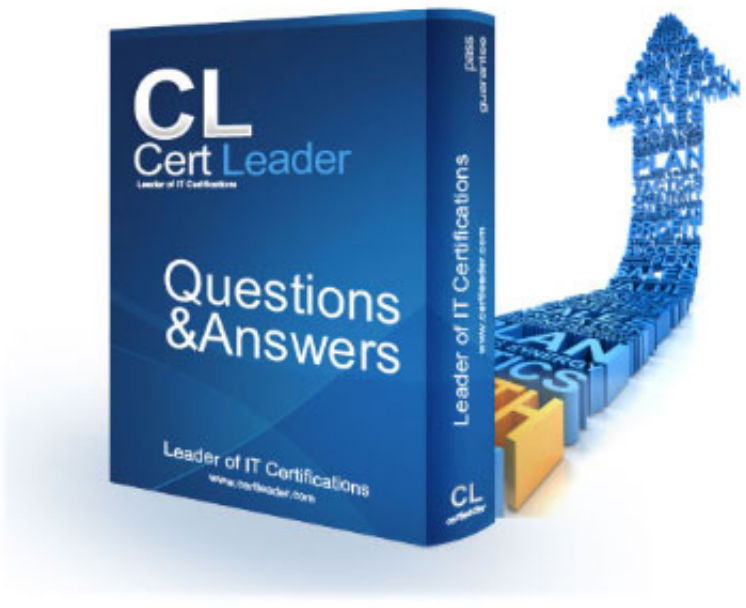
CC Dumps

Certified in Cybersecurity (CC)

https://www.certleader.com/CC-dumps.html



NEW QUESTION 1
Structured way to align IT with business goals while managing risks and meeting all industry and government regulations

A. GRC
B. Policies
C. Law
D. Stanfard

Answer: A

NEW QUESTION 2
In the context of cybersecurity, typical threat actors include the following:

A. Insiders (either deliberately, by simple human error, or by gross incompetence).
B. Outside individuals or informal groups (either planned or opportunistic, discovering vulnerability).
C. Technology (such as free-running bots and artificial intelligence
D. All

Answer: D

NEW QUESTION 3
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 4
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 5
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 6
A chief information security officer (CISO) at a large organization documented a policy that establishes the acceptable use of cloud environments for all staff. This is an example of

A. Technical control
B. Physical control
C. Cloud control
D. Management/Administrative control

Answer: D

NEW QUESTION 7
Common network device used to connect networks?

A. Server
B. Endpoint
C. Router
D. Switch

Answer: C

NEW QUESTION 8
A set of security controls or system settings used to ensure uniformity of configuration through the IT environment?

A. Patches
B. Inventory
C. Baseline
D. Policy

Answer: C

NEW QUESTION 9
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 10
Which is related to Standard

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

Answer: A

NEW QUESTION 10
255.255.255.0 Address represents

A. Broadcast
B. Unicast
C. Subnet mask
D. Global Address

Answer: C

NEW QUESTION 13
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 15
Example of Token based Authentication

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

Answer: C

NEW QUESTION 17
TCP and UDP reside at which layer of the osi model?

A. Session
B. Transport
C. Data link
D. Presentation

Answer: D

NEW QUESTION 21
Mark has purchased a MAC LAPTOP. He is scared of losing his screen and planning to buy an insurance policy. So, which risk management strategy is?

A. Risk acceptance
B. Risk deterrence
C. Risk transference
D. Risk mitigation

Answer: C

NEW QUESTION 22
Type 1 authentication posses

A. Users may share their credential with others
B. User may forgot their passwords
C. Passwords may be intercepted and stolen
D. ALL

Answer: D

NEW QUESTION 24
Which OSI layer VPN works

A. Layer 5
B. Layer 6
C. Layer 1
D. Layer 3

Answer: D

NEW QUESTION 26
Which of the following is not a protocol of the OSI layer 3

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

Answer: D

NEW QUESTION 29
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 33
What is meant by non-repudiation?

A. If a user does something, they can't later claim that they didn't do it.
B. Controls to protect the organization's reputation from harm due to inappropriate social media postings by employees, even if on their private accounts and personal time.
C. It is part of the rules set by administrative controls.
D. It is a security feature that prevents session replay attacks.

Answer: A

NEW QUESTION 34
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 35
Which drives for the IPv6 introduction

A. IPv4 was not secured
B. IPv4 not combatible with new devices
C. Because IPv4 was projected to be exhausted
D. IPV6 support WiFi

Answer: C

NEW QUESTION 38

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 43
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 47
Timiting access to resources based on the sensitivity of the information that the resource contains and the authorization of the user to access information with that level of sensitivity.

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

Answer: B

NEW QUESTION 51
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 53
Which type of attack takes advantage of vulnerabilities in validation?

A. ARP spoofing
B. Pharming attacks
C. Cross-site scripting (XSS)
D. DNS poisoning

Answer: C

NEW QUESTION 57
A _____ creates an encrypted tunnel to protect your personal data and communications

A. HTTPS
B. VPN
C. Anti-virus
D. IDS

Answer: B

NEW QUESTION 58
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 62
The common term used to describe the mechanisms that control the temperature and humidity in a data center

A. VLAN (virtual local area network)

B. STAT (system temperature and timing)
C. TAWC (temperature and water control)
D. HVAC (heating, ventilation and air conditioning)

Answer: D

NEW QUESTION 66
The last phase in the data security cycle is

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

Answer: B

NEW QUESTION 71
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 75
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 78
Centralized organizational function fulfilled by an information security team that monitors, detects and analyzes events on the network or system to prevent and resolve issues before they result in business disruptions.

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

Answer: C

NEW QUESTION 83
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 85
What is the difference between BCP and DRP

A. BCP is about restoring IT and communications back to full operations after a disruption, while DRP is about maintaining critical business functions
B. DRP is about restoring IT and communications back to full operations after a disruption, while BCP i about maintaining critical business functions
C. DRP and BCP are the same
D. BCP is about maintaining critical business functions before a disaster occurs

Answer: B

NEW QUESTION 87
Which layer does VLAN hopping belong to?

A. Layer 3
B. Layer 4
C. Layer 7
D. Layer 2

Answer: D

NEW QUESTION 90
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 92
What is the purpose of defense in depth in information security

A. To Implement only technical controls to prevent a cyber attack
B. To provide unrestricted access to organization assets
C. To establish variable barriers across multiple layers and mission of the organization
D. To guarantee that a cyber attack will not occur

Answer: C

NEW QUESTION 93
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 95
The prevention of authorized access to resources or the delaying of time-critical operations. (Time-critical may be milliseconds or it may be hours, depending upon the service provided.)

A. DDOS
B. Authetication
C. Authentication
D. Availablity

Answer: A

NEW QUESTION 96
Which version of TLS is considered to be the most secure and recommended for use?

A. TLS 1.0
B. TLS 1.1
C. TLS 1.2
D. TLS 1.3

Answer: D

NEW QUESTION 98
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 100
What does Personally Identifiable Information (Pll) pertain to?

A. Information about an individual's health status
B. Data about an individual that could be used to identify them (Correct)
C. Trade secrets, research, business plans and intellectual property
D. The importance assigned to information by its owner

Answer: B

NEW QUESTION 101
What security feature used in HTTPS

A. IPSec
B. SSH
C. ICMP
D. SSL/TLS

Answer: D

NEW QUESTION 105
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 106
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 108
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 112
What is the difference between hub and switch

A. A hub is less likely to be used in home network
B. A hub can create separate broad cast domains when used to create Vlan
C. A hub retransmits traffic to all devices, while a switch route traffic to a specific devices
D. A switch retransmits traffic to all devices, while a hub route traffic to a specific devices

Answer: C

NEW QUESTION 115
What does Criticality represents?

A. The need for consultation with the involved business ensure critical systems are identified and available
B. The importance an organization gives to data or an information system in performing its operations or achieving its mission
C. The need for security professional to ensure the appropriate levels of availavility are provided
D. All of the above

Answer: B

NEW QUESTION 117
Information should be consistently and readily accessible for authorized parties ?

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

Answer: C

NEW QUESTION 120
Is an integrated platform and graphical tool for performing security testing of web applications.

A. Burb suite

B. Wireshark C Fiddler
C. ZenMap

Answer: A

NEW QUESTION 124
Which Prevents Threat

A. Antivirus
B. IDS
C. SIEM
D. HIDS

Answer: A

NEW QUESTION 125
A security practitioner who needs step-by-step instructions to complete a provisioning task

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

Answer: C

NEW QUESTION 126
When Operating in A Cloud Environment, What Cloud Deployment Model Provides Security Teams With The Greatest Access To Forensic Information?

A. FaaS
B. SaaS
C. PaaS
D. laaS

Answer: D

NEW QUESTION 130
Which of the following attacks can TLS help mitigate?

A. Cross-site Scripting (XSS) Attacks
B. Social Engineering Attacks
C. Man-in-the-middle (MiTm) Attacks (Correct)
D. SQL Injection Attacks

Answer: C

NEW QUESTION 131
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 136
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 141
Which of the following is NOT one of the four typical ways of managing risk?

A. Accept
B. Avoid
C. Mitigate
D. Monitor

Answer: D

NEW QUESTION 146
Which is an authorized simulated attack performed on a computer system to evaluate its security.

A. Penetration test
B. Security Testing
C. Automated Testing
D. Regression Testing

Answer: A

NEW QUESTION 148
Which type of database combines related records and fields into a logical tree structure?

A. Relational
B. Hierarchical
C. Object-oriented
D. Network

Answer: B

NEW QUESTION 149
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 154
What is an IP address

A. A physical address used to connect multiple devices in a network
B. An address that denotes the vendor or manufacturer of the physical network interface
C. A Logical address associated with a unique network interface within the network
D. An Address that represents the network interface within the network

Answer: C

NEW QUESTION 158
Which is the loopback address

A. ::1
B. 127.0.0.1
C. 255.255.255.0
D. Both A and B

Answer: D

NEW QUESTION 160
Which aspect of cybersecurity is MOST impacted by Distributed Denial of Service (DDoS) attacks?

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

Answer: C

NEW QUESTION 164
The means by which a threat actor carries out their objectives

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

Answer: B

NEW QUESTION 166
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 167
What is a threat in the context of cybersecurity

A. An inherent weakness or flaw in a system
B. Something in need of protection
C. The means by which a threat actor carries out their objectives
D. A person or thing that takes action to exploit a target organizations system vulnerabilities

Answer: D

NEW QUESTION 172
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 communications back to full operations after the disruptions
D. Guiding the actions of emergency response personnel during the disruption

Answer: C

NEW QUESTION 174
How many bits represent the organization unique identifier (oui) in mac addresses?

A. 16 Bits
B. 48 Bits
C. 24 Bits
D. 32 Bits

Answer: C

NEW QUESTION 179
Removing the design belief that the network has any trusted space. Security is managed at eachpossible level, representing the most granular asset. Micro segmentation of workloads is a tool of the model.

A. Zero Trust
B. DMZ
C. VLAN
D. Micro Segmentation

Answer: A

NEW QUESTION 184
Which layer of OSI the Firewall works

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

Answer: D

NEW QUESTION 187
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 192
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 196
Which type of encryption uses only one shared key to encrypt and decrypt?

A. Public key
B. Asymmetric
C. Symmetric
D. TCB key

Answer: C

NEW QUESTION 201
Type of cyber attack carried out over a LAN that involves sending malicious packets to a default gateway on a LAN

A. ARP Poisoning
B. Syn Flood
C. Ping of death
D. Trojan

Answer: A

NEW QUESTION 206
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 210
What is the primary factor in the reliability of information and system

A. Authenticity
B. Confidentiality
C. Integrity
D. Availability

Answer: C

NEW QUESTION 215
What is IPSEC reply attack

A. An attack where an attacker modifies packets in transit
B. An attack where an attacker eavesdrops on network traffic
C. An attack where an attacker overloads a network with traffic
D. An attack where an attacker attempts to inject packets in an existing sessio

Answer: D

NEW QUESTION 218
Which plan provides the team with immediate response procedures and check lists and guidance for management?

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

Answer: A

NEW QUESTION 219
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 224
How does IPSec protect against reply attacks

A. By using sequence numbers
B. By limiting access to the network
C. By using digital signatures
D. By encryption all network traffic

Answer: A

NEW QUESTION 229
XenServer, LVM, Hyper-V, ESXi are

A. Type 2 Hypervisor
B. Type 1 Hypervisor
C. Both
D. None

Answer: B

NEW QUESTION 231
The internet standards organization, made up of network designers, operators, vendors and researchers, that defines protocol standards

A. ISO
B. NIST
C. IETF
D. GDPR

Answer: C

NEW QUESTION 236
Organization experiences a security event that does not affect the confidentiality integrity and availability of its information system. What term BEST describes this situation?

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

Answer: D

NEW QUESTION 238
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 242
How often should an organization test its business continuity plan

A. Continually
B. Annually
C. Routinely
D. Daily

Answer: C

NEW QUESTION 243
Selvaa presents a userid and a password to a system in order to log on. Which of the following characteristics must the userid have?

A. Autherization
B. Authentication
C. Availability
D. Identification

Answer: D

NEW QUESTION 247
Which access control model grants permission based on the sensitivity of the data and the user job functions

A. DAC

B. RBAC
C. MAC
D. RUBAC

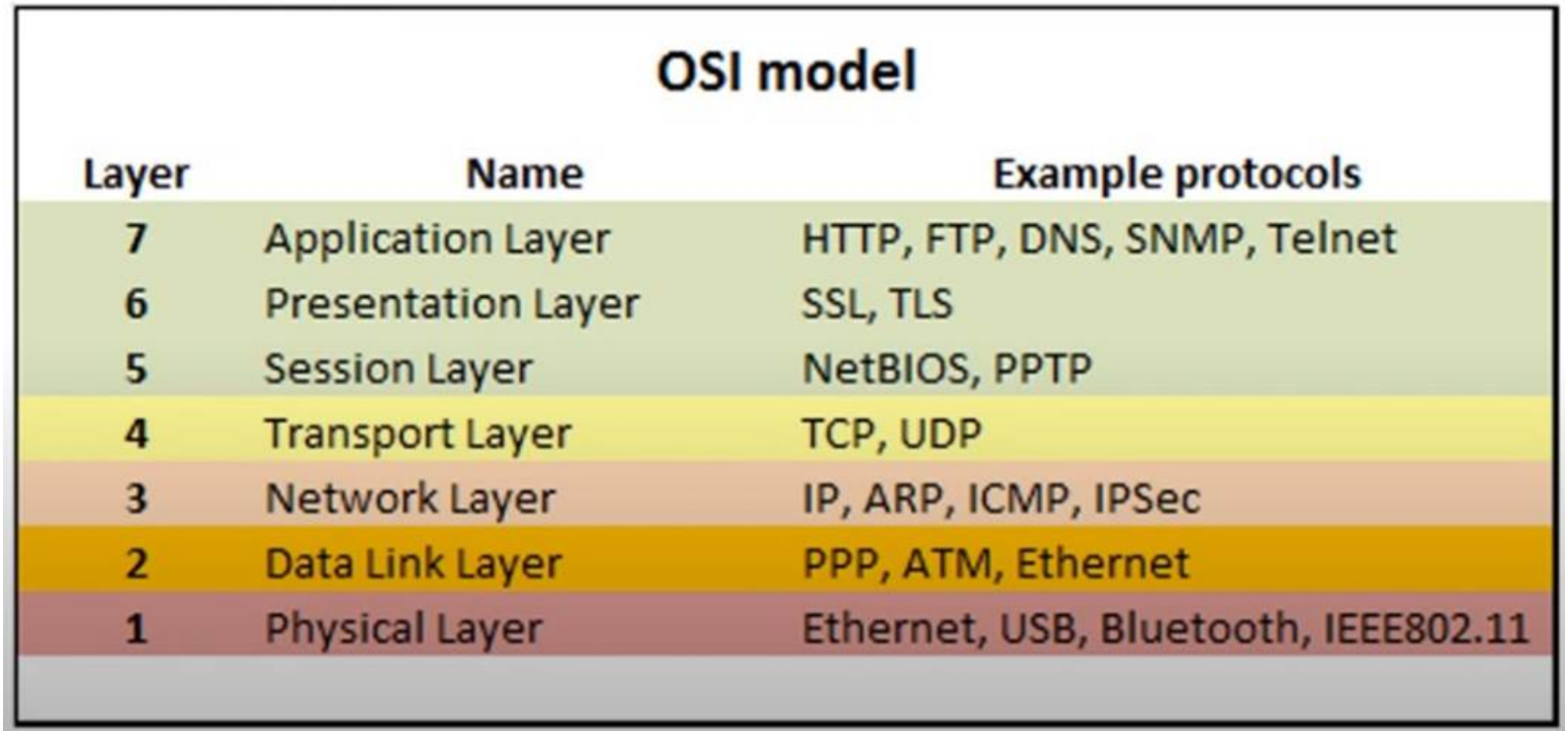
Answer: B

NEW QUESTION 249
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 254
Exhibit.



IPSec works in which layer of OSI Model

A. Layer 2
B. Layer 5
C. Layer 3
D. Layer 7

Answer: C

NEW QUESTION 256
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 259
A logical group of workstations, servers and network devices that appear to be on the same LAN despite their geographical distribution.

A. LAN
B. VPN
C. WLAN
D. VLAN

Answer: D

NEW QUESTION 260

A company performs an analysis of its information systems requirements functions and interdependences in order to prioritize contingency requirement. What is this process called?

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

Answer: D

NEW QUESTION 263
A method for risk analysis that is based on the assignment of a descriptor such as low, medium or high.

A. Quantitative Risk Analysis
B. Risk Assessment
C. Risk Mitigation
D. Qualitative Risk Analys

Answer: D

NEW QUESTION 267
Which type of control is used to identify that an attack has occurred or is currently occurring

A. Preventive control
B. Detective control
C. Corrective control
D. Recovery control

Answer: B

NEW QUESTION 272
A company has implemented Mandatory access control for its confidential data which of the following statement is true

A. The data can be accessed by users who possess a need to know
B. Access controls cannot be changed by anyone except the system administrato
C. The owner of the data can modify the access control
D. The system adminstrator can change the access contrls

Answer: B

NEW QUESTION 276
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 281
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 285
An agreement between a cloud service provider and a cloud service customer based on a taxonomy of cloud computing- specific terms

A. Memorandum of Understanding
B. Memorandam on Agreement
C. SLA
D. AII

Answer: C

NEW QUESTION 288
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 293
The mitigation of violations of security policies and recommended practices

A. DR
B. IR
C. Threat hunting
D. Incident response

Answer: D

NEW QUESTION 295
Representation of data at Layer 3 of the Open Systems Interconnection (OSI) model.

A. Segment
B. Packet
C. Frame
D. None of the Above

Answer: B

NEW QUESTION 297
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 302
Which access control model is best suited for a large organization with many departments
that have different data access needs

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

Answer: B

NEW QUESTION 307
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 311
The testing or evaluation of security controls to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for an information system or organization.

A. Security Assessment
B. Risk Assessment
C. DRP
D. IRP

Answer: A

NEW QUESTION 315
Which type of malware encrypts a users file system and demands payment in exchange of decrypting key

A. Worm
B. Trojan
C. virus

D. Ransomware

Answer: D

NEW QUESTION 317
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 319
Actions, processes and tools for ensuring an organization can continue critical operations during a contingency.

A. BC
B. DR
C. IR
D. AII

Answer: A

NEW QUESTION 324
Devid's team recently implemented a new system that gathers information from a variety of different log sources, analyses that information, and then triggers automated playbooks in response to security events, what term BEST describes this technology?

A. SIEM
B. Log Repository
C. IPS
D. SOAR

Answer: D

NEW QUESTION 325
_____ are virtual separations within a switch and are used mainly to limit broadcast traffic

A. LAN
B. WAN
C. VLAN
D. MAN

Answer: C

NEW QUESTION 330
Which type of application can intercept sensitive information such as passwords on a network segment?

A. Log server
B. Network Scanner
C. Firewall
D. Protocol Analyzer

Answer: D

NEW QUESTION 332
What is the main purpose of using digital signatures in communication security?

A. To encrypt sensitive data during transmission
B. To verify the identity of the sender and ensure the integrity of the message (Correct)
C. To prevent unauthorized access to a network
D. To compress data to reduce bandwidth usage

Answer: B

NEW QUESTION 337
What is the primary goal of Identity and Access Management (1AM) in cybersecurity?

A. To ensure 100% security against all threats
B. To provide secure and controlled access to resources
C. To eliminate the need for user authentication
D. To monitor network traffic for performance optimization

Answer: A

NEW QUESTION 339
Which of the following best describes the type of technology the team should implement to increase the work effort of buffer overflow attacks?

A. Address space layout randomization
B. Memory induction application
C. Input memory isolation
D. Read-only memory integrity checks

Answer: A

NEW QUESTION 344
What is the term used to denote the inherent set of privileges assigned to a user upon the creation of a new account?

A. Aggregation
B. Transitivity
C. Baseline
D. Entitlement

Answer: C

NEW QUESTION 347
A Company wants to ensure that its employees can access the network resources from anywhere in the world which access control model is best suited for this scenario

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

Answer: D

NEW QUESTION 350
Which is related to Privacy

A. GDPR
B. FIPS
C. MOU
D. AII

Answer: D

NEW QUESTION 351
What is the process of verifying a users identity called?

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

Answer: B

NEW QUESTION 352
Why is the recovery of IT often crucial to the recovery and sustainment of business operations

A. IT is not important to business operation
B. IT often the cause for the disaster
C. IT can be easily recovers without any impact of business operations
D. Many business rely heavily on IT for their operations

Answer: D

NEW QUESTION 356
Networks are often micro segmented networks, with firewalls at nearly every connecting point

A. DMZ
B. VPN
C. VLAN
D. Zero Trust

Answer: A

NEW QUESTION 358
Your organization is concerned about network security and wants to prevent unauthorized access to its resources by implementing a security model where the network has not
trusted space what type of security model is this

A. Zero trust
B. Trusted computing
C. Trusted platform modelus
D. Trusted execution environment

Answer: A

NEW QUESTION 363
Access control used in in high-security situations such as military and government organizations.

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

Answer: B

NEW QUESTION 367
Why is security training important?

A. Because it fulfills regulatory requirements.
B. Because it helps people to perform their job duties more efficiently.
C. Because it reduces the risk of certain types of attacks, like social engineering.
D. All

Answer: C

NEW QUESTION 368
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 370
Measure of the extent to which an entity is threatened by a potential circumstance or event and likelihood of occurrence

A. Impact
B. Risk
C. Threat
D. Threat Vector

Answer: B

NEW QUESTION 375

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 379
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 381
Granting a user access to services or the system

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

Answer: C

NEW QUESTION 383
Which of the following best describes a zero-day vulnerability?

A. A vulnerability that has been identified and patched by software vendors
B. A vulnerability that has not yet been discovered or publicly disclosed.
C. A vulnerability that can only be exploited by experienced hackers.
D. A vulnerability that affects only legacy systems.

Answer: B

NEW QUESTION 387
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 389
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 392
The purpose of risk identification:

A. Employees at all levels of the organization are responsible for identifying risk.
B. Identify risk to communicate it clearly.
C. Identify risk to protect against it.
D. ALL

Answer: D

NEW QUESTION 395
True or False? The IT department is responsible for creating the organization's business continuity plan

A. True
B. False

Answer: B

NEW QUESTION 400
Which is the first step in the risk management process

A. Risk response
B. Risk mitigation
C. Risk identification
D. Risk assessment

Answer: C

NEW QUESTION 402
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 403
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 405
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 409
What is the purpose of immediate response procedures and checklists in a BCP

A. To notify personnel that the BCP is being enacted
B. To provide guidance for management
C. To safeguard the confidentiality, integrity and availability of information
D. To ensure business operations are accounted for in the plan

Answer: A

NEW QUESTION 414
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 415
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 420

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 425
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 426
Permitting authorized access to information while protecting it from improper disclosure

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

Answer: B

NEW QUESTION 431
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 436
Ignoring the risk and proceeding the business operations

A. Risk Acceptance
B. Risk Mitigation
C. Risk Avoidance
D. Risk Transfer

Answer: A

NEW QUESTION 441
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 444
A company experiences a power outage that causes a major disruption in its operations. What type of plan will help the company sustain operations?

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

Answer: C

NEW QUESTION 447
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 451
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 453
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 455
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 458
Which layer provides the services to user?

A. Application layers
B. Session Layers
C. Presentation Layer
D. Physical Layer

Answer: A

NEW QUESTION 460
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 461
An unknown person obtaining access to the company file system without authorization is example of

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

Answer: B

NEW QUESTION 465
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 466
Which type of network is set up similar to the internet but is private to an organization. Select the MOST appropriate?

A. Extranet
B. VLAN
C. Intranet
D. VPN

Answer: B

NEW QUESTION 469
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 472
Which protocol is used for secure email

A. POP3S
B. IMAPS
C. SMTPS
D. AII

Answer: D

NEW QUESTION 475
What does the term "Two-factor authentication" refer to in Cybersecurity?

A. Using two different antivirus programs
B. Verifying identity with two independent factors
C. Accessing two different networks simultaneously
D. Changing passwords every two weeks

Answer: B

NEW QUESTION 476
Which of the following does not normally influence an organization's retention policy for logs?

A. Laws
B. Corporate governance
C. Regulations
D. Audits

Answer: D

NEW QUESTION 478
The amount of risk, at a broad level, that an organization is willing to accept in pursuit of its strategic objectives.

A. Risk Assessment
B. Risk Transfer
C. Risk Appetite
D. Risk Management

Answer: C

NEW QUESTION 482
Walmart has large ecommerce presence in world. Which of these solutions would ensure the LOWEST possible latency for their customers using their services?

A. CDN
B. SaaS
C. Load Balancing
D. Decentralized Data Centers

Answer: A

NEW QUESTION 486
allows for extremely granular restrictions within the IT environment, to the point where rules can be applied to individual machines and/or users,

A. DMZ
B. Microsegmentation
C. VLAN
D. NAC

Answer: B

NEW QUESTION 487
An analysis of an information system's requirements, functions, and interdependencies used to characterize system contingency requirements and priorities in the event of a significant disruption.

A. BIA
B. DR
C. BCP
D. IRP

Answer: A

NEW QUESTION 490
Example of Technical controls

A. Security Guard
B. GPS installed in vehicle to track location
C. Door Lock
D. None

Answer: B

NEW QUESTION 491
A large organization is planning to create a DRP. Which of the following is the BEST document to provide a high-level overview of the plan?

A. Technical guides for IT personnel
B. Department specific plans
C. Full copies of the plan for critical disaster recovery team members
D. Execute summary

Answer: D

NEW QUESTION 495
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 497
Provides confidentiality by hiding or obscuring a message so that it cannot be understood by anyone except the intended recipient.

A. Hashing
B. Encoding
C. Cryptography
D. AII

Answer: C

NEW QUESTION 499
Natalia is concerned about the security of his organization's domain name records and would like to adopt a technology that ensures their authenticity by adding digital signatures. Select the MOST appropriate technology to use?

A. DNSSIGN
B. DNSSEC
C. CERTDNS
D. DNS2

Answer: B

NEW QUESTION 504
A device that routes traffic to the port of a known device

A. Switch
B. Hub
C. Router

D. Ethernet

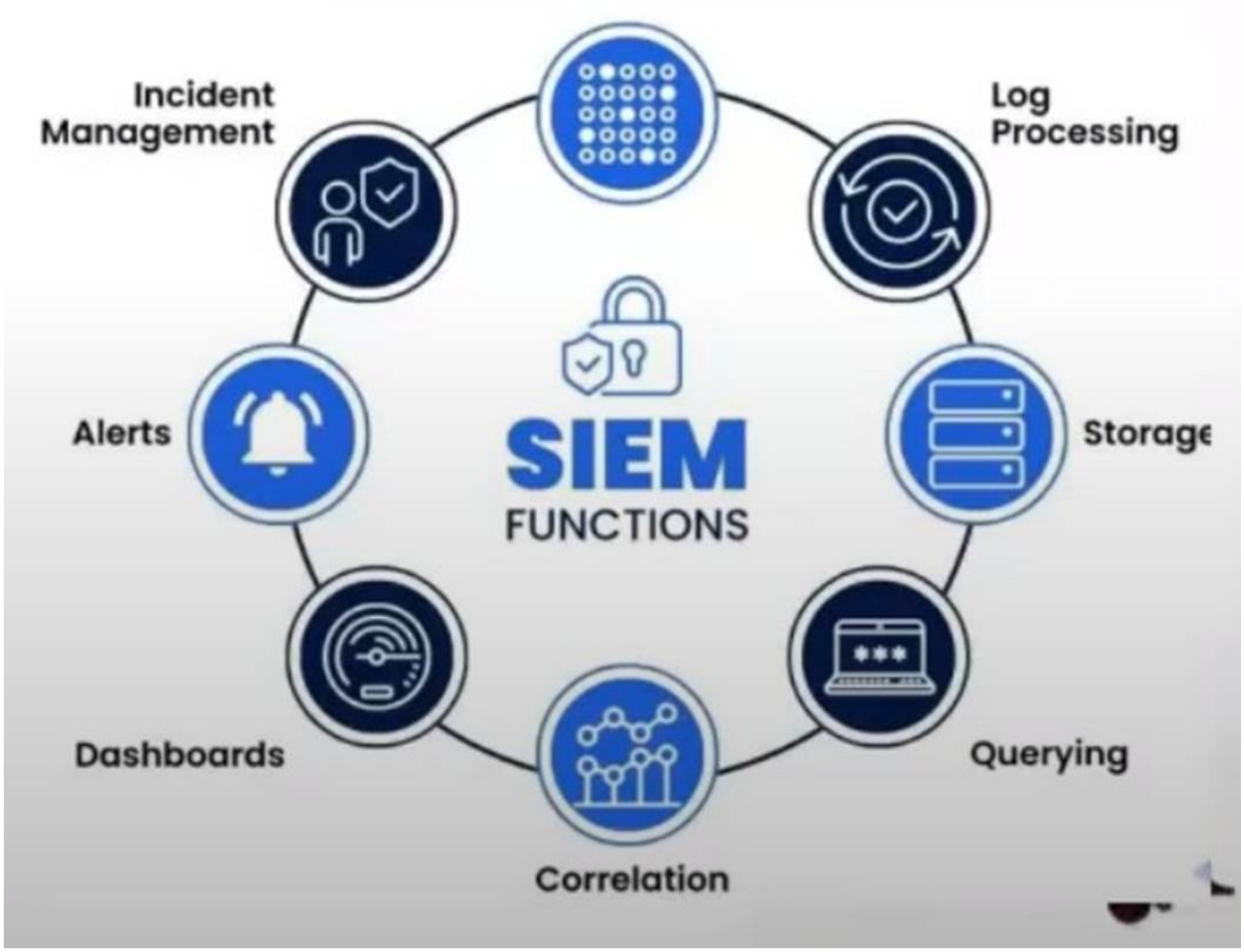
Answer: A

NEW QUESTION 506
Which is not the function of IPS

A. To encrypt network traffic
B. To monitor network traffic
C. To filter network traffic
D. To detect and prevent attacks

Answer: A

NEW QUESTION 511
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 515
A hacker gains access to an organization system without authorization and steal confidential data. What term best describes this ?

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

Answer: C

NEW QUESTION 519
In which cloud model does the cloud customer have less responsibility over the infrastructure

A. FaaS
B. SaaS
C. laaS
D. PaaS

Answer: B

NEW QUESTION 522
Which of the following properties is not guaranteed by Digital signatures

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

Answer: B

NEW QUESTION 524
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 526
Incident management is also known as

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

Answer: D

NEW QUESTION 530
The practice of sending fraudulent communications that appear to come from a reputable source

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

Answer: D

NEW QUESTION 532
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 533
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 538
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 543
What is the purpose of the CIA triad terms

A. To make security more understable to management and users
B. To describe security using relevant and meaningful words
C. To define the purpose of security
D. AII

Answer: D

NEW QUESTION 548
Why Red book is important in BCP

A. To have hard copy for easy access
B. Easy to carry and transfer
C. A hurricane hits, the power is out and all the facilities are compromised and there is no access to electronic backups
D. AII

Answer: C

NEW QUESTION 550
Protection against an individual falsely denying having performed a particular action

A. Authentication
B. Identification
C. Verification
D. Non repudiation

Answer: D

NEW QUESTION 555
What does the concept of integrity applied to

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

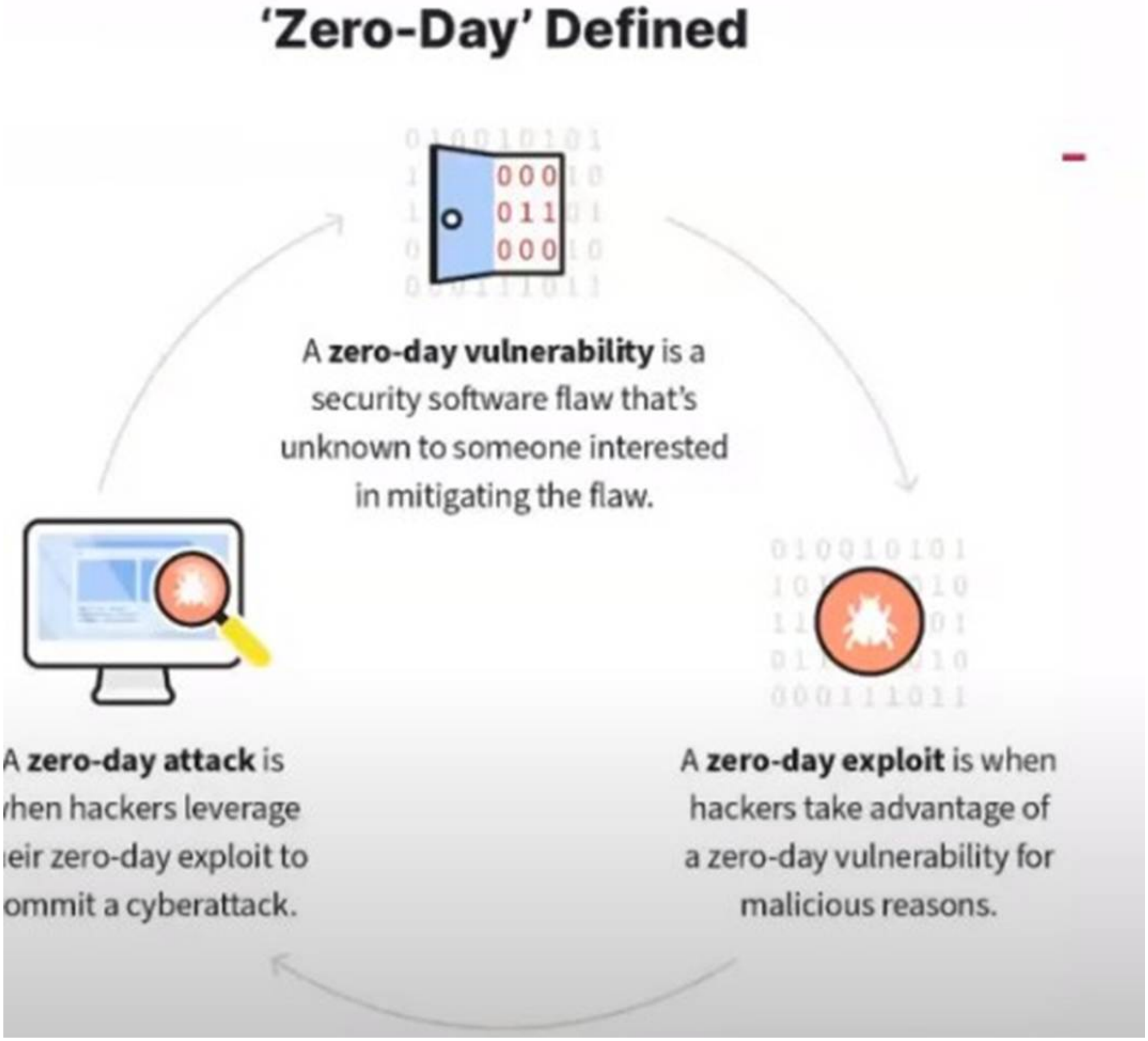
Answer: D

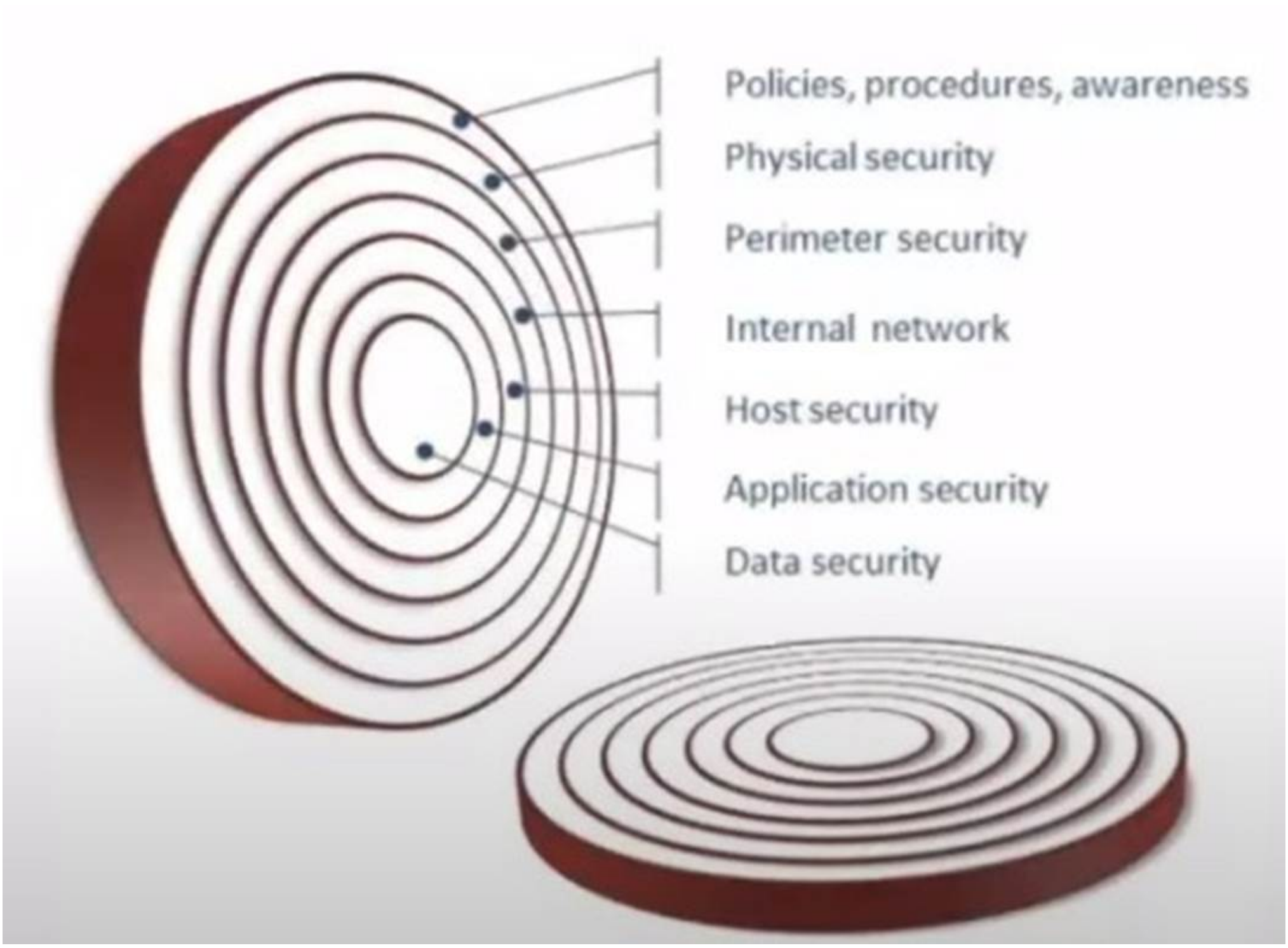
NEW QUESTION 560
What is the primary goal of a risk management process in cybersecurity?

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 565
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 566
Which one of the following groups is NOT normally part of an organization's cybersecurity incident response team?

A. Technical Subject Matter Experts
B. Cybersecurity Experts
C. Management
D. Law Enforcement

Answer: D

NEW QUESTION 568
Raj is considering a physical deterrent control to dissuade unauthorized people from entering the organization's property. Which of the following would serve this purpose?

A. A wall
B. Razor tape
C. A sign
D. A hidden camera

Answer: A

NEW QUESTION 573
Is the right of an individual to control the distribution of information about themselves

A. Confidentiality
B. Integrity
C. Privacy
D. Availability

Answer: C

NEW QUESTION 578
DDOS attack affect which OSI layer

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

Answer: D

NEW QUESTION 580
Which of these is the most efficient and effective way to test a business continuity plan

A. Simulations
B. Discussions
C. Walkthroughs
D. Reviews

Answer: A

NEW QUESTION 582
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 585
Port scanning attack target which OSI layer

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

Answer: A

NEW QUESTION 587
Which is not possible models for an Incident Response Team (IRT):

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

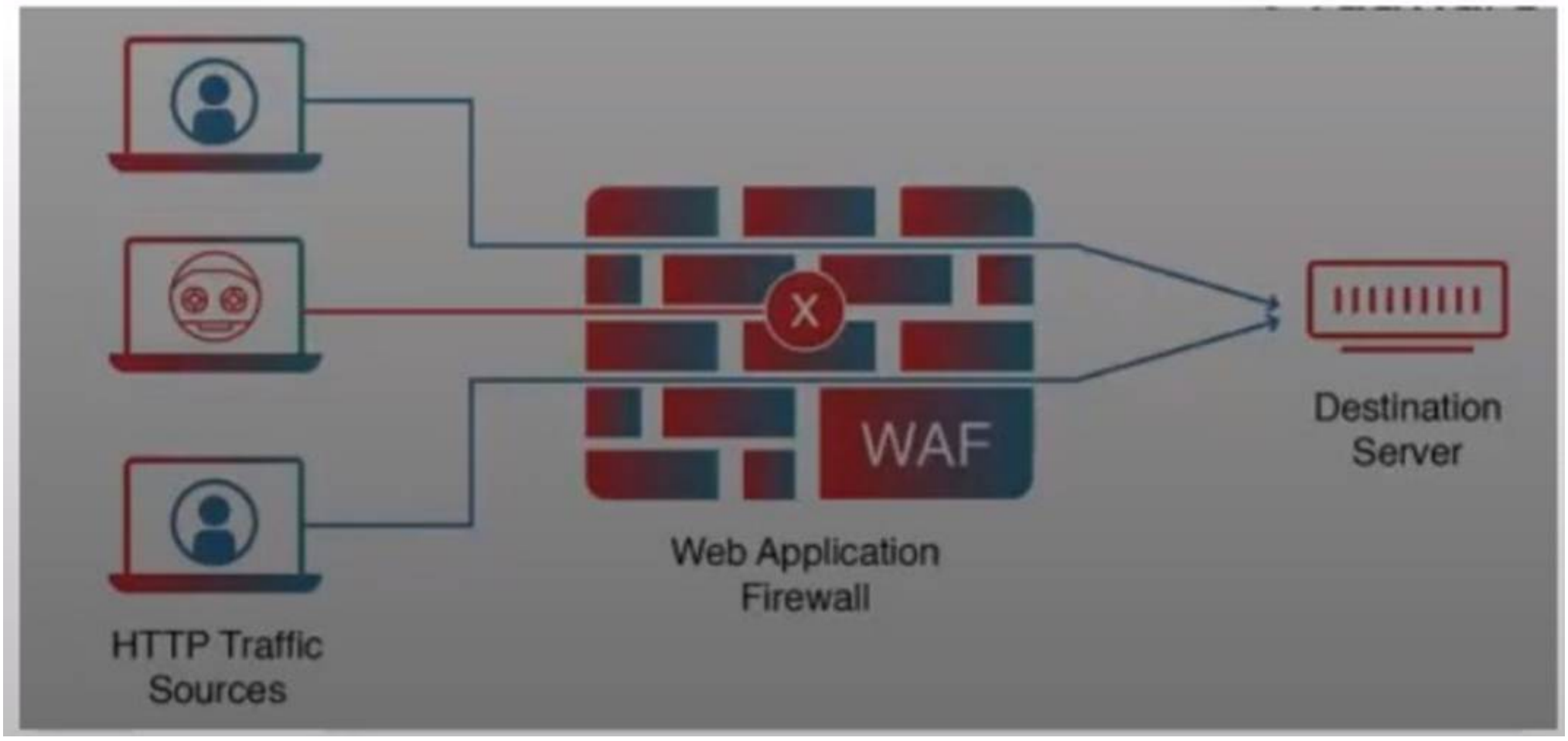
Answer: D

NEW QUESTION 591
Uses multiple types of access controls in literal or theoretical layers to help an organization avoid a monolithic security

A. DMZ
B. VLAN
C. Defence in Depth
D. VPN

Answer: C

NEW QUESTION 596
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 601
What is the purpose of the post incident phase of incident response?

A. To detect and analyze incidents
B. To prepare for future incidents
C. To document lessons learned and improve future incident response effectiveness
D. To containment and eradicate incidents

Answer: C

NEW QUESTION 603
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 605
EKristal is the security administrator for a large online service provider. Kristal learns that the company is harvesting personal data of its customers and sharing the data with local governments where the company operates, without the knowledge of the users, to allow the governments to persecute users on the basis of their political and philosophical beliefs. The published user agreement states that the company will not share personal user data with any entities without the users' explicit permission. According to the ISC2 Code of Ethics, to whom does Kristal ultimately report in this situation?

A. The company Kristal works for
B. The governments of the countries where the company operates
C. ISC2
D. The users

Answer: D

NEW QUESTION 607
A backup is which type for security control

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

Answer: C

NEW QUESTION 610

.....

Thank You for Trying Our Product

* 100% Pass or Money Back

All our products come with a 90-day Money Back Guarantee.

* One year free update

You can enjoy free update one year. 24x7 online support.

* Trusted by Millions

We currently serve more than 30,000,000 customers.

* Shop Securely

All transactions are protected by VeriSign!

100% Pass Your CC Exam with Our Prep Materials Via below:

https://www.certleader.com/CC-dumps.html