff. Which of the following would MOST likely help mitigate this issue?

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

Answer: C

NEW QUESTION 436
- (Exam Topic 3)
A cybersecunty administrator needs to implement a Layer 7 security control on a network and block potential attacks. Which of the following can block an attack at Layer 7? (Select TWO)

A. HIDS
B. NIPS
C. HSM
D. WAF
E. HIPS
F. NIDS
G. Stateless firewall

Answer: BD

NEW QUESTION 439
- (Exam Topic 3)
A security modern may have occurred on the desktop PC of an organization's Chief Executive Officer (CEO) A duplicate copy of the CEO's hard drive must be stored securely to ensure appropriate forensic processes and the chain of custody are followed. Which of the following should be performed to accomplish this task?

A. Install a new hard drive in the CEO's PC, and then remove the old hard drive and place it in a tamper-evident bag
B. Connect a write blocker to the hard drive Then leveraging a forensic workstation, utilize the dd command m a live Linux environment to create a duplicate copy
C. Remove the CEO's hard drive from the PC, connect to the forensic workstation, and copy all the contents onto a remote fileshare while the CEO watches
D. Refrain from completing a forensic analysts of the CEO's hard drive until after the incident is confirmed, duplicating the hard drive at this stage could destroy evidence

Answer: B

Explanation:
"To obtain a forensically sound image from nonvolatile storage, you need to ensure that nothing you do alters data or metadata (properties) on the source disk or file system. A write blocker assures this process by preventing any data on the disk or volume from being changed by filtering write commands at the driver and OS level. Data acquisition would normally proceed by attaching the target device to a forensics workstation or field capture device equipped with a write blocker."
For purposes of knowing, https://security.opentext.com/tableau/hardware/details/t8u write blockers like this are the most popular hardware blockers

NEW QUESTION 444
- (Exam Topic 3)
The Chief Security Officer (CSO) at a major hospital wants to implement SSO to help improve in the environment patient data, particularly at shared terminals. The Chief Risk Officer (CRO) is concerned that training and guidance have been provided to frontline staff, and a risk analysis has not been performed. Which of the following is the MOST likely cause of the CRO's concerns?

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

Answer: D

NEW QUESTION 447
- (Exam Topic 3)
A financial analyst is expecting an email containing sensitive information from a client. When the email arrives, the analyst receives an error and is unable to open

the encrypted message. Which of the following is the MOST likely cause of the issue?

A. The S/MME plug-in is not enabled.
B. The SLL certificate has expired.
C. Secure IMAP was not implemented
D. POP3S is not supported

Answer: A

NEW QUESTION 452
- (Exam Topic 3)
An enterprise has hired an outside security firm lo conduct a penetration test on its network and applications, The enterprise provided the firm with access to a guest account. Which af the following BEST represents the type of testing that is being used?

A. Black-box
B. Red-team
C. Gray-box
D. Bug bounty
E. White-box

Answer: C

NEW QUESTION 455
- (Exam Topic 3)
Developers are writing code and merging it into shared repositones several times a day, where it is tested automabecally. Which of the following concepts does this BEST represent?

A. Functional testing
B. Stored procedures
C. Elasticity
D. Continuous integration

Answer: C

NEW QUESTION 459
- (Exam Topic 3)
An employee has been charged with fraud and is suspected of using corporate assets. As authorities collect evidence, and to preserve the admissibility of the evidence, which of the following forensic techniques should be used?

A. Order of volatility
B. Data recovery
C. Chain of custody
D. Non-repudiation

Answer: C

NEW QUESTION 464
- (Exam Topic 3)
A financial organization has adopted a new secure, encrypted document-sharing application to help with its customer loan process. Some important PII needs to be shared across this new platform, but it is getting blocked by the DLP systems. Which of the following actions will BEST allow the PII to be shared with the secure application without compromising the organization’s security posture?

A. Configure the DLP policies to allow all PII
B. Configure the firewall to allow all ports that are used by this application
C. Configure the antivirus software to allow the application
D. Configure the DLP policies to whitelist this application with the specific PII
E. Configure the application to encrypt the PII

Answer: D

NEW QUESTION 465
- (Exam Topic 3)
A global pandemic is forcing a private organization to close some business units and reduce staffing at others. Which of the following would be BEST to help the organization’s executives determine the next course of action?

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

Answer: D

Explanation:
Business continuity may be defined as "the capability of an organization to continue the delivery of products or services at pre-defined acceptable levels following a disruptive incident”,[1] and business continuity planning [2][3] (or business continuity and resiliency planning) is the process of creating systems of prevention and recovery to deal with potential threats to a company.[4] In addition to prevention, the goal is to enable ongoing operations before and during execution of disaster recovery.[5] Business continuity is the intended outcome of proper execution of both business continuity planning and disaster recovery.

NEW QUESTION 469
- (Exam Topic 3)
After reading a security bulletin, a network security manager is concerned that a malicious actor may have breached the network using the same software flaw. The exploit code is publicly available and has been reported as being used against other industries in the same vertical. Which of the following should the network security manager consult FIRST to determine a priority list for forensic review?

A. The vulnerability scan output
B. The IDS logs
C. The full packet capture data
D. The SIEM alerts

Answer: A

NEW QUESTION 472
- (Exam Topic 3)
Which of the following would satisfy three-factor authentication?

A. Password, retina scanner, and NFC card
B. Password, fingerprint scanner, and retina scanner
C. Password, hard token, and NFC card
D. Fingerpnint scanner, hard token, and retina scanner

Answer: C

NEW QUESTION 476
- (Exam Topic 3)
A critical file server is being upgraded and the systems administrator must determine which RAID level the new server will need to achieve parity and handle two simultaneous disk failures. Which of the following
RAID levels meets this requirements?

A. RAID 0+1
B. RAID 2
C. RAID 5
D. RAID 6

Answer: C

NEW QUESTION 480
- (Exam Topic 3)
A company wants to deploy PKI on its Internet-facing website. The applications that are currently deployed are:
www.company.com (main website) contactus.company.com (for locating a nearby location) quotes.company.com (for requesting a price quote)
The company wants to purchase one SSL certificate that will work for all the existing applications and any future applications that follow the same naming conventions, such as store.company.com. Which of the following certificate types would BEST meet the requirements?

A. SAN
B. Wildcard
C. Extended validation
D. Self-signed

Answer: B

NEW QUESTION 484
- (Exam Topic 3)
An organization suffered an outage and a critical system took 90 minutes to come back online. Though there was no data loss during the outage, the expectation was that the critical system would be available again within 60 minutes Which of the following is the 60-minute expectation an example of:

A. MTBF
B. RPO
C. MTTR
D. RTO

Answer: D

Explanation:
https://www.enterprisestorageforum.com/management/rpo-and-rto-understanding-the-differences/

NEW QUESTION 485
- (Exam Topic 3)
Which of the following types of controls is a turnstile?

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

Answer: A

Explanation:

https://en.wikipedia.org/wiki/Turnstile#:~:text=A%20turnstile%20(also%20called%20a,%2C%20a%20pass%2C

NEW QUESTION 486
- (Exam Topic 3)
A database administrator needs to ensure all passwords are stored in a secure manner, so the administrate adds randomly generated data to each password before string. Which of the following techniques BEST explains this action?

A. Predictability
B. Key stretching
C. Salting
D. Hashing

Answer: C

Explanation:
https://www.techtarget.com/searchsecurity/definition/salt

NEW QUESTION 490
- (Exam Topic 3)
The manager who is responsible for a data set has asked a security engineer to apply encryption to the data on a hard disk. The security engineer is an example of a:

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

Answer: D

NEW QUESTION 494
- (Exam Topic 3)
An organization is tuning SIEM rules based off of threat intelligence reports. Which of the following phases of the incident response process does this scenario represent?

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

Answer: A

NEW QUESTION 496
- (Exam Topic 3)
A security analyst is logged into a Windows file server and needs to see who is accessing files and from which computers Which of the following tools should the analyst use?

A. netstat
B. net share
C. netcat
D. nbtstat
E. net session

Answer: A

NEW QUESTION 500
- (Exam Topic 3)
A network administrator has been asked to design a solution to improve a company's security posture The administrator is given the following, requirements?
• The solution must be inline in the network
• The solution must be able to block known malicious traffic
• The solution must be able to stop network-based attacks
Which of the following should the network administrator implement to BEST meet these requirements?

A. HIDS
B. NIDS
C. HIPS
D. NIPS

Answer: D

NEW QUESTION 502
- (Exam Topic 3)
A network technician is installing a guest wireless network at a coffee shop. When a customer purchases an Item, the password for the wireless network is printed on the recent so the customer can log in. Which of the following will the technician MOST likely configure to provide the highest level of security with the least amount of overhead?

A. WPA-EAP
B. WEP-TKIP

C. WPA-PSK
D. WPS-PIN

Answer: A

NEW QUESTION 504
- (Exam Topic 3)
Which of the following provides the BEST protection for sensitive information and data stored in cloud-based services but still allows for full functionality and searchability of data within the cloud-based services?

A. Data encryption
B. Data masking
C. Anonymization
D. Tokenization

Answer: A

NEW QUESTION 509
- (Exam Topic 3)
Which of the following allows for functional test data to be used in new systems for testing and training purposes to protect the read data?

A. Data encryption
B. Data masking
C. Data deduplication
D. Data minimization

Answer: B

NEW QUESTION 512
- (Exam Topic 3)
A RAT that was used to compromise an organization's banking credentials was found on a user's computer. The RAT evaded antivirus detection. It was installed by a user who has local administrator rights to the system as part of a remote management tool set. Which of the following recommendations would BEST prevent this from reoccurring?

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

Answer: C

NEW QUESTION 517
- (Exam Topic 3)
Which of the following would MOST likely support the integrity of a voting machine?

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

Answer: D

NEW QUESTION 518
- (Exam Topic 3)
An organization with a low tolerance for user inconvenience wants to protect laptop hard drives against loss or data theft. Which of the following would be the MOST acceptable?

A. SED
B. HSM
C. DLP
D. TPM

Answer: A

NEW QUESTION 519
- (Exam Topic 3)
When used at the design stage, which of the following improves the efficiency, accuracy, and speed of a database?

A. Tokenization
B. Data masking
C. Normalization
D. Obfuscation

Answer: C

NEW QUESTION 523

- (Exam Topic 3)
Which of the following would be BEST to establish between organizations that have agreed cooperate and are engaged in early discussion to define the responsibilities of each party, but do not want to establish a
contractually binding agreement?

A. An SLA
B. AnNDA
C. ABPA
D. AnMOU

Answer: D

NEW QUESTION 527
- (Exam Topic 3)
An auditor is performing an assessment of a security appliance with an embedded OS that was vulnerable during the last two assessments. Which of the following BEST explains the appliance's vulnerable state?

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

Answer: C

NEW QUESTION 529
- (Exam Topic 3)
A company processes highly sensitive data and senior management wants to protect the sensitive data by utilizing classification labels. Which of the following access control schemes would be BEST for the company to implement?

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

Answer: D

NEW QUESTION 533
- (Exam Topic 3)
A security analyst has received an alert about being sent via email. The analyst's Chief information Security Officer (CISO) has made it clear that PII must be handle with extreme care From which of the following did the alert MOST likely originate?

A. S/MIME
B. DLP
C. IMAP
D. HIDS

Answer: B

Explanation:
Network-based DLP monitors outgoing data looking for sensitive data. Network-based DLP systems monitor outgoing email to detect and block unauthorized data transfers and monitor data stored in the cloud.

NEW QUESTION 535
- (Exam Topic 3)
Two hospitals merged into a single organization. The privacy officer requested a review of ait records to ensure encryption was used Guring record storage, in compliance with regulations. During the review, the officer discovered that medical diagnosis codes and patient names were left unsecured. Which of the following types of data does this combination BEST represent?

A. Personal heath information
B. Personally Kentifiable information
C. Tokenized data
D. Proprietary data

Answer: B

NEW QUESTION 537
- (Exam Topic 3)
An organization's help desk is flooded with phone calls from users stating they can no longer access certain websites. The help desk escalates the issue to the security team, as these websites were accessible the previous day. The security analysts run the following command: ipconfig /flushdns, but the issue persists. Finally, an analyst changes the DNS server for an impacted machine, and the issue goes away. Which of the following attacks MOST likely occurred on the original DNS server?

A. DNS cache poisoning
B. Domain hijacking
C. Distributed denial-of-service
D. DNS tunneling

Answer: D

NEW QUESTION 538
- (Exam Topic 3)
Some laptops recently went missing from a locked storage area that is protected by keyless RFID-enabled locks. There is no obvious damage to the physical space. The security manager identifies who unlocked the door, however, human resources confirms the employee was on vacation at the time of the incident. Which of the following describes what MOST likely occurred?

A. The employee's physical access card was cloned.
B. The employee is colluding with human resources
C. The employee's biometrics were harvested
D. A criminal used lock picking tools to open the door.

Answer: A

NEW QUESTION 540
- (Exam Topic 3)
A cybersecurity manager has scheduled biannual meetings with the IT team and department leaders to discuss how they would respond to hypothetical cyberattacks. During these meetings, the manager presents a scenario and injects additional information throughout the session to replicate what might occur in a dynamic cybersecurity event involving the company, its facilities, its data, and its staff. Which of the following describes
what the manager is doing?

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

Answer: C

NEW QUESTION 542
- (Exam Topic 3)
When selecting a technical solution for identity management, an architect chooses to go from an in-house to a third-party SaaS provider. Which of the following risk management strategies is this an example of?

A. Acceptance
B. Mitigation
C. Avoidance
D. Transference

Answer: D

NEW QUESTION 547
- (Exam Topic 3)
Law enforcement officials sent a company a notification that states electronically stored information and paper documents cannot be destroyed. Which of the following explains this process?

A. Data breach notification
B. Accountability
C. Legal hald
D. Chain of custody

Answer: C

NEW QUESTION 552
- (Exam Topic 3)
A recent malware outbreak across a subnet included successful rootkit installations on many PCs, ensuring persistence by rendering remediation efforts ineffective. Which of the following would BEST detect the
presence of a rootkit in the future?

A. FDE
B. NIDS
C. EDR
D. DLP

Answer: C

NEW QUESTION 556
- (Exam Topic 3)
A pharmaceutical sales representative logs on to a laptop and connects to the public WiFi to check emails and update reports. Which of the following would be BEST to prevent other devices on the network from directly accessing the laptop? (Choose two.)

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

Answer: AB

NEW QUESTION 557
- (Exam Topic 3)
Which of the following will provide the BEST physical security countermeasures to stop intruders? (Select TWO.)

A. Alarms
B. Signage
C. Lighting
D. Access control vestibules
E. Fencing
F. Sensors

Answer: DE

Explanation:
Alarms=deterrent, Signage=deterrent, Lighting=deterrent, Mantraps=physical countermeasure, Fencing=physical countermeasure and Sensors are either reactive or technical. https://www.professormesser.com/security-plus/sy0-501/physical-security-controls-2/

NEW QUESTION 561
- (Exam Topic 3)
Which of the following describes the ability of code to target a hypervisor from inside

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

Answer: B

Explanation:
Virtual machine escape is an exploit in which the attacker runs code on a VM that allows an operating system running within it to break out and interact directly with the hypervisor. https://whatis.techtarget.com/definition/virtual-machine-escape#:~:text=Virtual%20machine%20escape%20is%

NEW QUESTION 565
- (Exam Topic 3)
Which of the following would be used to find the MOST common web-application vulnerabilities?

A. OWASP
B. MITRE ATT&CK
C. Cyber Kill Chain
D. SDLC

Answer: A

NEW QUESTION 567
- (Exam Topic 3)
Rapidly infect computers. Once infected, computers are encrypted and held for ransom. Which of the following would BEST prevent this attack from reoccurring?

A. Configure the perimeter firewall to deny inbound external connections to SMB ports.
B. Ensure endpoint detection and response systems are alerting on suspicious SMB connections.
C. Deny unauthenticated users access to shared network folders.
D. Verify computers are set to install monthly operating system, updates automatically

Answer: A

NEW QUESTION 569
- (Exam Topic 3)
A nuclear plant was the victim of a recent attack, and all the networks were air gapped. A subsequent investigation revealed a worm as the source of the issue. Which of the following BEST explains what happened?

A. A malicious USB was introduced by an unsuspecting employee.
B. The ICS firmware was outdated
C. A local machine has a RAT installed.
D. The HVAC was connected to the maintenance vendor.

Answer: A

NEW QUESTION 573
- (Exam Topic 3)
A administrator needs to allow mobéle BYOD devices to access network resources, As the devices are not enrolled to the domain and do not have policies applied to them, which of the following are best practces for authentication and infrastructure security? (Select TWO)

A. Create a new network for the mobile devices and block the commurycaton to the intemal network and servers
B. Use a captive portal for user authentication
C. Authenticate users using OAuth for more resiliency.
D. Implement SSO and allow communication to the intemal network.
E. Use the existing network and allow communscation to the internal network and servers
F. Use a new and updated RADIUS server to mamntain the best solution

Answer: BC

NEW QUESTION 576
- (Exam Topic 3)
An attacked is attempting to exploit users by creating a fake website with the URL www.validwebsite.com. The attacker's intent is to imitate the look and feel of a legitimate website to obtain personal information from unsuspecting users. Which of the following social-engineering attacks does this describe?

A. Information elicitation
B. Type squatting
C. Impersonation
D. Watering-hole attack

Answer: D

NEW QUESTION 580
- (Exam Topic 3)
A security analyst receives the configuration of a current VPN profile and notices the authentication is only applied to the IP datagram portion of the packet. Which of the following should the analyst implement to authenticate the entire packet?

A. AH
B. ESP
C. SRTP
D. LDAP

Answer: B

NEW QUESTION 582
- (Exam Topic 3)
Which of the following holds staff accountable while escorting unathorized personal?

A. Locks
B. Badges
C. Cameras
D. Visitor logs

Answer: D

NEW QUESTION 587
- (Exam Topic 3)
A commercial cyber-threat intelligence organization observes IoCs across a variety of unrelated customers. Prior to releasing specific threat intelligence to other paid subscribers, the organization is MOST likely obligated by contracts to:

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

Answer: B

NEW QUESTION 590
- (Exam Topic 3)
A global pandemic is forcing a private organization to close some business units and reduce staffing at others. Which of the following would be BEST to help the organization’s executives determine the next course of action?

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

Answer: D

NEW QUESTION 591
- (Exam Topic 3)
A security analyst reports a company policy volation ina case in which a large amount of sensitive data is being downloaded after hours from various mobile devices to an external site. Upon further investigation, the analyst notices that successful login attempts are being conducted with impossible travel times during the same time periods when the unauthorized dowloads are occurring. The @nalyst also discovers a couple of WAP are using the same SSID, but they have non-siandard DHCP configurations and an overlapping channel. Which of the following attacks is being conducted?

A. Evil twin
B. Jamming
C. DNS poisoning
D. Bluesnarfing
E. DDoS

Answer: A

NEW QUESTION 595
- (Exam Topic 3)
A cybersecurity analyst reviews the log files from a web server and sees a series of files that indicates a directory-traversal attack has occurred. Which of the following is the analyst MOST likely seeing?

A. http://sample.url.com/<script>Please-Visit-Our-Phishing-Site</script>

B. http://sample.url.com/someotherpageonsite/../../../etc/shadow

C. http://sample.url.com/select-from-database-where-password-null

D. http://redirect.sameple.url.sampleurl.com/malicious-dns-redirect

A. Option A
B. Option B
C. Option C
D. Option D

Answer: B

NEW QUESTION 600
- (Exam Topic 3)
A user contacts the help desk to report the following:
Two days ago, a pop-up browser window prompted the user for a name and password after connecting to the corporate wireless SSID. This had never happened before, but the user entered the information as requested.
The user was able to access the Internet but had trouble accessing the department share until the next day. The user is now getting notifications from the bank about unauthorized transactions.
Which of the following attack vectors was MOST likely used in this scenario?

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

Answer: A

NEW QUESTION 602
- (Exam Topic 3)
A vulnerability assessment report will include the CVSS score of the discovered vulnerabilities because the score allows the organization to better.

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

Answer: D

Explanation:
The Common Vulnerability Scoring System (CVSS) is a free and open industry standard for assessing the severity of computer system security vulnerabilities. CVSS attempts to assign severity scores to
vulnerabilities, allowing responders to prioritize responses and resources according to threat https://en.wikipedia.org/wiki/Common_Vulnerability_Scoring_System

NEW QUESTION 607
- (Exam Topic 3)
hich of the following would be MOST effective to contain a rapidly spreading attack that is affecting a large number of organizations?

A. Machine learning
B. DNS sinkhole
C. Blocklist
D. Honeypot

Answer: C

NEW QUESTION 609
- (Exam Topic 3)
An attacker is exploiting a vulnerability that does not have a patch available. Which of the following is the attacker exploiting?

A. Zero-day
B. Default permissions
C. Weak encryption
D. Unsecure root accounts

Answer: A

NEW QUESTION 611
- (Exam Topic 3)
The IT department’s on-site developer has been with the team for many years. Each time an application is released, the security team is able to identify multiple

vulnerabilities. Which of the following would BEST help the team ensure the application is ready to be released to production?

A. Limit the use of third-party libraries.
B. Prevent data exposure queries.
C. Obfuscate the source code.
D. Submit the application to QA before releasing it.

Answer: D

NEW QUESTION 616
- (Exam Topic 3)
A manufacturer creates designs for very high security products that are required to be protected and controlled

A. Session replay
B. Evil twin
C. Bluejacking
D. ARP poisoning

Answer: B

NEW QUESTION 620
- (Exam Topic 3)
A developer is concerned about people downloading fake malware-infected replicas of a popular game. Which of the following should the developer do to help verify legitimate versions of the game for users?

A. Digitally sign the relevant game files.
B. Embed a watermark using steganography.
C. Implement TLS on the license activation server.
D. Fuzz the application for unknown vulnerabilities.

Answer: A

NEW QUESTION 622
- (Exam Topic 3)
An attacker is trying to gain access by installing malware on a website that is known to be visited by the target victims. Which of the following is the attacker MOST likely attempting?

A. A spear-phishing attack
B. A watering-hole attack
C. Typo squatting
D. A phishing attack

Answer: B

NEW QUESTION 627
- (Exam Topic 3)
A malicious actor recently penetration a company's network and moved laterally to the datacenter. Upon investigation, a forensics firm wants to know was in the memory on the compromised server. Which of the following files should be given to the forensics firm?

A. Security
B. Application
C. Dump
D. Syslog

Answer: C

Explanation:
Dump files are a special type of files that store information about your computer, the software on it, and the data loaded in the memory when something bad happens. They are usually automatically generated by Windows or by the apps that crash, but you can also manually generate them https://www.digitalcitizen.life/view-contents-dump-file/

NEW QUESTION 630
- (Exam Topic 3)
The Chief Executive Officer (CEO) of an organization would like staff members to have the flexibility to work from home anytime during business hours, incident during a pandemic or crisis, However, the CEO is concerned that some staff members may take advantage of the of the flexibility and work from high-risk countries while on holidays work to a third-party organization in another country. The Chief information Officer (CIO) believes the company can implement some basic to mitigate the majority of the risk. Which of the following would be BEST to mitigate CEO's concern? (Select TWO).

A. Geolocation
B. Time-of-day restrictions
C. Certificates
D. Tokens
E. Geotagging
F. Role-based access controls

Answer: AE

NEW QUESTION 634
- (Exam Topic 3)
Which of the following algorithms has the SMALLEST key size?

A. DES
B. Twofish
C. RSA
D. AES

Answer: B

NEW QUESTION 637
- (Exam Topic 3)
A security analyst needs to produce a document that details how a security incident occurred, the steps that were taken for recovery, and how future incidents can be avoided. During which of the following stages of the response process will this activity take place?

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

Answer: C

NEW QUESTION 638
- (Exam Topic 3)
A symmetric encryption algorithm Is BEST suited for:

A. key-exchange scalability.
B. protecting large amounts of data.
C. providing hashing capabilities,
D. implementing non-repudiation.

Answer: D

NEW QUESTION 641
- (Exam Topic 3)
A company is setting up a web server on the Internet that will utilize both encrypted and unencrypted
web-browsing protocols. A security engineer runs a port scan against the server from the Internet and sees the following output:

Port	Protocol	State	Service
22	tcp	open	ssh
25	tcp	filtered	smtp
53	tcp	filtered	domain
80	tcp	open	http
443	tcp	open	https

Which of the following steps would be best for the security engineer to take NEXT?

A. Allow DNS access from the internet.
B. Block SMTP access from the Internet
C. Block HTTPS access from the Internet
D. Block SSH access from the Internet.

Answer: D

NEW QUESTION 644
- (Exam Topic 3)
A university with remote campuses, which all use different service providers, loses Internet connectivity
across all locations. After a few minutes, Internet and VoIP services are restored, only to go offline again at random intervals, typically within four minutes of services being restored. Outages continue throughout the day, impacting all inbound and outbound connections and services. Services that are limited to the local LAN or WiFi network are not impacted, but all WAN and VoIP services are affected.
Later that day, the edge-router manufacturer releases a CVE outlining the ability of an attacker to exploit the SIP protocol handling on devices, leading to resource exhaustion and system reloads. Which of the following BEST describe this type of attack? (Choose two.)

A. DoS
B. SSL stripping
C. Memory leak
D. Race condition
E. Shimming
F. Refactoring

Answer: AD

NEW QUESTION 649
- (Exam Topic 3)
An analyst needs to identify the applications a user was running and the files that were open before the user’s computer was shut off by holding down the power button. Which of the following would MOST likely contain that information?

A. NGFW
B. Pagefile
C. NetFlow
D. RAM

Answer: C

NEW QUESTION 652
- (Exam Topic 3)
While checking logs, a security engineer notices a number of end users suddenly downloading files with the .t ar.gz extension. Closer examination of the files reveals they are PE32 files. The end users state they did not initiate any of the downloads. Further investigation reveals the end users all clicked on an external email containing an infected MHT file with an href link a week prior. Which of the following is MOST likely occurring?

A. A RAT was installed and is transferring additional exploit tools.
B. The workstations are beaconing to a command-and-control server.
C. A logic bomb was executed and is responsible for the data transfers.
D. A fireless virus is spreading in the local network environment

Answer: A

NEW QUESTION 653
- (Exam Topic 3)
An organization is developing an authentication service for use at the entry and exit ports of country borders. The service will use data feeds obtained from passport systems, passenger manifests, and high-definition video feeds from CCTV systems that are located at the ports. The service will incorporate machine-learning techniques to eliminate biometric enrollment processes while still allowing authorities to identify passengers with increasing accuracy over time. The more frequently passengers travel, the more accurately the service will identify them. Which of the following biometrics will MOST likely be used, without the need for enrollment? (Choose two.)

A. Voice
B. Gait
C. Vein
D. Facial
E. Retina
F. Fingerprint

Answer: BD

NEW QUESTION 657
- (Exam Topic 3)
A systems administrators considering diferent backup solitons forthe IT rkashuchre The company 5 looky fre sokton tha ofes the fastest recovery ime whie aso saving the most amount of storage used to maintain the backups Which of the following recovery solubons would be the BEST option to meet these requirements?

A. Snapshot
B. Differentiated
C. Full
D. Tape

Answer: B

NEW QUESTION 662
- (Exam Topic 3)
An engineer is configuring AAA authentication on a Cisco MDS 9000 Series Switch. The LDAP server is located under the IP 10.10.2.2. The data sent to the LDAP server should be encrypted. Which command should be used to meet these requirements?

A. ldap-server 10.10.2.2 key SSL_KEY
B. ldap-server host 10.10.2.2 key SSL_KEY
C. ldap-server 10.10.2.2 port 443
D. ldap-server host 10.10.2.2 enable-ssl

Answer: D

NEW QUESTION 666
- (Exam Topic 3)
A security analyst is reviewing the output of a web server log and notices a particular account is attempting to transfer large amounts of money:

```
GET http://yourbank.com/transfer.do?acctnum=087646958&amount=500000 HTTP/1.1
GET http://yourbank.com/transfer.do?acctnum=087646958&amount=5000000 HTTP/1.1
GET http://yourbank.com/transfer.do?acctnum=087646958&amount=1000000 HTTP/1.1
GET http://yourbank.com/transfer.do?acctnum=087646958&amount=500 HTTP/1.1
```

Which of the following types of attack is MOST likely being conducted?

A. SQLi
B. CSRF
C. Session replay
D. API

Answer: C

NEW QUESTION 670
- (Exam Topic 3)
Which of the following cloud models provides clients with servers, storage, and networks but nothing else?

A. SaaS
B. PaaS
C. IaaS
D. DaaS

Answer: C

NEW QUESTION 673
- (Exam Topic 3)
A security analyst is hardening a network infrastructure. The analyst is given the following requirements:
* Preserve the use of public IP addresses assigned to equipment on the core router.
* Enable "in transport" encryption protection to the web server with the strongest ciphers.
Which of the following should the analyst implement to meet these requirements? (Select TWO).

A. Configure VLANs on the core router.
B. Configure NAT on the core router.
C. Configure BGP on the core router.
D. Enable AES encryption on the web server.
E. Enable 3DES encryption on the web server.
F. Enable TLSv2 encryption on the web server.

Answer: AE

NEW QUESTION 674
- (Exam Topic 3)
An engineer needs to deploy a security measure to identify and prevent data tampering within the enterprise.
Which of the following will accomplish this goal?

A. Antivirus
B. IPS.
C. FTP
D. FIM

Answer: D

NEW QUESTION 678
- (Exam Topic 3)
Administrators have allowed employees to access their company email from personal computers. However, the administrators are concerned that these computers are another attack Surface and can result in user accounts being breached by foreign actors. Which of the following actions would provide the MOST secure solution?

A. Enable an option in the administration center so accounts can be locked if they are accessed from different geographical areas.
B. Implement a 16-character minimum length and 30-day expiration password policy.
C. Set up a global mail rule to disallow the forwarding of any company email to email addresses outside the organization,
D. Enforce a policy that allows employees to be able to access their email only while they are connected to the Internet via VPN.

Answer: A

NEW QUESTION 679
- (Exam Topic 3)
An organization is concerned that is hosted web servers are not running the most updated version of the software. Which of the following would work BEST to help identify potential vulnerabilities?

A. Hping3 –s comptia, org –p 80
B. Nc -1 –v comptia, org –p 80
C. nmp comptia, org –p 80 –aV
D. nslookup –port=80 comtia.org

Answer: C

Explanation:
Nmap is used to discover hosts and services on a computer network by sending packets and analyzing the responses. Nmap provides a number of features for probing computer networks, including host discovery and service and operating system detection.

NEW QUESTION 682
- (Exam Topic 3)
A security analyst is performing a forensic investigation compromised account credentials. Using the Event Viewer, the analyst able to detect the following message, ''Special privileges assigned to new login.'' Several of these messages did not have a valid logon associated with the user before these privileges were assigned.
Which of the following attacks is MOST likely being detected?

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

Answer: A

NEW QUESTION 684
- (Exam Topic 3)
A smart retail business has a local store and a newly established and growing online storefront. A recent storm caused a power outage to the business and the local ISP, resulting in several hours of lost sales and delayed order processing. The business owner now needs to ensure two things:
* Protection from power outages
* Always-available connectivity In case of an outage
The owner has decided to implement battery backups for the computer equipment Which of the following would BEST fulfill the owner's second need?

A. Lease a point-to-point circuit to provide dedicated access.
B. Connect the business router to its own dedicated UPS.
C. Purchase services from a cloud provider for high availability
D. Replace the business's wired network with a wireless network

Answer: C

NEW QUESTION 689
- (Exam Topic 3)
A security administrator checks the table of a network switch, which shows the following output:

VLAN	Physical address	Type	Port
1	001a:42ff:5113	Dynamic	GE0/5
1	0faa:abcf:ddee	Dynamic	GE0/5
1	c6a9:6b16:758e	Dynamic	GE0/5
1	a3aa:b6a3:1212	Dynamic	GE0/5
1	8025:2ad8:bfac	Dynamic	GE0/5
1	b839:f995:a00a	Dynamic	GE0/5

Which of the following is happening to this switch?

A. MAC Flooding
B. DNS poisoning
C. MAC cloning
D. ARP poisoning

Answer: A

NEW QUESTION 690
- (Exam Topic 3)
In which of the following risk management strategies would cybersecurity insurance be used?

A. Transference
B. Avoidance
C. Acceptance
D. Mitigation

Answer: A

NEW QUESTION 695
- (Exam Topic 3)
A Chief Security Officer (CSO) is concerned about the amount of PII that is stored locally on each salesperson’s laptop. The sales department has a higher-than-average rate of lost equipment. Which of the following recommendations would BEST address the CSO’s concern?

A. Deploy an MDM solution.
B. Implement managed FDE.
C. Replace all hard drives with SEDs.
D. Install DLP agents on each laptop.

Answer: B

NEW QUESTION 697
.....

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questons and Answers in PDF Format

SY0-601 Practice Exam Features:

* SY0-601 Questions and Answers Updated Frequently

* SY0-601 Practice Questions Verified by Expert Senior Certified Staff

* SY0-601 Most Realistic Questions that Guarantee you a Pass on Your FirstTry

* SY0-601 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year