Name:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Date:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Security Systems Analysis Exam**

|  |  |  |  |
| --- | --- | --- | --- |
| **Matching** |  |  |  |
| a. Access controls | m. Passphrase |
| b. Access credentials | n. Preventative administrative controls |
| c. | Authentication | o. Preventative physical controls |
| d. | Authorization | p. Preventative technical controls |
| e. | Biometrics | q. Profile-based anomaly detection |
| f. | Centralized access control administration | r. | Security awareness |
| g. | Console | s. | Security survey |
| h. | Contact chip | t. | Sensor |
| i. | Contactless chip | u. | Signature detection |
| j. | Cryptographic keys | v. | Statistical anomaly detection |
| k. | Identification | w. | Surveillance cameras |
| l. | Intrusion detection system | x. | Threshold detection |
| 1.\_\_\_\_\_ | An attitude held by security personnel and by non-security client employees that |
|  | places a high value on detecting, deterring and reporting security exposures such as crime, safety hazards, fire hazards, theft , intrusions, and |
|  | vandalism |
| 2.\_\_\_\_\_ | A program that monitors a system for malicious activity and in turn reports that activity |
| 3.\_\_\_\_\_ | A program that monitors a system by analyzing previous system patterns and |
|  | analyzing current system patterns that are highly deviated from an individual user’s activity  |
| 4.\_\_\_\_\_ | Includes policies, hiring practices, and security awareness |
| 5.\_\_\_\_\_ | Cryptographic operations in which a string of bits are used by a cryptographic |
|  | be read through private keys or digital signatures |
| 6.\_\_\_\_\_ | Method used to verify a person’s identity |
| 7.\_\_\_\_\_ | Access to a location and/or information that is granted to a proven individual |
| 8.\_\_\_\_\_ | A program that records by counting the number of times that an incident occurs within a system |
| 9.\_\_\_\_\_ | Are capable of obtaining 24-hour steady video |  |
| 10.\_\_\_\_\_ | Used to identify potential security-related problem areas |

11.\_\_\_\_\_ Used in conjunction with access controls, typically in the form of card readers and access cards

12.\_\_\_\_\_ A program that monitors the normal activity of a system and then informs the user if unusual or anomalous activity is detected

13.\_\_\_\_\_ A small integrated circuit that functions through wireless technology

14.\_\_\_\_\_ A program that scans a system against already known computer viruses, malware, or attacks, and alerts the user if an attack in detected

15.\_\_\_\_\_ A security device that allows the user and the system to communicate with each other; includes a controller, a card reader, door contacts, and a control locking device

16.\_\_\_\_\_ A statement, phrase or series of words that replaces a password and is used for access to a computer system

17.\_\_\_\_\_ A device that detects some form of input/information (i.e. motion, light, heat) and sends the information to the console

18.\_\_\_\_\_ Access control that is administered and controlled at one location

19.\_\_\_\_\_ Identity confirmation

20.\_\_\_\_\_ Includes passwords, encryption, and antivirus software

21.\_\_\_\_\_ A control unit that an individual uses to communicate with a computer system that also works together with sensors; includes a display and a keyboard

22.\_\_\_\_\_ Authorization and access that is based on an individual’s unique characteristics including handprints, fingerprints or retinal scans

23.\_\_\_\_\_ Includes badges, swipe cards, guards, and fences

24.\_\_\_\_\_ A small integrated circuit which must come in contact with a reader in order for the two to communicate with each other

**Multiple Choice**

25.\_\_\_ With security awareness, security personnel protect which of the following?

* 1. The client’s employees
	2. The client’s property
	3. The client’s image
	4. All of the above
1. \_\_\_ The three initial steps taken with a security threat do not include which of the following?
	1. Identify the threat
	2. Ask for a second opinion on the threat
	3. Report the threat
	4. Discuss and develop a solution that eliminates the threat
2. \_\_\_ Although access controls can take many forms, the term as it is applied in the traditional security industry means\_\_\_\_\_\_\_\_\_\_\_, as opposed to something such as a fence or turnstile.
	1. Physical Security
	2. Intrusion Detection Systems
	3. Electronic access control systems
	4. Surveillance Systems
3. \_\_\_ A typical access control system has which of the following?
	1. Controller
	2. Credential reader
	3. Door position contacts
	4. All of the above
4. \_\_\_ Distinct functions of security and access control do not include which of the following?
	1. Installation
	2. Identification
	3. Authorization
	4. Authentication
5. \_\_\_ Security systems, by their very nature, use which of the following?
	1. Centralization
	2. Integration
	3. Suspicion
	4. Transmission
6. \_\_\_ Which of the following takes the place of a password?
	1. Passphrase
	2. Authentication
	3. Signature Detection
	4. Access Controls
7. \_\_\_ Which of the following contains a small integrated circuit?
	1. Biometrics
	2. Console
	3. Contact chip
	4. Cryptographic Keys
8. \_\_\_ When a match is found, an alert is sent for further actions; which of the following does this describe?
	1. Threshold detection
	2. Profile based anomaly detection
	3. Centralized Access Control Administration
	4. Signature Detection
9. \_\_\_ Which of the following has a controller, credential reader, door position contacts, and means of controlling the locking device or door operator?
	1. Surveillance Cameras
	2. Access Controls
	3. Contactless Chip
	4. Sensor
10. \_\_\_ Which of the following is technology that has moved into the mainstream with the development of RFID, which uses RF induction and transmission?
	1. Contactless chip
	2. Cryptographic Keys
	3. Sensor
	4. Surveillance Cameras