Course 3 glossary

Terms and definitions from Course 3

A

Access controls: Security controls that manage access, authorization, and accountability of information

Advanced Encryption Standard (AES): A tool that converts data to unintelligible cybertext, and back into its original form with the proper key

Application programming interface (API): A library function or system access point with well-defined syntax and code that communicates with other applications and third-parties

Artificial intelligence (AI)

A broader concept encompassing ML and other technologies that creates systems capable of learning, reasoning, and problem-solving

Asset management: The process of tracking assets and the risks that affect them

Attack vectors: Pathways attackers use to penetrate security defenses

Attribute-based access control (ABAC): A security model where access is granted based on attributes, like user, resource, and environment

Auditing: The process of recording and reviewing system activity to ensure compliance with security policies, and identifying potential security breaches

Authentication: The process of verifying who someone is

Authentication, authorization, and auditing (**AAA):** A security framework that is used to verify the identity of users or groups in computer systems, and grant them access based on their privileges

Authorization: The concept of granting access to specific resources in a system

Automation: The use of technology to reduce human and manual effort to perform common and repetitive tasks

B

Bucket: A virtual container that holds objects

Business continuity plan (BCP): A document that outlines the procedures to sustain business operations during and after a significant disruption

C

Cloud-native design: The method of creating and deploying applications and services that are optimized for cloud environments

Confidential computing: The protection of data in use with hardware-based Trusted Execution Environment (TEE)

Container: A software package that holds only the components necessary to execute a particular application

Container clusters: Dynamic systems that manage and place containers, grouped in pods

Container layer: Writable space in a container

Container runtimes Software that is responsible for running and managing containers

Context-aware access controls: Decisions about granting or denying access to resources are based on the user's identity and contextual information

D

Data at rest: Data that is not being accessed or actively moving from device to device, or network to network

Data classification: The process of analyzing data to determine its sensitivity and value

Data discovery: The process of searching, identifying, and analyzing large amounts of data within an organization to uncover hidden patterns, relationships, and insights

Data encryption: The process of converting data from a readable format to an encoded format

Data governance: A set of processes that ensures that data assets are managed throughout an organization

Data localization: The requirement that all data generated within a country's borders remain within those borders

Data retention: The process of storing data, including how long it needs to be stored

Data retention period: The length of time an organization keeps information

Data sovereignty: Data stored in a physical location has to follow the regulations of that geographic location

Data stewards: Subject matter experts who are responsible for collecting and managing data, and preserving the quality of the data

Disaster recovery plan (DRP): A plan that allows an organization's security team to outline the steps needed to minimize the impact of a security incident

Discretionary access control (DAC): A security model where the owner of the data or resource has the discretion to grant or revoke access to other users

E

Ephemerality: The concept that things only exist for a short amount of time

H

Hypervisor: The abstraction layer that sits between the physical computer and the virtual machine

I

Identity and access management services (IAM): A collection of processes and technologies that helps organizations manage digital identities in their environment

Infrastructure as code (IaC): The practice of automating and managing infrastructure using reusable scripts

Immutability: The concept of being unable to change an object after it is created and assigned a value

Internet of Things (IoT): The interconnection of everyday objects and devices that enables them to collect, exchange, and analyze data through the internet

K

Kernel: Component of an operating system that manages processes and memory

M

Machine learning (ML): A subset of AI that uses algorithms to learn from data, allowing computers to make decisions and predictions without explicit programming

Managed service: A service, application, or ecosystem managed by a third party

Mandatory access control (MAC): A strict security model where access is granted based on predefined security policies

Micro-segmentation: A security technique that divides a network into smaller, isolated segments

Multi-factor authentication (MFA): A security measure that requires a user to verify their identity in two or more ways to access a system or network

Mutual Transport Layer Security (mTLS): A protocol that provides mutual authentication and encryption between servers

N

Network access control (NAC): A security solution that enforces policy-based access control to network resources, ensuring that only authorized devices and users can access the network

O

Open Authorization (OAuth): A method that allows users to grant applications access to their information on other sites or systems, without the need to share their passwords

OpenID: A protocol that is used for single sign-on functionality, allowing users to authenticate once and access multiple services

P

Patching: The process of installing updates to software to address vulnerabilities, improve stability, or add new features

Perimeter protection: The security measures implemented at the edge of a network or system to defend against unauthorized access and cyber threats

Policy as code (PaC): The use of code to define, manage, and automate policies, rules, and conditions using a high-level programming language

Posture management: The continuous process of monitoring, assessing, and maintaining the security stance of an organization's cloud resources

R

Rate limiting: A method that prevents an operation's frequency from exceeding a set limit or value

Rehydration: A cloud-native process where new servers are created with the latest updates and patches, allowing for the workload to be transferred from old servers, and for the outdated servers to be decommissioned or destroyed

Recovery point objective (RPO): The maximum acceptable length of time during which data might be lost from an application due to a major incident

Recovery time objective (RTO): The target time allowed for the recovery of a service in the event of a disaster

Risk tiering: A process that enables organizations to identify and categorize their assets based on their importance and potential impact

Role-based access control (RBAC): A method of controlling access to resources based on the roles assigned to users

S

Secrets: Sensitive information, like Application Programming Interface (API) keys, passwords, and certificates that are used to authenticate and authorize access to systems

Secure configuration: The practice of setting up your cloud resources with the proper security settings and configurations to minimize potential risks

Shared responsibility model: The implicit and explicit agreement between the customer and the cloud service provider (CSP) regarding the shared accountability for security controls

Software bill of materials (SBOM): A machine-readable list of each piece of software, and its components involved in the supply chain

Single sign-on (SSO): A technology that combines several different logins into one

T

Tags: Custom metadata fields you can attach to a data entry to provide context

Tag templates: Reusable structures that you can use to rapidly create new tags

Threat management strategy: A comprehensive plan that addresses the various types of cyber threats an organization may face

Transport Layer Security (TLS): A security protocol that encrypts data transmitted between two communicating applications

V

Vulnerability remediation: The process of identifying, assessing, and resolving security vulnerabilities in your cloud environment