Автоматизация расчета метрик для контроля процессов ИБ

Беляков Игорь

Зачем нам вообще эти метрики?

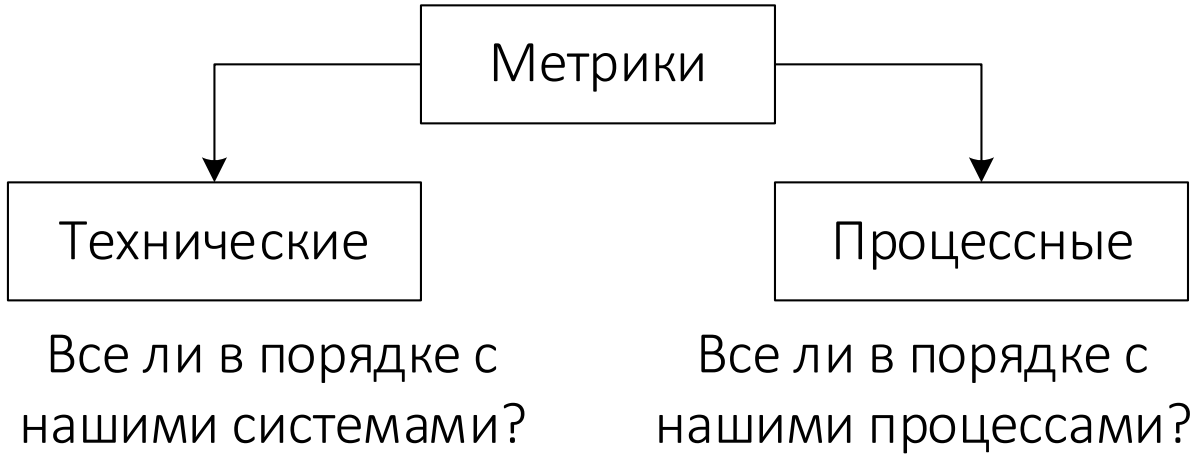
Есть 2 основных причины

1. Для прохождения комплаенса.
2. Чтобы убедиться, что все в порядке.

А зачем автоматизировать?

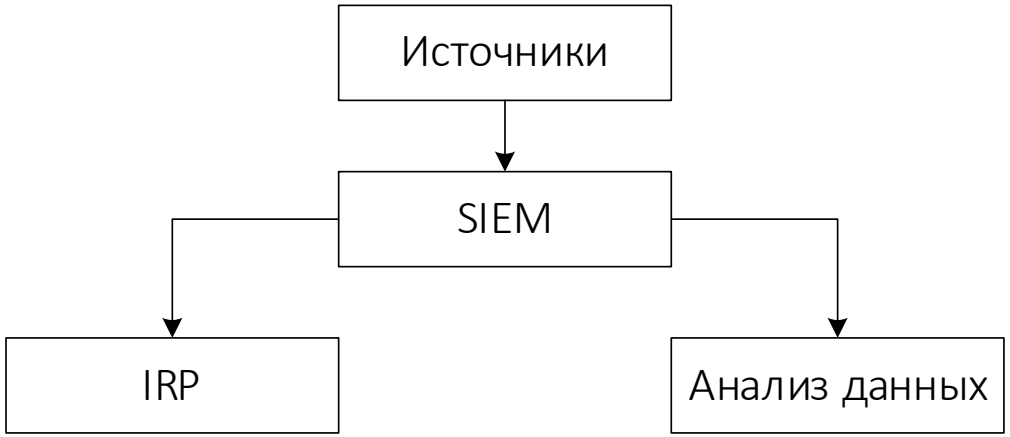
… для экономии тродозатрат

Какие метрики стоит контролировать



- Например:
- Технические: на всех ли хостах работает антивирус? Какие тренды по выявленным угрозам?
- Процессные: Сколько времени уходит на обработку инцидентов? Как часто сотрудники запрашивают доступ?

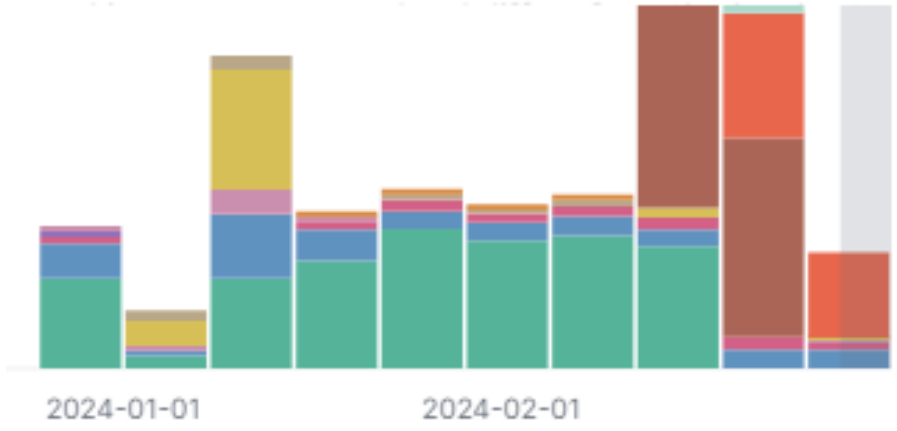
Автоматизация технических метрик

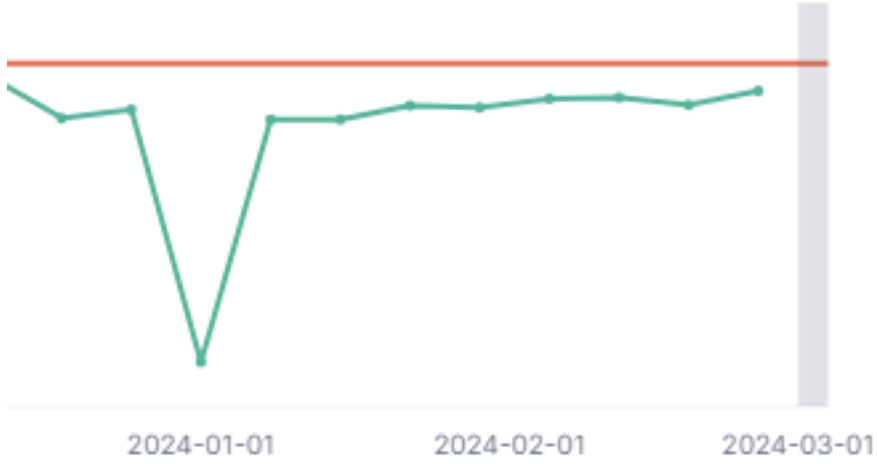


Например, ELK

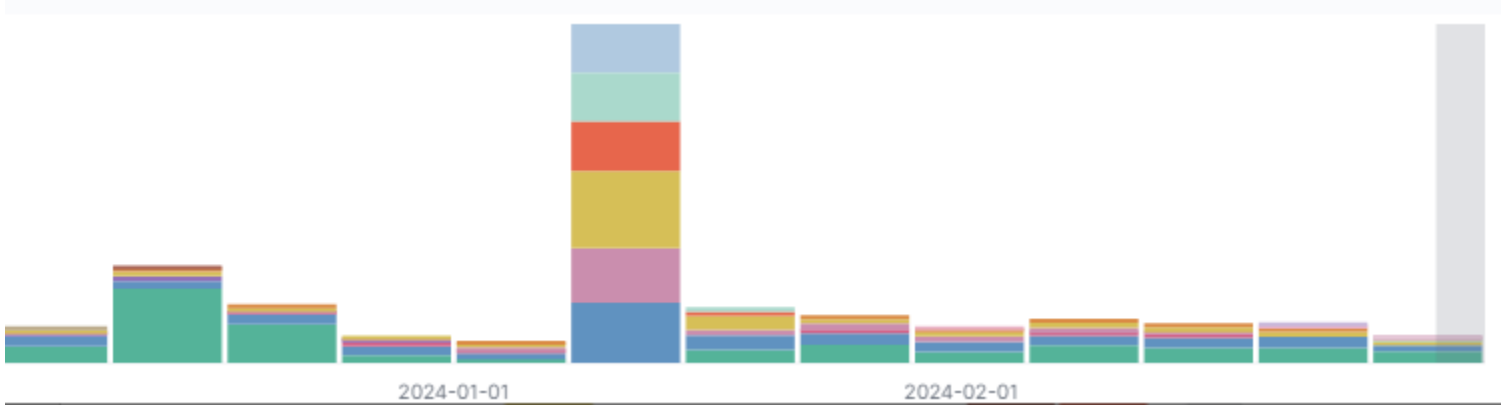
- SIEM является центром обработки. Включая логи СЗИ
- Дополнительное преимущество. В такой схеме можно не грузить СИЕМ запросами на формирование сложных отчетов за большой период времени.

Пример технических метрик

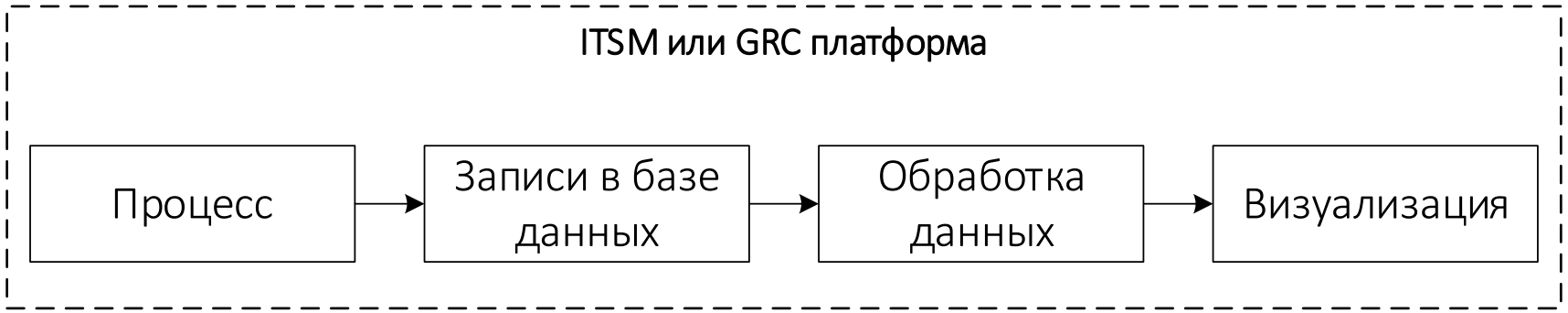




1. Работает ли антивирус?
2. На всех хостах?
3. Нет ли аномалий по сетевым атакам?



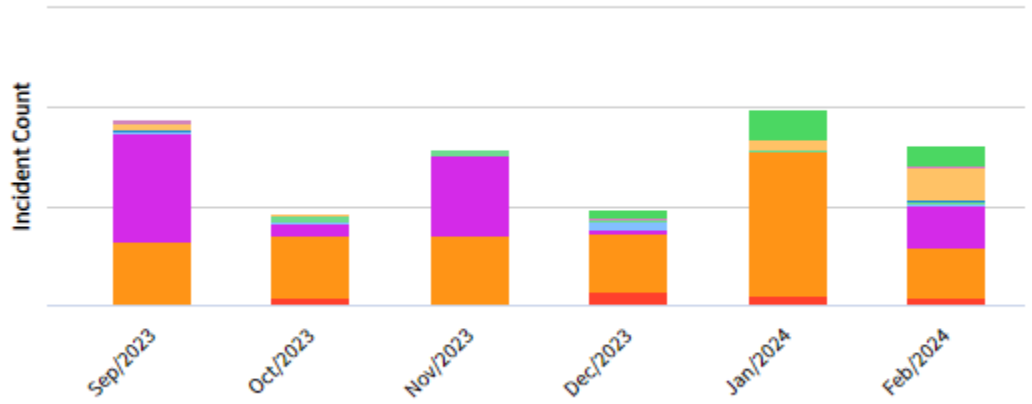
Автоматизация процессных метрик



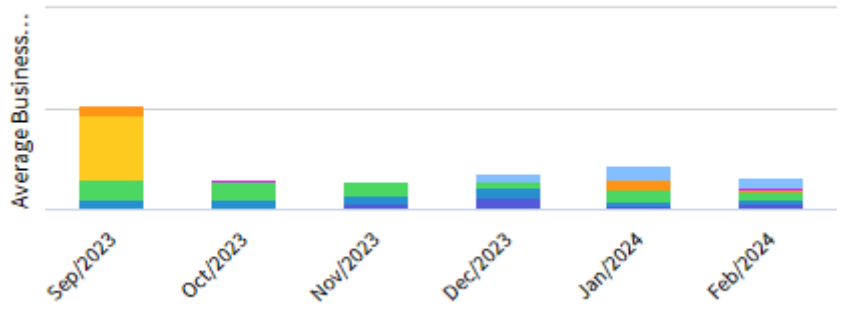
- *Данная опция доступна только для формализованных процессов и для работы с которыми используется нормальная ITSM или GRC система*

Пример процессных метрик

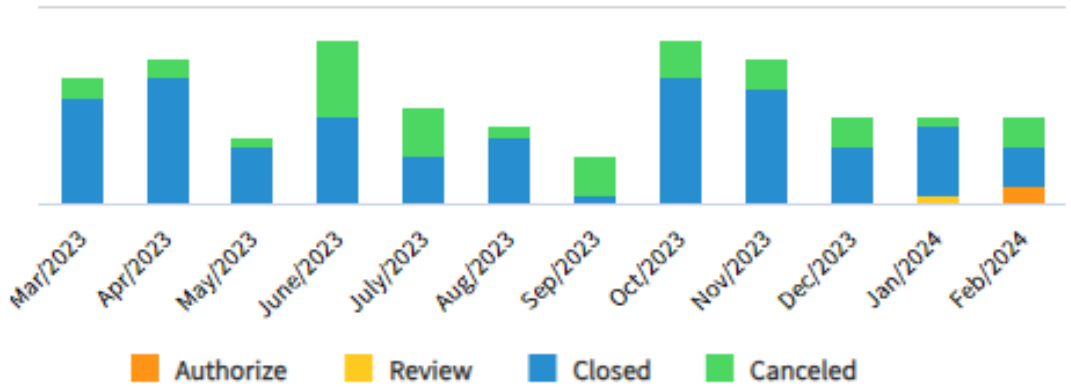
Количество инцидентов



IRP Среднее время разрешения инцидента



Privileged access stats



Преимущества

1. Вы всегда знаете, что у вас все в порядке.
2. Наглядно видно изменение трендов и аномалии в работе систем или процессов
3. Если требование по расчету метрия является обязательным, то автоматизация экономит время сотрудников

Спасибо за внимание