

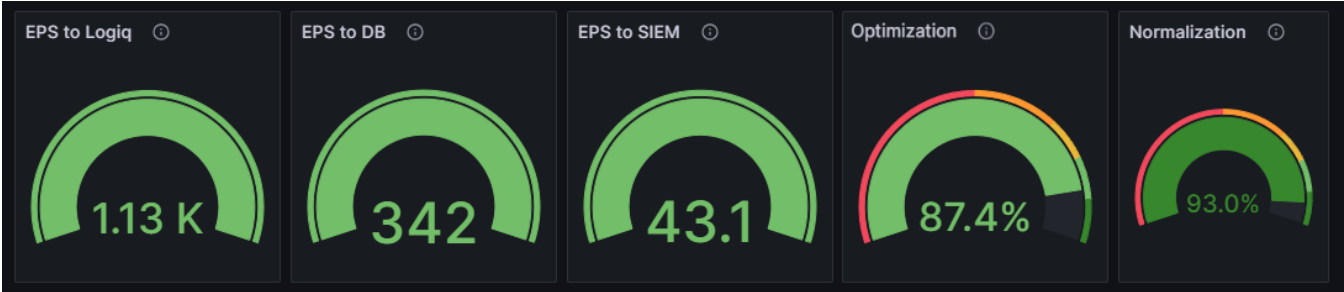
Блок «Работа бизнес логики»

В данной статье описаны показатели системы, отображаемые в блоке **Работа бизнес логики**.

Данный блок можно разделить на три основных части:

- Поток событий;
- Скорость обработки событий конвейером Сатурн;
- Скорость записи/чтения в ClickHouse.

Поток событий



В данном блоке отображаются следующие показатели:

- **EPS to Logiq** — количество событий, получаемых системой в секунду;
- **EPS to DB** — количество событий, записываемых в слой хранения (базу данных) в секунду;
- **EPS to SIEM** — количество событий, записываемых в SIEM-систему в секунду;
- **Optimization** — процент оптимизации событий (процент событий, которые не были записаны в SIEM-систему по отношению к событиям, записанным в базу данных);
- **Normalization** — процент нормализованных системой событий.

Скорость обработки событий конвейером Сатурн



В данном блоке отображаются следующие показатели:

- **Duration rate** — длительность обработки событий, входящих в каждый из этапов конвейера;
- **Events in rate** — количество событий, входящих в каждый этап конвейера;
- **Events filtered rate** — количество обработанных событий в каждом из этапов конвейера;
- **Events out rate** — количество событий, выходящих из каждого этапа конвейера.

Также, для каждого графика существует таблица показателей каждого этапа конвейера со следующими столбцами:

- **Name** — имя этапа конвейера;
- **Mean** — усредненное значение;
- **Last** — последнее значение, не равное нулю;
- **Max** — максимальное значение;
- **Min** — минимальное значение.

Скорость записи/чтения в ClickHouse

Clickhouse read/write speed							
User	Database	Type	Queries	ReadRows	MemoryUsed	ElapsedAvg	Threads
logger	logger	Select	1	0	0 B	0.0100	1
logger	default	Select	3	0	0 B	0	3
Total					0 B		4

Данная таблица состоит из следующих столбцов:

- **User** — пользователь системы, совершивший запись.чтение в базу данных;
- **Database** — база данных, в которую была произведена запись/чтение;
- **Type** — тип запроса, который использовался для фильтрации событий;
- **Queries** — количество запросов;
- **ReadRows** — количество прочитанных столбцов;
- **MemoryUsed** — количество использованной памяти;
- **ElapsedAvg** — среднее время, затраченное на запись/чтение;
- **Threads** — количество потоков, которые использовались для записи/чтения.