



ISC2

Exam Questions CC

Certified in Cybersecurity (CC)

About ExamBible

Your Partner of IT Exam

Found in 1998

ExamBible is a company specialized on providing high quality IT exam practice study materials, especially Cisco CCNA, CCDA, CCNP, CCIE, Checkpoint CCSE, CompTIA A+, Network+ certification practice exams and so on. We guarantee that the candidates will not only pass any IT exam at the first attempt but also get profound understanding about the certificates they have got. There are so many alike companies in this industry, however, ExamBible has its unique advantages that other companies could not achieve.

Our Advances

* 99.9% Uptime

All examinations will be up to date.

* 24/7 Quality Support

We will provide service round the clock.

* 100% Pass Rate

Our guarantee that you will pass the exam.

* Unique Gurantee

If you do not pass the exam at the first time, we will not only arrange FULL REFUND for you, but also provide you another exam of your claim, ABSOLUTELY FREE!

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 is multi-factor authentication (MFA)?

- A. A type of authentication that uses only one method
- B. A type of authentication that uses only two methods
- C. A type of authentication that uses more than two methods (Correct)
- D. A type of authentication that uses only one factor

Answer: C

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

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 6

Common network device used to connect networks?

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

Answer: C

NEW QUESTION 7

Example of Dynamic authorization

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

Answer: D

NEW QUESTION 8

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 9

In Which of the following access control models can the creator of an object delegate permission

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

Answer: C

NEW QUESTION 10

Ping flood attack target which OSI layer

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

Answer: B

NEW QUESTION 10

255.255.255.0 Address represents

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

Answer: C

NEW QUESTION 12

What is the first phase in System Development Life Cycle

- A. Requirements Analysis Phase
- B. Feasibility Study
- C. Design Phase
- D. Development Phase

Answer: B

NEW QUESTION 17

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

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

Answer: C

NEW QUESTION 19

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 23

TCP and UDP reside at which layer of the OSI model?

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

Answer: D

NEW QUESTION 24

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

- A. SOC
- B. SIEM solutions
- C. Data Loss Prevention
- D. Cryptography

Answer: C

NEW QUESTION 26

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 31

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 32

A company wants to ensure that its employees can evacuate the building in case of an emergency which physical control is best suited for this scenario

- A. Fire Alarms
- B. Exit signs
- C. Emergency lighting
- D. Emergency exit doors

Answer: D

NEW QUESTION 35

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 37

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 41

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 43

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 47

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 51

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 53

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 55

Are a measure of an organization's baseline of security performance

- A. Security Assessment
- B. Secuirty Audit
- C. Security Benchmark
- D. Security Management

Answer: C

NEW QUESTION 58

After an Earthquake disrupting business operations, which documents contains the reactive procedures required to return business to normal operations

- A. The Business Impact Analysis
- B. The Business Continuity Plan
- C. The Disaster Recovery plan
- D. The Business Impact Plan

Answer: C

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 64

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 66

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 70

Which of the following is endpoint

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

Answer: C

NEW QUESTION 74

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 76

Which layer does VLAN hopping belong to?

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

Answer: D

NEW QUESTION 77

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 82

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 84

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 is the best practise to clear SSD storage after usage in term of cyber security

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

Answer: D

NEW QUESTION 88

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 91

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 93

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 96

While taking the certification exam for ISC2 CC, You notice another candidate for the certification cheating. What should you do?

- A. Yell at the other candidate for violating test security.
- B. Nothing—each person is responsible for their own actions.
- C. Report the candidate to ISC2.
- D. Call local law enforcement.

Answer: C

NEW QUESTION 99

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 104

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 109

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 113

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 114

Information should be consistently and readily accessible for authorized parties ?

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

Answer: C

NEW QUESTION 119

6 Which access control method uses attributes and rules to define access policies that are evaluate by a central Policy Decision Point (PDP)

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

Answer: D

NEW QUESTION 122

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

- A. Burp suite
- B. Wireshark C Fiddler
- C. ZenMap

Answer: A

NEW QUESTION 127

Which Prevents Threat

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

Answer: A

NEW QUESTION 130

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 131

Which threats are directly associated with malware? Select that apply.

- A. APT
- B. Ransomware
- C. Trojan
- D. DDOS

Answer: C

NEW QUESTION 133

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 134

In DAC, the policy specifies that a subject who has been granted access to information can do the following:

- A. Change security attributes on subjects, objects, information systems or system components
- B. Choose the security attributes to be associated with newly created or revised objects
- C. Change the rules governing access control
- D. ALL

Answer: D

NEW QUESTION 139

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 141

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 144

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 147

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 151

Which of the following uses registered port

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

Answer: D

NEW QUESTION 156

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 157

The magnitude of the harm expected as a result of the consequences of an unauthorized disclosure, modification, destruction or loss of information is known as

- A. Threat
- B. Vulnerability
- C. Impact
- D. Likelihood

Answer: C

NEW QUESTION 158

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 162

Which of the following is not a source of redundant power

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

Answer: D

NEW QUESTION 167

The means by which a threat actor carries out their objectives

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

Answer: B

NEW QUESTION 172

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 173

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

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

Answer: C

NEW QUESTION 178

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 179

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 184

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 fdff:ffff:ffff:ffff:ffff:ffff:ffff
- C. bcOO:: to bdff:ffff:ffff:ffff:ffff:ffff:ffff
- D. ccOO:: to cdff:ffff:ffff:ffff:ffff:ffff:ffff

Answer: B

NEW QUESTION 185

Some Employee of his organization launched a privilege escalation attack to gain root access on one of the organization's database servers. The employee does have an authorized user account on the server. What log file would be MOST likely to contain relevant information??

- A. Database application log
- B. Firewall log
- C. Operating system log
- D. IDS log

Answer: C

NEW QUESTION 186

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 187

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 190

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 194

What goal of security is enhanced by a strong business continuity program?

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

Answer: B

NEW QUESTION 198

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 199

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 201

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 205

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 209

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

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

Answer: A

NEW QUESTION 212

What is the end goal of DRP

- A. All System backup restored
- B. DR site activated
- C. Shifting the Infrastructure to new place
- D. Business restored to full last-known reliable operations.

Answer: D

NEW QUESTION 213

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 216

Which is the SSH port

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

D. 22

Answer: D

NEW QUESTION 219

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 222

How often should an organization test its business continuity plan

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

Answer: C

NEW QUESTION 227

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 231

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

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

Answer: D

NEW QUESTION 236

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 241

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 244

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 248

Exhibit.

OSI model		
Layer	Name	Example protocols
7	Application Layer	HTTP, FTP, DNS, SNMP, Telnet
6	Presentation Layer	SSL, TLS
5	Session Layer	NetBIOS, PPTP
4	Transport Layer	TCP, UDP
3	Network Layer	IP, ARP, ICMP, IPSec
2	Data Link Layer	PPP, ATM, Ethernet
1	Physical Layer	Ethernet, USB, Bluetooth, IEEE802.11

IPSec works in which layer of OSI Model

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

Answer: C

NEW QUESTION 249

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 253

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 258

Which of the following best describes the puposes of a business impact analysis?

- A. To document a predetermined set of instructions or procedures for restoring IT and communications services after a disruption
- B. To mitigate security violation and ensure that business operation can continue during a contingency
- C. To provide a high level overview of the disaster recovery plan
- D. To analyze an information systems requirements and functions in order to determine system contingency priorities

Answer: D

NEW QUESTION 261

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 263

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

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

Answer: B

NEW QUESTION 267

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 272

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 274

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 278

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 282

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 283

Which type of attack will most effectively maintain remote access and control over the victims computer

- A. Phishing
- B. Trojans
- C. XSS
- D. RootKits

Answer: D

NEW QUESTION 284

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 286

Who must follow HIPAA Compliance

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

Answer: B

NEW QUESTION 287

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 290

A company security team detected a cyber attack against it information systems and activates a set of procedures to mitigate the attack., What type of plan is this?

- A. Business continuity plan
- B. Incident response plan
- C. Disaster recvoery plan
- D. Security operation plan

Answer: B

NEW QUESTION 291

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 295

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 298

Natalia is concerned that users on her network may be storing sensitive information, such as social security numbers, on their hard drives without proper authorization or security controls. What 3rd -party security service can she implement to best detect this activity?

- A. IDS - Intrusion Detection System
- B. IPS - Intrusion Prevention System
- C. DLP - Data Loss Protection
- D. TLS - Transport Layer Security

Answer: C

NEW QUESTION 302

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 303

What is the process of verifying a users identity called?

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

Answer: B

NEW QUESTION 304

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 307

What is privacy in the context of Information Security?

- A. Protecting data from unauthorized access
- B. Ensuring data is accurate and unchanged
- C. Making sure data is always accessible when needed.
- D. Disclosed without their consent

Answer: A

NEW QUESTION 311

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 315

Which security control mostly used to prevent data breach

- A. Physical control
- B. Logical Control
- C. Adminstrative Control
- D. RBAC

Answer: B

NEW QUESTION 317

Restoring IT and communications back to full operation after a disruption.

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

Answer: C

NEW QUESTION 320

Which of these is an example of deterrent control

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

Answer: B

NEW QUESTION 324

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 329

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 331

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 332

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 334

An employee unintentionally shares confidential information with an unauthorized party. What term best describes this situation?

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

Answer: D

NEW QUESTION 336

Granting a user access to services or the system

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

Answer: C

NEW QUESTION 339

WF attack in which a subscriber currently authenticated to an Server and connected through a secure session browses to an attacker's website, causing the subscriber to unknowingly invoke unwanted actions at the Server

- A. XSS
- B. CSRF
- C. Spoofing
- D. ALL

Answer: B

NEW QUESTION 344

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 346

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

- A. True
- B. False

Answer: B

NEW QUESTION 351

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 356

Which type of fire suppression system is more friendly to electronics

- A. Carbon di Oxide based
- B. Chemical based
- C. Water based
- D. Foam based

Answer: A

NEW QUESTION 358

When the ISC2 Mail server sends mail to other mail servers it becomes —?

- A. SMTP Server
- B. SMTP Peer
- C. SMTP Master
- D. SMTP Client

Answer: D

NEW QUESTION 361

Which of the following protocols is a secure alternative to using telnet?

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

Answer: B

NEW QUESTION 366

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 369

Which of these activities is often associated with DR efforts?

- A. Running anti-malware solutions
- B. Scanning the IT environment for vulnerabilities
- C. Zero-day exploits
- D. Employees returning to the primary production location

Answer: D

NEW QUESTION 374

What is the purpose of immediate response procedures and checklists in a BCP

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

Answer: A

NEW QUESTION 376

What kind of control is, when we add a backup firewall that takes over if the main one stops working?

- A. Clustering
- B. High availability(HA)
- C. Load balancing
- D. Component redundancy

Answer: B

NEW QUESTION 379

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 381

Which of the following is the least secure communications protocol?

- A. CHAP
- B. Ipsec
- C. PAP
- D. EAP

Answer: C

NEW QUESTION 384

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 385

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 386

Permitting authorized access to information while protecting it from improper disclosure

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

Answer: B

NEW QUESTION 387

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 389

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 391

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 396

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 397

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 398

A security event, or combination of security events, that constitutes a secu incident in which an intruder gains, or attempts to gain, access to a system or system resource without authorization

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

Answer: A

NEW QUESTION 403

Which access control model can grant access to a given object based on complex rules

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

Answer: A

NEW QUESTION 406

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 408

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 413

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 414

A company data center has been breached by hackers and all its systems have been taken down what is the main objective of the DRP in such a scenario?

- A. To relocate the data center to another location
- B. To ensure the physical safety of employees in the data center
- C. To investigate and prosecute the hackers responsible of the attack
- D. To restore the IT systems to their last known state

Answer: D

NEW QUESTION 417

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 420

Which uses encrypted, machine-generated codes to verify a user's identity.

- A. Basic Authentication
- B. Form Based Authentication
- C. Token Based Authentication
- D. All

Answer: C

NEW QUESTION 421

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 424

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 425

The process of applying secure configurations (to reduce the attack surface)

- A. Security Assessment
- B. Security Evaluation
- C. Security Benchmark
- D. Security Hardening

Answer: D

NEW QUESTION 429

What is the primary goal of implementing input validation in application security?

- A. To ensure all inputs are stored in a secure database
- B. To prevent unauthorized access to the application
- C. To validate and sanitize user inputs to prevent code injection attacks (Correct)
- D. To encrypt sensitive data transmitted between the client and server

Answer: C

NEW QUESTION 434

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 435

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 437

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

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

Answer: D

NEW QUESTION 440

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 443

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 445

What is the primary purpose of a honeypot in cybersecurity?

- A. To lure and detect attackers
- B. To encrypt sensitive data
- C. To enhance network performance
- D. To manage user access

Answer: A

NEW QUESTION 447

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 451

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 454

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 455

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 457

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 459

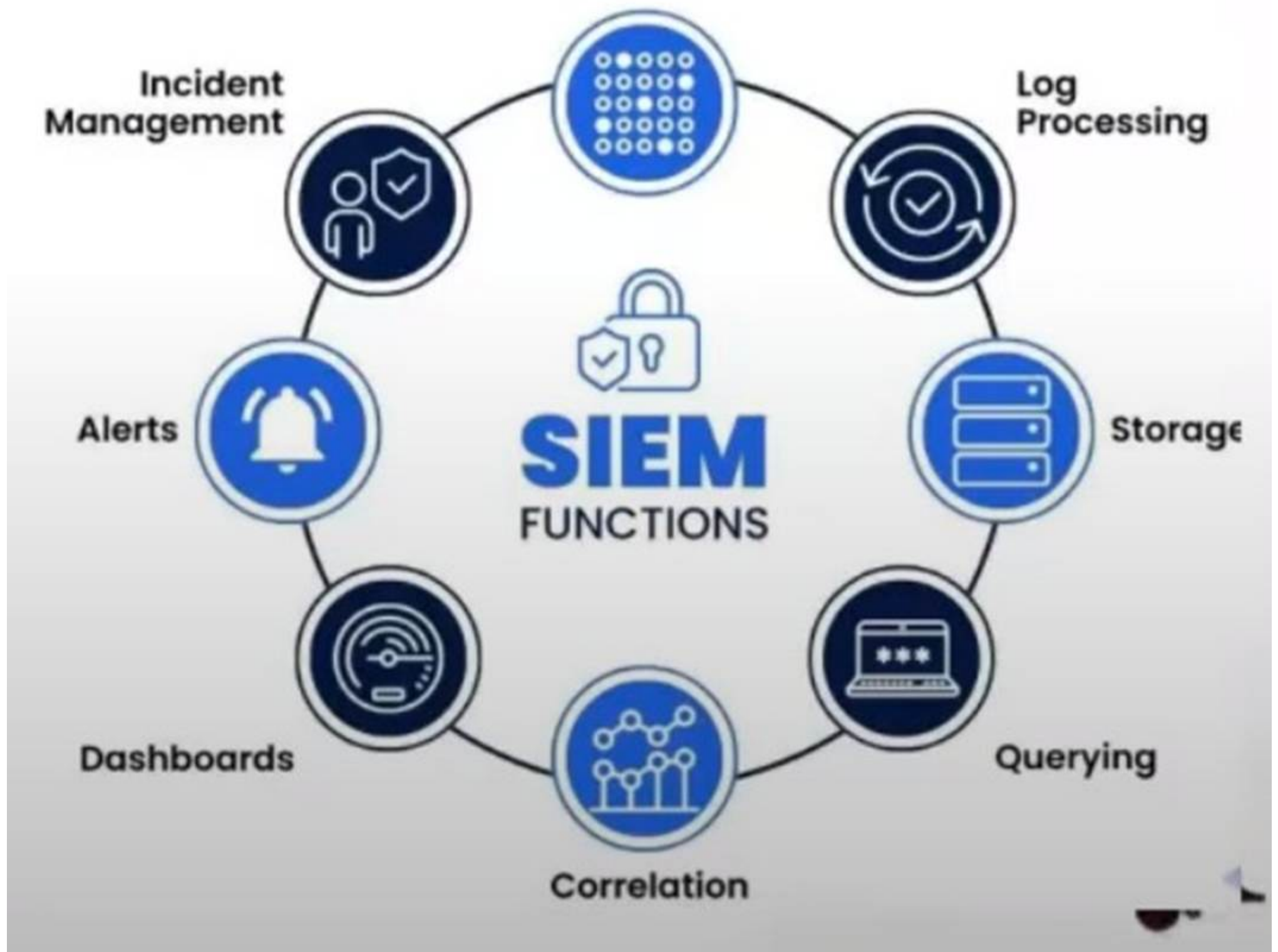
Government can imposes financial penalties as a consequence of breaking a

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

Answer: B

NEW QUESTION 463

Exhibit.



What is the purpose of a Security Information and Event Management (SIEM) system?

- A. Encrypting files
- B. Monitoring and analyzing security events -
- C. Blocking malicious websites
- D. Managing user passwords

Answer: B

NEW QUESTION 467

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 470

Incident management is also known as

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

Answer: D

NEW QUESTION 475

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

- A. Procedure
- B. Policy

- C. Standard
- D. Law

Answer: B

NEW QUESTION 480

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 483

Which ensure maintaining business operations during or after an incident

- A. Incident Response
- B. Business Continuity
- C. Disaster Recovery
- D. All

Answer: C

NEW QUESTION 488

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 491

What is the most important aspect of security awareness/training?

- A. Maximizing business capabilities
- B. Protecting assets
- C. Protecting health and human safety
- D. Ensuring the confidentiality of data

Answer: C

NEW QUESTION 495

Load balancing safe guard which CIA triad

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

Answer: B

NEW QUESTION 498

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 502

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 506

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 510

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 511

What is the BEST defense against dumpster diving attacks?

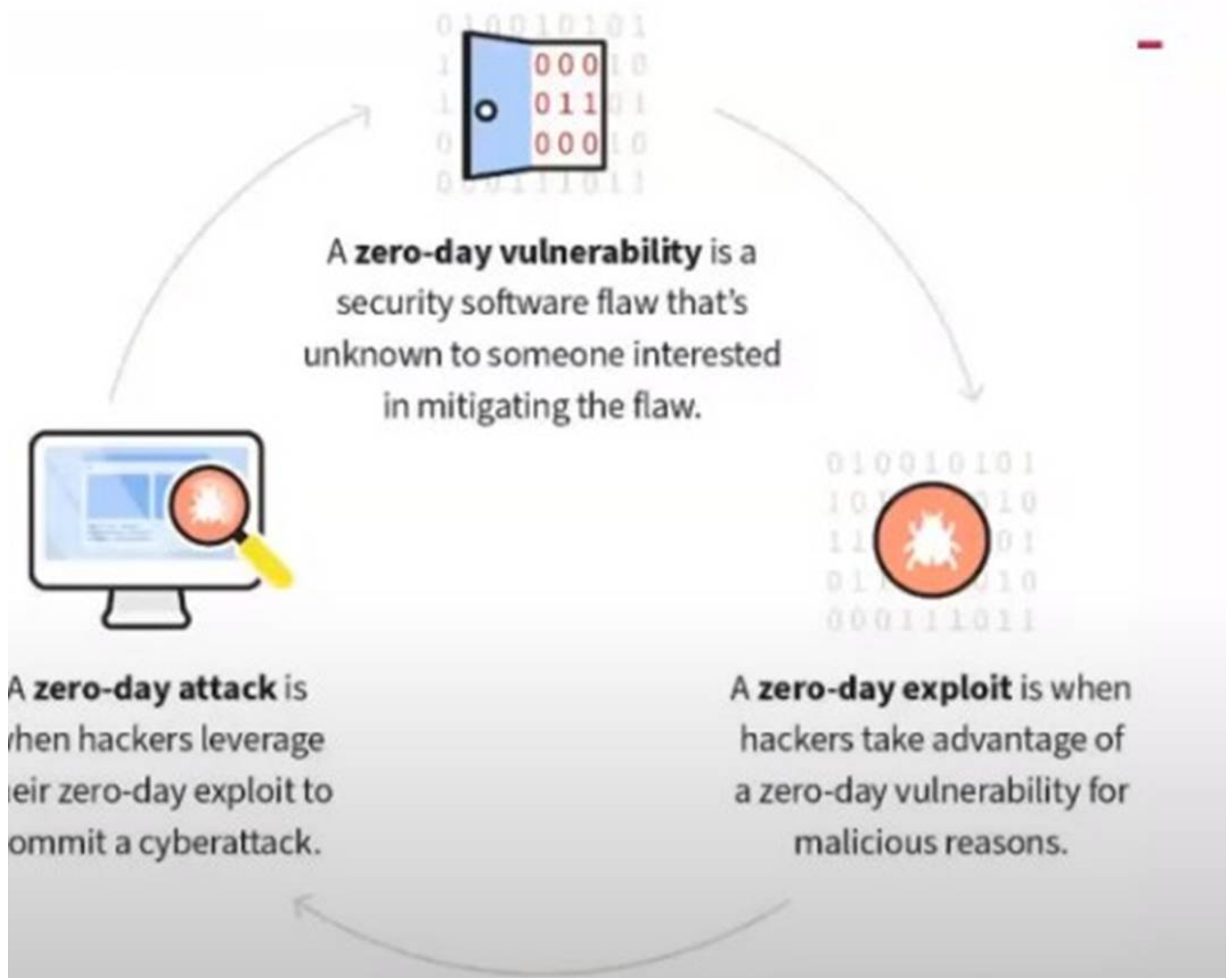
- A. Anti-malware software
- B. Clean desk policy
- C. Data loss prevention tools
- D. Shredding

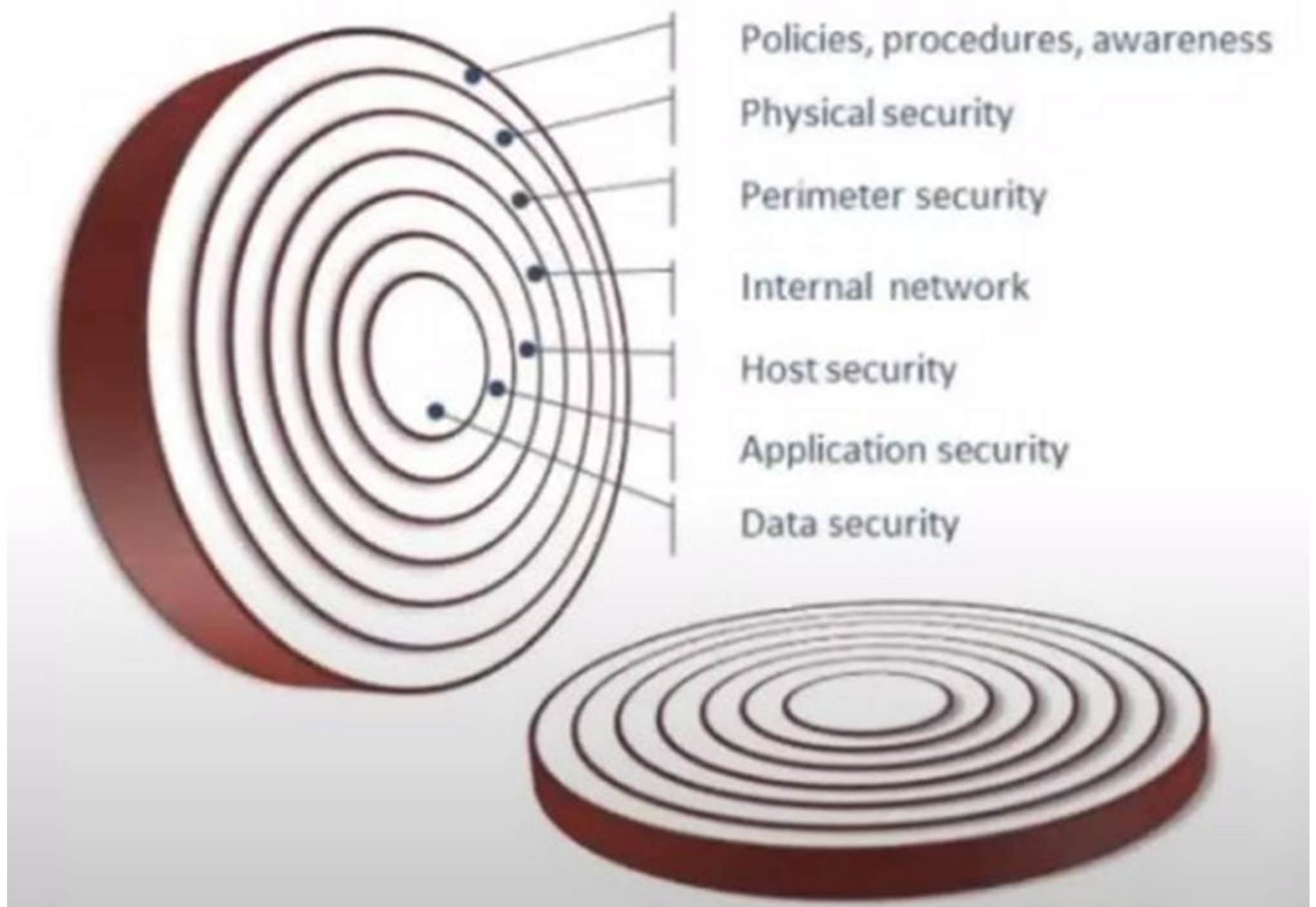
Answer: D

NEW QUESTION 515

Exhibit.

'Zero-Day' Defined





What kind of vulnerability is typically not identifiable through a standard vulnerability assessment?

- A. File permissions
- B. Buffer overflow
- C. Zero-day vulnerability
- D. Cross-site scripting

Answer: C

NEW QUESTION 518

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 523

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 527

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 530

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 533

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

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

Answer: D

NEW QUESTION 534

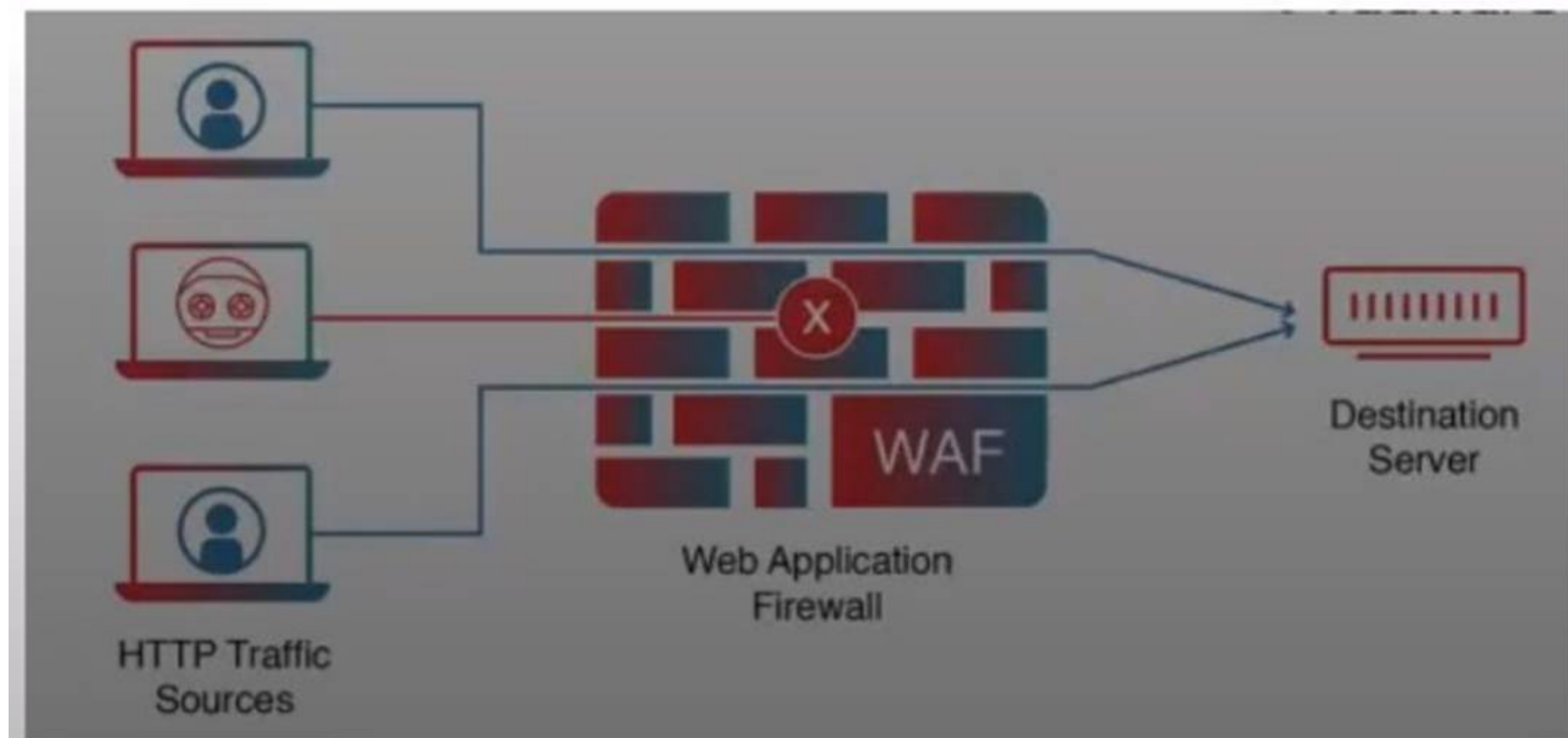
Uses multiple types of access controls in literal or theoretical layers to help an organization avoid a monolithic security

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

Answer: C

NEW QUESTION 539

Exhibit.



What is the PRIMARY purpose of a web application firewall (WAF)?

- A. To protect the web server from DDoS attacks
- B. To monitor network traffic for intrusions
- C. To filter and block malicious web traffic and requests
- D. To manage SSL certificates

Answer: C

NEW QUESTION 541

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 542

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 544

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 549

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 550

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 551

A backup is which type for security control

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

Answer: C

NEW QUESTION 554

Token Ring used in which OSI Layer

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

Answer: D

NEW QUESTION 558

Which device is used to control traffic flow in network

- A. SDN
- B. Switch
- C. Hub

D. Router

Answer: D

NEW QUESTION 559

.....

Relate Links

100% Pass Your CC Exam with Examible Prep Materials

<https://www.examible.com/CC-exam/>

Contact us

We are proud of our high-quality customer service, which serves you around the clock 24/7.

Viste - <https://www.examible.com/>