**Glossary terms from module 3**

**Terms and definitions from Course 2, Module 3**

**Chronicle:** A cloud-native tool designed to retain, analyze, and search data

**Incident response:** An organization’s quick attempt to identify an attack, contain the damage, and correct the effects of a security breach

**Log:** A record of events that occur within an organization’s systems

**Metrics:** Key technical attributes such as response time, availability, and failure rate, which are used to assess the performance of a software application

**Operating system (OS):** The interface between computer hardware and the user

**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

**SIEM tools:** A software platform that collects, analyzes, and correlates security data from various sources across your IT infrastructure that helps identify and respond to security threats in real-time, investigate security incidents, and comply with security regulations

**Splunk Cloud:** A cloud-hosted tool used to collect, search, and monitor log data

**Splunk Enterprise:** A self-hosted tool used to retain, analyze, and search an organization's log data to provide security information and alerts in real-time