

Management 414: SANS CISSP® 10 Domains +S QUIZ -- Domain 7

1. What must be true about audit trails in order to help ensure their admissibility into court?
 - a) They are conducted on a regular basis
 - b) They are synchronized to GMT
 - c) They are in commonly accepted format
 - d) They are safely stored in a central repository
2. What should you do in order to correlate the many logs produced by your different systems?
 - a) Configure for daylight saving changes
 - b) Standardize your systems on 24-hour based GMT
 - c) Store all logs in a common format on a central server
 - d) Use a reliable and accurate time source
3. In the context of intrusion detection, how does integrity checking work?
 - a) By comparing the current hash values of files to their known good hash values
 - b) By monitoring changes to the Modify, Access, and Create (MAC) timestamps of critical files
 - c) By evaluating the properly syntax, field size, and content of network packets
 - d) By verifying the identity and authorization of all requested transactions, sessions, and services
4. What is the most important reason that sensitive audit information should be given proper care?
 - a) It often contains the private data of staff or clients
 - b) To avoid possible second amendment privacy issues
 - c) So as not to alert a suspect to your investigation
 - d) It lists vulnerabilities in your network
5. Which of the following is the MOST efficient deterrent against fraud?
 - a) Firewalls
 - b) Audit Trails
 - c) Vulnerability Assessments
 - d) Armed guards
6. What is usually the first step that should be taken before hiring any given individual?
 - a) Verification of past employment
 - b) Blood test
 - c) Family history
 - d) Interview friends

Management 414: SANS CISSP® 10 Domains +S QUIZ - Domain 7

7. What is one way to cut down on the amount of fraud in the IT department?
 - a) Suspect everyone.
 - b) Install monitoring software on every PC without telling anyone.
 - c) Regularly rotate positions.
8. Which of the following ensures that individuals are responsible for their own actions?
 - a) Encryption
 - b) Auditing
 - c) Virtual Private Network
9. Ensuring that only people that have a need to access certain information or resources will be authorized to do so is an example of:
 - a) Least Privilege
 - b) Need to Know
 - c) Minimal Access
10. Ensuring that only the minimum required access is given at any time is an example of which of the following?
 - a) Need to Know
 - b) Maximum Access
 - c) Least Privilege
 - d) Due Course
11. Policies, standards, guidelines, personnel screening, and security awareness training fall under which of the following control category?
 - a) Preventative controls
 - b) Detective controls
 - c) Directive controls
 - d) Corrective controls
12. Firewalls, encryption, identification, and authentication fall under which of the following control category?
 - a) Preventive controls
 - b) Directive controls
 - c) Corrective controls
 - d) Detective controls
13. Log review, auditing, and integrity checkers fall under which of the following control categories?
 - a) Preventative controls
 - b) Corrective controls
 - c) Detective controls
 - d) Directive controls

Management 414: SANS CISSP® 10 Domains +S QUIZ - Domain 7

14. Instruction manuals and audit trails fall under which of the following control categories?
 - a) Directive controls
 - b) Preventative controls
 - c) Detective controls
 - d) Corrective controls
15. Which of the following monitoring techniques records all keys, and in some cases, all mouse clicks and menu selections while a user is at a computer?
 - a) Sniffer
 - b) Anti-virus
 - c) Keystroke
16. Which of the following is NOT considered a popular widespread monitoring tool or technique?
 - a) Firewall
 - b) Real time
 - c) Ad hoc
 - d) Passive
17. Ensuring that due care is carried out in accordance with best practices of the industry is sometimes referred to as:
 - a) Simple Man rule
 - b) Enforcement Man rule
 - c) Good Man rule
 - d) Prudent Man rule
18. Which of the following cryptographic techniques are usually used to ensure the integrity of information?
 - a) Intrusion Detection Systems
 - b) Digital Signatures
 - c) Firewalls
19. Which of the following is usually NOT the purpose or intention of systems auditing?
 - a) Identify compromise or misuse
 - b) Determine the effectiveness of controls
 - c) Point out the need for additional controls
 - d) Measure the degree of damage
20. Which of the following is commonly used to ensure continuous services by using multiple servers?
 - a) Firewall
 - b) Intrusion Detection System

Management 414: SANS CISSP® 10 Domains +S QUIZ - Domain 7

- c) Anti-Virus
 - d) Load Sharing
21. Which of the following is the common term for backing up and saving information in accordance with laws or corporate guidance?
- a) Audit trail
 - b) Differential backup
 - c) Due diligence
 - d) Records retention
22. Which of the following is MOST effective for insuring that sensitive or classified information is not destroyed or transferred to those without adequate authorization?
- a) Encrypt all classified or proprietary information.
 - b) Apply Public Key Infrastructure (PKI) authentication to all information.
 - c) Perform regular audits of the information classification system.
 - d) Clearly mark the information with its classification.
23. What term refers to the controlling of access to computer facilities and the movement of data within the network?
- a) Operations control
 - b) Access control
 - c) Authentication
 - d) Records retention
24. What would you use to monitor ALL passwords entered on the keyboard?
- a) A software sniffer
 - b) A keyboard driver
 - c) A hardware keyboard adapter
 - d) A keyboard trojan
25. Correctly identifying and authenticating users is referred to as which of the following?
- a) Perimeter defenses
 - b) Intrusion prevention
 - c) Intrusion response
 - d) Egress filtering
26. Measuring the baseline of activity over time and highlighting exceptions is referred to as which of the following?
- a) Heuristic sampling
 - b) Anomaly identification
 - c) Histogram graphing
 - d) Signature identification

Management 414: SANS CISSP® 10 Domains +5 QUIZ - Domain 7

27. Which of the following is necessary in order for audit information to be useful?
- a) It needs to be securely stored.
 - b) It needs to be centrally managed.
 - c) It needs to be available in real-time.
 - d) It needs to be reviewed regularly.
28. Why is it important to manually process part of your logs?
- a) To ensure that your tools are working properly.
 - b) To demonstrate due diligence.
 - c) To verify that the log files are readable.
 - d) To remain familiar with the details of the process.
29. Why is it important to collect all logs at a centralized logging host?
- a) To allow for system wide reporting of pre-attack activity.
 - b) To provide manageable review and retention of logs.
 - c) To prevent attackers from covering their tracks by deleting logs.
 - d) To create redundant copies for disaster recovery.
30. In view of the legal implications associated with the security oriented actions taken by a company or individual, which of the following is most important?
- a) Interfacing with those who can provide the proper expertise
 - b) Understanding the relevant legal requirements, limitations, and penalties
 - c) Documenting in detail your actions, intentions, and the results
 - d) Give prior notification to your management and legal department of the actions, and their rational, you intend to take
31. Which of the following choices best describes the process of watching for anomalies in an established network activity baseline?
- a) Baseline analysis
 - b) Anomaly analysis
 - c) Passive network analysis
 - d) Traffic analysis
32. What is the difference between network traffic analysis and network trend analysis?
- a) Traffic analysis looks at the general activity patterns of specific types of traffic
 - b) Trend analysis looks at general indicators over a longer time period
 - c) Traffic analysis is based on an anomaly baseline that can be compared to subsequent network activity
 - d) Trend analysis is based on the anticipated statistics for a given network

Management 414: SANS CISSP® 10 Domains +S QUIZ - Domain 7

33. Which are the three common types of intrusion detection?

- a) Stealth, anomaly identification, and host based
- b) Host based, network based, and signature identification
- c) Packet filtering, stateful inspection, and proxy
- d) Integrity checking, anomaly identification, and attack signature identification