**Glossary terms from module 4**

**Terms and definitions from Course 6, Module 4**

**Anomaly-based analysis:** A detection method that identifies abnormal behavior

**Array:** A data type that stores data in a comma-separated ordered list

**Common Event Format (CEF):** A log format that uses key-value pairs to structure data and identify fields and their corresponding values

**Configuration file:** A file used to configure the settings of an application

**Endpoint:** Any device connected on a network

**Endpoint detection and response (EDR):** An application that monitors an endpoint for malicious activity

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

**Host-based intrusion detection system (HIDS):** An application that monitors the activity of the host on which it’s installed

**Intrusion detection systems (IDS)**: An application that monitors system activity and alerts on possible intrusions

**Key-value pair:** A set of data that represents two linked items: a key, and its corresponding value

**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 occurring on computer systems and networks

**Network-based intrusion detection system (NIDS):** An application that collects and monitors network traffic and network data

**Object:** A data type that stores data in a comma-separated list of key-value pairs

**Search Processing Language (SPL)**: Splunk’s query language

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

**Signature:** A pattern that is associated with malicious activity

**Signature analysis:** A detection method used to find events interest

**Suricata**: An open-source intrusion detection system, intrusion prevention system, and network analysis tool

**Telemetry:** The collection and transmission of data for analysis

**Wildcard**: A special character that can be substituted with any other character

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

**Zero-day:** An exploit that was previously unknown