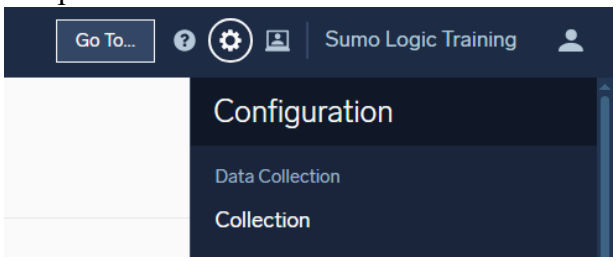
SIEM Data Collection

Data Collection in Security Information and Event Management is the process of collecting security-related logs and event data from multiple sources within the organisation's IT infrastructure. It is a first step in the SIEM workflow, which allows the Analysts to analyse and detect security threats. Thanks to data collection, the security professionals are able to correlate events from different sources to gain the understanding of the anomaly context. In SUMO Logic data is collected by collectors which require additional source specification.

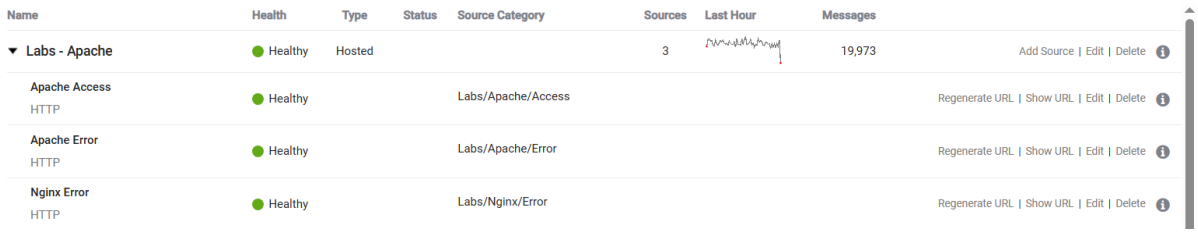
Collectors

Collectors in SUMO SIEM are agents that gather and ingest the data from different sources: devices, servers, or cloud services. Later, they forward the created messages to SIEM to parse, map, and enrich those, turning them into records. To understand what type of data collector is gathering, it requires a source. A source is a configuration that specifies how and what kind of data the collector ingests.

To reach the existing collectors in SUMO Logic's new UI, click the configuration gear icon, and click the Collection option.



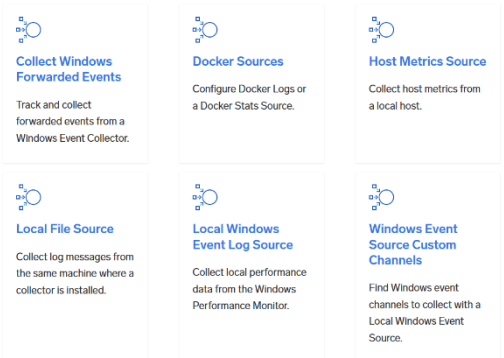
The list shows all of the installed collectors. The details are listed next to the names of the collectors.



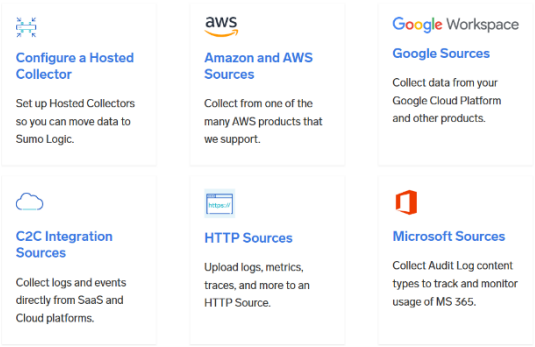
The list shows the name of the collector and the configured sources. The green circle next to the name shows that the data is flowing into the collector without any errors. Then we see the type of collector, which in this case is a hosted one. We see how many sources this specific collector has, the last hour activity, and the number of messages the collector has delivered.

There are 2 types of collectors: installed and hosted.

Installed collectors are installed on on-premise machines and servers. They are used for log sources such as Windows Event Logs or Sys Logs. There are plenty of available sources to install. The list is available on the Sumo documentation website. Beneath are a couple of examples.



The hosted collectors are cloud-based. Being managed by SUMO Logic, they do not require installation on the machines. They ingest logs from Amazon Web Services, such as CloudTrail or S3, as well as Microsoft Azure or HTTP sources. Beneath are some of the available sources.



Data collection is a constant process of ingesting data from across an organization's IT infrastructure into one centralized SIEM. It is crucial for compliance, threat detection, and incident response.