

Автоматизация управления инцидентами

Как уйти от ручного труда и не выгореть



Спикер: Беляев Д.А

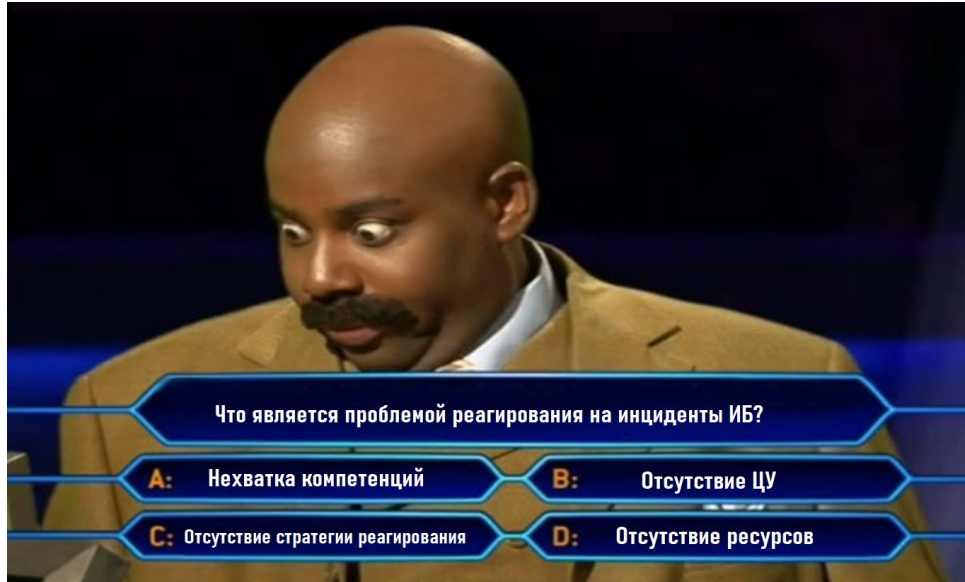
Инцидент - это?

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



Что является проблемой реагирования на инциденты ИБ?

А: Нехватка компетенций

В: Отсутствие ЦУ

С: Отсутствие стратегии реагирования

D: Отсутствие ресурсов



- 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.

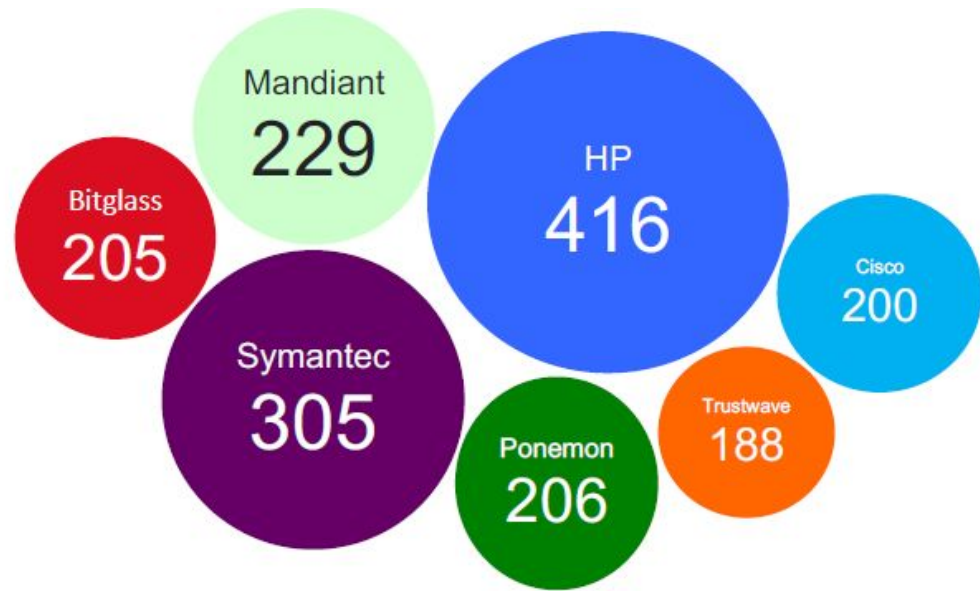
СКОЛЬКО ДНЕЙ В
СРЕДНЕМ ТРАТЯТ

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



Решение



Работа в SIEM

The screenshot displays the MaxPatrol SIEM interface. The top navigation bar includes 'MaxPatrol SIEM', 'Assets', 'Events', 'Incidents', 'Data collection', and 'System'. The main area is titled 'Source monitoring' and shows a table of monitored sources. A tooltip is visible over one of the sources, indicating that no events were received during a specific time period.

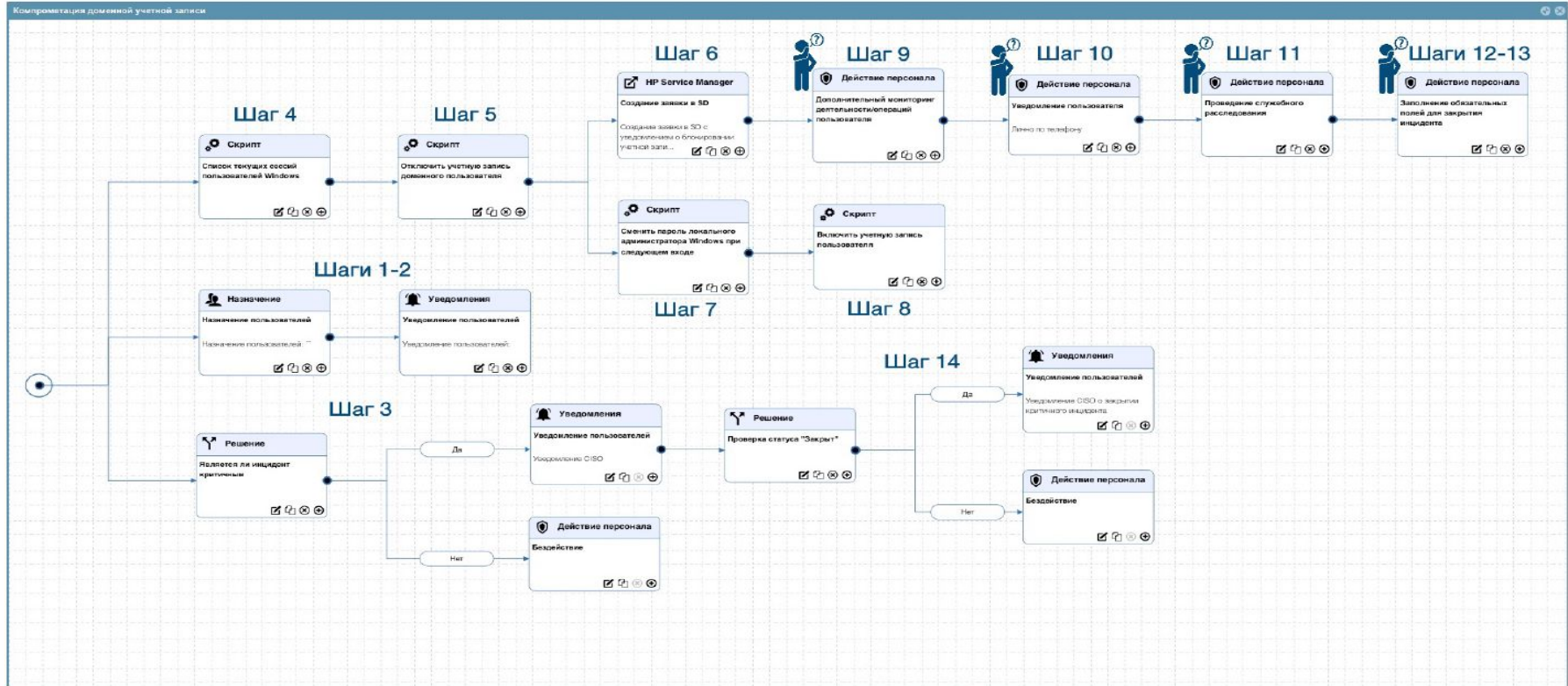
St.	Source	Vendor	Product	Application	Last data received	Delay	Event flow, EPS
	10.10.10.10	microsoft	windows		Today at 5:03 PM	2 h 0 min	0
	10.10.10.10	cisco	asa		Today at 5:03 PM	0 min	38
1	10.10.10.10	microsoft	windows	Security	Today at 4:47 PM	0 min	17
	10.10.10.10	microsoft	windows	Directory Service	Today at 4:43 PM	0 min	0
	10.10.10.10	microsoft	active_directory	Security	Today at 4:47 PM	0 min	0
	10.10.10.10	microsoft	active_directory	Security	Today at 4:47 PM	0 min	0
	10.10.10.10	microsoft	windows	Security	Today at 4:47 PM	0 min	8
	10.10.10.10	microsoft	windows	Directory Service	Today at 4:32 PM	0 min	0

Tooltip: No events from the source for the period 16:56-16:59, August 12.

Filters: All sources (6), Unmonitored (6), Monitored (2), With alerts (2).

Total 8 sources, 1 selected | Total event flow 63 EPS

Пример работы SOAR



Преимущества

Когда работаешь
в ручную



Когда автоматизируешь



- 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](https://vk.com/da.belyaev)



[@da_belyaev](https://t.me/da_belyaev)



+7-905-486-49-11



da.belyaev@mail.ru

Беляев Дмитрий
Александрович
Начальник СИБ



**АО ПЕРВЫЙ
ИНВЕСТИЦИОННЫЙ
БАНК**