Section Introduction, Aggregation

This section of the SIEM domain will introduce you to aggregation, and how it is used to collect and manage logs coming from a range of log sources. In large businesses the volume of incoming logs can be extremely large, and the SIEM needs to be able to ingest and store these in a functional manner, and that's where aggregation comes in. Using techniques such as deduplication and combining logs we can reduce the total storage needed.

LEARNING OBJECTIVES

By the end of this section you will have achieved the following objectives:

- Understand what aggregation is, and the role it plays in SIEM.
- Understand the different formats of data going into a SIEM.