

1.

Distributed databases, data warehouses, big data, and File shares are all classified as what?

1 point

☒

Data source types

☐

Data center types

☐

Database types

☐

Data models
2.

Hadoop, MongoDB, and BigTable are all examples of which data source type?

1 point

☐

Data warehouses

☐

File Shares

☒

Big data databases

☐

Distributed databases
3.

Data that has been organized into a formatted repository, typically a database, so its elements can be made addressable, is an example of which data model type?

1 point

☐

Semi-structured data

☐

Structureless data

☒

Structured data

☐

Unstructured data
4.

Which of the following is the primary difference between a flat file database and a relational database?

1 point

☒

All the data in a flat file database is stored in a single table.

☐

Flat file databases consist of a table that references internally stored files.

☐

Flat file databases consist of a table that references externally stored files.

☐

All the data in a relational database is stored in a single table.
5.

In the video *Securing the Crown Jewels*, the "Real-Time Monitor & Protection" phase contains which three (3) of the following items?

1 point

☒

Activity Monitoring

☒

Blocking & Quarantine

☒

Dynamic Data Masking

☐

Vulnerability Assessment

☐

Reconfigure, Mask & Encrypt
6.

In the video *Leveraging Security Industry Best Practices*, where would you turn to look for help on establishing security benchmarks for your database?

1 point

☐

Common Vulnerability and Exposures (CVE).

☒

Center for Internet Security (CIS).

☐

Central Intelligence Agency (CIA).

☐

Department of Defense/Defence Information Systems Agency (DoD/DISA).
7.

Most of the time, how do users access data?

1 point

☐

Through a database client.

☒

Through an application.

☐

Directly from a database.

☐

Directly from a hardened repository.
8.

True or False: In a vulnerability assessment test, it is not uncommon to fail more than 50% of the tests before the operating system and database are hardened.

1 point

☒

True

☐

False
9.

Which of these hosting environments requires the service provider to manage the largest number of different data sources?

1 point

☒

On Premises

☐

PaaS

☐

IaaS

☐

SaaS
10.

While data security is an ongoing process, what is the correct order to consider these steps?

1 point

☐

Identification & Baseline,Real-time Monitor & Protection, Raise the Bar

☐

Raise the Bar, Identification & Baseline, Real-time Monitor & Protection

☒

Identification & Baseline, Raise the Bar, Real-time Monitor & Protection

☐

Real-time Monitor & Protection, Identification & Baseline, Raise the Bar
11.

To automatically terminate a session if an attempt is made to access data in a sensitive table, such as Social Security (SSN) ID numbers, you would set up which type of rule?

1 point

☒

An Access rule.

☐

An Aggregator rule.

☐

An Exclude rule.

☐

An Exception rule.
12.

True or False: Data monitoring products such as IBM Guardium are fully capable of blocking access to sensitive data based upon access parameters configured in policy rules.

1 point

☒

True

☐

False
13.

In which two (2) ways can security events collected by a data monitoring tool be logged to a security incident and event management (SIEM) system?

1 point

☒

Configure bidirectional communication between the monitoring and SIEM systems, if available.

☐

Configure your SIEM system to read the monitoring systems local syslog file.

☐

Export security events from your monitoring tool and import them into your SIEM tool.

☒

Configure the monitoring system to write to the SIEM systems syslog file.
14.

True or False: Data monitoring tools such as IBM Guardium are designed to monitor activities within a database, but external products, such as a privileged identity management (PIM) tool would be required to monitor changes to the data monitoring tool itself, such as the addition of new users or the alteration of existing user accounts.

1 point

☐

True

☒

False
15.

True or False: In the IBM Guardium data monitoring tool, it is possible to create a report that shows not only how many SQL unauthorized access attempts were made by an individual, but also exactly which SQL statements were disallowed.

1 point

☒

True

☐

False
16.

Which activity should be considered suspicious and might indicate inappropriate activity is being attempted?

1 point

☒

Attempts are made to SELECT lists of usernames and passwords by a non-administrator account.

☐

Data accessed by an accounting application dramatically increases in the last few days of every month.

☐

A known user attempts to run invalid SQL statements against data his ID is authorized to access.

☐

A user routinely enters the incorrect password once or twice before entering the correct password for his account.
17.

Which two (2) activities should be considered suspicious and warrant further investigation?

1 point

☒

There were attempts to purge event logs.

☐

An authorized user attempts to run SQL statements with invalid syntax.

☒

The data monitoring logging system was manually shut down.

☐

It takes an authorized user 3 attempts to enter the correct password.

Coursera Honor Code

[Learn more](#)

[↗](#)

☒

I, **Giang Pham**, understand that submitting work that isn't my own may result in permanent failure of this course or deactivation of my Coursera account.

Submit

Save draft