

ISC2

Exam Questions CC

Certified in Cybersecurity (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. Stanford

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

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

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

Answer: C

NEW QUESTION 4

What are registered port used for

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

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

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

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

Answer: C

NEW QUESTION 7

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 8

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 9

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 10

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 10

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 14

IDS can be described in terms of what fundamental functional components?

- A. Response
- B. Information Sources
- C. Analysis
- D. All of the choices.

Answer: D

NEW QUESTION 16

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 21

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 24

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 25

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 27

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

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

Answer: D

NEW QUESTION 29

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 32

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 33

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 38

Port forwarding is also known as

- A. Port mapping
- B. Tunneling
- C. Punch through
- D. ALL

Answer: D

NEW QUESTION 43

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 44

Which layer does VLAN hopping belong to?

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

Answer: D

NEW QUESTION 45

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 47

The prevention of unauthorized 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. Authentication
- C. Availability
- D. Availability

Answer: A

NEW QUESTION 49

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 51

What does Personally Identifiable Information (PII) 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 52

A tool used to inspect outbound traffic to reduce threats

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

Answer: C

NEW QUESTION 57

What security feature used in HTTPS

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

Answer: D

NEW QUESTION 62

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 64

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 68

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 71

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 76

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 78

Information should be consistently and readily accessible for authorized parties ?

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

Answer: C

NEW QUESTION 83

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 84

Which of the following attacks can TLS help mitigate?

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

Answer: C

NEW QUESTION 89

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 90

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 94

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 95

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 98

A structured approach used to oversee and manage risk for an enterprise

- A. Risk Assessment
- B. Risk threshold
- C. Risk Management Framework
- D. Risk appetite

Answer: C

NEW QUESTION 103

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 104

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 108

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 112

Which of the following uses registered port

- A. HTTP
- B. SMB
- C. TCP
- D. MS Sql server

Answer: D

NEW QUESTION 115

The means by which a threat actor carries out their objectives

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

Answer: B

NEW QUESTION 118

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 119

Exhibit.



information security is not built on which of the following?

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

Answer: C

NEW QUESTION 120

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 121

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 126

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 130

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

- A. acOO:: to adff:ffff:ffff:ffff:ffff:ffff:ffff
- B. fcOO:: to fdf:ffff:ffff:ffff:ffff:ffff:ffff
- C. bcOO:: to bdf:ffff:ffff:ffff:ffff:ffff:ffff
- D. ccOO:: to cdf:ffff:ffff:ffff:ffff:ffff:ffff

Answer: B

NEW QUESTION 134

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 136

Hashing used to safe guard which CIA triad

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

Answer: C

NEW QUESTION 139

What is the primary factor in the reliability of information and system

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

Answer: C

NEW QUESTION 141

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. All

Answer: C

NEW QUESTION 143

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 148

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. Technical control

Answer: A

NEW QUESTION 152

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 153

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 158

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 163

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 164

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 167

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

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

Answer: B

NEW QUESTION 169

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 171

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 173

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 175

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 176

Which encryption type used in HTTPS communication

- A. Symmetric
- B. Asymmetric
- C. None
- D. Both A and B

Answer: D

NEW QUESTION 177

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 178

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 183

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 184

Which of the following is often associated with DR planning?

- A. Checklists

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

Answer: D

NEW QUESTION 185

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 190

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

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

Answer: C

NEW QUESTION 193

Which type of authentication is something which you

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

Answer: C

NEW QUESTION 198

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 203

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

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

Answer: A

NEW QUESTION 204

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 207

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 208

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 213

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 215

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 216

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

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

Answer: C

NEW QUESTION 220

Which type of attack attempts to gain information by observing the devices power consumption

- A. DOS
- B. Side Channels
- C. XSS
- D. XSRF

Answer: B

NEW QUESTION 222

What is the purpose of multi-factor authentication (MFA) in IAM?

- 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 227

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

- A. BCP
- B. IRP
- C. DRP
- D. None

Answer: B

NEW QUESTION 230

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 235

Permitting authorized access to information while protecting it from improper disclosure

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

Answer: B

NEW QUESTION 236

Example of Type 1 Authentication

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

Answer: A

NEW QUESTION 238

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 240

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 242

Ignoring the risk and proceeding the business operations

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

Answer: A

NEW QUESTION 245

What is Remanence

- A. The ability of retaining magnetization in storage disk after deletion
- B. Files or pieces of files get scattered throughout your disks.
- C. Data corruption due to disk failure
- D. All

Answer: A

NEW QUESTION 250

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 254

Who should participate in creation a business continuity plan

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

Answer: D

NEW QUESTION 257

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

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

Answer: C

NEW QUESTION 260

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 263

Port used in DNS

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

Answer: A

NEW QUESTION 265

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

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

Answer: C

NEW QUESTION 269

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 274

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

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

Answer: A

NEW QUESTION 279

A common network device used to filter traffic?

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

Answer: D

NEW QUESTION 282

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 287

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 288

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 289

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 293

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 297

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 301

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 305

Load balancing safe guard which CIA triad

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

Answer: B

NEW QUESTION 310

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 312

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 313

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

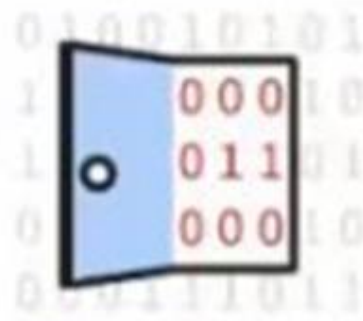
- A. to eliminate all cybersecurity risks
- B. to transfer all cybersecurity risks to a third party
- C. to identify, assess, and mitigate cybersecurity risks to an acceptable level (Correct)
- D. to ignore cybersecurity risks and focus on incident response

Answer: C

NEW QUESTION 318

Exhibit.

'Zero-Day' Defined



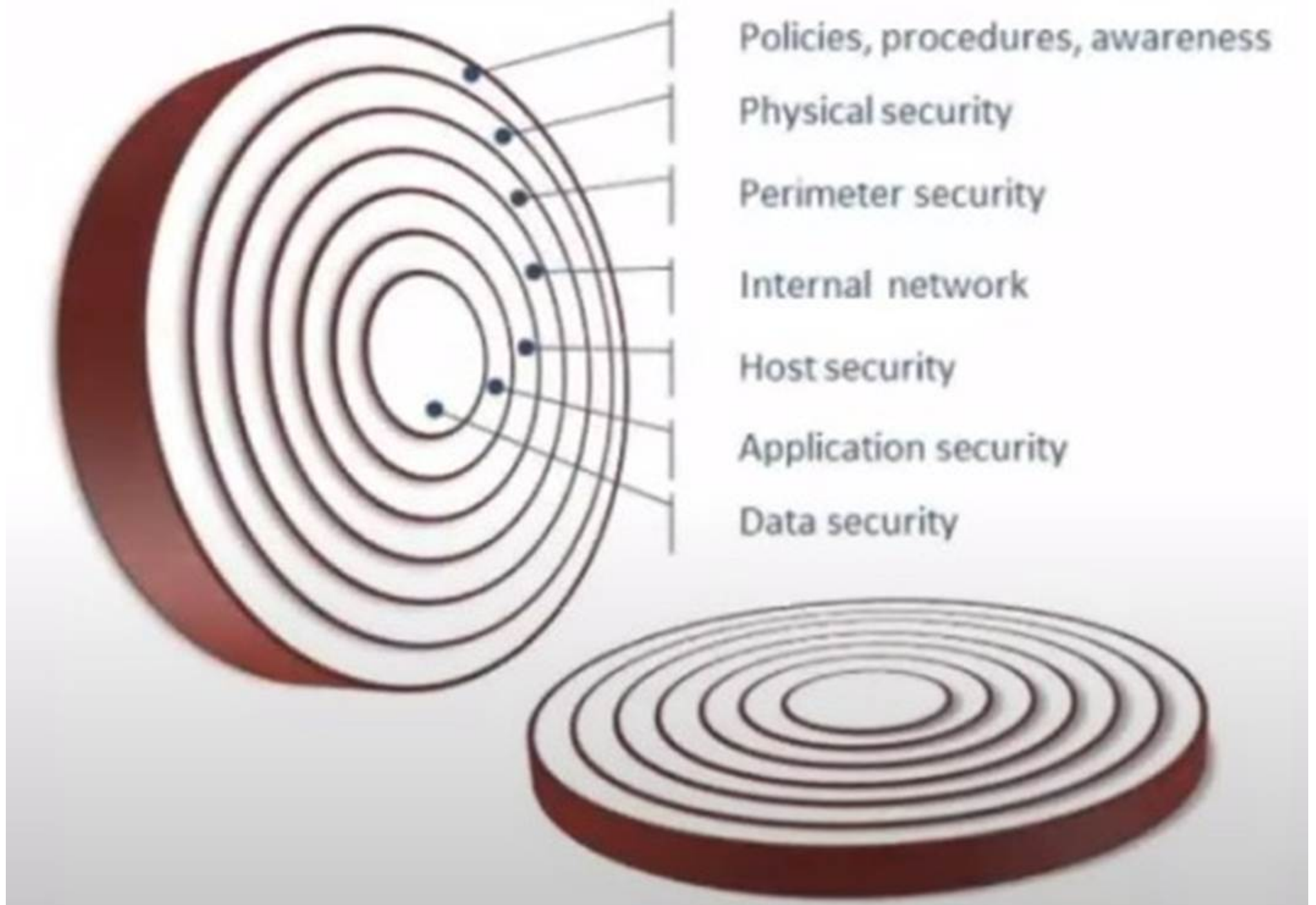
A **zero-day vulnerability** is a security software flaw that's unknown to someone interested in mitigating the flaw.



A **zero-day 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 321

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 324

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 325

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

- A. Confidentiality
- B. Integrity

- C. Privacy
- D. Availability

Answer: C

NEW QUESTION 330

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 334

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 learned stages

Answer: C

NEW QUESTION 338

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

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

Answer: D

NEW QUESTION 343

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

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

Answer: A

NEW QUESTION 348

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 350

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 355

A standard that defines wired communications of network devices

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

Answer: D

NEW QUESTION 360

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 364

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 368

.....

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](#)