Google Cloud

Glossary terms from module 3

Terms and definitions from Course 4 Module 3

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

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

Playbook: A manual that provides details about any operational action

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

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