Google Cloud

Glossary terms from module 2

Terms and definitions from Course 4 Module 2

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

Correlation: The relationship between two or more security events

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

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

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

Procedures: The specific implementation of a technique

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

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

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

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

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