Advanced Skill Certificate in Online Gaming Analytics

Game Data Security and Privacy.

API (Application Programming Interface)

An API is a set of rules and protocols that enables different software applications to communicate with each other. In the context of game data security and privacy, APIs are often used to facilitate the transfer of data between different systems, such as between a game client and a server. APIs can be a potential point of vulnerability for data breaches, so it is important to ensure that they are properly secured.

Authentication

Authentication is the process of verifying the identity of a user, device, or system. In the context of game data security and privacy, authentication is used to ensure that only authorized users have access to sensitive data. Common methods of authentication include passwords, two-factor authentication, and biometric data.

CCPA (California Consumer Privacy Act)

The CCPA is a data privacy law that went into effect in California in 2020. It gives residents of California the right to know what personal data is being collected about them, the right to request that their data be deleted, and the right to opt out of the sale of their personal data. Game companies that collect personal data from California residents must comply with the CCPA.

Data Encryption

Data encryption is the process of converting plaintext data into a coded form that cannot be read by unauthorized users. This is an important security measure for protecting sensitive game data, such as player account information and financial transactions. There are two main types of encryption: symmetric encryption, which uses the same key for encryption and decryption, and asymmetric encryption, which uses a public key for encryption and a private key for decryption.

Data Privacy

Data privacy is the practice of protecting personal data from unauthorized access, use, or disclosure. In the context of online gaming, data privacy is an important concern due to the sensitive nature of the data that is collected from players, such as their names, addresses, and financial information. Game companies must take appropriate measures to ensure the privacy of this data, such as encrypting it and limiting access to it.

GDPR (General Data Protection Regulation)

The GDPR is a data privacy law that went into effect in the European Union in 2018. It gives residents of the EU the right to know what personal data is being collected about them, the right to request that their data be deleted, and the right to opt out of the sale of their personal data. Game companies that collect personal

data from EU residents must comply with the GDPR.

Hashing

Hashing is a one-way function that maps data of arbitrary size to a fixed size. It is often used for storing passwords, as it allows for the verification of a password without actually storing the password itself. Instead, the password is hashed and the hash value is stored. When a user attempts to log in, their password is hashed and compared to the stored hash value.

Intrusion Detection System (IDS)

An IDS is a system that monitors network traffic for signs of malicious activity, such as attempts to access unauthorized data or launch a denial-of-service attack. When an IDS detects suspicious activity, it can alert system administrators or take automated action to stop the attack.

Penetration Testing

Penetration testing is the practice of simulating a cyber attack on a system in order to identify vulnerabilities that could be exploited by attackers. It is an important part of a comprehensive security strategy for game data, as it allows organizations to identify and address potential security weaknesses before they can be exploited.

Personal Data

Personal data is any information that can be used to identify a specific individual, such as their name, address, or financial information. In the context of game data security and privacy, it is important to protect personal data from unauthorized access, use, or disclosure in order to comply with data privacy laws and protect the rights of players.

Privacy Policy

A privacy policy is a document that outlines how an organization collects, uses, and protects the personal data of its users. In the context of online gaming, a privacy policy should explain what data is collected from players, how it is used, and what steps are taken to protect it. Game companies are required to have a privacy policy in order to comply with data privacy laws.

Security Audit

A security audit is a comprehensive evaluation of an organization's security systems and practices. It is used to identify vulnerabilities and ensure that appropriate security measures are in place. Security audits can be conducted by internal teams or external experts.

Vulnerability Scanning

Vulnerability scanning is the practice of using automated tools to identify weaknesses in a system that could be exploited by attackers. It is an important part of a comprehensive security strategy, as it allows organizations to proactively identify and address potential security threats.

Zero Day Exploit

A zero day exploit is a security vulnerability that is unknown to the software vendor and for which no patch is available. It is called a "zero day" exploit because the vendor has had zero days to fix the vulnerability. These types of exploits can be particularly dangerous, as they allow attackers to take advantage of a vulnerability before it is discovered and fixed.