Google Cloud

Course 4 glossary

Terms and definitions from Course 4

A

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

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

B

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

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

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

Correlation: The relationship between two or more security events

D

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

F

False positive: An alert that incorrectly detects the presence of a threat

I

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

L

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

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

P

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

Playbook: A manual that provides details about any operational action

Procedures: The specific implementation of a technique

Q

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

R

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

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

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

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

S

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

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

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

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

U

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

V

Vulnerability management: The process of finding and patching vulnerabilities

Y

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