

ISC2

Exam Questions CC

Certified in Cybersecurity (CC)



NEW QUESTION 1

What federal law requires the use of vulnerability scanning on information systems operated by federal government agencies?

- A. FISMA
- B. HIPAA
- C. GLBA
- D. FERPA

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

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 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 developpe

Answer: D

NEW QUESTION 5

What is the recommended fire suppression system for server rooms

- A. Foam based
- B. Water based
- C. Powder based
- D. ftac hacorl

Answer: D

NEW QUESTION 6

Common network device used to connect networks?

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

Answer: C

NEW QUESTION 7

Part of a zero-trust strategy that breaks LANs into very small and highly localized zones using firewalls.

- A. Zero Trust
- B. DMZ
- C. VPN
- D. Micro Segmentation

Answer: D

NEW QUESTION 8

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 9

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

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

Answer: C

NEW QUESTION 10

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 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

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 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 23

Also known as a virtual machine monitor or VMM, is software that creates and runs virtual machines (VMs)

- A. Hypervisor
- B. Simulation
- C. Emulation
- D. Cloud Controller

Answer: A

NEW QUESTION 27

Which drives for the IPv6 introduction

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

Answer: C

NEW QUESTION 30

What is the importance of identifying roles and responsibilities in incident response planning?

- A. To prevent incidents from happening
- B. To ensure that everyone knows their job in the incident response process
- C. To reduce the impact of the incident
- D. To choose an appropriate containment strategy

Answer: B

NEW QUESTION 32

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 34

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 35

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 38

Limiting 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 39

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 42

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 43

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 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 48

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 49

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

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

Answer: B

NEW QUESTION 50

Faking the sending address of a transmission to gain illegal entry into a secure system.

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

Answer: C

NEW QUESTION 55

Which of the following is endpoint

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

Answer: C

NEW QUESTION 60

Which of the following is a subject?

- A. file
- B. fence
- C. filename
- D. user

Answer: D

NEW QUESTION 64

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 66

Which layer does VLAN hopping belong to?

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

Answer: D

NEW QUESTION 71

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

- A. Business continuity planning is about restoring IT and communications back to full operations after a disruption, while disaster recovery planning is about maintaining critical 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 thing
- D. Business continuity planning is about maintaining critical business functions before disaster occurs

Answer: B

NEW QUESTION 73

Is a way to prevent unwanted devices from connecting to a network.

- A. DMZ
- B. VPN
- C. VLAN
- D. NAC

Answer: D

NEW QUESTION 76

What is the best practice to clear SSD storage after usage in terms of cyber security?

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

Answer: D

NEW QUESTION 81

A tool used to inspect outbound traffic to reduce threats

- A. Anti-malware
- B. NIDC
- C. DLP
- D. Firewall

Answer: C

NEW QUESTION 82

What security feature is used in HTTPS?

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

Answer: D

NEW QUESTION 85

A cyber security professional observes an unusual occurrence in the network or system. What term best describes this situation?

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

Answer: C

NEW QUESTION 90

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 91

Difference between Sniffing and Snooping

- A. Sniffing is the process of intercepting and collecting network traffic as it passes over a digital network
- 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 network
- 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 snooping is a thread

Answer: A

NEW QUESTION 96

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. All

Answer: A

NEW QUESTION 97

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 100

Information should be consistently and readily accessible for authorized parties ?

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

Answer: C

NEW QUESTION 105

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 106

Which of the following is a type of risk that involves the unauthorized use or disclosure of confidential information such as passwords, financial data or personal information?

- A. Compliance risk
- B. Reputational risk
- C. Operational risk
- D. Information risk

Answer: D

NEW QUESTION 111

What is the primary goal of network segmentation in cybersecurity?

- A. To increase network speed
- B. To isolate and protect critical assets
- C. To centralize data storage
- D. To expand the network's coverage

Answer: B

NEW QUESTION 115

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 119

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 122

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 124

Which of the following is a characteristic of cloud

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

Answer: B

NEW QUESTION 126

The method of distributing network traffic equally across a pool of resources that support an application

- A. Vlan
- B. DNS
- C. VPN
- D. Load Balancing

Answer: D

NEW QUESTION 130

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 131

Created by switches to logically segment a network without altering its physical topology.

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

Answer: C

NEW QUESTION 136

Exhibit.



information security is not built on which of the following?

- A. Confidentiality
- B. Availability
- C. Accessibility
- D. Integrity

Answer: C

NEW QUESTION 138

What does a breach refer to in the context of cybersecurity

- A. An unauthorized access to a system or system resources
- B. Any observable occurrence in a network or system
- C. A deliberate security incident
- D. A previously known system vulnerability

Answer: A

NEW QUESTION 139

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 finance department

Answer: C

NEW QUESTION 143

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 to determine the extent of the damage
- C. Restore data from backup systems
- D. Contact the enforcement to investigate the cyberattack

Answer: A

NEW QUESTION 145

Some Employee of his organization launched a privilege escalation attack to gain root access on one of the organization's database servers. The 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 149

What is knowledge based authentication

- A. Authentication based on a passphrase or secret code
- B. Authentication based on a token or memory card
- C. Authentication based on biometrics or measurable characteristics
- D. Authentication based on something you do

Answer: A

NEW QUESTION 152

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 155

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 159

Hashing used to safeguard which CIA triad

- A. Confidentiality
- B. Availability
- C. Integrity
- D. All

Answer: C

NEW QUESTION 164

Modern solutions try to provide a more holistic approach detecting rootkits, ransomware and spyware.

- A. Antivirus
- B. IDS
- C. IPS

D. Anti Malware

Answer: D

NEW QUESTION 168

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 171

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 172

A prolonged and targeted cyberattack in which an intruder gains access to a network and remains undetected for an extended period of time.

- A. Spoofing
- B. Phishing
- C. DOS
- D. Advanced Persistent Threat

Answer: D

NEW QUESTION 175

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 179

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

- A. Physical control
- B. Logical Control
- C. Administrative Control
- D. Thechnical control

Answer: A

NEW QUESTION 182

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 183

Which is the SSH port

- A. 21
- B. 23
- C. 24
- D. 22

Answer: D

NEW QUESTION 188

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 190

What is the range of private ports

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

Answer: C

NEW QUESTION 194

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 198

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 200

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 201

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 202

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 207

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 211

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 administrator
- C. The owner of the data can modify the access control
- D. The system administrator can change the access controls

Answer: B

NEW QUESTION 216

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 219

What is the priority of incident response in the context of incident management

- A. Protect the organization mission and objectives
- B. Reduce the impact of the incident
- C. Protect life health and safety
- D. Resume interrupted operations as soon as possible

Answer: C

NEW QUESTION 224

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. Memorandum on Agreement
- C. SLA
- D. All

Answer: C

NEW QUESTION 228

Sending employees to work at a customer's home can open your business to more risk of bodily injury or property damage claims. So, to reduce risk and avoid potential losses, you decide not to offer those kinds of services

- A. Risk Acceptance
- B. Risk Assessment
- C. Risk Avoidance
- D. Risk Control

Answer: C

NEW QUESTION 231

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 235

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 238

John was recently offered a consulting opportunity as a side job. He is concerned that this might constitute a conflict of interest. Which one of the following sources that he needs to refer to take an appropriate decision?

- A. ISC2 Code of ethics
- B. Organizational code of ethics
- C. Country code of ethics
- D. Organizational security policy

Answer: B

NEW QUESTION 243

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 248

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 250

A measure of the degree to which an organization depends on the information or information system for the success of a mission or of a business function.

- A. Availability
- B. Criticality
- C. Authorization
- D. Confidentiality

Answer: B

NEW QUESTION 251

Which of the following is often associated with DR planning?

- A. Checklists
- B. Antivirus
- C. firewall
- D. All

Answer: D

NEW QUESTION 254

Shaun is planning to protect their data in all states(Rest, Motion, use), defending against data leakage. What would be the BEST solution to implement?

- A. End to end encryption.
- B. Hashing
- C. DLP
- D. Threat Modeling

Answer: C

NEW QUESTION 259

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 264

Which layer of the OSI layer model is responsible for associate MAC addresses to network devices

- A. Physical layer
- B. Network layer C Data link layer
- C. Transport layer

Answer: C

NEW QUESTION 269

A company wants to ensure that its employees cannot bring unauthorized electronic devices into the workspace which physical control is best suited for this

- A. Metal Detectors
- B. Security gaurds
- C. RFID scanners
- D. Baggage X-ray machinces

Answer: A

NEW QUESTION 274

Works via encapsulation and wrapping a packet inside another packet.

- A. Network segmentation
- B. Load balancing
- C. Tunnelling
- D. Data encryption

Answer: C

NEW QUESTION 276

Example of Deterrent controls

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

Answer: A

NEW QUESTION 278

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 279

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 283

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 286

Which type of authentication is something which you

- A. Type1
- B. Type 2
- C. Type 3
- D. Type 4

Answer: C

NEW QUESTION 289

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 290

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 293

Which of these is an example of deterrent control

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

Answer: B

NEW QUESTION 295

A Company IT system experienced a system crash that result in a loss of data. What term best describes this event?

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

Answer: A

NEW QUESTION 300

Which is strongly used for Securing Wi-Fi

- A. WPA2
- B. WEP
- C. WPA
- D. SSL

Answer: A

NEW QUESTION 303

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 304

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 308

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 313

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 314

What is sensitivity in the context of confidentiality

- A. The harm caused to external 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 315

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

- A. True
- B. False

Answer: B

NEW QUESTION 317

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 318

At which layer of the OSI Layer model is the target of a buffer overflow attack

- A. Layer 7
- B. Layer 3
- C. Layer 5
- D. Layer 4

Answer: A

NEW QUESTION 321

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 325

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 326

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 330

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 333

John joined the ISC2 Organizations, his manager asked to check the authentications in security module. What would John use to ensure a certain control is working as he want and expect it to?

- A. Security Testing
- B. Security assessment
- C. Security audit
- D. Security walkthrough

Answer: A

NEW QUESTION 336

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 340

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 343

Ignoring the risk and proceeding the business operations

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

Answer: A

NEW QUESTION 348

What should been done to limit the damage caused by the ransomware attack

- A. Use a different email client to prevent malicious attachments
- B. Add more Administrative users to the Domain Admins group
- C. Delete all emails with attachments
- D. Limit the use of administrative privileges to only when required

Answer: D

NEW QUESTION 349

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 354

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 356

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 359

Which of the following physical controls is used to protect against eavesdropping and data theft through electromagnetic radiation

- A. EMI Shielding
- B. Screening rooms
- C. White noise generators
- D. ALL

Answer: A

NEW QUESTION 361

Who should participate in creation a business continuity plan

- A. Onlymembersfrom the management team
- B. only members from the IT department
- C. Onlymembersfrom thefinancedepartment
- D. Members from across the organization

Answer: D

NEW QUESTION 364

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 365

Which protocol is used for secure email

- A. POP3S
- B. IMAPS
- C. SMTPS
- D. All

Answer: D

NEW QUESTION 368

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 369

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 372

Dani is an ISC2 member and an employee of New Corporation. One of Dani's colleagues offers to share a file that contains an illicit copy of a newly released movie. What should Dani do

- A. Inform ISC2
- B. Inform law enforcement
- C. Accept the movie
- D. Refuse to accept

Answer: D

NEW QUESTION 375

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 380

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 385

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 387

Can be considered to be a fingerprint of the file or message

- A. Hashing .
- B. encryption
- C. decryption
- D. encoding

Answer: A

NEW QUESTION 388

Example of Technical controls

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

Answer: B

NEW QUESTION 390

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 392

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 396

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. All

Answer: C

NEW QUESTION 397

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 402

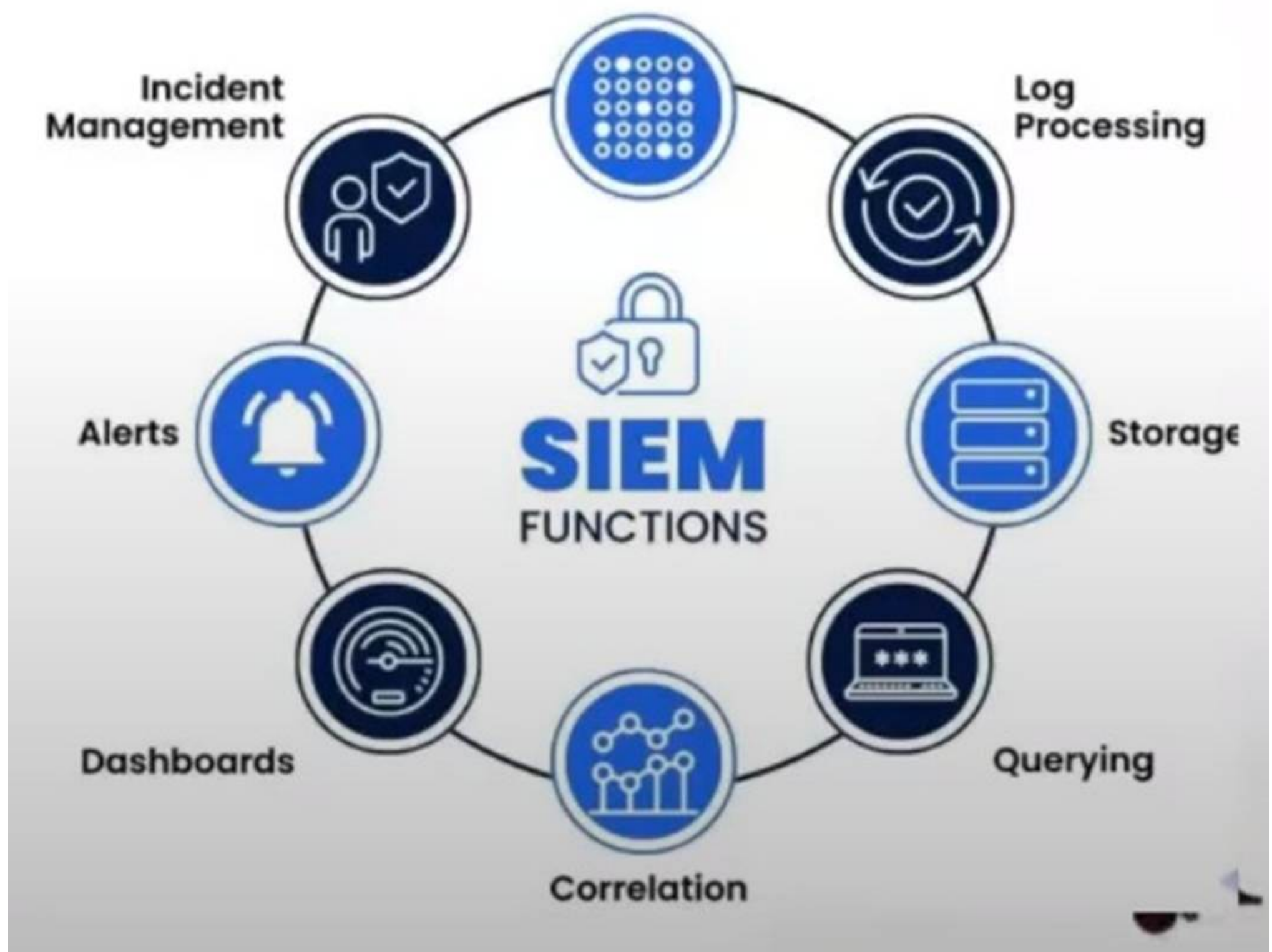
Which is not the function of IPS

- 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 406

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 408

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 411

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

- A. FaaS
- B. SaaS
- C. IaaS
- D. PaaS

Answer: B

NEW QUESTION 415

Which of the following properties is not guaranteed by Digital signatures

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

Answer: B

NEW QUESTION 420

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 423

A company's governing board may agree that legal services will examine any third-party contracts, so they create a _____ stating that aside from legal services, no other department in the company has the authority to review third-party contracts

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

Answer: B

NEW QUESTION 426

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. All

Answer: D

NEW QUESTION 431

What is the purpose of the CIA triad terms

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

Answer: D

NEW QUESTION 435

Load balancing is a security guard which CIA triad

- A. Confidentiality
- B. Availability
- C. Integrity
- D. All

Answer: B

NEW QUESTION 437

A company's 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 439

Protection against an individual falsely denying having performed a particular action

- A. Authentication

- B. Identification
- C. Verification
- D. Non repudiation

Answer: D

NEW QUESTION 440

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 445

What is the BEST defense against dumpster diving attacks?

- A. Anti-malware software
- B. Clean desk policy
- C. Data loss prevention tools
- D. Shredding

Answer: D

NEW QUESTION 449

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

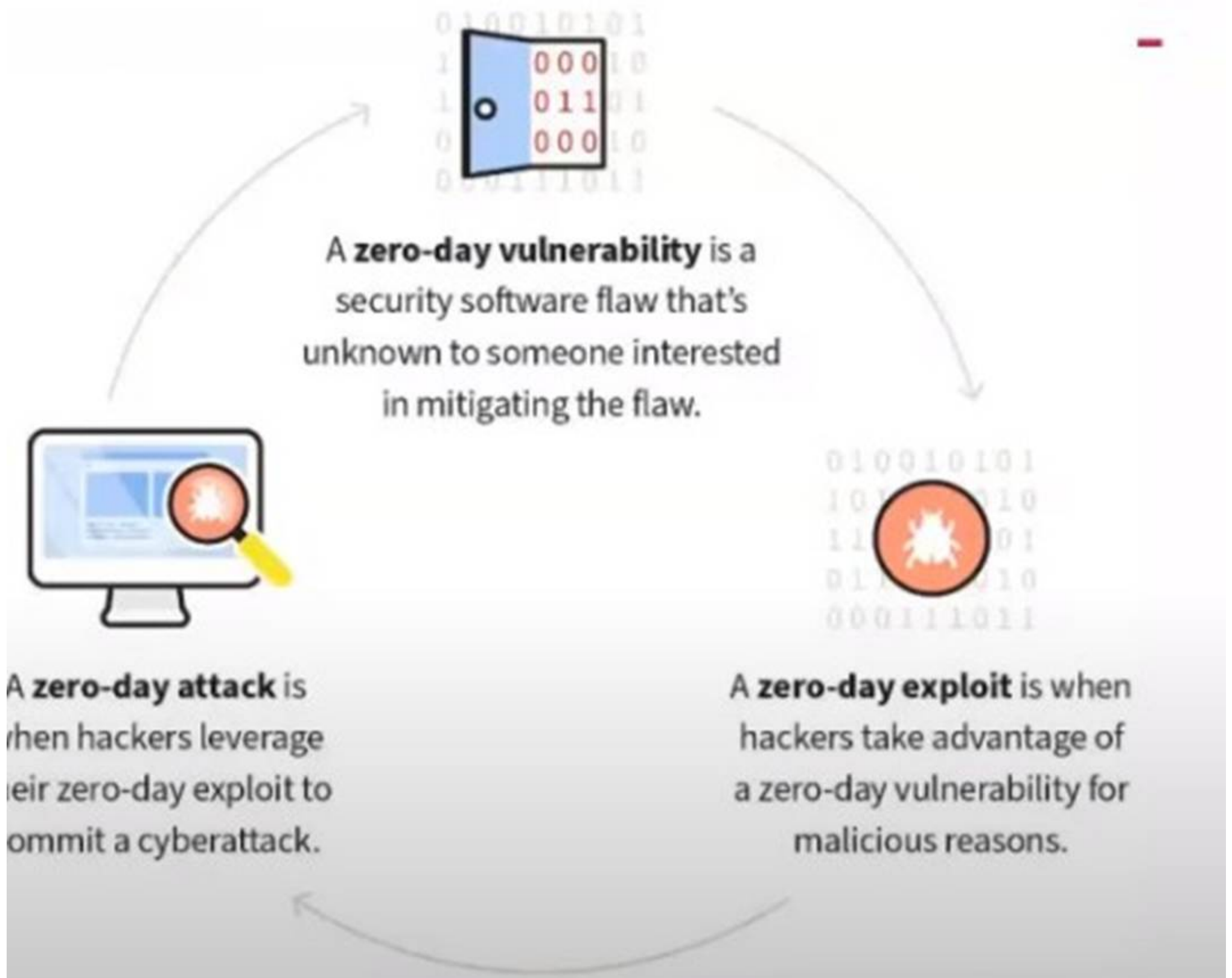
- A. Basic
- B. Kerberos
- C. Token Based
- D. Federated

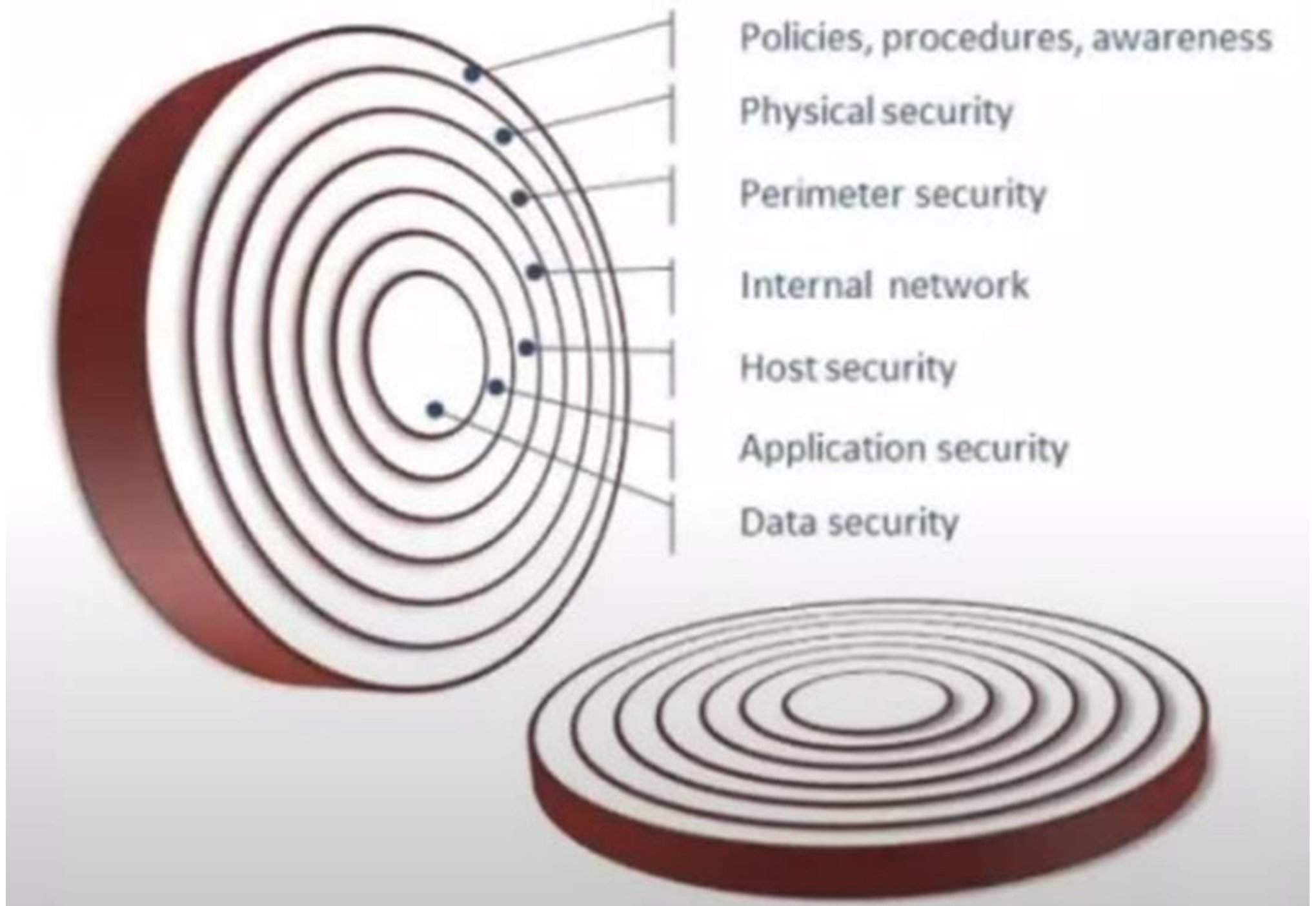
Answer: D

NEW QUESTION 453

Exhibit.

'Zero-Day' Defined





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 456

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 457

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 460

What does the term business in business continuity planning refer to?

- A. The financial performance of the organization
- B. The technical systems of the organization
- C. The operation aspects of the organization
- D. The physical infrastructure of the organization

Answer: C

NEW QUESTION 462

Port scanning attack target which OSI layer

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

Answer: A

NEW QUESTION 466

Why is an asset inventory much important?

- A. It tells you what to encrypt
- B. The law requires it
- C. It contains a price list
- D. You can't protect what you don't know you have

Answer: D

NEW QUESTION 467

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 470

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 471

A standard that defines wired communications of network devices

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

Answer: D

NEW QUESTION 476

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 477

Which of the following is unlikely to be a member of the disaster recovery team

- A. Executive Management
- B. Public Relations
- C. Billing Clerk
- D. IT personnel

Answer: C

NEW QUESTION 480

EKristol 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 482

Token Ring used in which OSI Layer

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

Answer: D

NEW QUESTION 483

.....

Thank You for Trying Our Product

We offer two products:

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

2nd - Questions and Answers in PDF Format

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 First Try
- * CC Practice Test Questions in Multiple Choice Formats and Updates for 1 Year

100% Actual & Verified — Instant Download, Please Click
[Order The CC Practice Test Here](#)