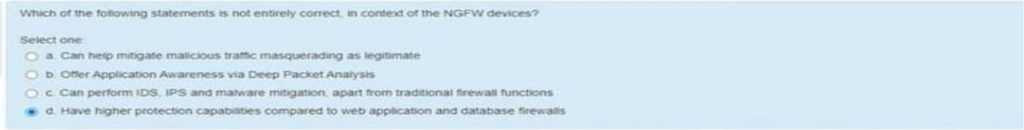
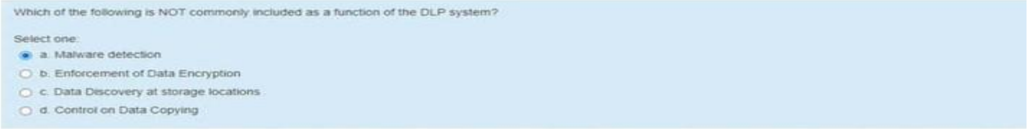
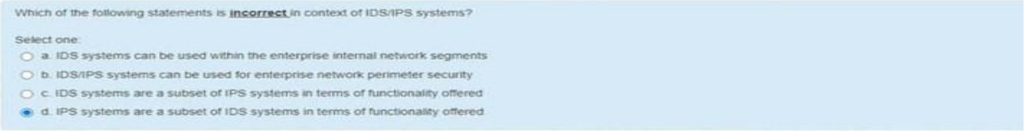

Which of the following statements is not entirely correct, in context of the NGFW devices?

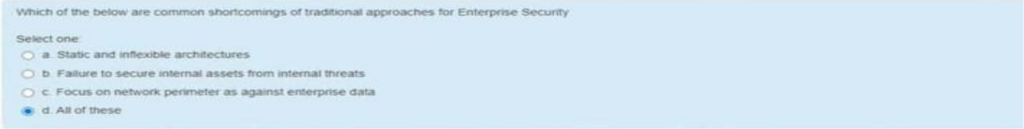
Select one:
○ a. Can help mitigate malicious traffic masquerading as legitimate
○ b. Offer Application Awareness via Deep Packet Analysis
○ c. Can perform IDS, IPS and malware mitigation, apart from traditional firewall functions
● d. Have higher protection capabilities compared to web application and database firewalls


Which of the following is NOT commonly included as a function of the DLP system?

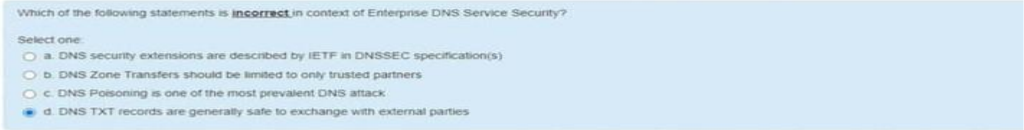
Select one:
● a. Malware detection
○ b. Enforcement of Data Encryption
○ c. Data Discovery at storage locations
○ d. Control on Data Copying


Which of the following statements is **incorrect** in context of IDS/IPS systems?

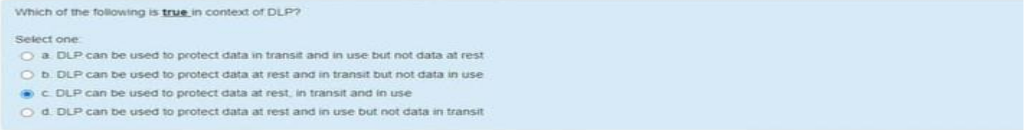
Select one:
○ a. IDS systems can be used within the enterprise internal network segments
○ b. IDS/IPS systems can be used for enterprise network perimeter security
○ c. IDS systems are a subset of IPS systems in terms of functionality offered
● d. IPS systems are a subset of IDS systems in terms of functionality offered


Which of the below are common shortcomings of traditional approaches for Enterprise Security

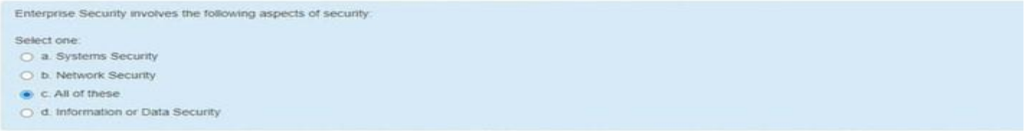
Select one:
○ a. Static and inflexible architectures
○ b. Failure to secure internal assets from internal threats
○ c. Focus on network perimeter as against enterprise data
● d. All of these


Which of the following statements is **incorrect** in context of Enterprise DNS Service Security?

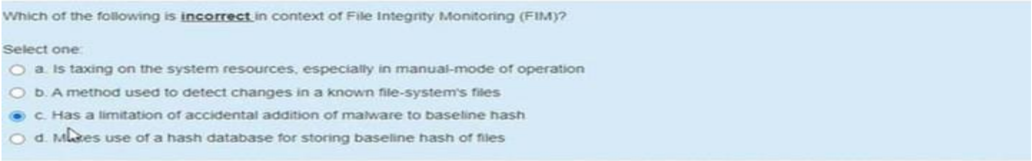
Select one:
○ a. DNS security extensions are described by IETF in DNSSEC specification(s)
○ b. DNS Zone Transfers should be limited to only trusted partners
○ c. DNS Poisoning is one of the most prevalent DNS attack
● d. DNS TXT records are generally safe to exchange with external parties


Which of the following is **true** in context of DLP?

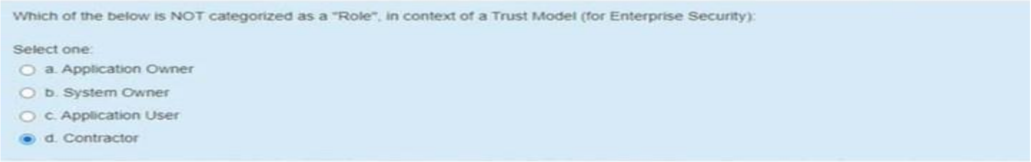
Select one:
○ a. DLP can be used to protect data in transit and in use but not data at rest
○ b. DLP can be used to protect data at rest and in transit but not data in use
● c. DLP can be used to protect data at rest, in transit and in use
○ d. DLP can be used to protect data at rest and in use but not data in transit


Enterprise Security involves the following aspects of security:

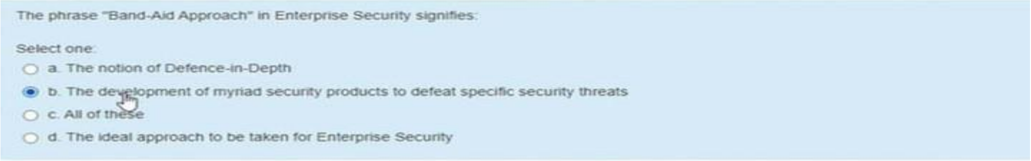
Select one:
○ a. Systems Security
○ b. Network Security
● c. All of these
○ d. Information or Data Security


Which of the following is **incorrect** in context of File Integrity Monitoring (FIM)?

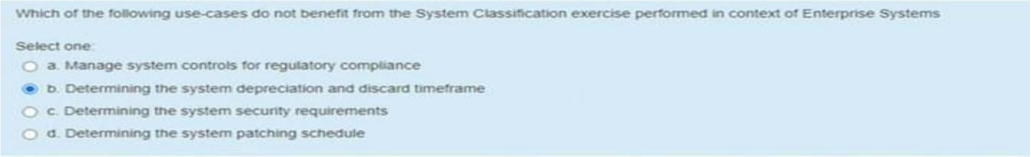
Select one:
○ a. Is taxing on the system resources, especially in manual-mode of operation
○ b. A method used to detect changes in a known file-system's files
● c. Has a limitation of accidental addition of malware to baseline hash
○ d. Makes use of a hash database for storing baseline hash of files


Which of the below is NOT categorized as a "Role", in context of a Trust Model (for Enterprise Security):

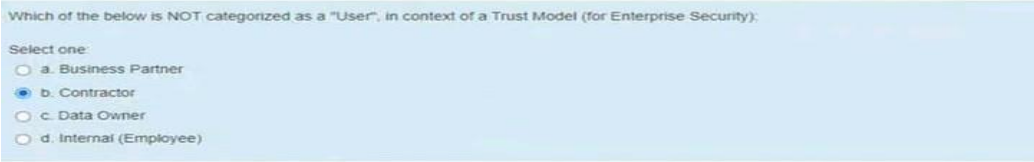
Select one:
○ a. Application Owner
○ b. System Owner
○ c. Application User
● d. Contractor


The phrase "Band-Aid Approach" in Enterprise Security signifies:

Select one:
○ a. The notion of Defence-in-Depth
● b. The development of myriad security products to defeat specific security threats
○ c. All of these
○ d. The ideal approach to be taken for Enterprise Security


Which of the following use-cases do not benefit from the System Classification exercise performed in context of Enterprise Systems

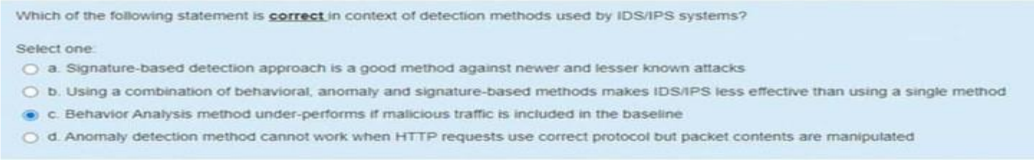
Select one:
○ a. Manage system controls for regulatory compliance
● b. Determining the system depreciation and discard timeframe
○ c. Determining the system security requirements
○ d. Determining the system patching schedule



Which of the below is NOT categorized as a "User", in context of a Trust Model (for Enterprise Security):

Select one:

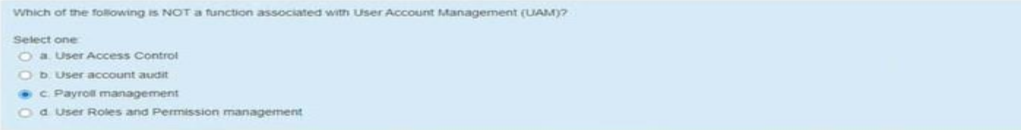
○ a. Business Partner
● b. Contractor
○ c. Data Owner
○ d. Internal (Employee)



Which of the following statement is **correct** in context of detection methods used by IDS/IPS systems?

Select one:

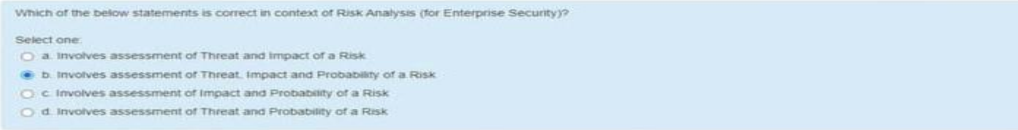
○ a. Signature-based detection approach is a good method against newer and lesser known attacks
○ b. Using a combination of behavioral, anomaly and signature-based methods makes IDS/IPS less effective than using a single method
● c. Behavior Analysis method under-performs if malicious traffic is included in the baseline
○ d. Anomaly detection method cannot work when HTTP requests use correct protocol but packet contents are manipulated



Which of the following is NOT a function associated with User Account Management (UAM)?

Select one:

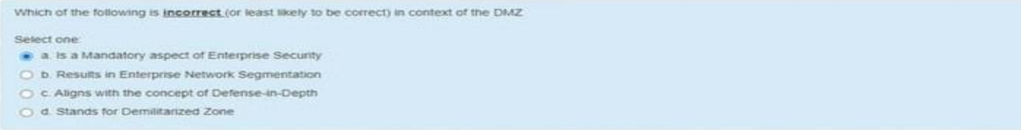
○ a. User Access Control
○ b. User account audit
● c. Payroll management
○ d. User Roles and Permission management



Which of the below statements is correct in context of Risk Analysis (for Enterprise Security)?

Select one:

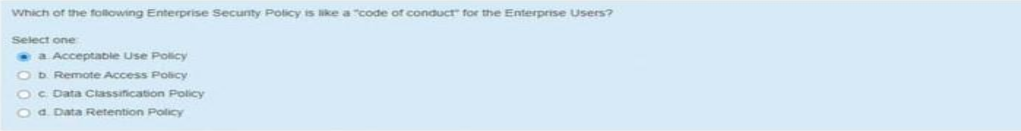
○ a. Involves assessment of Threat and Impact of a Risk
● b. Involves assessment of Threat, Impact and Probability of a Risk
○ c. Involves assessment of Impact and Probability of a Risk
○ d. Involves assessment of Threat and Probability of a Risk



Which of the following is **incorrect** (or least likely to be correct) in context of the DMZ

Select one:

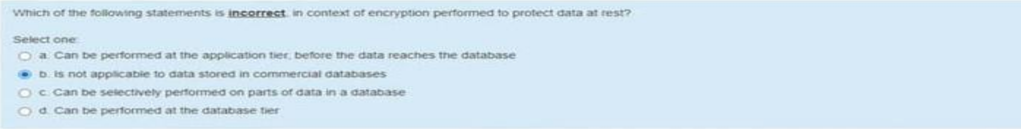
● a. Is a Mandatory aspect of Enterprise Security
○ b. Results in Enterprise Network Segmentation
○ c. Aligns with the concept of Defense-in-Depth
○ d. Stands for Demilitarized Zone



Which of the following Enterprise Security Policy is like a "code of conduct" for the Enterprise Users?

Select one:

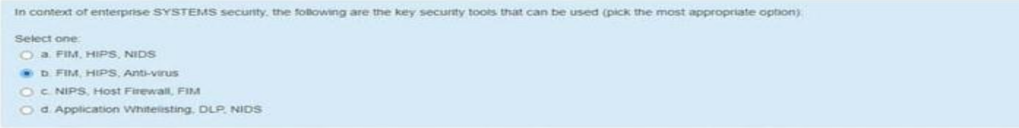
● a. Acceptable Use Policy
○ b. Remote Access Policy
○ c. Data Classification Policy
○ d. Data Retention Policy



Which of the following statements is **incorrect**, in context of encryption performed to protect data at rest?

Select one:

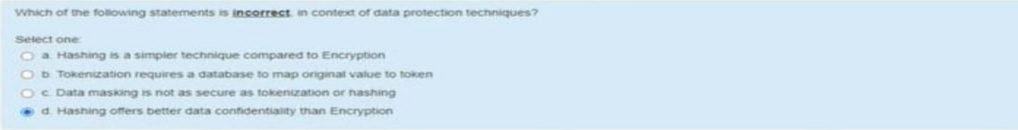
○ a. Can be performed at the application tier, before the data reaches the database
● b. Is not applicable to data stored in commercial databases
○ c. Can be selectively performed on parts of data in a database
○ d. Can be performed at the database tier



In context of enterprise SYSTEMS security, the following are the key security tools that can be used (pick the most appropriate option):

Select one:

○ a. FIM, HIPS, NIDS
● b. FIM, HIPS, Anti-virus
○ c. NIPS, Host Firewall, FIM
○ d. Application Whitelisting, DLP, NIDS



Which of the following statements is **incorrect**, in context of data protection techniques?

Select one:

○ a. Hashing is a simpler technique compared to Encryption
○ b. Tokenization requires a database to map original value to token
○ c. Data masking is not as secure as tokenization or hashing
● d. Hashing offers better data confidentiality than Encryption