Wrap-up; Glossary terms from module 4

Congratulations!
You've made it to the end of this section.
You've made so much progress in your security journey.
Let's review what we learned.
You learned all about how to read and analyze logs.
You examined how log files are created and used for analysis.
You also compared different types of common log formats and learned how to read them.
You extended your understanding on intrusion detection systems by comparing network-based systems and host-based systems.
You also learned how to interpret signatures.
You examined how signatures are written and also how they detect, log, and alert on intrusions.
You interacted with Suricata in the command line to examine and interpret signatures and alerts.
Lastly, you learned how to search in SIEM tools like Splunk and Chronicle.
You learned about the importance of crafting tailored queries to locate events.
At the forefront of incident response, monitoring and analyzing network traffic for indicators of compromise is one of the primary goals.
Being able to perform in-depth log analysis and knowing how to read and write signatures and how to access log data are all skills that you'll use as a security analyst.

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

Revision #2
Created 6 November 2023 05:30:35 by naruzkurai
Updated 6 November 2023 05:32:36 by naruzkurai