DirectCertify

Unlock Your Potential, Certify Your Success

CertNexus

AIP-210 Exam

CertNexus Certified Artificial Intelligence Practitioner Exam

Exam Latest Version: 6.1

DEMO Version

Full Version Features:

• 90 Days Free Updates

• 30 Days Money Back Guarantee

• Instant Download Once Purchased

• 24 Hours Live Chat Support

Full version is available at link below with affordable price.

https://www.directcertify.com/certnexus/aip-210

Question 1. (Single Select)

You and your team need to process large datasets of images as fast as possible for a machine learning task. The project will also use a modular framework with extensible code and an active developer community. Which of the following would BEST meet your needs?

A: Caffe
B: Keras
C: Microsoft Cognitive Services
D: TensorBoard

Correct Answer: A

Explanation:

Caffe is a deep learning framework that is designed for speed and modularity. It can process large datasets of images efficiently and supports various types of neural networks. It also has a large and active developer community that contributes to its code base and documentation. Caffe is suitable for image processing tasks such as classification, segmentation, detection, and recognition

Question 2. (Multi Select)

Which three security measures could be applied in different ML workflow stages to defend them against malicious activities? (Select three.)

A: Disable logging for model access.
B: Launch ML Instances In a virtual private cloud (VPC).
C: Monitor model degradation.
D: Use data encryption.
E: Use max privilege to control access to ML artifacts.
F: Use Secrets Manager to protect credentials.

Correct Answer: B, D, F

Explanation:

Security measures can be applied in different ML workflow stages to defend them against malicious activities, such as data theft, model tampering, or adversarial attacks. Some of the security measures are:

Launch ML Instances In a virtual private cloud (VPC): A VPC is a logically isolated section of a cloud provider's network that allows users to launch and control their own resources. By launching ML instances in a VPC, users can enhance the security and privacy of their data and models, as well as restrict the access and traffic to and from the instances.

Use data encryption: Data encryption is the process of transforming data into an unreadable format using a secret key or algorithm. Data encryption can protect the confidentiality, integrity, and availability of data at rest (stored in databases or files) or in transit (transferred over networks). Data encryption can prevent unauthorized access, modification, or leakage of sensitive data.

Use Secrets Manager to protect credentials: Secrets Manager is a service that helps users securely store, manage, and retrieve secrets, such as passwords, API keys, tokens, or certificates. Secrets Manager can help users protect their credentials from unauthorized access or exposure, as well as rotate them automatically to comply with security policies.

Question 3. (Multi Select)

Which three security measures could be applied in different ML workflow stages to defend them against malicious activities? (Select three.)

A: Disable logging for model access.
B: Launch ML Instances In a virtual private cloud (VPC).
C: Monitor model degradation.
D: Use data encryption.
E: Use max privilege to control access to ML artifacts.
F: Use Secrets Manager to protect credentials.

Correct Answer: B, D, F

Explanation:

Security measures can be applied in different ML workflow stages to defend them against malicious activities, such as data theft, model tampering, or adversarial attacks. Some of the security measures are:

Launch ML Instances In a virtual private cloud (VPC): A VPC is a logically isolated section of a cloud provider's network that allows users to launch and control their own resources. By launching ML instances in a VPC, users can enhance the security and privacy of their data and models, as well as restrict the access and traffic to and from the instances.

Use data encryption: Data encryption is the process of transforming data into an unreadable format using a secret key or algorithm. Data encryption can protect the confidentiality, integrity, and availability of data at rest (stored in databases or files) or in transit (transferred over networks). Data encryption can prevent unauthorized access, modification, or leakage of sensitive data.

Use Secrets Manager to protect credentials: Secrets Manager is a service that helps users securely store, manage, and retrieve secrets, such as passwords, API keys, tokens, or certificates. Secrets Manager can help users protect their credentials from unauthorized access or exposure, as well as rotate them automatically to comply with security policies.

Question 4. (Single Select)

A healthcare company experiences a cyberattack, where the hackers were able to reverse-engineer a dataset to break confidentiality.

Which of the following is TRUE regarding the dataset parameters?

A: The model is overfitted and trained on a high quantity of patient records.
B: The model is overfitted and trained on a low quantity of patient records.
C: The model is underfitted and trained on a high quantity of patient records.
D: The model is underfitted and trained on a low quantity of patient records.

Correct Answer: B

Explanation:

Overfitting is a problem that occurs when a model learns too much from the training data and

fails to generalize well to new or unseen data. Overfitting can result from using a low quantity of training data, a high complexity of the model, or a lack of regularization. Overfitting can also increase the risk of reverse-engineering a dataset from a model's outputs, as the model may reveal too much information about the specific features or patterns of the training data. This can break the confidentiality of the data and expose sensitive information about the individuals in the dataset .

Question 5. (Single Select)

When working with textual data and trying to classify text into different languages, which approach to representing features makes the most sense?

A: Bag of words model with TF-IDF
B: Bag of bigrams (2 letter pairs)
C: Word2Vec algorithm
D: Clustering similar words and representing words by group membership

Correct Answer: B

Explanation:

A bag of bigrams (2 letter pairs) is an approach to representing features for textual data that involves counting the frequency of each pair of adjacent letters in a text. For example, the word "hello" would be represented as {"he": 1, "el": 1, "ll": 1, "lo": 1}. A bag of bigrams can capture some information about the spelling and structure of words, which can be useful for identifying the language of a text. For example, some languages have more common bigrams than others, such as "th" in English or "ch" in German .

DirectCertify

Unlock Your Potential, Certify Your Success

Full version is available at link below with affordable price.

https://www.directcertify.com/certnexus/aip-210

30% Discount Coupon Code: LimitedTime2025