Data Partition

Data partitioning in SIEM is a method of organising and dividing large volumes of data into manageably separated sections. Companies using SIEM have a set budget for the security teams. They wanted to get the most value for the best price. One of the SOC analyst's responsibilities is to divide the data based on its importance and put it in different tiers to achieve the most cost-effective security solutions. In SUMO Logic, the partitioned data is divided into 3 tiers.

Data Tiers

The first tier is the Continuous Tier. It is also called the “hot” data storage and is used for the most available data that is instantly searchable. It allows the analysts to track events in real time coming from the critical security logs, such as endpoints, firewalls, or authentication, creating your SIEM system. The data in this tier supports alerts, allowing fast reaction to a potential security breach. Because of the vast amount of data ingested and analysed in real-time, this tier is the most expensive.

The second tier is the Frequent Tier. This is called the “warm” data used for the data you need to frequently access to troubleshoot and investigate issues. Data is searchable, but the process is slower compared to the Continuous Tier. You can use it to store your compliance logs, or anything that is not security critical for your organization, yet not ready to be archived and put away into the infrequent tier. This option is less expensive than the Continuous Tier.

The third tier is the Infrequent Tier. This data is called “cold” data and is not searchable by default. The logs stored here need to be rehydrated first (brought back to a searchable tier). It is usually used to troubleshoot hard-to-reproduce issues. You might use this tier to store debug logs, OS logs, or thread dumps. This is the cheapest of the three tiers.