Google Cloud

Cloud Cybersecurity Certificate glossary

Terms and definitions from the Cloud Cybersecurity Certificate

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

Advanced persistent threat (APT): An adversary that possesses sophisticated levels of expertise, significant resources, and achieves its objectives through multiple attack vectors

Aggregation: The process of collecting and consolidating diverse forms of data

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

Anomaly-based detection: An alternative to signature-based detection that involves creating a normal baseline for network activity

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

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

Assured Workloads: Tool that manages security and compliance of Google Cloud workloads

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

Blue team: A group responsible for defending the organization's systems and networks from simulated attacks

Boolean constraints: Constraints that are either enforced or not enforced for a resource; govern a specific behavior

Bucket: A virtual container that holds objects

Business continuity (BC): An organization's ability to maintain their everyday productivity by establishing a risk disaster recovery plan

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

C

Chain of custody: The process of documenting and preserving evidence in a way that maintains its integrity, and establishes a clear timeline for handling

Cloud audit: An assessment of the cloud environment that is usually conducted by a third party

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

Cloud organizational policy: A set of restrictions or constraints on a specific cloud service, or list of services

Cloud Protection +: A specialized insurance policy developed by Google in collaboration with insurance carriers available through the Risk Protection Plan

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 (CSPM): 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

Compensating controls: Measures that make other controls more effective

Compliance: The process of adhering to internal and external standards, and government regulations

Compliance lifecycle: The process for ensuring compliance objectives are met and maintained to support the business goals

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

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

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

Constraint: A restriction against a Google Cloud service, or a list of services

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

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

Control inheritance: The process of using controls or compliance certifications and audits that are already provided by a cloud service provider

Correlation: The relationship between two or more security events

Cyber insurance: A type of policy that covers businesses against financial losses resulting from cyber incidents

D

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

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

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

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

Disaster recovery (DR): A strategic and systematic approach to recovering essential infrastructure and systems when a disaster happens

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

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

F

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

False positive: An alert that incorrectly identifies malicious activity

G

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

H

Hierarchy: A system that organizes or ranks things, usually by power or importance

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

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

Incident: A violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices

Incident detection: The process of identifying and addressing security threats in the cloud environment

Incident response: The process of identifying, investigating, and mitigating security incidents promptly and effectively

Indicators of compromise (IoC): Observable evidence that suggests signs of a potential security incident

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

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

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

Likelihood: The probability that a vulnerability will be exploited by a threat actor, and includes the extent of the impact of the threat

List constraints: Rules that allow or disallow a set of values

Log: A record of events that occur within an organization's systems

Log analysis: The process of examining logs to identify events of interest

Log management: The process of collecting, storing, analyzing, and disposing of log data

Logging: The recording of events happening on computer systems and networks

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

MITRE: A not-for-profit organization that conducts research to support government agencies

MITRE ATT&CK®: A framework used to understand and approach threats

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

Multicloud cloud security posture management (CSPM): The process of assessing the security of assets throughout a multicloud environment

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

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

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

N

National Vulnerability Database (NVD): A publicly accessible repository of data about known system and software vulnerabilities

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

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

Non-compliance: The failure to follow standards and regulations that are set by internal standards and policy, or external laws and regulations

O

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

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

OWASP® Top Ten: A regularly updated report of critical security risks for web applications

P

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

Penetration testing (pen testing): A process where a red team simulates cyber attacks to identify vulnerabilities in an organization's security infrastructure

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

Playbook: A manual that provides details about any operational action

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

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

Procedures: The specific implementation of a technique

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

Q

Querying alerts: The act of scanning through numerous security alerts from your cloud infrastructure to identify possible threats

R

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

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

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

Red team: A group of ethical hackers who mimic potential adversaries in order to examine the security defenses of an organization

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

Region: A group of zones

Regular expression (RegEx): A sequence of characters that forms a pattern

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

Replication: The process of continuously creating copies of data to multiple locations to support availability

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

Risk: The measure of how much a threat impacts the confidentiality, integrity, and availability of an asset

Risk Protection Program: A solution that provides insurance carriers with accurate information about an organization's level of risk

Risk management framework: A set of practices, processes, and technologies that enable an organization to identify, assess, analyze, and manage risk within an organization

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

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

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

Role binding reports: Sets of one or more members and identities, known as principals, who have a permission or role granted by the cloud security team

Router: A network device that connects multiple networks together

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

Security Command Center Google Cloud's centralized vulnerability and threat reporting service

Security control: A safeguard designed to reduce specific security risks

Security domain: A collection of tightly coupled security practices that address a specific security discipline

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

Security information and event management (SIEM): An application that collects and analyzes log data to monitor critical activities in an organization

Security monitoring: A systematic process of surveilling systems to detect and handle potential security breaches or incidents

Security Operations (SecOps): The practice of combining people, processes, business, and technology to effectively protect an organization's data and infrastructure

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

Security orchestration, automation, and response (SOAR): A collection of applications, tools, and workflows that use automation to respond to security events

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

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

Tabletop exercises: Scenario-based exercises that involve an organization's security team and other stakeholders

Tactics: A malicious actor's reason for performing an action or technique

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

Techniques: The specific actions a malicious actor used to accomplish their goal

Term: Definition

Threat: Any situation or circumstance that can negatively impact assets

Threat hunting: A proactive method of identifying previously unknown threats within a network

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

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

Threat modeling: The process of identifying assets, their vulnerabilities, and how each is exposed to threats

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

U

Underwriting: An insurer's process of pricing an insurance policy

Unified data model (UDM): A data model used to process and store data

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

Vulnerabilities: Weaknesses that can be exploited by threat actors

Vulnerability management: The process of finding and patching vulnerabilities

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

W

Web Security Scanner: Detects vulnerabilities in App Engine, GKE, and Compute Engine applications

Y

YARA-L: A computer language used to create detection rules for searching through ingested log data

Z

Zone: The collective number of data centers in an area