Google Cloud

Course 1 glossary

Terms and definitions from Course 1

A

Allow policy: A type of access a principal has, and sets conditions on this access

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

Artifact: A digital object, like a file or image, that is used in the software development lifecycle

B

Bucket: A virtual container that holds objects

C

Cloud computing: The practice of using on-demand computing resources as services hosted over the internet

Cloud cybersecurity: The practice of ensuring the confidentiality, integrity, and availability of cloud-based data, applications, and infrastructure by preventing unauthorized access or criminal exploitation

Cloud cybersecurity ecosystem: The network of people, processes, and technologies that work together to keep the cloud secure

Cloud data storage: A solution that enables organizations to keep, access, and maintain digital data on off-site, cloud-based storage devices

Cloud security architect: A professional who designs and develops security controls and measures within an organization's cloud infrastructure

Cloud Security controls: Controls that safeguard cloud environments from threats, and minimize the effects of harmful attacks

Cloud security engineer: A professional who implements and manages secure cloud workloads and infrastructure

Cloud security posture management: The process of monitoring and configuring cloud assets for security and compliance with best practices, regulations, and organization policy

Commit: The specific change made to a file

Compliance team: A team within an organization that ensures processes act in accordance with laws, regulations, and standards

Compute: Computation performed by a physical computer in a remote environment

Configuration drift: When a resource's configuration has altered from its original or expected state

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

Continuous delivery: Continuous release of software builds to a testing environment

Continuous deployment: Deploys builds into a production environment in real time

Continuous integration: The phase where developers continuously create and update code that's uploaded into a shared repository

Continuous integration and continuous delivery (CI/CD): A process DevSecOps teams use to create software and automate updates

D

Data center: A physical building that stores servers, computer systems, and associated components

Defense in depth: A layered approach to vulnerability management that reduces risk

Deny policy: A constraint that sets rules to prevent principals from carrying out certain actions

Detective control: A measure used to identify suspicious activity if it occurs

DevSecOps: A culture that consists of guidelines, best practices, and tools that development, operation, and security teams use to collaborate

Digital transformation: When an organization modernizes their applications, services, and customer relationships by using new technologies

E

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

F

Failure domain: A resource that can fail without impacting the availability of data

G

GitOps: A framework that applies version control, collaboration, compliance, and CI/CD best practices to automate cloud infrastructure

H

Hybrid cloud: A cloud model that combines public and private models, so organizations can enjoy both cloud services, and the control features of on-premises cloud models

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

I

Identity control: A measure that helps authenticate a user before they access resources, like networks or storage

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

Information risk management: The process of identifying, assessing, and minimizing potential threats to information assets

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

Instance: A server resource that runs workloads in the cloud

L

Landing zone: A modular and scalable configuration that enables organizations to adopt Google Cloud for their business needs

Latency: The time it takes for data to travel from one location to another

Lift and shift: A migration model where workloads are moved to the cloud with little to no modifications

M

Multicloud: A strategy of using more than one cloud service provider

Multi-tenant environment: An environment in which cloud infrastructure and resources are shared among users

N

Network control: A measure that helps protect access through network path

O

On-premises: Information technology infrastructure that's physically located in an organization's own data center or office

P

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

Principals: Represent either end users, or applications

Private cloud: A cloud model in which all cloud resources are dedicated to a single user or organization, and are created, managed, and owned within on-premises data centers

Protective control: A measure that protects access to resources and shields against malicious attacks

Provenance: A description of the processes and tools used to build an artifact

Public cloud: A cloud model that delivers computing, storage, and network resources through the internet, allowing users to share on-demand resources

R

Recovery control: A measure that restores access and functionality in the event of failures

Redundancy: The practice of having multiple copies of data in different locations to avoid a single point of failure

Region: A group of zones

Repository: A centralized place to store, download, and share data

Resiliency: The ability to prepare for, respond to, and recover from disruptions

Responsive control: An application or tool that uses automation to respond to security events

Roles: A collection of permissions that can be applied to principals

Router: A network device that connects multiple networks together

S

Security hardening: The process of strengthening a system to reduce its vulnerabilities and attack surface

Security operations center (SOC): A part of an organization that detects and responds to cybersecurity incidents

Service level agreement (SLA): Quantifies the availability of services

Shared fate model: An approach that emphasizes the CSP's involvement in the customer's entire security journey, and offers resources to securely manage their environment at each stage

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

Shift left: Security checks and practices are implemented at the beginning and throughout each phase of the software development lifecycle

Single-tenant environment: An environment in which cloud infrastructure and resources are dedicated to a single user

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

Software development lifecycle: A process for developing, testing, and monitoring software

Software pipeline: A process that uses automation and tools to facilitate movement through each phase of the software development lifecycle

Software supply chain: Includes the people, processes, and tools that play a part in software development

Stakeholder: A person or organization who can affect or be affected by a system

Structured data: Data organized in a certain format, like rows and columns

Switch: A device that makes connections between specific devices on a network by sending and receiving data

T

Threat intelligence: The collection, analysis, and evaluation of cyber threat information

Term: Definition

U

Unstructured data: Data that is not organized in any easily identifiable way

V

Virtualization: Technology that creates a virtual version of physical infrastructure, such as servers, storage, and networks

Virtual private cloud (VPC): A private cloud hosted within a public cloud, enabling organizations to use the public cloud's resources, while being completely isolated from other cloud users

Z

Zone: The collective number of data centers in an area