Exam Questions CC

Certified in Cybersecurity (CC)

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

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
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 3
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 4
Common network device used to connect networks?

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

Answer: C

NEW QUESTION 5
Example of Dynamic authorization

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

Answer: D

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
An entity that acts to exploit a target organizations system vulnerabilities is a

A. Attacker
B. Threat vector
C. Threat
D. Threat Actor

Answer: D

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 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
In which of the following phases of an incident recovery plan the incident responses prioritized

A. Post incident activity
B. Containment eradication and recovery
C. Detection and analysis
D. Preparation

Answer: C

NEW QUESTION 12
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 13
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 15
A popular way of implementing "least privilege"

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

Answer: C

NEW QUESTION 16
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 21
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 22
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 25
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 27
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 32
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 33
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 38
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 41

A cybercrime in which the attacker floods a server with internet traffic to prevent users from accessing connected online services and sites

A. Phising
B. Virus
C. Spoofing
D. DDOS

Answer: D

NEW QUESTION 44
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 49
Which element of the security policy framework includes recommendation that are NOT bindings?

A. Procedures
B. Guidelines
C. Standards
D. Policies

Answer: C

NEW QUESTION 52
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 56
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 58
What is the range of well known ports

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

Answer: A

NEW QUESTION 59
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 62
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 66
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 68
Which of the following is a subject?

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

Answer: D

NEW QUESTION 71
Which layer does VLAN hopping belong to?

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

Answer: D

NEW QUESTION 76
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 78
Is a way to prevent unwanted devices from connecting to a network.

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

Answer: D

NEW QUESTION 82
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 83
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 87
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 90
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 92
A tool used to inspect outbound traffic to reduce threats

A. Anti-ma I ware
B. NIDC
C. DLP
D. Firewall

Answer: C

NEW QUESTION 93
A cyber security professional observes an unusual occurrence in the network or system. What term best describes this situations

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

Answer: C

NEW QUESTION 94
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 99
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 101
Which Regulation addresses personal privacy

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

Answer: B

NEW QUESTION 103
Which of the following principles aims primarily at fraud detection

A. Defense in depth

B. Least privilege
C. Separation of duties
D. Privileged account

Answer: C

NEW QUESTION 105
Information should be consistently and readily accessible for authorized parties ?

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

Answer: C

NEW QUESTION 109
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 112
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 114
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 119
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 122
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 126
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 128
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 129
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 130
Which of the following is not a source of redundant power

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

Answer: D

NEW QUESTION 133
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 138
The requirement of both the manager and the accountant to approve the transaction fund exceeding $ 50000. Which security concept best suits this

A. MAC
B. Defence in Depth
C. Two Person integrity
D. Principle of least privilege

Answer: C

NEW QUESTION 141
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 146
What does a breach refer to in the context of cybersecurity

A. An unauthorized access to a system or system recours
B. Any observable occurance in a network or system
C. A deiberate security incident
D. A previously know system vulnerablity

Answer: A

NEW QUESTION 151
Which layer of OSI the Firewall works

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

Answer: D

NEW QUESTION 152
Which addresses reserved for internal network use and are not routable on the internet.

A. acOO:: to adff:ffff:ffff:ffff:ffff:ffff:ffff:ffff
B. fcOO:: to fdff:ffff:ffff:ffff:ffff:ffff:ffff:ffff
C. bcOO:: to bdff:ffff:ffff:ffff:ffff:ffff:ffff:ffff
D. ccOO:: to cdff:ffff:ffff:ffff:ffff:ffff:ffff:ffff

Answer: B

NEW QUESTION 153
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 157
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 160
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 161
provide integrity services that allow a recipient to verify that a message has not been altered.

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

Answer: A

NEW QUESTION 162
Hashing used to safe guard which CIA triad

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

Answer: C

NEW QUESTION 165
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 166
What is the primary factor in the reliability of information and system

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

Answer: C

NEW QUESTION 169
Which phase of the access control process(AAA) does a user prove his/her identity?

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

Answer: A

NEW QUESTION 170
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 171
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 175
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 178
A company network experience a sudden flood of network packets that causes major slowdown in internet traffic. What type of event it this?

A. Security incident
B. Natural disaster
C. Exploit
D. Adverse event

Answer: D

NEW QUESTION 183
Which of the following is not an element of system security configuration management

A. Baselines
B. Updates
C. Inventory
D. Audit logs

Answer: D

NEW QUESTION 187
XenServer, LVM, Hyper-V, ESXi are

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

Answer: B

NEW QUESTION 190
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 192
The process of running a simulated instances of a computer system in a layer abstracted from the underlying hardware server or workstation

A. Containerization
B. Simulation
C. Emulation
D. Virtualization

Answer: D

NEW QUESTION 197
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 200
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. All

Answer: A

NEW QUESTION 203
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 204
How often should an organization test its business continuity plan

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

Answer: C

NEW QUESTION 208
What is the first step in incident response planning

A. Develop a policy approved by management
B. Identify critical data and systems
C. Train staff on incident response

D. implement an incident response team

Answer: A

NEW QUESTION 211
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 215
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 216
Which of the following cloud service models provides the most suitable environment for customers to build and operate their own software?

A. SaaS
B. laaS
C. PaaS

Answer: A

NEW QUESTION 221
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 226
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 227
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 232
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 233
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 237
Juli is listening to network traffic and capturing passwords as they are sent to the authentication server. She plans to use the passwords as part of a future attack. What type of attack is this?

A. Brute-force attack
B. Dictionary attack
C. Social engineering attack
D. Replay attack

Answer: D

NEW QUESTION 242
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. All

Answer: C

NEW QUESTION 245
Derrick logs on to a system in order to read a file. In this example. Derrick is the ______?

A. Subject
B. Object
C. Process
D. Predicate

Answer: A

NEW QUESTION 247
Which of the following documents contains elements that are NOT mandatory

A. Procedures
B. Policies
C. Regulations
D. Guidelines

Answer: D

NEW QUESTION 249
What is the benefit of subnet

A. By increasing network bandwidth
B. By improving network security
C. By reducing network congestion
D. By simplifying network management

Answer: C

NEW QUESTION 254
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 256
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 260
Which type of attack will most effectively maintain remote access and control over the victims computer

A. Phising
B. Trojans
C. XSS
D. RootKits

Answer: D

NEW QUESTION 263
Actions, processes and tools for ensuring an organization can continue critical operations during a contingency.

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

Answer: A

NEW QUESTION 265
The Bell and LaPadula access control model is a form of

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

Answer: B

NEW QUESTION 267
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 272
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 276
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 277
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 280
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 285
Example of Deterrent controls

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

Answer: A

NEW QUESTION 289
Which is related to Privacy

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

Answer: D

NEW QUESTION 292
What is the process of verifying a users identity called?

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

Answer: B

NEW QUESTION 297
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 298
Which document serve as specifications for the implementation of policy and dictates mandatory requirements

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

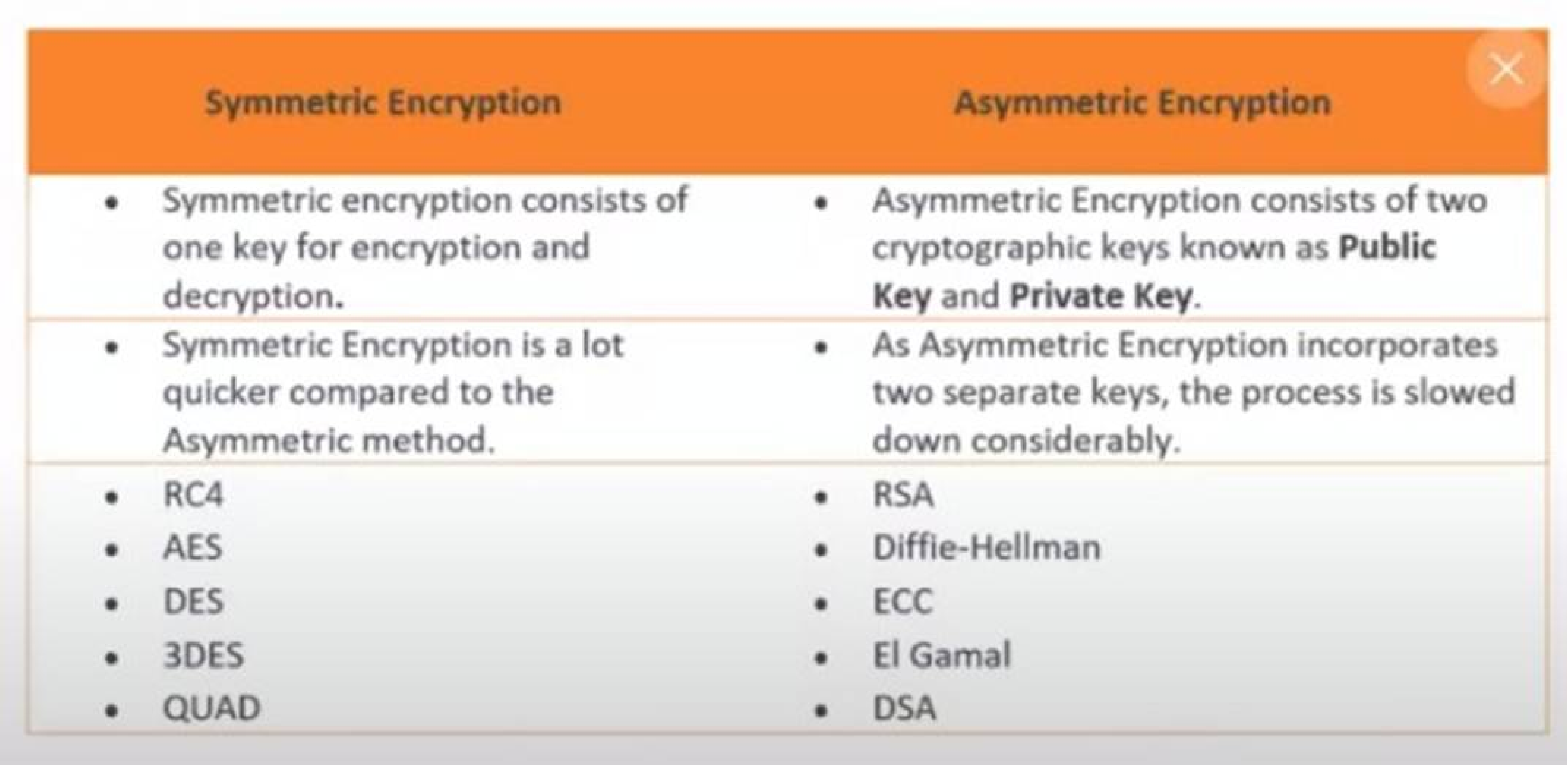
Answer: C

NEW QUESTION 299
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 303
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 304
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 307
Which is strongly used for Securing Wi-Fi

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

Answer: A

NEW QUESTION 312
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 316
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 321
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 322
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 326
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 330
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 332
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 336
Which of the following protocols is a secure alternative to using telnet?

A. SSH
B. HTTPS
C. SFTP
D. LDAPS

Answer: B

NEW QUESTION 337
What is the purpose of multi-factor authentication (MFA) in 1AM?

A. To simplify user access
B. To eliminate the need for authentication
C. To add an additional layer of security by requiring multiple forms of verification
D. To grant unrestricted access to all users

Answer: C

NEW QUESTION 341
Which of the following is the least secure communications protocol?

A. CHAP

B. Ipsec
C. PAP
D. EAP

Answer: C

NEW QUESTION 343
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 344
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 348
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 350
Permitting authorized access to information while protecting it from improper disclosure

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

Answer: B

NEW QUESTION 351
Example of Type 1 Authentication

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

Answer: A

NEW QUESTION 356
organization experiences a security event that potentially jeopardizes the confidentiality, integrity or availability of its information system. What term best describes this situation?

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

Answer: C

NEW QUESTION 359
Malicious code that acts like a remotely controlled "robot" for an attacker, with other Trojan and worm capabilities.

A. Rootkit
B. Ma l ware
C. Bot

D. Virus

Answer: C

NEW QUESTION 362
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 365
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 368
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 373
Which one of the following cryptographic algorithms does not depend upon the prime factorization problem?

A. RSA - Rivest-Shamir-Adleman
B. GPG - GNU Privacy Guard
C. ECC - Elliptic curve cryptosystem
D. PGP - Pretty Good Privacy

Answer: C

NEW QUESTION 374
Which layer provides the services to user?

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

Answer: A

NEW QUESTION 376
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 378
Which of the following documents identifies the principles and rules governing an organization's protection of information systems and data

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

Answer: C

NEW QUESTION 383
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 384
What are the primary responsibilities of a computer incident response team (CIRT) during an incident?

A. To determine the difference between minor and major incident
B. To troubleshoot network and system issues
C. To provide medical assistance at accident scenes
D. To asses the amount and scope of damage caused by the incident

Answer: D

NEW QUESTION 386
A Hacker launched a specific attack to exploit a known system vulnerability. What term best describes this situation?

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

Answer: C

NEW QUESTION 391
An outward-facing IP address used to access the Internet.

A. Global Address
B. Private Address
C. Public Address
D. DNS

Answer: C

NEW QUESTION 396
Port used in DNS

A. 53
B. 80
C. 45
D. 54

Answer: A

NEW QUESTION 398
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 402
Often offered by third-party organizations and cover specific
advisory or compliance objectives.

A. Standard
B. PolicyC Procedure
C. Laws or Regulations

Answer: A

NEW QUESTION 404
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 406
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 409
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 411
A device that routes traffic to the port of a known device

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

Answer: A

NEW QUESTION 414
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 417
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 422
Which of the following properties is not guaranteed by Digital signatures

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

Answer: B

NEW QUESTION 424
Incident management is also known as

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

Answer: D

NEW QUESTION 428
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 companvhahppn pivpn nprmkcinn to review third-party contracts

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

Answer: B

NEW QUESTION 433
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 436
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 441
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. All

Answer: D

NEW QUESTION 444
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. All

Answer: C

NEW QUESTION 449
Load balancing safe guard which CIA triad

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

Answer: B

NEW QUESTION 454
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 456
Protection against an individual falsely denying having performed a particular action

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

Answer: D

NEW QUESTION 459
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 464
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 468
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 469
What is the BEST defense against dumpster diving attacks?

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

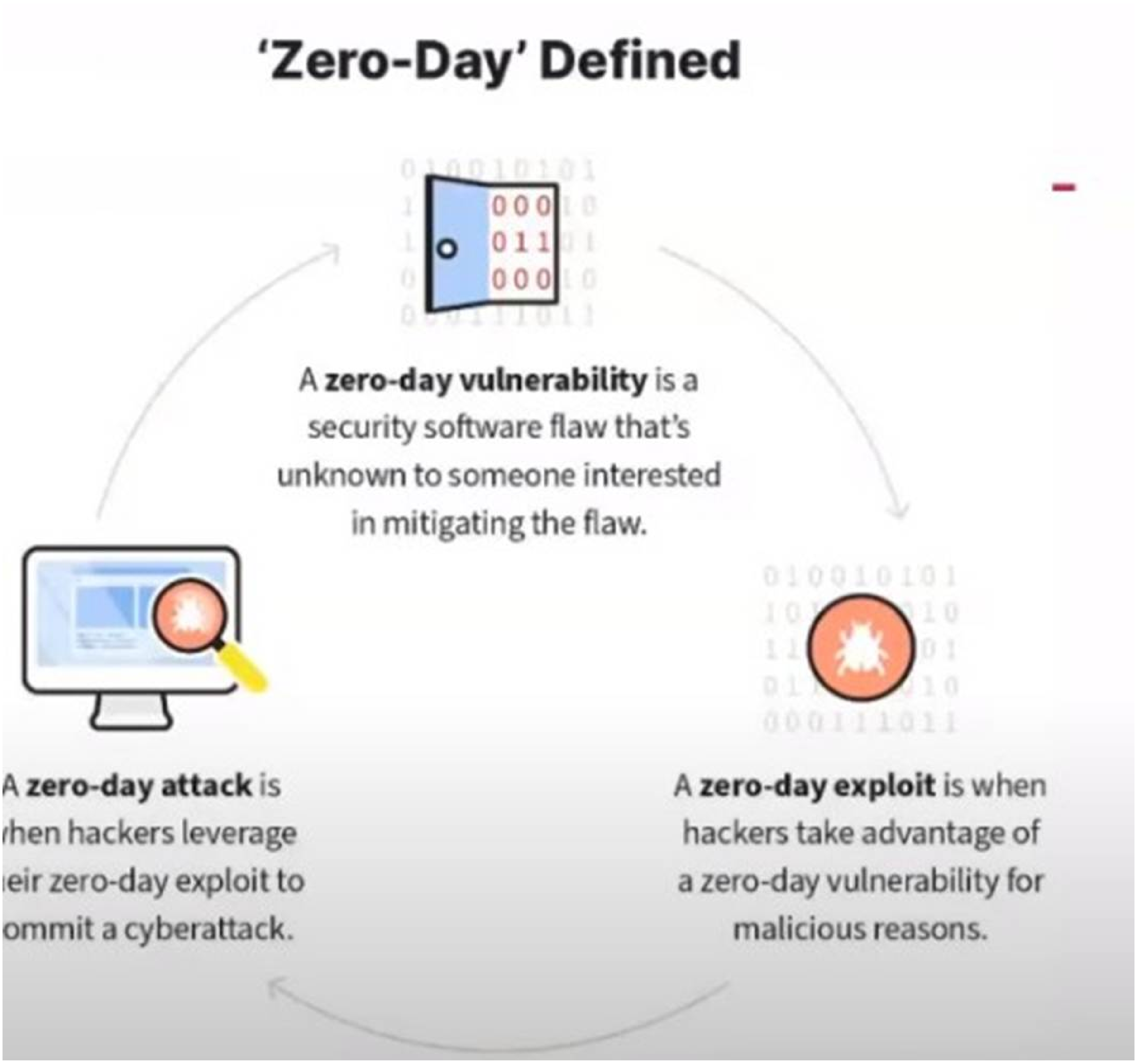
Answer: D

NEW QUESTION 473
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 476
Exhibit.

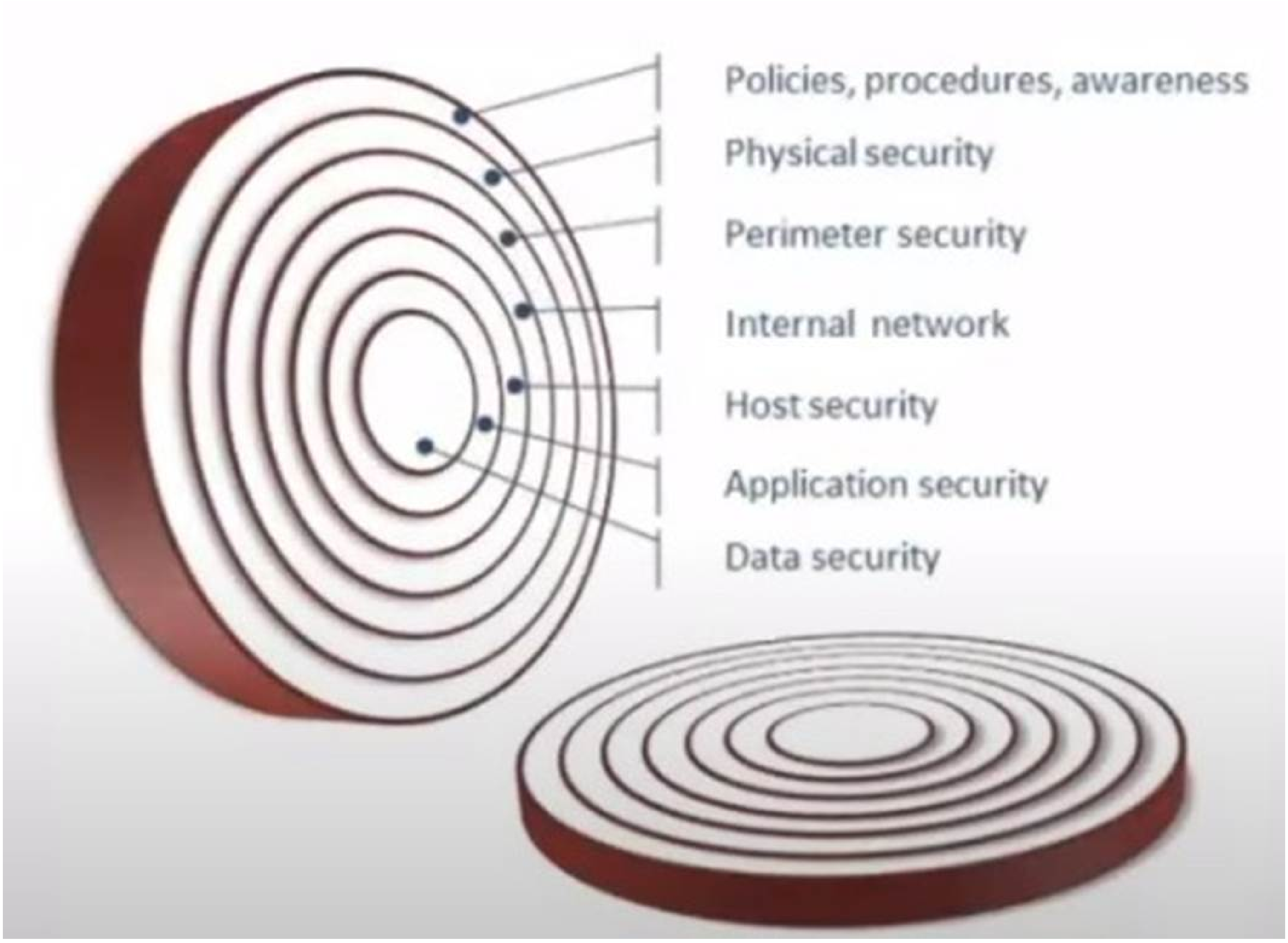


‘Zero-Day’ Defined

A **zero-day vulnerability** is a security software flaw that’s unknown to someone interested in mitigating the flaw.

A **zero-day exploit** is when hackers take advantage of a zero-day vulnerability for malicious reasons.

A **zero-day attack** is hen hackers leverage eir zero-day exploit to ommit a cyberattack.



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 481
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 484
The Order of controls used in Defence in Depth

A. Assests, Physical control
B. Administrative Controls, Logical/Techincal Controls
C. Assests, Administrative Controls, Physical controls, Logical/Techincal Controls
D. Physical control
E. Administrative Controls, Logical/Techincal Controls, Assests
F. Assests, Administrative Controls, Logical/Techincal Controls, Physical controls

Answer: D

NEW QUESTION 487
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 491
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 492
DDOS attack affect which OSI layer

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

Answer: D

NEW QUESTION 494
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 495
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 500
The prevention of authorized access to resources or the delaying of time critical operations.

A. ARP Poisoning
B. Syn Flood
C. Denial-of-Service (DoS)
D. All

Answer: C

NEW QUESTION 502
How do IT professionals differentiate between typical IT problems and security incidents?

A. By providing medical assistance at accident scenes
B. By collection evidence and reposting the incident
C. By receiving specific training on incident response
D. By participating in remediation and lessons learns stages

Answer: C

NEW QUESTION 506
Port scanning attack target which OSI layer

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

Answer: A

NEW QUESTION 508
Which is not possible models for an Incident Response Team (IRT):

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

Answer: D

NEW QUESTION 511
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 512
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. All

Answer: A

NEW QUESTION 516
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 521
A standard that defines wired communications of network devices

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

Answer: D

NEW QUESTION 526
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 530
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 531
......