ONE PAGE SUMMARY

IT & Software › Cyber Security › Identity and Access Management

Introduction to Identity and Access Management

Mastering Identity and Access Management for Cyber Security Success

DEFINITION

> Identity and Access Management (IAM) is a framework for managing user identities and access rights. It ensures that the right individuals have appropriate access to technology resources.

KEY CONCEPTS

Authentication

The process of verifying a user's identity, often through passwords or biometrics.

Authorization

Determining what resources a user can access after their identity is confirmed.

User Provisioning

The process of creating, managing, and deleting user accounts and access permissions.

Single Sign-On (SSO)

A user authentication process that allows access to multiple applications with one set of credentials.

Multi-Factor Authentication (MFA)

An additional security layer requiring two or more verification methods to access resources.

EXAMPLES

→ Using a fingerprint to unlock a smartphone.

→ Logging into a corporate network with a username and password.

→ Accessing multiple applications with one login through SSO.

MEMORY TIPS

★ Remember 'AAA' for Authentication, Authorization, and Accounting.

★ Think of SSO as a 'one key for many doors' concept.

★ Use 'MFA' as 'More Factors, Always' for security.

COMMON MISTAKES

✗ Confusing authentication with authorization.

✗ Neglecting to update access rights after employee role changes.

✗ Overlooking the importance of regular security audits.

QUICK RECAP

Identity and Access Management is essential for securing user access to resources. Key components include authentication, authorization, and user provisioning. Understanding these concepts helps protect sensitive information.