ISC2

Exam Questions CC

Certified in Cybersecurity (CC)

NEW QUESTION 1
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 2
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 3
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 4
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 5
Common network device used to connect networks?

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

Answer: C

NEW QUESTION 6
What is the importance of non-repudiation in todays world of ecommerce

A. It ensures that people are not held responsible for transaction that did not conduct
B. It ensures that people are held responsible for transactions they conducted
C. It ensures that transactions are not conducted online
D. It ensures that transactions are conducted online

Answer: B

NEW QUESTION 7
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 8
Which is related to Standard

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

Answer: A

NEW QUESTION 9
255.255.255.0 Address represents

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

Answer: C

NEW QUESTION 10
What is the first phase in System Development Life Cycle

A. Requirements Analysis Phase
B. Feasibilty Study
C. Design Phase
D. Development Phase

Answer: B

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 15
A organization's security system which involves in preventing, detecting, analyzing, and responding to cybersecurity incidents.

A. Business continuity team
B. Disaster recovery team
C. Incident response team
D. Security operations center

Answer: D

NEW QUESTION 19
TCP and UDP reside at which layer of the osi model?

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

Answer: D

NEW QUESTION 23
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 24
A hacker gains access to a compony network and begins to intercept network traffic in order to steal login credentials which OSI layer is being attacked

A. Data Link layer
B. Physical layer
C. Network Layer
D. Application laver

Answer: D

NEW QUESTION 29
System capabilities designed to detect and prevent the unauthorized use and transmission of information.

A. SOC
B. SIEM solutions
C. Data Loss Prevention
D. Crytography

Answer: C

NEW QUESTION 30
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 33
A popular way of implementing "least privilege"

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

Answer: C

NEW QUESTION 37
Which type of control is used to minimize the impact of an attack and to restore normal operations as quick as possible

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

Answer: C

NEW QUESTION 42
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 46
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 50
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 52

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 53
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 56
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 60
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 63
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 66
What is the main purpose of using multi-factor authentication (MFA) in a security system?

A. To prevent data breaches
B. To protect against malware
C. To ensure data integrity
D. To add an extra layer of security to user authentication

Answer: D

NEW QUESTION 68
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 70
The documentation of a predetermined set of instructions or procedures to detect, respond to andlimit consequences of a malicious cyberattack against an organization's information systems(s).

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

Answer: B

NEW QUESTION 74
Which of the following is endpint

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

Answer: C

NEW QUESTION 77
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 82
Which of the following is a subject?

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

Answer: D

NEW QUESTION 83
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 85
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 86
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 88
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 90
Which Regulation addresses personal privacy

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

Answer: B

NEW QUESTION 91
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 96
Which component of the incident response plan involves identifying critical data and systems?

A. Detection and Analysis
B. Preparation
C. Cantainment
D. Eradication

Answer: B

NEW QUESTION 97
A company needs to protect its confidential data from unauthorized access which logical control is best suited for this scenario

A. Encryption
B. Firewall
C. Antivirus
D. Hashing

Answer: A

NEW QUESTION 100
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 103
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 106
Which threats are directly associated with malware? Select that apply.

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

Answer: C

NEW QUESTION 107
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 110
Is defined as the process of identifying, estimating and prioritizing risks

A. Risk Assessment
B. Risk Treatment
C. Risk mitigation
D. Risk Management

Answer: A

NEW QUESTION 113
Which is the component of a Business Continuity (BC) plan

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

Answer: D

NEW QUESTION 114
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 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 120
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 124
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 126
Which of the following uses registered port

A. HTTP

B. SMB
C. TCP
D. MS Sql server

Answer: D

NEW QUESTION 129
Which of the following is a characteristic of cloud

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

Answer: B

NEW QUESTION 133
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 135
Which of the following is not a source of redundant power

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

Answer: D

NEW QUESTION 139
The means by which a threat actor carries out their objectives

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

Answer: B

NEW QUESTION 140
Which of these tool is commonly used to crack passwords

A. Bup Suite
B. Nslookup
C. Wireshark
D. John the ripper

Answer: D

NEW QUESTION 142
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 144
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 147
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 151
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 152
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 156
Which layer of OSI the Firewall works

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

Answer: D

NEW QUESTION 157
Who should participate in creating a BCP

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

Answer: C

NEW QUESTION 159
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 164
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 167

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 169
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 172
What is knowledge based authentication

A. Authentication based on a passphrase or secret code
B. Autheication based on a token or memory card
C. Authentication based on biometrics or measurble charestrisirtcs
D. Authencication based on something you do

Answer: A

NEW QUESTION 173
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 174
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 176
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 177
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 181
Which maintains that a user or entity should only have access to the spec data, resources and applications needed to complete a required task.

A. Zero Trust
B. Defence in Depth

C. Least Privileges
D. AII

Answer: C

NEW QUESTION 186
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 189
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 191
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 196
XenServer, LVM, Hyper-V, ESXi are

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

Answer: B

NEW QUESTION 198
Which is the SSH port

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

Answer: D

NEW QUESTION 199
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
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 206
A type of malware that is capable of self propagation and can infect multiple systems on network without the need for human intervention

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

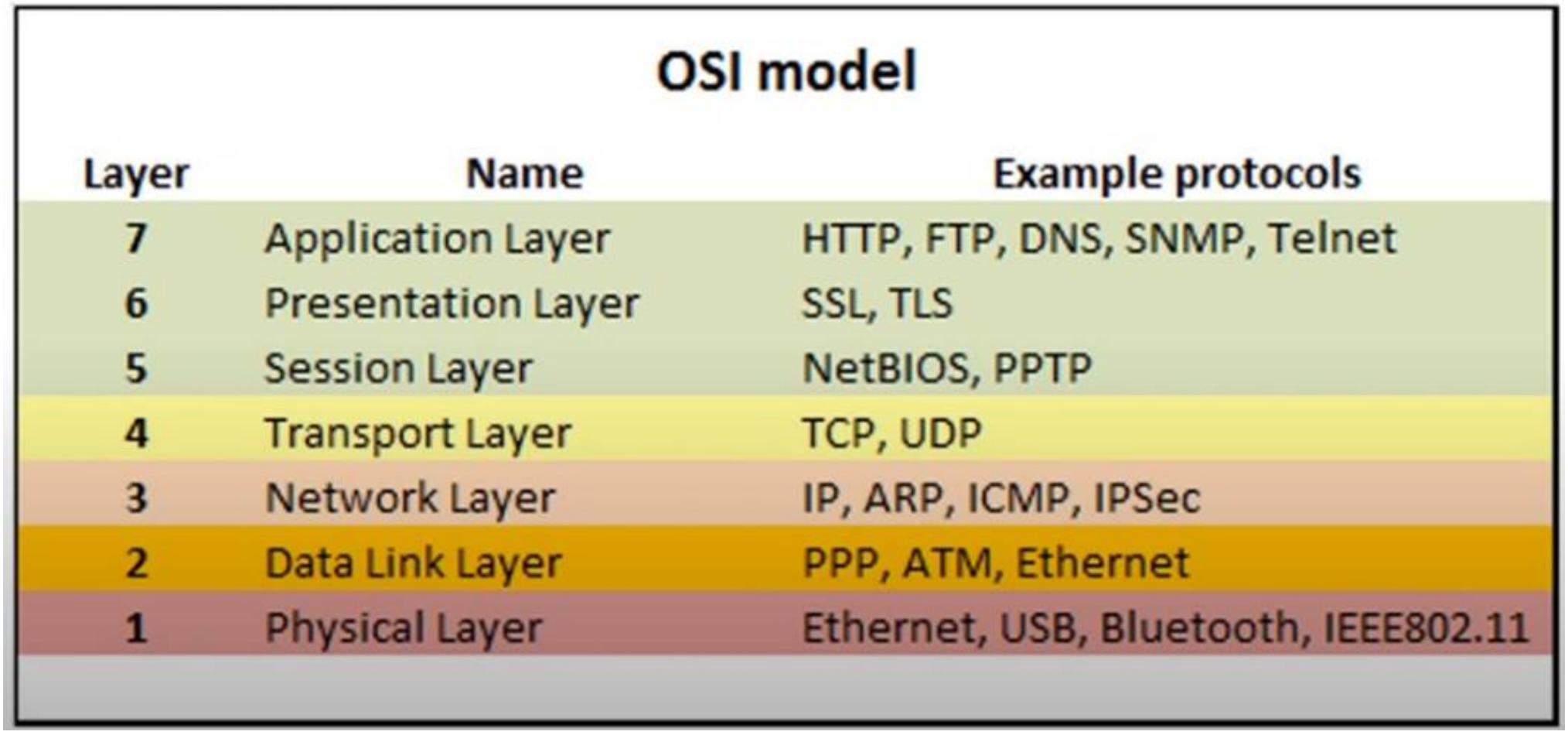
Answer: A

NEW QUESTION 211
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 214
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 218
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 221
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 223
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 228
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 232
Which of the following is NOT one of the three main components of a sql database?

A. Views
B. Schemas
C. Tables
D. Object-oriented interfaces

Answer: D

NEW QUESTION 235
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 238
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 242
Which penetration testing technique requires the team to do the MOST work and effort?

A. White box
B. Blue box
C. Gray box
D. Black box

Answer: D

NEW QUESTION 245
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 247
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 248
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 253
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 255
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 257
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. AII

Answer: A

NEW QUESTION 267
Who must follow HIPAA Compliance

A. Energy Sector
B. Health Care
C. Finance Sector
D. ALL

Answer: B

NEW QUESTION 270
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 275
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 279
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 283
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 285
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 290
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 292
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 296
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 300
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 302
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 307
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 311
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 312
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 317
Which of these is an example of deterrent control

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

Answer: B

NEW QUESTION 319
An IP network protocol standardized by the Internet Engineering Task Force (IETF) through RFC 792 to determine if a particular service or host is available.

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

Answer: B

NEW QUESTION 321
An organization develops a set of procedures to restore critical business processes after a significant disruption. What type of plan is this?

A. bcp
B. IRP
C. DRP
D. None

Answer: A

NEW QUESTION 322
Which is strongly used for Securing Wi-Fi

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

Answer: A

NEW QUESTION 324
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 325
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 329
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 332
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
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 342
Ignoring the risk and proceeding the business operations

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

Answer: A

NEW QUESTION 345
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 347
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 351
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 355
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 358
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 361
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 362
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 365
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 370
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 373
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 375
In incident terminology the Zero day is

A. Days with a cybersecurity incident

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

Answer: B

NEW QUESTION 377
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 378
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 381
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 386
Which protocol is used for secure email

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

Answer: D

NEW QUESTION 387
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 391
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 394
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 395
A common network device used to filter traffic?

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

Answer: D

NEW QUESTION 397
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 402
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 404
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 405
Government can imposes financial penalties as a consequence of breaking a

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

Answer: B

NEW QUESTION 409
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 412
Which of the following is not a feature of a cryptographic hash function

A. Deterministic
B. Unique
C. Useful
D. Reversible

Answer: D

NEW QUESTION 417

Incident management is also known as

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

Answer: D

NEW QUESTION 418
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 419
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 421
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 426
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 427
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 431
Load balancing safe guard which CIA triad

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

Answer: B

NEW QUESTION 435
Protection against an individual falsely denying having performed a particular action

A. Authentication
B. Identification

C. Verification
D. Non repudiation

Answer: D

NEW QUESTION 439
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 442
Which of the following is very likely to be used in a disaster recovery (DR) effort?

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

Answer: C

NEW QUESTION 443
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 444
What is the BEST defense against dumpster diving attacks?

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

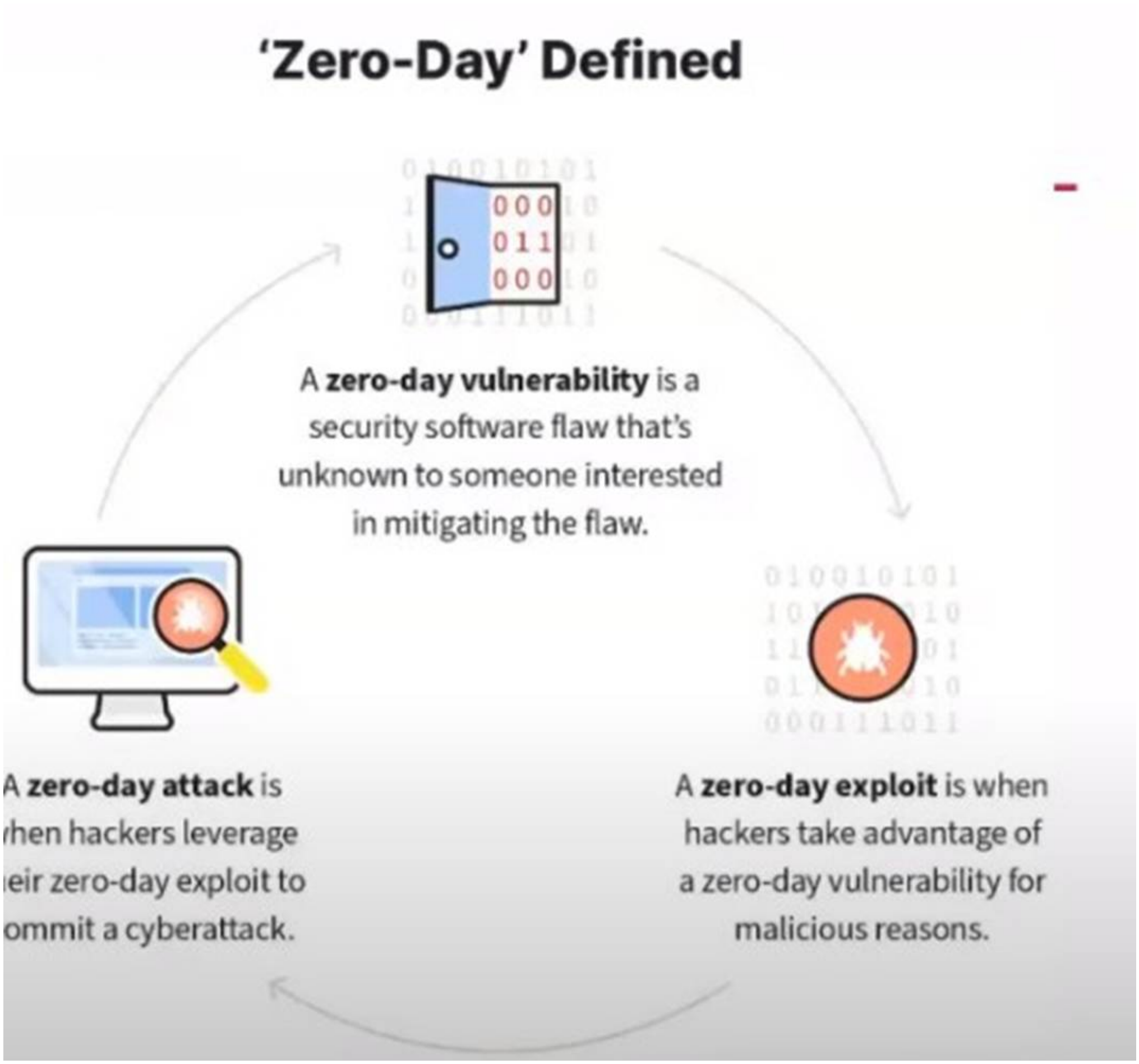
Answer: D

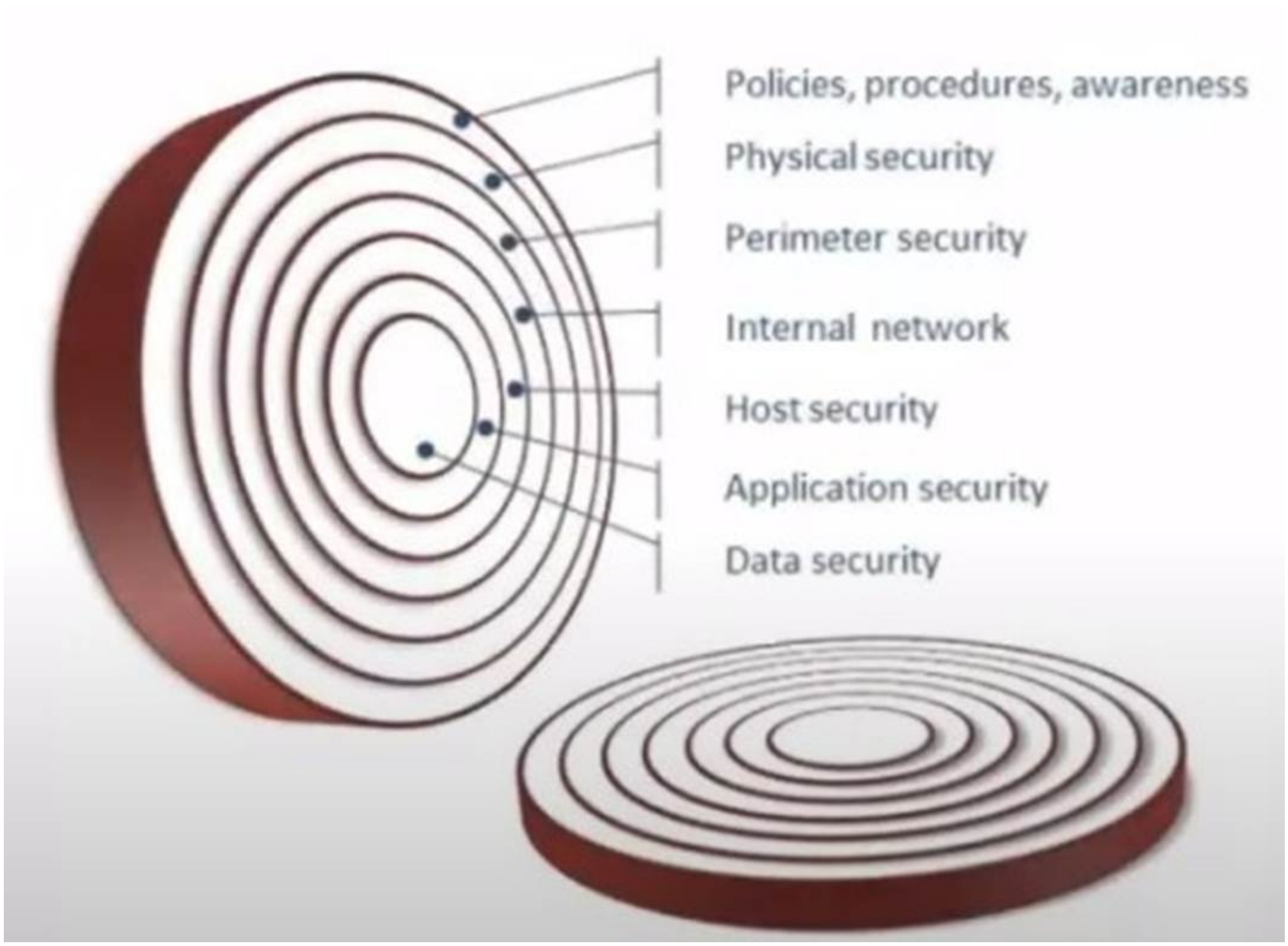
NEW QUESTION 448
Which authentication helps build relationships between different technology providers, enabling automatic identification and user access. Employees no longer need to enter separate usernames and passwords when visiting a new service provider

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

Answer: D

NEW QUESTION 449
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 450
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 453
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 456
DDOS attack affect which OSI layer

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

Answer: D

NEW QUESTION 461
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 465
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 466
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 471
Port scanning attack target which OSI layer

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

Answer: A

NEW QUESTION 472
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 477
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 482
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 483
What is the potential impact of an IPSec reply attack

A. Modification of network traffic
B. Disruption of network communication
C. Unauthorized access to network resources
D. ALL

Answer: A

NEW QUESTION 484
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 487
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 488
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 493
A standard that defines wired communications of network devices

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

Answer: D

NEW QUESTION 496
A backup is which type for security control

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

Answer: C

NEW QUESTION 500
Which device is used to control traffic flow in network

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

Answer: D

NEW QUESTION 503
.....

Thank You for Trying Our Product

We offer two products:

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

2nd - Questons and Answers in PDF Format

CC Practice Exam Features:

* CC Questions and Answers Updated Frequently

* CC Practice Questions Verified by Expert Senior Certified Staff

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

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