Exam Questions CC

Certified in Cybersecurity (CC)

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

NEW QUESTION 1
What federal law requires the use of vulnerability scanning on information systems operated by federal government agencies?

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

Answer: A

NEW QUESTION 2
In the context of cybersecurity, typical threat actors include the following:

A. Insiders (either deliberately, by simple human error, or by gross incompetence).
B. Outside individuals or informal groups (either planned or opportunistic, discovering vulnerability).
C. Technology (such as free-running bots and artificial intelligence
D. All

Answer: D

NEW QUESTION 3
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 4
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 5
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 6
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 7
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 8
Part of a zero-trust strategy that breaks LANs into very small and highly localized zones using firewalls.

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

Answer: D

NEW QUESTION 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
Which is related to Standard

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

Answer: A

NEW QUESTION 10
255.255.255.0 Address represents

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

Answer: C

NEW QUESTION 12
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 16
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 21
Example of Token based Authentication

A. Kerberos
B. Basic
C. OAuth
D. NTLN

Answer: C

NEW QUESTION 22
TCP and UDP reside at which layer of the osi model?

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

Answer: D

NEW QUESTION 25
Which term describes a communication tunnel that provides point-to-point transmission of both authentication and data traffic over an untrusted network?

A. Zero Trust
B. DMZ
C. VPN
D. None of the Above

Answer: C

NEW QUESTION 28
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 32
Type 1 authentication posses

A. Users may share their credential with others
B. User may forgot their passwords
C. Passwords may be intercepted and stolen
D. ALL

Answer: D

NEW QUESTION 37
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 40
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 44
A popular way of implementing "least privilege"

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

Answer: C

NEW QUESTION 47
What is the primary goal of incident management

A. To potect life health and safety
B. To reduce the impacrt of an incident
C. To prepare for any incident
D. To resume interrupted operations as soon as possible

Answer: C

NEW QUESTION 48
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 51
Which is the Not 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. Manacomont

Answer: D

NEW QUESTION 53
Which drives for the IPv6 introduction

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

Answer: C

NEW QUESTION 57
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 62
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 66
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 69
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 70
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 71
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 73
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 74
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 79
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 80
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 82
What is the range of well known ports

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

Answer: A

NEW QUESTION 86
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 91

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 95
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 96
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 98
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 101
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 103
In information systems terms, the activities necessary to restore IT and communications services of an organization during and after an outage

A. IR
B. BC
C. Risk Management
D. DR

Answer: D

NEW QUESTION 105
What security feature used in HTTPS

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

Answer: D

NEW QUESTION 109
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 114
Difference between Sniffing and Snooping

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

Answer: A

NEW QUESTION 116
Which Regulation addresses personal privacy

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

Answer: B

NEW QUESTION 117
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 119
What is the difference between hub and switch

A. A hub is less likely to be used in home network
B. A hub can create separate broad cast domains when used to create Vlan
C. A hub retransmits traffic to all devices, while a switch route traffic to a specific devices
D. A switch retransmits traffic to all devices, while a hub route traffic to a specific devices

Answer: C

NEW QUESTION 123
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 127
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 128
Information should be consistently and readily accessible for authorized parties ?

A. Confidentiality
B. Authentication
C. Availability

D. Non-repudiation

Answer: C

NEW QUESTION 133
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 136
Is an integrated platform and graphical tool for performing security testing of web applications.

A. Burb suite
B. Wireshark C Fiddler
C. ZenMap

Answer: A

NEW QUESTION 141
Which Prevents Threat

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

Answer: A

NEW QUESTION 142
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 146
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 149
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. Reputatuinal risk
C. Operational risk
D. Information risk

Answer: D

NEW QUESTION 153
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 157
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 159
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 164
Which of the following security controls is designed to prevent unauthorized access to sensitive information by ensuring that it is only accessible to authorized users?

A. Encryption
B. Firewall
C. Antivirus
D. Access control

Answer: D

NEW QUESTION 165
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 168
What does a breach refer to in the context of cybersecurity

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

Answer: A

NEW QUESTION 170
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 175
Which layer of OSI the Firewall works

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

Answer: D

NEW QUESTION 179
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 184
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 185
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 186
Hashing used to safe guard which CIA triad

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

Answer: C

NEW QUESTION 188
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 192
What is the primary factor in the reliability of information and system

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

Answer: C

NEW QUESTION 197
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 200
A company network experience a sudden flood of network packets that causes major slowdown in internet traffic. What type of event it this?

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

Answer: D

NEW QUESTION 205
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 206
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 210
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 215
The internet standards organization, made up of network designers, operators, vendors and researchers, that defines protocol standards

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

Answer: C

NEW QUESTION 220
Organization experiences a security event that does not affect the confidentiality integrity and availability of its information system. What term BEST describes this situation?

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

Answer: D

NEW QUESTION 223
What is the main purpose of creating baseline in ensuring system integrity

A. To compare the baseline with the current state of the systems
B. To protect the information
C. To understand the current state of the system
D. AII

Answer: A

NEW QUESTION 228
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 232
A _____ is a distributed denial-of-service (DDoS) attack in which an attacker attempts to flood a targeted server with Internet Control Message Protocol (ICMP) packets.

A. DOS
B. Syn flood
C. Smurf attack
D. Phishing attack

Answer: C

NEW QUESTION 235
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 240
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 241
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 contigency
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 243
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 245
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 246
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 249
An agreement between a cloud service provider and a cloud service customer based on a taxonomy of cloud computing- specific terms

A. Memorandum of Understanding
B. Memorandam on Agreement

C. SLA
D. AII

Answer: C

NEW QUESTION 253
A type of malware that downloads onto a computer disguised as a legitimate program

A. Worm
B. Trojan
C. virus
D. Ransomware

Answer: B

NEW QUESTION 254
The mitigation of violations of security policies and recommended practices

A. DR
B. IR
C. Threat hunting
D. Incident response

Answer: D

NEW QUESTION 259
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 263
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 264
DevOps team has updated the application source code, Tom has discovered that many unauthorized changes have been made. What is the BEST control Tom can implement to prevent a recurrence of this problem?

A. Backup
B. File labels
C. Security audit
D. Hashing

Answer: D

NEW QUESTION 269
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 273
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 275
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 278
Which of the following is often associated with DR planning?

A. Checklists
B. Antivirus
C. firewall
D. AII

Answer: D

NEW QUESTION 282
Security commensurate with the risk and the magnitude of harm resulting from the loss, misuse or unauthorized access to or modification of information

A. Risk Management
B. Risk Assessment
C. Risk Mitigation
D. Adequate Security

Answer: D

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 288
_____ 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 291
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 292
Example of Deterrent controls

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

Answer: A

NEW QUESTION 295
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 298
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 300
Networks are often micro segmented networks, with firewalls at nearly every connecting point

A. DMZ
B. VPN
C. VLAN
D. Zero Trust

Answer: A

NEW QUESTION 301
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 302
Which security control mostly used to prevent data breach

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

Answer: B

NEW QUESTION 304
Why is security training important?

A. Because it fulfills regulatory requirements.
B. Because it helps people to perform their job duties more efficiently.
C. Because it reduces the risk of certain types of attacks, like social engineering.
D. AII

Answer: C

NEW QUESTION 307
Restoring IT and communications back to full operation after a disruption.

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

Answer: C

NEW QUESTION 308
Which of these is an example of deterrent control

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

Answer: B

NEW QUESTION 309
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 312
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 316
Which is strongly used for Securing Wi-Fi

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

Answer: A

NEW QUESTION 321
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 326
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 329
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 331
Which is the first step in the risk management process

A. Risk response
B. Risk mitigation
C. Risk identification
D. Risk assessment

Answer: C

NEW QUESTION 332

A/hich layer of the OSI Layer model is the target of a buffer overflow attack

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

Answer: A

NEW QUESTION 334
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 335
Which type of attack attempts to gain information by observing the devices power consumption

A. DOS
B. Side Channles
C. XSS
D. XSRF

Answer: B

NEW QUESTION 336
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 337
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 341
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
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 343
John joined the ISC2 Organizations, his manager asked to check the authentications in security module. What would John use to ensure a certain control is working as he want and expect it to?

A. Security Testing
B. Security assessment

C. Security audit
D. Security walkthrough

Answer: A

NEW QUESTION 344
What cybersecurity principle focuses on granting users only the privileges necessary to perform their job functions?

A. Least privilege (Correct)
B. defense in depth
C. separation of duties
D. need-to-know basis

Answer: A

NEW QUESTION 349
Permitting authorized access to information while protecting it from improper disclosure

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

Answer: B

NEW QUESTION 354
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 359
Ignoring the risk and proceeding the business operations

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

Answer: A

NEW QUESTION 364
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 366
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 369
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 374
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 378
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 380
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 381
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 384
Who should participate in creation a business continuity plan

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

Answer: D

NEW QUESTION 388
An unknown person obtaining access to the company file system without authorization is example of

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

Answer: B

NEW QUESTION 389
A new BYOD policy has been enforced in NEW Corp which type of control is used to enforce thissecurity policies

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

Answer: C

NEW QUESTION 392
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 396
Port used in DNS

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

Answer: A

NEW QUESTION 399
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 403
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 407
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 408
What is the primary purpose of a honeytoken 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 410
Example of Technical controls

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

Answer: B

NEW QUESTION 414
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 416
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 419
A device that routes traffic to the port of a known device

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

Answer: A

NEW QUESTION 420
Government can imposes financial penalties as a consequence of breaking a

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

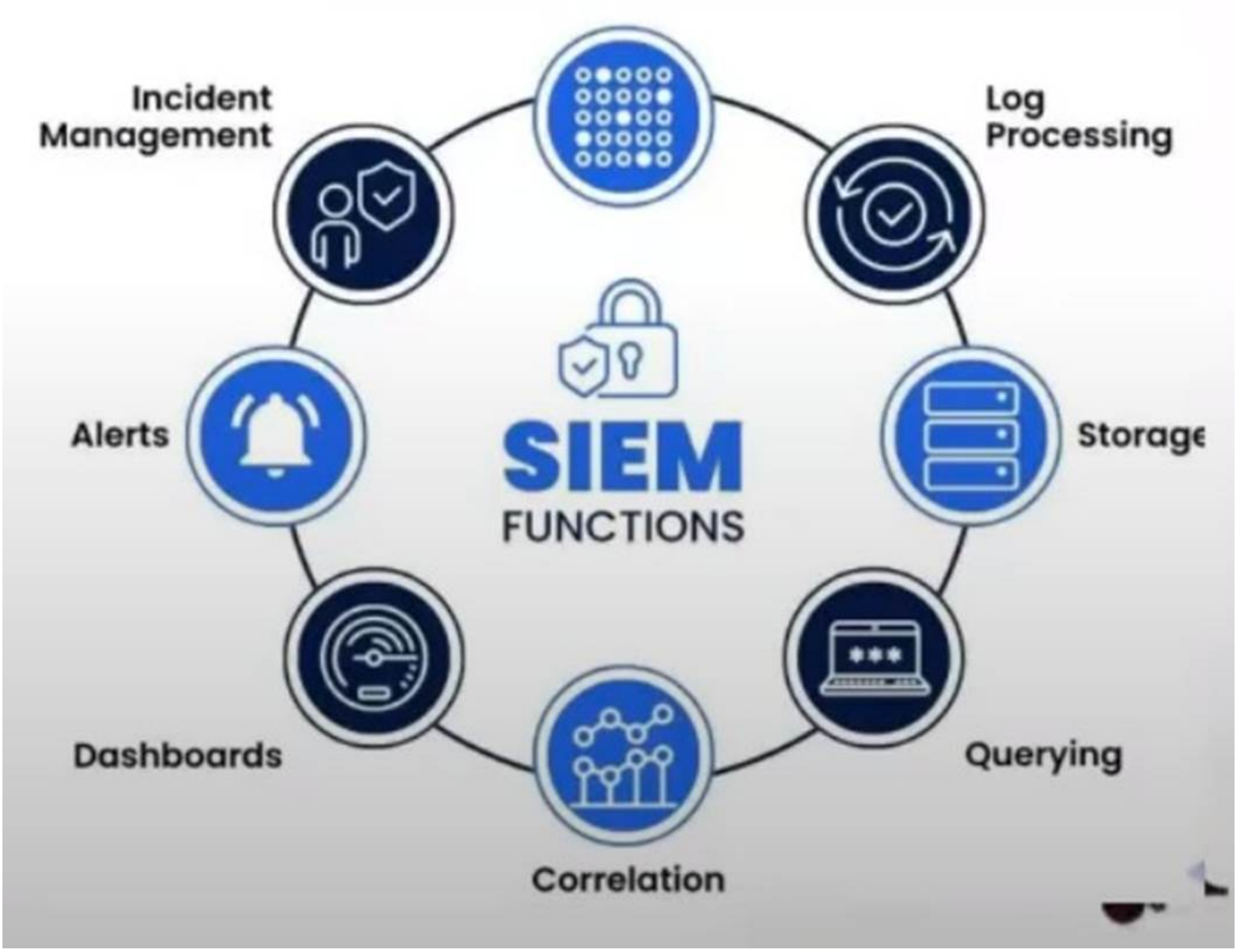
Answer: B

NEW QUESTION 423
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 425
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 430
What principle states that individuals should only have the minimum set of permissions necessary to carry out their job functions?

A. Least privilege
B. Two person control
C. Job rotation
D. Separation of privileges

Answer: A

NEW QUESTION 434
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 435
Load balancing safe guard which CIA triad

A. Confidentiality
B. Availablity
C. Integrity

D. All

Answer: B

NEW QUESTION 439
Protection against an individual falsely denying having performed a particular action

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

Answer: D

NEW QUESTION 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 447
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 449
Devid is worried about distributed denial of service attacks against his company's primary web application, which of the following options will provide the MOST resilience against large-scale ddos attacks?

A. Implement a CDN
B. Increase the number of servers in the web application server cluster
C. Contract for DDoS mitigation services via the company's IPS
D. Increase the amount of bandwidth available from one or more ISPs

Answer: A

NEW QUESTION 453
Raj is considering a physical deterrent control to dissuade unauthorized people from entering the organization's property. Which of the following would serve this purpose?

A. A wall
B. Razor tape
C. A sign
D. A hidden camera

Answer: A

NEW QUESTION 457
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 458
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 459
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 464
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 469
Which is not possible models for an Incident Response Team (IRT):

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

Answer: D

NEW QUESTION 470
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 473
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 477
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 478

The harmonization of automated computing tasks, providing a consolidated and reusable workflow

A. Cloud Orchestration
B. Cloud Manager
C. Cloud broker
D. Cloud Controller

Answer: A

NEW QUESTION 482
A Company critical functions were disrupted due to a system outage. What plan should theorganization have in place to sustain these operations during and after a significant disruptions?

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

Answer: B

NEW QUESTION 483
Token Ring used in which OSI Layer

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

Answer: D

NEW QUESTION 484
Methods or mechanisms cybercriminals use to gain illegal, unauthorized access to computer systems and networks.

A. Attacker
B. Threat Vector
C. Threat
D. Threat actor

Answer: B

NEW QUESTION 488
Which device is used to control traffic flow in network

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

Answer: D

NEW QUESTION 490
.....

THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual CC Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the CC Product From:

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

Money Back Guarantee

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