**Question 1**

**0 / 1.5 pts**

Joanna's organization has a policy that requires a user's password to be immediately reset to lock accounts if the account is determined to have been successfully phished. What type of control is this?

A detective control

**Correct Answer**

A directive control

**You Answered**

A preventive control

A compensating control

**Question 2**

**1.5 / 1.5 pts**

What technology is record-level encryption most commonly associated with?

Stored audio files

**Correct!**

Databases

Physical disks

Removable storage

**Question 3**

**1.5 / 1.5 pts**

Brandon wants to deploy a detective control that will help him with physical security threats. Which of the following fits his needs?

Fencing

**Correct!**

Video surveillance

Bollards

Lighting

**Question 4**

**1.5 / 1.5 pts**

Which of the following is not a major concern related to downtime caused by patching and system updates?

Security systems or functions being offline during restart or shutdown processes

Unexpected extended downtime

**Correct!**

Attackers compromising the system or service while it is offline

Dependencies between systems or services related to downtime

**Question 5**

**1.5 / 1.5 pts**

The web server that Angela's organization manages was recently compromised and the SSL certificate's private key was accessed by attackers. Angela's team has completed remediation and has created a new CSR, including a new private key that they have secured. What type of control type best describes the creation of a new key and certificate in this circumstance?

**Correct!**

Corrective

Detective

Compensating

Deterrent

**Question 6**

**1.5 / 1.5 pts**

Gary has implemented record-level encryption for his database. How many keys will he use in a typical implementation of record-level encryption?

One key per table

**Correct!**

One key per record

One key per database

One key per column

**Question 7**

**1.5 / 1.5 pts**

Brian's organization uses a process where a secure module boots systems, then monitors them as each boot stage proceeds. It validates each signed boot stage and reports on whether the boot process was correct or not when complete. What is the secure module used to verify these stages called?

A secure initiation manager

A boot hash

**Correct!**

A root of trust

A cryptographic boot manager

**Question 8**

**1.5 / 1.5 pts**

Murali has deployed a file integrity monitoring tool and has configured alerts to notify him if files are modified. What control type best describes this solution?

Directive

Deterrent

**Correct!**

Detective

Preventive

**Question 9**

**1.5 / 1.5 pts**

Which of the following sensor types is commonly used to detect footsteps?

Infrared

**Correct!**

Pressure

Ultrasonic

Microwave

**Question 10**

**1.5 / 1.5 pts**

Valerie's organization has deployed a zero-trust solution, and Valerie receives an authentication prompt when she is attempting to access a file server. What component of the zero-trust architecture is she interacting with?

The trust manager

A policy administrator

The policy engine

**Correct!**

A policy enforcement point

**Question 11**

**1.5 / 1.5 pts**

Quentin wants to deploy a single sign-on system to allow his users to log in to cloud services. Which of the following technologies is he most likely to deploy?

**Correct!**

OpenID

TACACS+

LDAP

Kerberos

**Question 12**

**1.5 / 1.5 pts**

Valerie wants to use a certificate to handle multiple subdomains for her website, including the sales.example.com and support.example.com subdomains. What type of certificate should she use?

A CRL certificate

**Correct!**

A wildcard certificate

A self-signed certificate

A root of trust certificate

**Question 13**

**1.5 / 1.5 pts**

Which of the following is not true for a secure cryptographic hash system?

**Correct!**

Hashes may generate the same output for multiple inputs.

Hashes are a one-way function.

Hashes are commonly used to verify the integrity of files.

Hashes generate a fixed length output.

**Question 14**

**0 / 1.5 pts**

Log monitoring is an example of what control category?

**You Answered**

Technical

**Correct Answer**

Operational

Physical

Managerial

**UnansweredQuestion 15**

**0 / 1.5 pts**

What role does a subordinate CA have in a CA hierarchy?

**Correct Answer**

Subordinate CAs provide control over certificate issuance while avoiding the cost of being a root CA.

Subordinate CAs review certificate signing requests before forwarding them to the root CA.

Subordinate CAs issue certificates based on subdomains.

Subordinate CAs validate root CA activities to ensure auditability.

**UnansweredQuestion 16**

**0 / 1.5 pts**

Isaac wants to deploy sensors to detect intruders in a facility, but he is concerned about the sensors being overly sensitive. What type of sensor is best suited to detecting intruders in an open office environment without significant expense or issues with sensitivity?

Ultrasonic

Microwave

Pressure

**Correct Answer**

Infrared

**UnansweredQuestion 17**

**0 / 1.5 pts**

Ilya wants to create a certificate signing request. Which of the following is not a typical part of a CSR?

**Correct Answer**

The organization's phone number

A contact email address

The organization's legal name

The common name of the server

**UnansweredQuestion 18**

**0 / 1.5 pts**

What data obfuscation technique relies on a lookup table that allows you to match the data you want to secure to a randomly generated value to ensure that the actual value is not easily accessible?

Hashing

**Correct Answer**

Tokenization

Randomization

Masking

**UnansweredQuestion 19**

**0 / 1.5 pts**

Annie notices that her browser shows that the certificate for the site she is visiting is not valid. After performing some checks, she sees that the certificate is on the CA's certificate revocation list. Which of the following is not a reason for a certificate to be on a CRL?

The certificate's private key was compromised.

**Correct Answer**

The certificate expired.

The CA is compromised.

The certificate was signed with a stolen key.

**UnansweredQuestion 20**

**0 / 1.5 pts**

Jared wants to estimate the downtime that will result as part of a planned change. Which of the following methods will most effectively help him estimate downtime?

Average the downtime from other recent changes.

Contact the vendor for time estimates for the change.

Use a fixed maintenance window.

**Correct Answer**

Perform the change in a test environment.

Part 2

What advantage do microwave sensors have over infrared sensors?

They do not interfere with sensitive equipment.

They can detect heat signatures.

**Correct!**

They can penetrate some types of walls.

They are cheaper than infrared sensors.

**Question 2**

**1.5 / 1.5 pts**

Adam has been asked to implement an allow list for websites that his servers can visit. What concern should he raise about the implementation of allow lists?

Allow lists do not prevent sites from being visited if they are not on the allow list.

Allow lists are prone to error, allowing unwanted sites to be added.

Allow lists cannot be configured to allow entire domains to be visited, creating significant overhead.

**Correct!**

Allow lists can be difficult to manage and cause failures if sites that are needed are not added.

**Question 3**

**1.5 / 1.5 pts**

Which of the following activities should Alaina not restrict as part of her preparation for a change window?

Patching

**Correct!**

Scaling clustered systems up or down

Modifying database configurations

Changing hostnames

**Question 4**

**1.5 / 1.5 pts**

What are considerations like database and network connectivity, authentication system access, and network time availability considered in the context of change management processes?

Standard operating procedures

Allowed services

Denied services

**Correct!**

Dependencies

**Question 5**

**0 / 1.5 pts**

Christina wants to implement a physical security control that has the greatest flexibility in how it is applied because she knows that exceptions to security practices may be required at times. Which of the following solutions has the greatest flexibility?

**Correct Answer**

Security guards

Access control vestibules

Access badges

**You Answered**

Video surveillance

**Question 6**

**1.5 / 1.5 pts**

Frank configures an access control list to ensure that only specific IP addresses are able to connect to a service. What type of control has he deployed?

Managerial

Physical

**Correct!**

Technical

Operational

**Question 7**

**1.5 / 1.5 pts**

What data obfuscation technique relies on a lookup table that allows you to match the data you want to secure to a randomly generated value to ensure that the actual value is not easily accessible?

Masking

Randomization

**Correct!**

Tokenization

Hashing

**Question 8**

**1.5 / 1.5 pts**

Charles wants to reduce the threat scope of compromised credentials. What type of the following security controls is best suited to meeting this need?

Single sign-on

Federation

Multifactor authentication (MFA)

**Correct!**

Zero trust

**Question 9**

**1.5 / 1.5 pts**

Christina wants to authenticate individuals as part of her AAA implementation. What will she need to do to authenticate users?

Use identity proofing for each user she creates.

**Correct!**

Ensure that users provide an identity and one or more authentication factors.

Match users to roles and ensure that rights are assigned.

Conduct biometric enrollments for every user.

**Question 10**

**1.5 / 1.5 pts**

What challenge drives the need for key exchange mechanisms?

**Correct!**

The need to exchange keys in a way that prevents others from obtaining a copy

The number of keys required for symmetric encryption

The need to determine if a key is public

The need to securely return keys to their owner after they are traded

**Question 11**

**1.5 / 1.5 pts**

What term describes a collection of honeypots on a network intended to capture information about cybersecurity threats?

A darknet

**Correct!**

A honeynet

A honeyfarm

A honeycluster

**Question 12**

**1.5 / 1.5 pts**

Anna has been told that her organization has deployed microwave sensors in the organization's warehouses. What are microwave sensors most frequently used to detect?

Glass break

Heat signatures

Pressure

**Correct!**

Motion

**Question 13**

**1.5 / 1.5 pts**

Jacob is concerned that the password used for one of his organization's services is weak, and he wants to make it harder to crack by making it harder to test possible keys during a brute-force attack. What is this technique called?

**Correct!**

Key stretching

Master keying

Key rotation

Passphrase armoring

**Question 14**

**1.5 / 1.5 pts**

What term describes the function of digital signatures related to proving that the signature was provided by the owner of a given private key?

Key stretching

**Correct!**

Nonrepudiation

Ledger-based validation

Authentication

**Question 15**

**1.5 / 1.5 pts**

Casey wants to prevent tailgating attacks on her datacenter. What type of physical security solution should she put in place?

Video surveillance

**Correct!**

An access control vestibule

Access badges

Bollards

**Question 16**

**1.5 / 1.5 pts**

Gary has implemented record-level encryption for his database. How many keys will he use in a typical implementation of record-level encryption?

One key per column

**Correct!**

One key per record

One key per table

One key per database

**Question 17**

**0 / 1.5 pts**

Isaac is conducting a physical penetration test and wants to bypass an access control vestibule. What must he accomplish?

**Correct Answer**

He needs to persuade an individual to allow him to follow them through two doors in a row.

He needs to acquire the individual's access PIN.

He needs to acquire an individual's access card.

**You Answered**

He needs to persuade an individual to allow him to follow them through a single door.

**Question 18**

**0 / 1.5 pts**

When is data on a drive that uses full-disk encryption at the greatest risk?

**You Answered**

During the system boot process

**Correct Answer**

When the system is logged in and in use

When the system is off

When the system is being shut down

**Question 19**

**1.5 / 1.5 pts**

Mahmoud has been asked to implement an allow list for websites that users at his company can visit. What concern should he bring up to management due to this request?

Allow lists are overly permissive and are likely to allow unwanted sites to be visited.

Allow lists cannot be used for websites.

**Correct!**

Using an allow list for websites will take a lot of time to maintain.

Using an allow list for websites is easily bypassed.

**Question 20**

**1.5 / 1.5 pts**

Rick checks the certificate for the site he is viewing and sees that it reads \*.example.com. What type of certificate is this, and why is it in use?

**Correct!**

It is a wildcard certificate and is used for multiple subdomains.

It is a self-signed certificate, and it is used for testing purposes.

It is a self-signed certificate and is used for multiple subdomains.

It is a wildcard certificate and is used for testing purposes.

Part 3