Автоматизация управления инцидентами

Как уйти от ручного труда и не выгореть

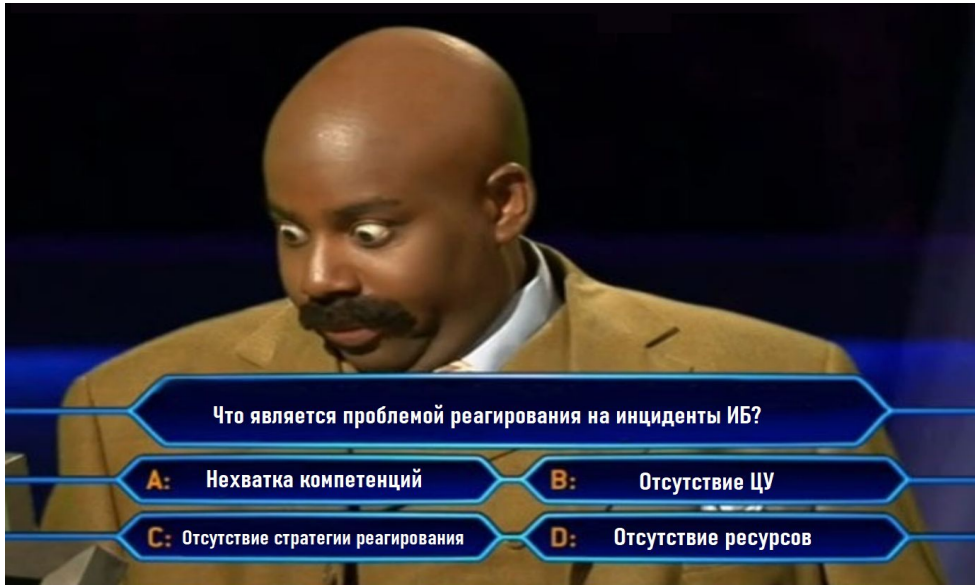
Спикер: Беляев Д.А

Инцидент - это?

Инцидент информационной безопасности - Появление одного или нескольких нежелательных или неожиданных событий ИБ, с которыми связана значительная вероятность компрометации бизнес-операций и создания угрозы ИБ.

ГОСТ Р ИСО/МЭК 18044

Проблемы управления инцидентами



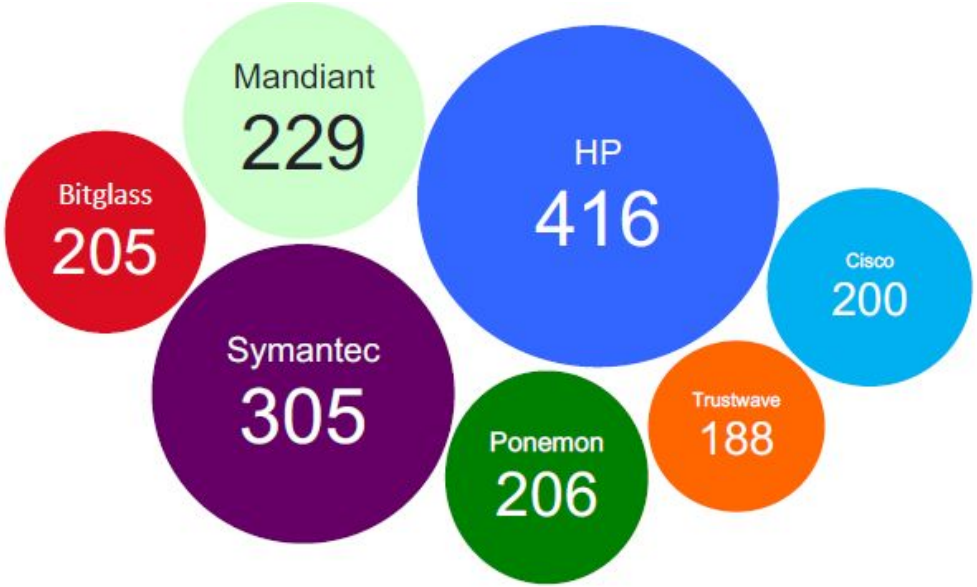
- Отсутствие связи с целями организации и бизнеса;
- Отсутствие поддерживающих управление инцидентами политик и процедур;
- Предоставление избыточных или дублирующих услуг;
- Неопределенные и не формализованные процессы и роли;
- Отсутствие контроля;
- Отсутствие коммуникаций, координации и разделения данных с другими командами;
- Ручные работы.

СКОЛЬКО ДНЕЙ В СРЕДНЕМ ТРАТЯТ

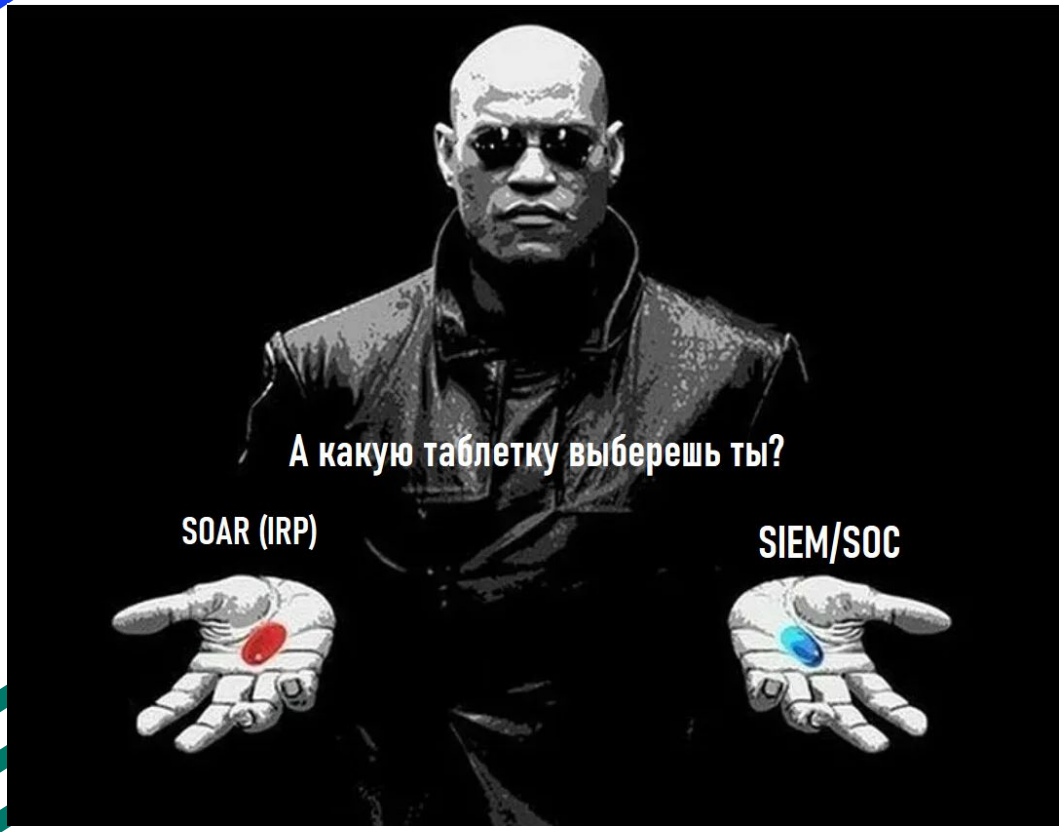
КОМПАНИИ НА ОБНАРУЖЕНИЕ

ИНЦИДЕНТА?

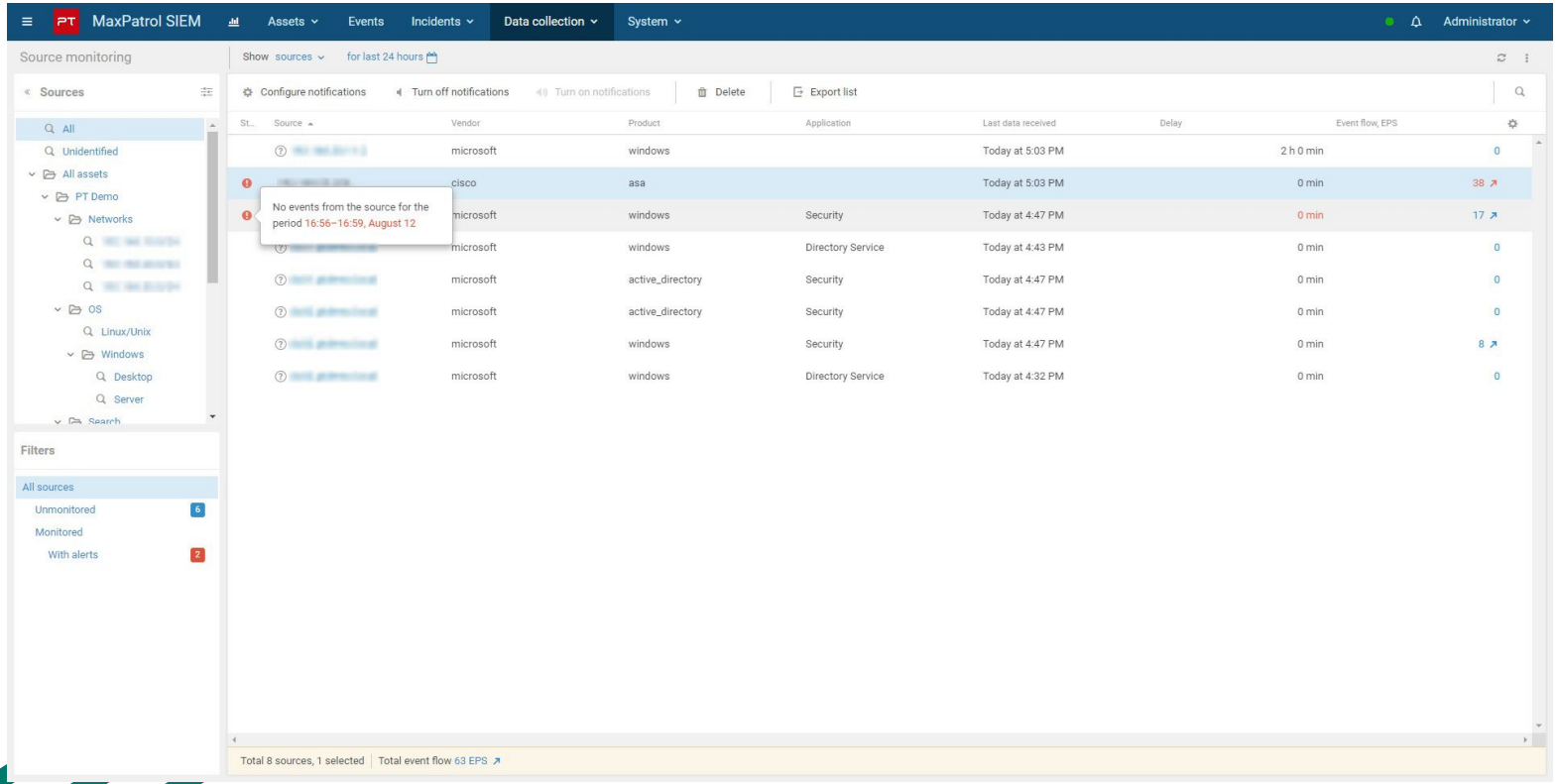
- После 12-ти минут непрерывного мониторинга аналитик пропускает 45% активности на мониторе
- После 22-х – 95%
- После 20-40 минут активного мониторинга у аналитика наступает психологическая слепота


Mandiant
229
HP
416
Bitglass
205
Cisco
200
Symantec
305
Trustwave
188
Ponemon
206

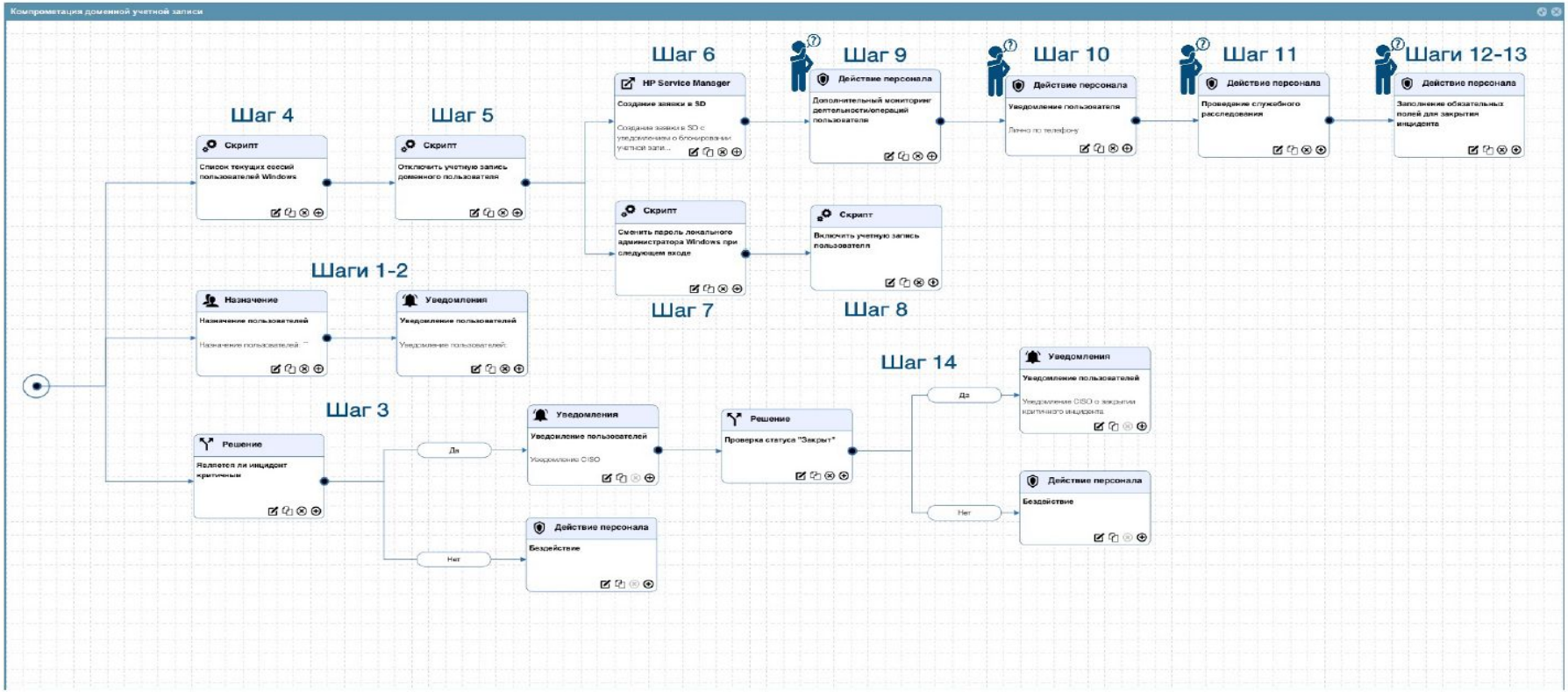
Решение



Работа в SIEM



Пример работы SOAR



Преимущества

- Экономия на L1;
- Минимизация рисков пропуска реального инцидента;
- Время реакции L2/L3;

Время менять подходы

«Улучшать — значит меняться, поэтому быть совершенным — значит меняться часто»

Уинстон Черчилль

Спасибо за внимание!
Ваши вопросы?

da.belyaev

@da_belyaev

+7-905-486-49-11

da.belyaev@mail.ru

Беляев Дмитрий Александрович
Начальник СИБ

АО ПЕРВЫЙ ИНВЕСТИЦИОННЫЙ БАНК