Exam Questions CC

Certified in Cybersecurity (CC)

https://www.2passeasy.com/dumps/CC/

NEW QUESTION 1
How do you distinguish Authentication and Identification

A. Both Same
B. Authentication is the process of verifying user identity and a user of a system or an application
C. Authentication is the process of verifying user identity and Identification is the ability to identify uniquely quely Identification is the process to allow resource access
D. Identification is the process of verifying user identity and Authentication is the process to allow resource access

Answer: B

NEW QUESTION 2
4 Embedded systems and network-enabled devices that communicate with the internet are considered as

A. Endpoint
B. Node
C. IOT
D. router

Answer: C

NEW QUESTION 3
Faking the sender address in a transmission to gain illegal entry into a secure system

A. Phishing
B. ARP
C. Spoofing
D. ALL

Answer: C

NEW QUESTION 4
What are registered port used for

A. Common protocols at the core of TCP/IP model
B. Used for web servers
C. Used for in housed or opensource applications
D. Proprietary applications from vendors and develope

Answer: D

NEW QUESTION 5
In Which of the following access control models can the creator of an object delegate permission

A. MAC
B. RBAC
C. ABAC
D. DAC

Answer: C

NEW QUESTION 6
Ping flood attack target which OSI layer

A. Layer 4
B. Layer 3
C. Layer 5
D. Layer 6

Answer: B

NEW QUESTION 7
Which is related to Standard

A. NIST
B. GDPR
C. HIPAA
D. ALL

Answer: A

NEW QUESTION 8
Requires that all instances of the data be identical in form,

A. Confidentiality
B. Availability
C. Consistency
D. ALL

Answer: C

NEW QUESTION 9
Which is an approach to networking that uses software-based controllers or application programming interfaces (APIs) to communicate with underlying hardware infrastructure and direct traffic on a network.

A. VLAN
B. SDN
C. VPN
D. SAN

Answer: B

NEW QUESTION 10
Which of the following is not a Social engineering technique

A. Pretexting
B. Baiting
C. Quid pro quo
D. Double Dealing

Answer: D

NEW QUESTION 10
Example of Token based Authentication

A. Kerberos
B. Basic
C. OAuth
D. NTLN

Answer: C

NEW QUESTION 11
Which term describes a communication tunnel that provides point-to-point transmission of both authentication and data traffic over an untrusted network?

A. Zero Trust
B. DMZ
C. VPN
D. None of the Above

Answer: C

NEW QUESTION 14
A popular way of implementing "least privilege"

A. MAC
B. DAC
C. RBAC
D. ABAC

Answer: C

NEW QUESTION 19
What type of attack does the attacker store and reuse login information. Select the BEST answer?

A. Man-in-the-middle attack
B. Smurf attack
C. DDoS attack
D. Replay attack

Answer: D

NEW QUESTION 20
Which is the Not the component of a Business Continuity (BC) plan

A. Immediate response procedures and checklists
B. Notification systems and call trees for alerting personnel
C. Guidance for management, including designation of authority for specific managers
D. Manacomont

Answer: D

NEW QUESTION 21
Embedded systems and network-enabled devices that communicate with the internet are considered as

A. Endpoint
B. Node
C. IOT
D. Router

Answer: C

NEW QUESTION 25
A company wants to ensure that its employees can evacuate the building in case of an emergency which physical control is best suited for this scenario

A. Fire Alarms
B. Exit signs
C. Emergency lighting
D. Emergency exit doors

Answer: D

NEW QUESTION 29
The process of how an organization is managed; usually includes all aspects of how decisions are made for that organization

A. Standard
B. Policy
C. Procedure
D. Governance

Answer: D

NEW QUESTION 34
Which one of the following controls is not particularly effective against the insider threat?

A. Least privilege
B. Background checks
C. Firewalls
D. Separation of duties

Answer: C

NEW QUESTION 35
What is an incident in the context of cybersecurity

A. Any observable occurrence in a network or system
B. A deliberate security incident in which an intruder gains access to a system or system resource without authorization
C. A particular attack that exploits system vulnerabilities
D. An event that actually or potentially jeopardizes the confidentiality integrity or availability of an information system.

Answer: D

NEW QUESTION 37
Which of the following is a systematic approach to protecting against cyber threats that involves a continuous cycle of identifying, assessing and prioritizing risks and implementing measures to reduce or eliminate those risks?

A. Security Assessment
B. Incident response
C. Peneteration testing
D. Risk Management

Answer: D

NEW QUESTION 41
The last phase in the data security cycle is

A. Encryption
B. Destruction
C. Archival
D. Backup

Answer: B

NEW QUESTION 43

Finance Server and Transactions Server has restored its original facility after a disaster, what should be moved in FIRST?

A. Management
B. Most critical systems
C. Most critical functions
D. Least critical functions

Answer: D

NEW QUESTION 44
Scans networks to determine everything that is connected as well as other information.

A. Burbsuite
B. Wireshark
C. Fiddler
D. Zen Mao

Answer: D

NEW QUESTION 49
What is a type of system architecture where a single instance can serve multiple distinct user groups.

A. Mutli-threading
B. Multi-processing
C. Multitenancy
D. Multi-cloud

Answer: C

NEW QUESTION 50
Are a measure of an organization's baseline of security performance

A. Security Assessment
B. Secuirty Audit
C. Security Benchmark
D. Security Management

Answer: C

NEW QUESTION 53
The documentation of a predetermined set of instructions or procedures to detect, respond to andlimit consequences of a malicious cyberattack against an organization's information systems(s).

A. IR
B. IRP
C. BCP
D. DRP

Answer: B

NEW QUESTION 57
Which of the following is endpint

A. Router
B. Firewall
C. Laptop
D. Switch

Answer: C

NEW QUESTION 62
Which TLS extension is used to optimize the TLS handshake process by reducing the number of round trips between the client and server?

A. TLS Renegotiation
B. TLS Heartbeat
C. TLS Session Resumption
D. TLS FastTrack

Answer: C

NEW QUESTION 63
Which layer does VLAN hopping belong to?

A. Layer 3
B. Layer 4

C. Layer 7
D. Layer 2

Answer: D

NEW QUESTION 64
COVID-19 is one of the perfect example of a situation, where a _____ plan is enacted to sustain the business

A. IRP
B. DRP
C. BCP
D. ALL

Answer: C

NEW QUESTION 65
What is the difference between business continuity planning and disaster recovery planning?

A. Business continuity planning is abount restoring IT and communincations back to full operations after a dustruption, while disaster recovery planning is about maintaining criticla business functions
B. Disaster recovery planning is about restoring IT and communications back to full operations after a disruption, while business continuity planning is about maintaining critical business functions
C. Business continuity planning and disaster recovery planning are the same thisg
D. Business continuity planning is about maintainig criticla business funtions before disasteroccurs

Answer: B

NEW QUESTION 68
What is the best practise to clear SSD storage after usage in term of cyber security

A. Zero fill
B. Degaussing
C. Clearing
D. Disintegration

Answer: D

NEW QUESTION 69
In information systems terms, the activities necessary to restore IT and communications services of an organization during and after an outage

A. IR
B. BC
C. Risk Management
D. DR

Answer: D

NEW QUESTION 73
which is the short form of IPv6 address 2001:0db8:0000:0000:0000:ffff:0000:0001

A. 2001:db8::ffff:0:1
B. 2001:db8:0000:ffff:0:1
C. 2001:db80::ffff:0000:1
D. 2001:db8::ffff:0000:0001

Answer: A

NEW QUESTION 74
A scammer will attempt to make a malicious website look exactly like a legitimate one that the victim knows and trusts

A. DOS
B. Virus
C. Spoofing
D. Phishing

Answer: C

NEW QUESTION 75
Difference between Sniffing and Snooping

A. Sniffing is the process of intercepting and collecting network traffic as it passes over a digital networ
B. Spoofing is the act of disguising a communication from an unknown source as being trustworthy.
C. Snooping is the process of intercepting and collecting network traffic as it passes over a digital networ
D. Sniffing is the act of disguising a communication from an unknown source as being trustworthy.
E. Both are same

F. Sniffing is not thread and snoofing is a thread

Answer: A

NEW QUESTION 78
Removing the design belief that the network has any trusted space. Security is managed at each possible level, representing the most granular asset. Micro segmentation of workloads is a tool of the model

A. Zero Trust
B. Defence in Depth
C. Least Privileges
D. AII

Answer: A

NEW QUESTION 79
The primary functionality of PAM is?

A. Validate the level of access a user have to a file
B. Prevent unauthorized access to organizational assets
C. Provide just-in-time access to critical resources
D. Manage centralized access control

Answer: C

NEW QUESTION 81
Information should be consistently and readily accessible for authorized parties ?

A. Confidentiality
B. Authentication
C. Availability
D. Non-repudiation

Answer: C

NEW QUESTION 82
What is the purpose of non-repudiation in information security?

A. To ensure data is always accessible when needed
B. To protect data from unauthorized access
C. To prevent the sender or recipient of a message from denying having sent or received the message
D. To ensure data is accurate and unchanged

Answer: C

NEW QUESTION 84
In what way do a victim's files get affected by ransomware?

A. By destroying them
B. By encrypting them
C. By stealing them
D. By selling them

Answer: B

NEW QUESTION 89
Which threats are directly associated with malware? Select that apply.

A. APT
B. Ransomeware
C. Trojan
D. DDOS

Answer: C

NEW QUESTION 92
Dylan is creating a cloud architecture that requires connections between systems in two different private VPCs. What would be the best way for Dylan to enable this access?

A. VPN Connection
B. Internet Gateway
C. Public IP Address
D. VPC Endpoint

Answer: D

NEW QUESTION 95
Which is the component of a Business Continuity (BC) plan

A. Immediate response procedures and checklists
B. Notification systems and call trees for alerting personnel
C. Guidance for management, including designation of authority for specific managers
D. ALL

Answer: D

NEW QUESTION 98
In DAC, the policy specifies that a subject who has been granted access to information can do the following:

A. Change security attributes on subjects, objects, information systems or system components
B. Choose the security attributes to be associated with newly created or revised objects
C. Change the rules governing access control
D. ALL

Answer: D

NEW QUESTION 103
When is the Business Continuity Plan Enacted?

A. When there is a event
B. When there is a incident
C. When there is a loss of business operations
D. When there is a natural disaster

Answer: C

NEW QUESTION 105
What is the primary purpose of a firewall in network security?

A. Encrypt data transmissions
B. Prevent unauthorized access
C. Monitor network traffic
D. Backup critical data

Answer: B

NEW QUESTION 106
Which of the following is a characteristic of cloud

A. Broad Network Access
B. Rapid Elasticity
C. Measured Service
D. AII

Answer: B

NEW QUESTION 108
Which of the following is not a source of redundant power

A. Generator
B. Utility
C. UPS
D. HVAC

Answer: D

NEW QUESTION 113
The means by which a threat actor carries out their objectives

A. Threat
B. Threat Vector
C. Exploit
D. Intrusion

Answer: B

NEW QUESTION 114
Which of these tool is commonly used to crack passwords

A. Bup Suite

B. Nslookup
C. Wireshark
D. John the ripper

Answer: D

NEW QUESTION 115
Which of the following security controls is designed to prevent unauthorized access to sensitive information by ensuring that it is only accessible to authorized users?

A. Encryption
B. Firewall
C. Antivirus
D. Access control

Answer: D

NEW QUESTION 117
Which layer of OSI the Firewall works

A. Layer 3
B. Layer 4
C. Layer 7
D. AII

Answer: D

NEW QUESTION 121
Who should participate in creating a BCP

A. Only members from the IT department
B. Only members from the management team
C. Members from across the organization
D. Only members from the finanace department

Answer: C

NEW QUESTION 123
A company network has been infected with malware and all its servers are down. What is the first step that the Disaster Recovery team should take to restore the systems?

A. Disconnect the affected systems from the network
B. Conduct a risk assessment of determine the extent of the damage
C. Restore data from backup systems
D. Contact the enforcement to investigate the cyberattack

Answer: A

NEW QUESTION 126
Some Employee of his organization launched a privilege escalation attack to gain root access on one of the organization's database serversiThe employee does have an authorized user account on the server. What log file would be MOST likely to contain relevant information??

A. Database application log
B. Firewall log
C. Operating system log
D. IDS log

Answer: C

NEW QUESTION 130
Communication between end systems is encrypted using a key, often known as _____?

A. Temporary Key
B. Section Key
C. Public Key
D. Session Key

Answer: D

NEW QUESTION 132
What is knowledge based authentication

A. Authentication based on a passphrase or secret code
B. Autheication based on a token or memory card
C. Authentication based on biometrics or measurble charestrisirtcs

D. Authencication based on something you do

Answer: A

NEW QUESTION 135
If a device is found that is not compliant with the security baseline, what will be the security team action

A. Report
B. Evaluate
C. Ignore
D. Disabled or isolated into a quarantine area until it can be checked and updated.

Answer: D

NEW QUESTION 136
What goal of security is enhanced by a strong business continuity program?

A. non-repudiation
B. Availability
C. Confidentiality
D. Integrity

Answer: B

NEW QUESTION 139
Which maintains that a user or entity should only have access to the spec data, resources and applications needed to complete a required task.

A. Zero Trust
B. Defence in Depth
C. Least Privileges
D. AII

Answer: C

NEW QUESTION 144
Configuration settings or parameters stored as data, managed through a software graphical user interface (GUI) is

A. Logical access control
B. Physical access control
C. Administrative Access control

Answer: A

NEW QUESTION 149
Security control used to protect against environmental threats such as fire, flood and earth quakes

A. Physical control
B. Logical Control
C. Adminstrative Control
D. Thechnical control

Answer: A

NEW QUESTION 154
What is the end goal of DRP

A. All System backup restored
B. DR site activated
C. Shifting the Infrastructure to new place
D. Business restored to full last-known reliable operations.

Answer: D

NEW QUESTION 158
What is the main purpose of creating baseline in ensuring system integrity

A. To compare the baseline with the current state of the systems
B. To protect the information
C. To understand the current state of the system
D. AII

Answer: A

NEW QUESTION 160

A portion of the organization's network that interfaces directly with the outside world; typically, this exposed area has more security controls and restrictions than the rest of the internal IT environment.

A. Virtual private network (VPN)
B. Virtual local area network (VLAN)
C. Zero Trust
D. Demilitarized zone (DMZ)

Answer: D

NEW QUESTION 163
What is the range of private ports

A. 0 - 1023
B. 1023-49151
C. 49152 - 65535
D. None

Answer: C

NEW QUESTION 167
Which Prevent crime by designing a physical environment that positively influences human behavior.

A. DMZ
B. Security Alarm
C. CPTED
D. CCTV

Answer: C

NEW QUESTION 169
A type of malware that is capable of self propagation and can infect multiple systems on network without the need for human intervention

A. Worm
B. Spy ware
C. Adwre
D. Virus

Answer: A

NEW QUESTION 170
A _____ is a distributed denial-of-service (DDoS) attack in which an attacker attempts to flood a targeted server with Internet Control Message Protocol (ICMP) packets.

A. DOS
B. Syn flood
C. Smurf attack
D. Phishing attack

Answer: C

NEW QUESTION 171
What is the recommended range of temperature for optimized maximum uptime and hardware life in a data center?

A. 62 F to 69 F
B. 64 F to 81 F
C. 82 F to 90 F
D. 91 F to 100 F

Answer: B

NEW QUESTION 173
Which of these components is very likely to be instrumental to any disaster recovery (DR) effort?

A. Routers
B. Laptops
C. Firewalls
D. Backups

Answer: D

NEW QUESTION 176
Mark is configuring an automated data transfer between two hosts and is choosing an authentication technique for one host to connect to the other host. What approach would be best-suited for this scenario?

A. Biometric
B. Smart Card
C. SSH Key
D. Hard Coded Password

Answer: C

NEW QUESTION 179
A type of malware that downloads onto a computer disguised as a legitimate program

A. Worm
B. Trojan
C. virus
D. Ransomware

Answer: B

NEW QUESTION 183
What is a security token used to authenticate a user to a web application, typically after they log in?

A. Captcha
B. API key
C. CSRF token
D. Session token

Answer: D

NEW QUESTION 185
DevOps team has updated the application source code, Tom has discovered that many unauthorized changes have been made. What is the BEST control Tom can implement to prevent a recurrence of this problem?

A. Backup
B. File labels
C. Security audit
D. Hashing

Answer: D

NEW QUESTION 188
are events that may indicate that an organization's systems or data have been compromised or that measures put in place to protect them have failed

A. Exploit
B. Security Incident
C. Threat
D. Rreach

Answer: B

NEW QUESTION 190
What does internal consistency of information refer to

A. Data being accurate, usefull and complete
B. Data being protected from errors or loss of information
C. All instances of data being identical in form content and meaning
D. Data being displayed and stored the same way on all system

Answer: C

NEW QUESTION 192
A company security team detected a cyber attack against it information systems and activates a set of procedures to mitigate the attack., What type of plan is this?

A. Business continuty plan
B. Incident response plan
C. Disaster recvoery plan
D. Security operation plan

Answer: B

NEW QUESTION 195
Example of Deterrent controls

A. CCTV
B. BCP
C. DRP
D. IRP

Answer: A

NEW QUESTION 197
Which of the following types of vulnerabilities cannot be discovered in the course of a routine vulnerability assessment?

A. Zero-day vulnerability
B. Kernel flaw
C. Buffer overflow
D. File and directory permissions

Answer: A

NEW QUESTION 202
Which of these is WEAKEST form of authentication we can implement?

A. Something you know
B. Something you are
C. Something you have
D. Biometric authentications

Answer: A

NEW QUESTION 207
Which document serve as specifications for the implementation of policy and dictates mandatory requirements

A. Policy
B. Guideline
C. Standard
D. Procedures

Answer: C

NEW QUESTION 208
Which security control mostly used to prevent data breach

A. Physical control
B. Logical Control
C. Adminstrative Control
D. RBAC

Answer: B

NEW QUESTION 213
Exhibit.

Symmetric Encryption	Asymmetric Encryption
• Symmetric encryption consists of one key for encryption and decryption.	• Asymmetric Encryption consists of two cryptographic keys known as **Public Key** and **Private Key**.
• Symmetric Encryption is a lot quicker compared to the Asymmetric method.	• As Asymmetric Encryption incorporates two separate keys, the process is slowed down considerably.
• RC4 • AES • DES • 3DES • QUAD	• RSA • Diffie-Hellman • ECC • El Gamal • DSA

How many keys would be required to support 50 users in an asymmetric cryptography system?

A. 100
B. 200
C. 50

D. 1225

Answer: A

NEW QUESTION 214
Which of these is an example of deterrent control

A. Biometric
B. Guard Dog
C. Encryption
D. Trunstile

Answer: B

NEW QUESTION 216
An IP network protocol standardized by the Internet Engineering Task Force (IETF) through RFC 792 to determine if a particular service or host is available.

A. IP
B. ICMP
C. IGMP
D. HTTP

Answer: B

NEW QUESTION 218
What is the first component the new security engineer should learn about in the incident response plan?

A. Detection and analysis
B. Preparation
C. Containment
D. Eradication

Answer: B

NEW QUESTION 220
An employee unintentionally shares confidential information with an unauthorized party. What term best describes this situation?

A. Event
B. Exploit
C. Intrusion
D. Breach

Answer: D

NEW QUESTION 221
Granting a user access to services or the system

A. Authentication
B. Identification
C. Authorization
D. Confidentiality

Answer: C

NEW QUESTION 224
WF attack in which a subscriber currently authenticated to an Server and connected through a secure session browses to an attacker's website, causing the subscriber to unknowingly invoke unwanted actions at the Server

A. XSS
B. CSRF
C. Spoofing
D. ALL

Answer: B

NEW QUESTION 226
What is sensitivity in the context of confidentiality

A. The harm caused to externl stakeholders if information is disclosed or modified
B. The ability of information to be accessed only by authorized individuals
C. The need for protection assigned to information by its owner
D. The Health status of the individuals

Answer: C

NEW QUESTION 230
Which type of fire suppression system is more friendly to electronics

A. Carbon di Oxide based
B. Chemical based
C. Water based
D. Foam based

Answer: A

NEW QUESTION 235
Which protocol would be most suitable to fulfill the secure communication requirements between clients and the server for a company deploying a new application?

A. FTP
B. HTTP
C. HTTPS
D. SMTP

Answer: C

NEW QUESTION 236
A company experiences a major IT outage and cannot perform its critical business functions. What type of plan will hep the company recover from this event?

A. BCP
B. IRP C DRP
C. BIA

Answer: C

NEW QUESTION 238
When the ISC2 Mail server sends mail to other mail servers it becomes —?

A. SMTP Server
B. SMTP Peer
C. SMTP Master
D. SMTP Client

Answer: D

NEW QUESTION 239
Which of these activities is often associated with DR efforts?

A. Running anti-malware solutions
B. Scanning the IT environment for vulnerabilities
C. Zero-day exploits
D. Employees returning to the primary production location

Answer: D

NEW QUESTION 243
What kind of control is, when we add a backup firewall that takes over if the main one stops working?

A. Clustering
B. High availability(HA)
C. Load balancing
D. Component redundancy

Answer: B

NEW QUESTION 247
The highest-level governance documents in an organization, usually approved and issued by management, usually to support a compliance initiative

A. Standard
B. Policy
C. Procedure
D. Laws or Regulations

Answer: B

NEW QUESTION 249
A set of instructions to help IT staff detect, respond to, and recover from network security incidents?

A. BCP
B. IRP

C. DRP
D. None

Answer: B

NEW QUESTION 254
Duke would like to restrict users from accessing a list of prohibited websites while connected to his network. Which one of the following controls would BEST achieve his objective?

A. URL Filter
B. IP Address Block
C. DLP Solution
D. IPS Solution

Answer: A

NEW QUESTION 257
What cybersecurity principle focuses on granting users only the privileges necessary to perform their job functions?

A. Least privilege (Correct)
B. defense in depth
C. separation of duties
D. need-to-know basis

Answer: A

NEW QUESTION 261
Example of Type 1 Authentication

A. Password
B. Smart Card
C. Finger Print
D. RSA Token

Answer: A

NEW QUESTION 266
1 _____ is a weighted factor based on a subjective analysis of the probability that a given threat or set of threats is capable of exploiting a given vulnerability or set of vulnerabilities.

A. Likelihood of occurrence
B. Threat Vector
C. Risk
D. Impact

Answer: A

NEW QUESTION 270
The practice of ensuring that an organizational process cannot be completed by a single person; forces collusion as a means to reduce insider threats.

A. Segregation of Duties
B. Principle of Least Privilege
C. Privileged Account
D. Rule-based access control

Answer: A

NEW QUESTION 272
Which plan is activated when both the Incident response and BCP fails

A. Risk Management
B. BIA
C. DRP
D. None

Answer: C

NEW QUESTION 273
A security event, or combination of security events, that constitutes a secu incident in which an intruder gains, or attempts to gain, access to a system or system resource without authorization

A. Intrusion
B. Exploit
C. Threat
D. Attack

Answer: A

NEW QUESTION 277
Which access control model can grant access to a given object based on complex rules

A. ABAC
B. DAC
C. MAC
D. RBAC

Answer: A

NEW QUESTION 280
An attack in which an attacker listens passively to the authentication protocol to capture information that can be used in a subsequent active attack to masquerade as the claimant

A. Eavesdropping Attack
B. CSRF
C. XSS
D. ARP Spoofing

Answer: A

NEW QUESTION 281
Who is responsible for publishing and signing the organization s policies?

A. The security office
B. Human resources
C. Senior management
D. The legal department

Answer: C

NEW QUESTION 282
Which type of control is used to restore systems or processes to their normal state after an attack has occurred

A. Compensatory Control
B. Recovery Control
C. Detective Control
D. Corrective Control

Answer: D

NEW QUESTION 287
What is the main challenge in achieving non repudiation in electronic transactions

A. Ensuring the identity of the sender and recipient is verified
B. Ensuring the authenticity and integrity of the message
C. Making sure the message is not tampered with during transmission
D. All of the above

Answer: D

NEW QUESTION 291
Which uses encrypted, machine-generated codes to verify a user's identity.

A. Basic Authentication
B. Form Based Authentication
C. Token Based Authentication
D. AII

Answer: C

NEW QUESTION 293
In incident terminology the Zero day is

A. Days with a cybersecurity incident
B. A previously unknown system vulnerability
C. Days without a cybersecurity incident
D. Days to solve a previously unknown system vulnerability

Answer: B

NEW QUESTION 296

A new BYOD policy has been enforced in NEW Corp which type of control is used to enforce thissecurity policies

A. Physical control
B. Logical Control
C. Administrative Control
D. Technical Control

Answer: C

NEW QUESTION 298
Which is a curated knowledge base and model for cyber adversary behavior, reflecting the various phases of an adversary's attack lifecycle and the platforms they are known to target

A. MITRE ATT&CK
B. CVE
C. Risk Management framework
D. Security Management

Answer: A

NEW QUESTION 300
What is the primary purpose of a honeytoken in cybersecurity?

A. To lure and detect attackers
B. To encrypt sensitive data
C. To enhance network performance
D. To manage user access

Answer: A

NEW QUESTION 304
A one-way spinning door or barrier that allows only one person at a time to enter a building or pass through an area.

A. Turnstile
B. ManTrap
C. Bollard
D. Gate

Answer: A

NEW QUESTION 305
A common network device used to filter traffic?

A. Server
B. Endpoint
C. Ethernet
D. Firewa

Answer: D

NEW QUESTION 307
When responding to a security incident, your team determines that the vulnerability that was exploited was not widely known to the security community, and that there are no currently known definitions/listings in common vulnerability databases or collections. This vulnerability and exploit might be called _____

A. Malware
B. Zero-day
C. Event
D. Attack

Answer: B

NEW QUESTION 309
The primary goal of a risk assessment

A. Avoid Risk
B. Estimate and Prioritize Risk
C. Ignore risk
D. Evaluate the Impact

Answer: B

NEW QUESTION 313
Set of rules that everyone must comply with and usually carry monetary penalties for noncompliance

A. Standard

B. Policy
C. Procedure
D. Laws or Regulations

Answer: A

NEW QUESTION 317
An external entity has tried to gain access to your organization's IT environment without proper authorization. This is an example of a(n)

A. Exploit
B. Intrusion
C. Event
D. Malware

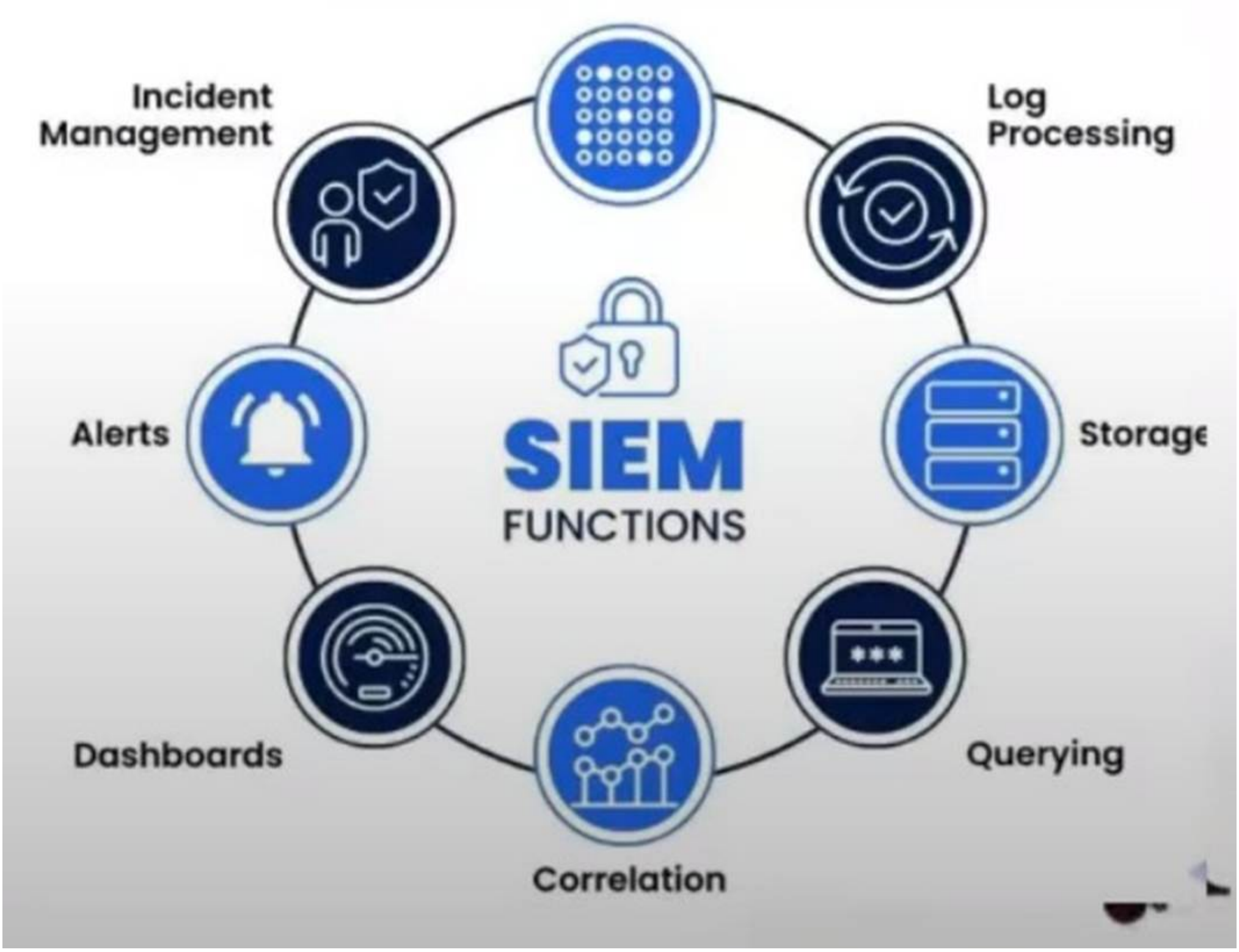
Answer: B

NEW QUESTION 319
Government can imposes financial penalties as a consequence of breaking a

A. Standard
B. Regulation
C. Policy
D. Procedures

Answer: B

NEW QUESTION 321
Exhibit.



What is the purpose of a Security Information and Event Management (SIEM) system?

A. Encrypting files
B. Monitoring and analyzing security events -
C. Blocking malicious websites
D. Managing user passwords

Answer: B

NEW QUESTION 322
Which of the following properties is not guaranteed by Digital signatures

A. Authentication
B. Confidentiality
C. Non-Repudiation
D. Integrity

Answer: B

NEW QUESTION 326
Which of the following is a common security measure to prevent Cross Site Scripting (XSS) attacks in web applications?

A. implementing strong password policies
B. using a firewall to block incoming traffic
C. validating and sanitizing user input (Correct)
D. encrypting data during transmission

Answer: C

NEW QUESTION 329
Incident management is also known as

A. Risk Management
B. Business Continuity management
C. Incident management
D. Crisis management

Answer: D

NEW QUESTION 331
A collection of actions that must be followed in order to complete a task or process in accordance with a set of rules

A. Policy
B. Procedure
C. Law
D. Standard

Answer: B

NEW QUESTION 332
The DLP solution should be deployed so that it can inspect all forms of data leaving the organization, including:

A. Posting to web pages/websites
B. Applications/application programming interfaces (APIs)
C. Copy to portable media
D. AII

Answer: D

NEW QUESTION 337
Which ensure maintaining business operations during or after an incident

A. Incident Response
B. Business Continuity
C. Disaster Recovery
D. AII

Answer: C

NEW QUESTION 342
What is the most important aspect of security awareness/training?

A. Maximizing business capabilities
B. Protecting assets
C. Protecting health and human safety
D. Ensuring the confidentiality of data

Answer: C

NEW QUESTION 347
Load balancing safe guard which CIA triad

A. Confidentiality
B. Availablity
C. Integrity
D. All

Answer: B

NEW QUESTION 348
A company primary data center goes down due to a hardware failure causing a major disruption to the IT and communications systems. What is the focus of disaster recovery planning in this scenario

A. Maintaining critical business functions during the disruption
B. Fixing the hardware failure
C. Restoring IT and communication system back to full operations after the disruptions.
D. Guiding the actions of emergency response personnel during the disruption

Answer: C

NEW QUESTION 349
What does the concept of integrity applied to

A. Organization
B. Information system and processes for business operations
C. People
D. ALL

Answer: D

NEW QUESTION 351
Which of the following is very likely to be used in a disaster recovery (DR) effort?

A. Guard dogs
B. Contract personnel
C. Data backups
D. Anti-malware solutions

Answer: C

NEW QUESTION 353
What is the primary goal of a risk management process in cybersecurity?

A. to eliminate all cybersecurity risks
B. to transfer all cybersecurity risks to a third party
C. to identify, assess, and mitigate cybersecurity risks to an acceptable level (Correct)
D. to ignore cybersecurity risks and focus on incident response

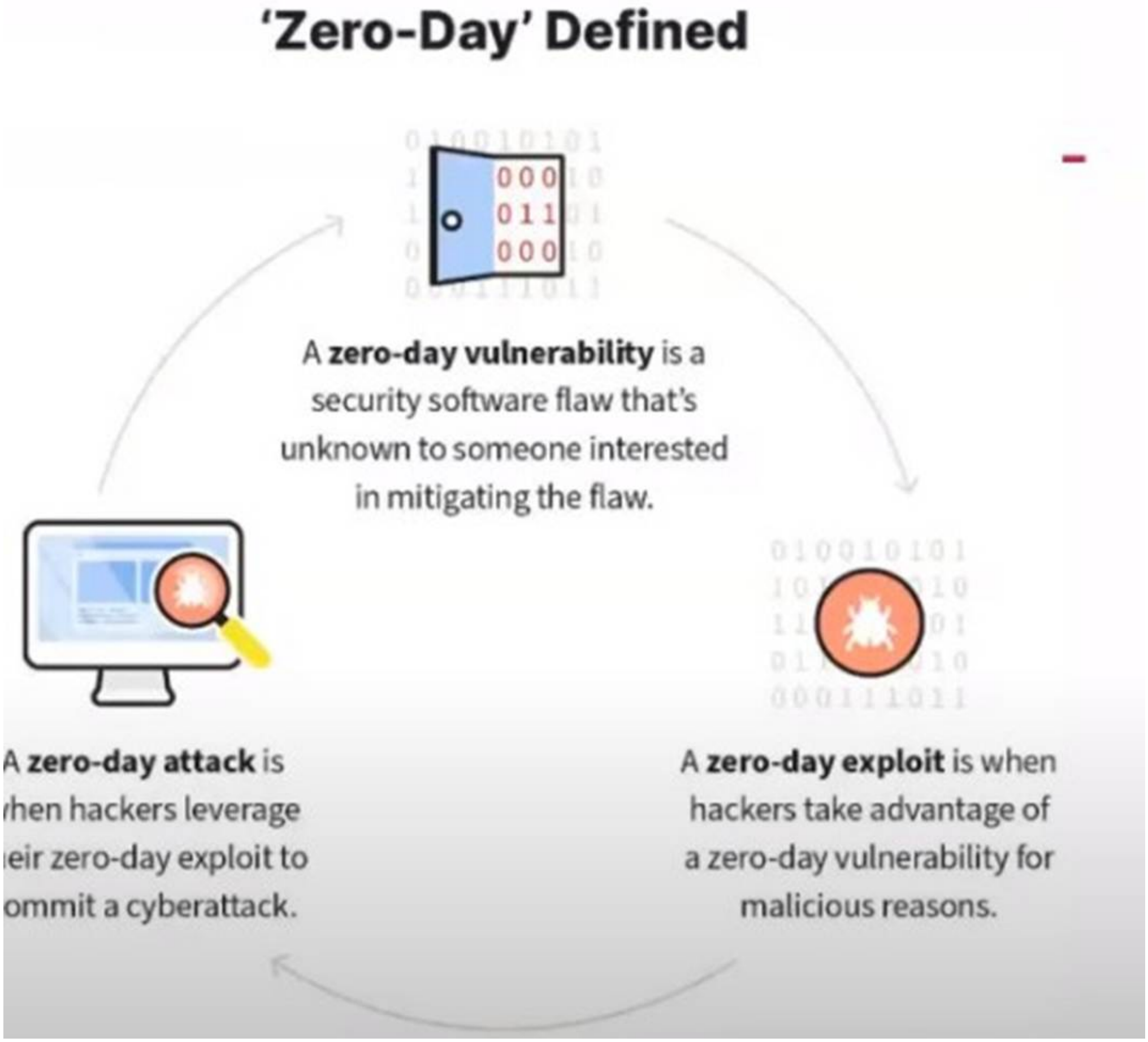
Answer: C

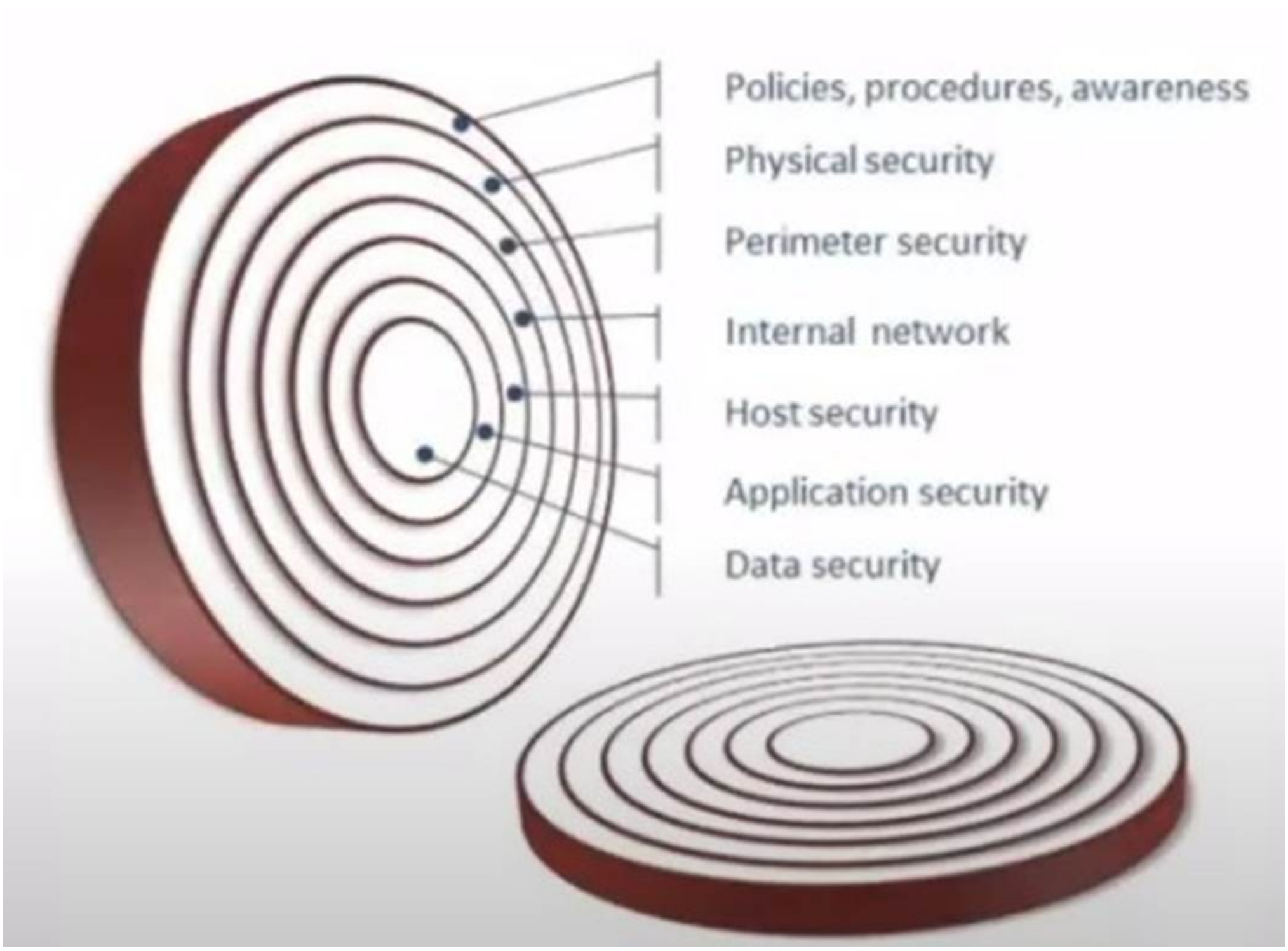
NEW QUESTION 354
Which authentication helps build relationships between different technology providers, enabling automatic identification and user access. Employees no longer need to enter separate usernames and passwords when visiting a new service provider

A. Basic
B. Kerberos
C. Token Based
D. Federated

Answer: D

NEW QUESTION 358
Exhibit.


'Zero-Day' Defined
000
011
000
A zero-day vulnerability is a security software flaw that's unknown to someone interested in mitigating the flaw.
A zero-day attack is when hackers leverage their zero-day exploit to commit a cyberattack.
A zero-day exploit is when hackers take advantage of a zero-day vulnerability for malicious reasons.



What kind of vulnerability is typically not identifiable through a standard vulnerability assessment?

A. File permissions
B. Buffer overflow
C. Zero-day vulnerability
D. Cross-site scripting

Answer: C

NEW QUESTION 363
An attackers place themselves between two devices (often a web browser and a web server)

A. Phishing
B. Spoofing
C. On Path
D. All

Answer: C

NEW QUESTION 367
DDOS attack affect which OSI layer

A. Network layer
B. Transport layer
C. Physical Layer
D. Both A and B

Answer: D

NEW QUESTION 370
Which is not possible models for an Incident Response Team (IRT):

A. Leveraged
B. Dedicated
C. Hybrid
D. Outsourced

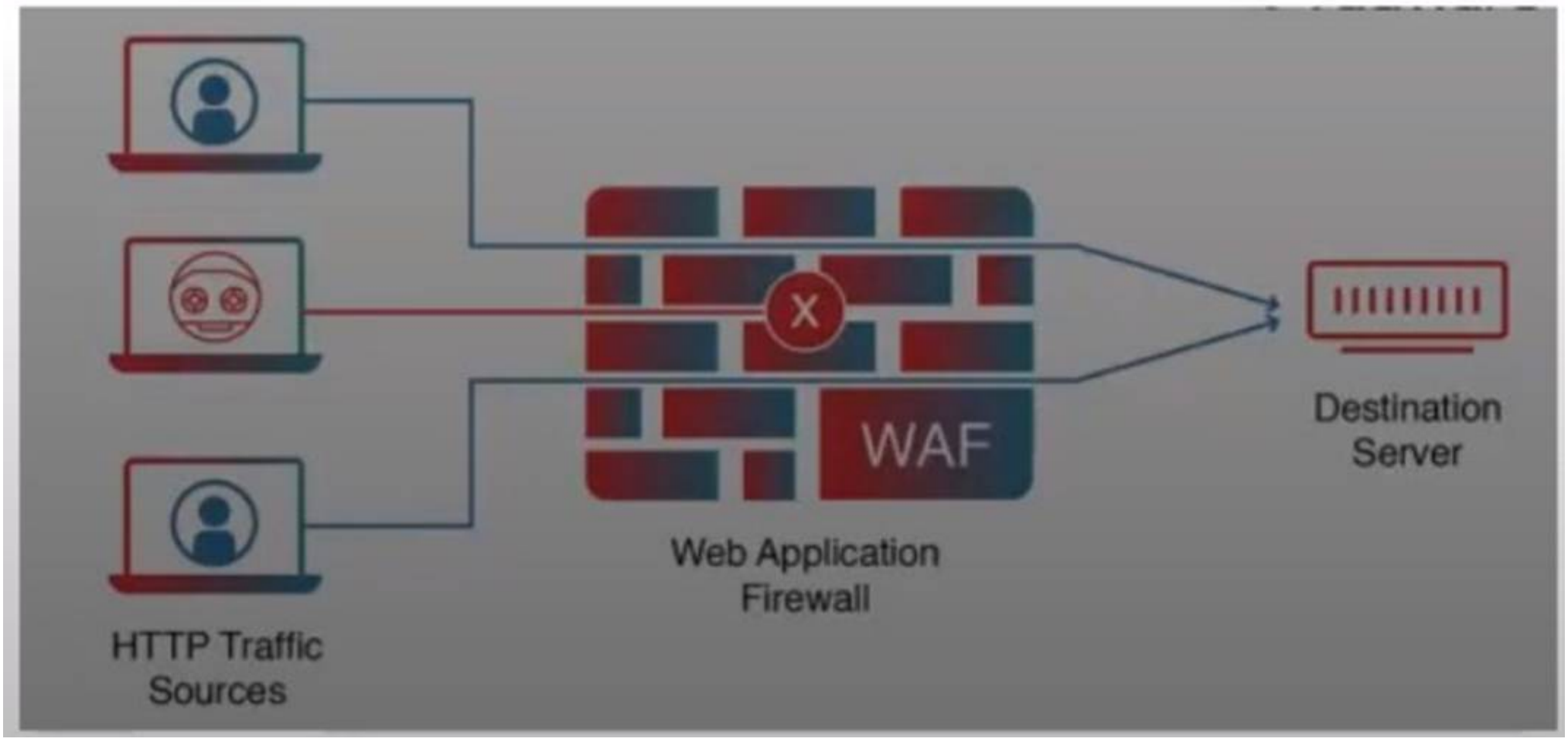
Answer: D

NEW QUESTION 372
You experienced a power outage that disrupted access to your data center. What type of security concern occurred?

A. Availability
B. Confidentiality
C. Non-Repudiation
D. Integrity

Answer: A

NEW QUESTION 373
Exhibit.



What is the PRIMARY purpose of a web application firewall (WAF)?

A. To protect the web server from DDoS attacks
B. To monitor network traffic for intrusions
C. To filter and block malicious web traffic and requests
D. To manage SSL certificates

Answer: C

NEW QUESTION 376
A hacker is trying to gain access to a company network which of the following scenarios would be an example of defense in depth

A. The company relies solely on a firewall to block unauthorized access
B. The company stores all sensitive data on a single server
C. The hacker is required to enter a username and password
D. None

Answer: C

NEW QUESTION 377
Four main components of Incident Response are

A. Preparation, Detection and Analysis, Containment, Eradication a
B. Preparation, Detection, Analysis and Containment
C. Detection, Analysis, Containment, Eradication and Recovery
D. AII

Answer: A

NEW QUESTION 380
Mark works in the security office. During research, Mark learns that a configuration change could better protect the organization's IT environment. Mark makes a proposal for this change, but the change cannot be implemented until it is approved, tested, and then cleared for deployment by the Change Control Board. This is an example of _____

A. Holistic security

B. Defense in depth
C. Threat intelligence
D. Segregation of duties

Answer: D

NEW QUESTION 384
A standard that defines wired communications of network devices

A. Switch
B. Hub
C. router
D. Ethernet

Answer: D

NEW QUESTION 387
Events with a negative consequence, such as system crashes, network packet floods, unauthorized use of system privileges, defacement of a web page or execution of malicious code that destroys data.

A. Breach
B. Incident
C. Adverse Event
D. Exploit

Answer: C

NEW QUESTION 392
The harmonization of automated computing tasks, providing a consolidated and reusable workflow

A. Cloud Orchestration
B. Cloud Manager
C. Cloud broker
D. Cloud Controller

Answer: A

NEW QUESTION 395
Token Ring used in which OSI Layer

A. Application
B. Network
C. Transport
D. Physical

Answer: D

NEW QUESTION 396
.....

THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual CC Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the CC Product From:

https://www.2passeasy.com/dumps/CC/

Money Back Guarantee

CC Practice Exam Features:

* CC Questions and Answers Updated Frequently

* CC Practice Questions Verified by Expert Senior Certified Staff

* CC Most Realistic Questions that Guarantee you a Pass on Your FirstTry

* CC Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year