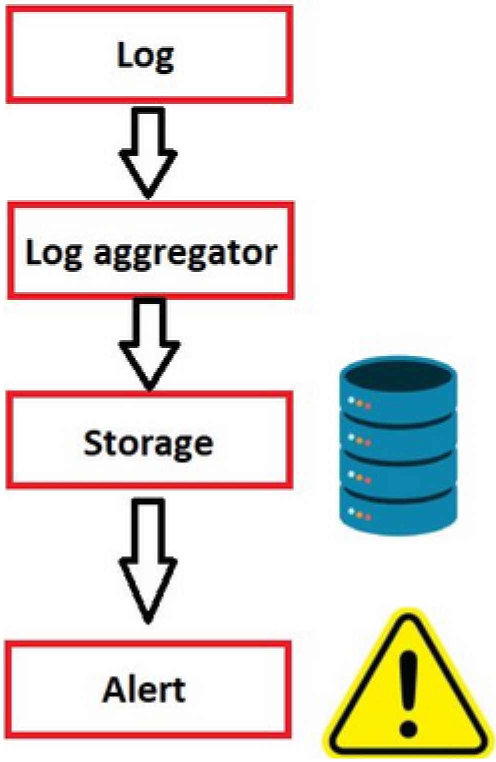
Alerting Analysis

By: Ryan Stewart

Alerting

Having collected, processed, and stored logs, the next step is to detect abnormal behavior within the data and generate alerts.



The timeliness of alerts is contingent on the **speed** of our search capabilities. For instance, for a log created today, we prefer to generate a warning immediately rather than waiting for two days to trigger an alert. As previously discussed, creating a suitable storage environment is essential. The alerts in a SIEM system are typically indicative of suspicious activities, **requiring investigation.** It is crucial to optimize alerts to avoid triggering them excessively, except in exceptional cases. Various methods can be employed to create alerts:

1. By searching stored data
2. Creating alarms while processing logs

Example alerts that can be generated include:

- *New user added to global administrator*
- *15 login failures in 3 minutes with the same IP address*

Creating high-quality alerts necessitates a deep understanding of the available data. Techniques such as blacklisting, whitelisting, and long tail log analysis contribute to more effective log searches.

Blacklist

This method is employed to identify undesirable situations. For instance, by compiling a list of prohibited process names (e.g., mimikatz.exe), alerts can be triggered when any process from this list appears in the logs. However, it is important to note that blacklisting is relatively easy to bypass, for instance, by using a different process name (e.g., mimikatz2.exe).

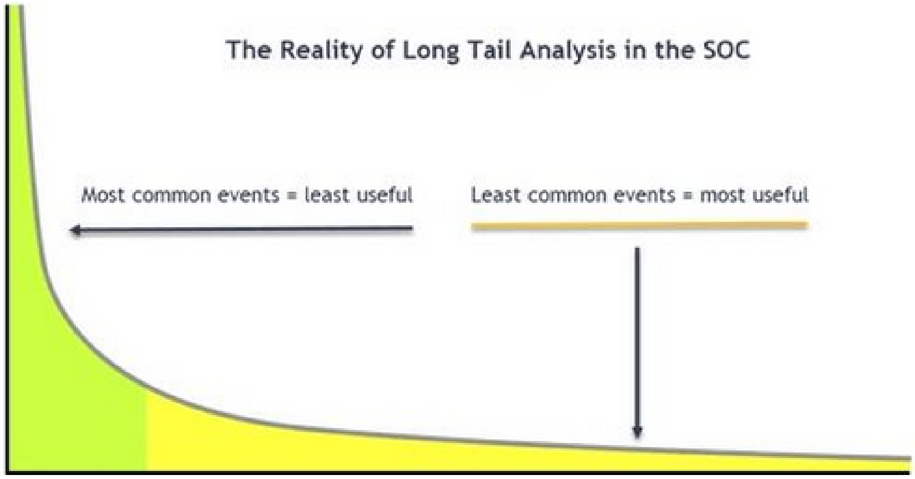
Whitelist

In contrast to blacklisting, whitelisting is used for desired situations. Maintaining a list of IP addresses associated with normal communication allows the system to generate an alert if communication occurs with an address outside of this list. While highly effective, managing and updating the whitelist can be challenging.

Long Tail Log Analysis

This method assumes that constantly occurring behaviors are normal. For instance, if an "Event ID 4624 An account was successfully logged on" log is consistently present on a device, it is considered normal. Suspicion is then directed towards logs that occur less frequently.

Utilizing these three methods, you can identify suspicious situations and create effective alerts to enhance your SIEM system's security capabilities.



Quiz Questions:

1. "The whitelist method is not only very effective but also very easy to manage." Is that true or false? [True/False] False

2. If you have 2 IP addresses that are certain to be malicious and you want to create an alert when these are accessed, which method should you use?

- Whitelisting
- Blacklist
- Long Tail