Google Cloud

Glossary terms from module 1

Terms and definitions from Course 4 Module 1

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

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

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

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

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

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

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

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

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

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

Vulnerability management: The process of finding and patching vulnerabilities