- 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 types:
  - Network: generated by network devices.
  - System: generated by operating systems
  - Application: generated by software applications and contain information relating to the events occurring within the application.
  - Security: generated by various devices or systems such as antivirus software and intrusion detection systems.
  - Authentication: generated whenever authentication occurs.
- Log management: the process of collecting, storing, analyzing, and disposing of log data.
- **Commonly used log formats:**
  - Syslog.
  - JavaScript Object Notation (JSON).
  - eXtensible Markup Language (XML).
  - Comma Separated Values (CSV).
  - Common Event Format (CEF).
- Telemetry: the collection and transmission of data for analysis.
- Host-based intrusion detection system: an application that monitors the activity of the host on which it's installed.

- Network-based intrusion detection system (NIDS): an application that collects and monitors traffic and network data.
- **Components of a NIDS rule:**
  - Action: It describes the action to take if network or system activity matches the signature. Examples include: alert, pass, drop, or reject.
  - Header: includes network traffic information like source and destination IP addresses, source and destination ports, protocol, and traffic direction.
  - Rule option: provide you with different options to customize signatures.
- Signature: a pattern that is associated with malicious activity.
- Signature analysis: a detection method used to find events of interest.
- Anomaly-based analysis: a detection method that is used to identify abnormal behavior
- **Anomaly-based analysis phases:**
  - The training phase: a baseline of normal or expected behavior must be established. Baselines are developed by collecting data that corresponds to normal system behavior.
  - The detection phase: the current system activity is compared against this baseline. Activity that happens outside of the baseline gets logged, and an alert is generated
- Search Processing Language (SPL): Splunk's query language.
- YARA-L: a computer language used to create rules for searching through ingested log data.