RoboSOC

Использование машинного обучения в SOC-ах

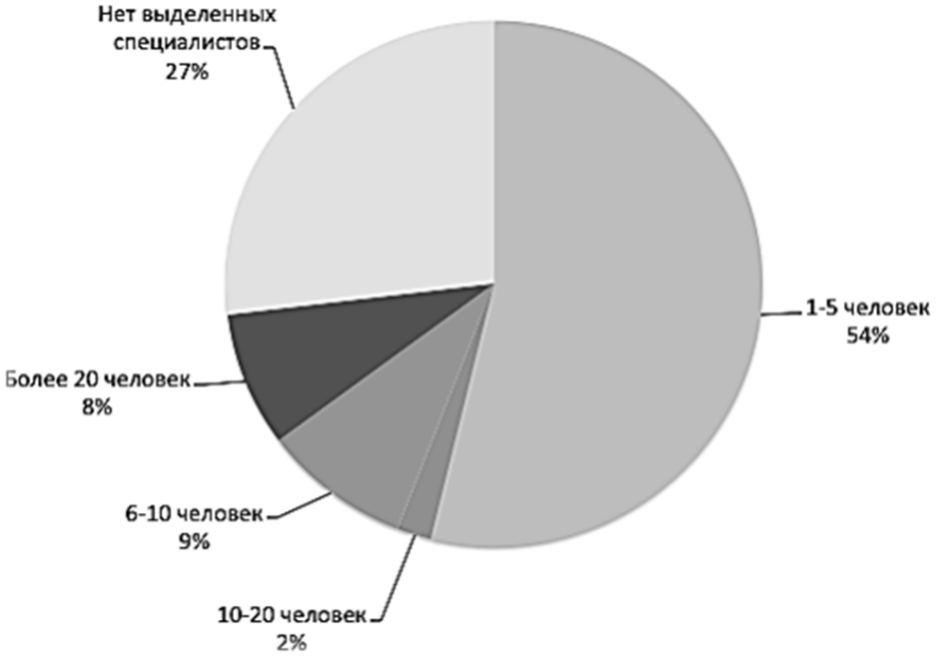
Хайретдинов Рустэм
Генеральный директор
ООО «Атак Киллер»

SOC-Forum Казахстан, Нурсултан 2019

Математика, бессердечная ты <censored>

- ИТ-сервисы круглосуточны
- Человек не может эффективно работать оператором больше 6 часов в сутки
- 1 рабочее место оператора SOC = 4 смены по 1 человеку + 1 запасной = вынь да положь $100К в год только на ФОТ на одно рабочее место
- Если задач больше, чем на 1 рабочее место, то X$100K

ЛЮДЕЙ НЕТ И НЕ БУДЕТ

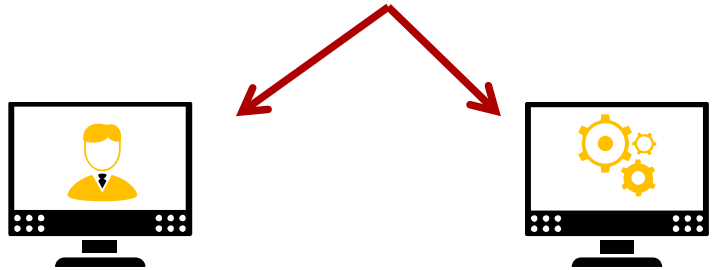


Количество ИБ-специалистов в организациях.
Источник: Anti-Malware.ru

ИБ-специалист это ИТ-джедай

- ИТ-инфраструктура + бизнес-процессы + compliance + коммуникации + стрессоустойчивость + собранность + ответственность
- За 50-70% от з/п программиста

Очевидно, что их катастрофически мало



Аутсорсинг **Машины**

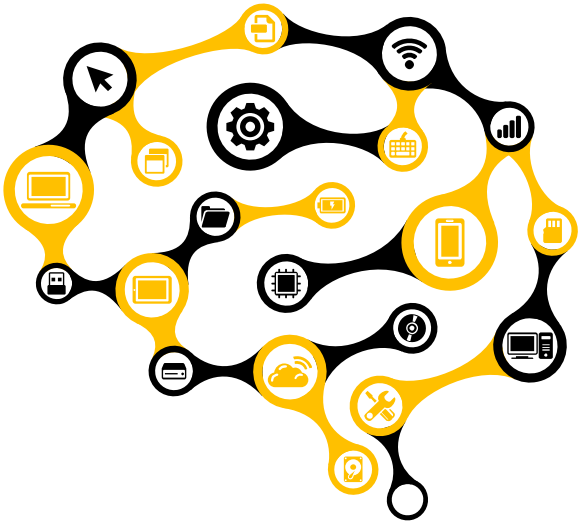
Специфика роботизации в безопасности

- Повышенные требования к точности
- Конкуренция с точными методами
- Исторические данные малополезны для новых угроз
- Несформулированная ответственность

Ключевые подходы

Используем все доступные методологии:
понимание бизнес-процесса, репутация, поведенческий анализ

Обрабатываем все события:
кибербезопасность, ошибки операторов,
мошеннические действия, компьютерные сбои и т.п.



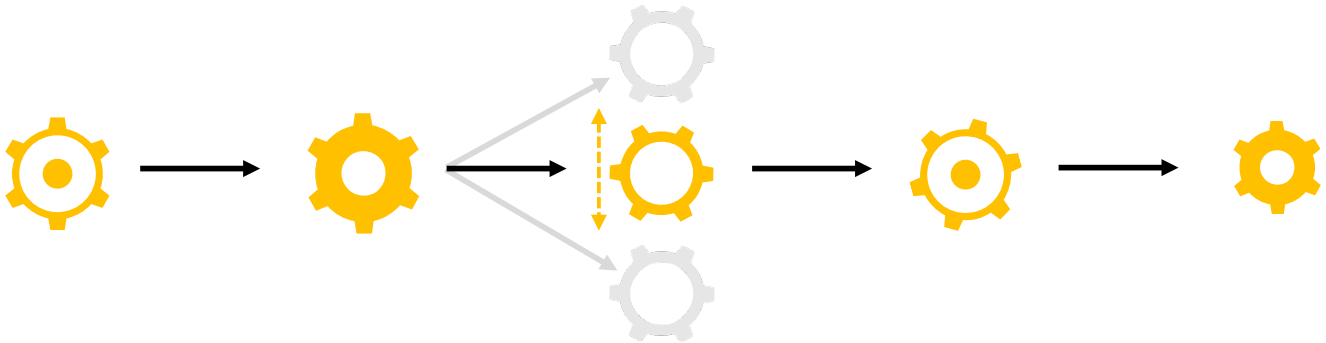
Решение «на дальних подступах»:
не отдавай инцидент, который можно решить на месте

Не полагайся на чёрные списки:
они про старые атаки

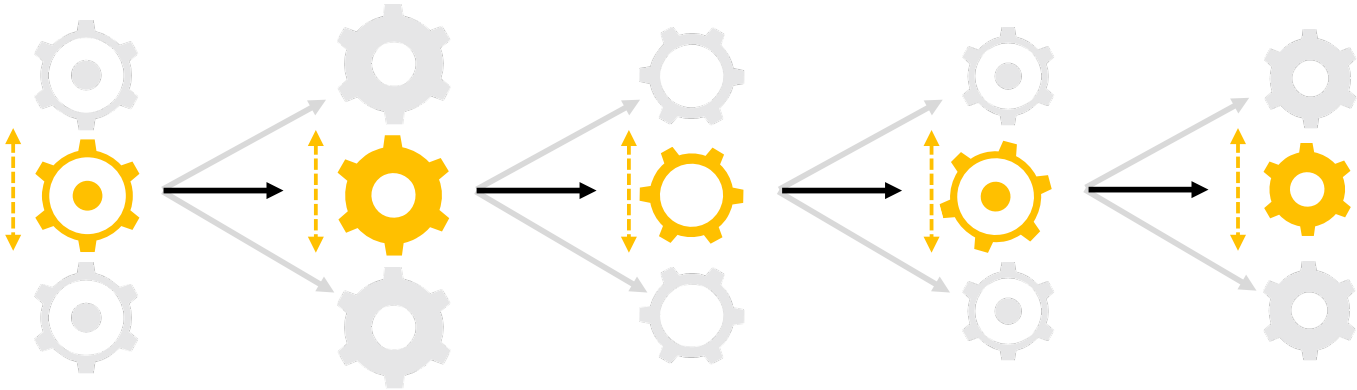
Повышение уровня абстракции:
данные –> информация -> бизнес-процессы

Идеальный процесс

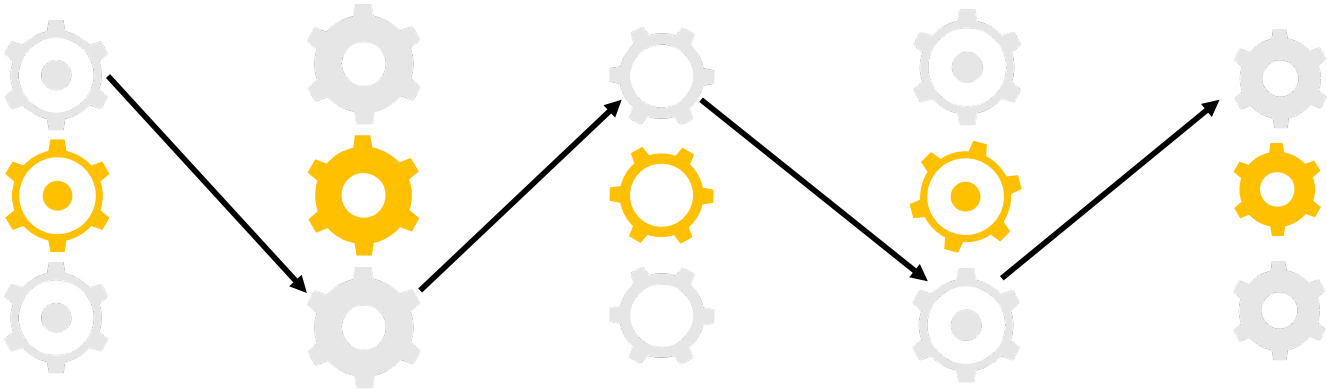
Аномалия узла



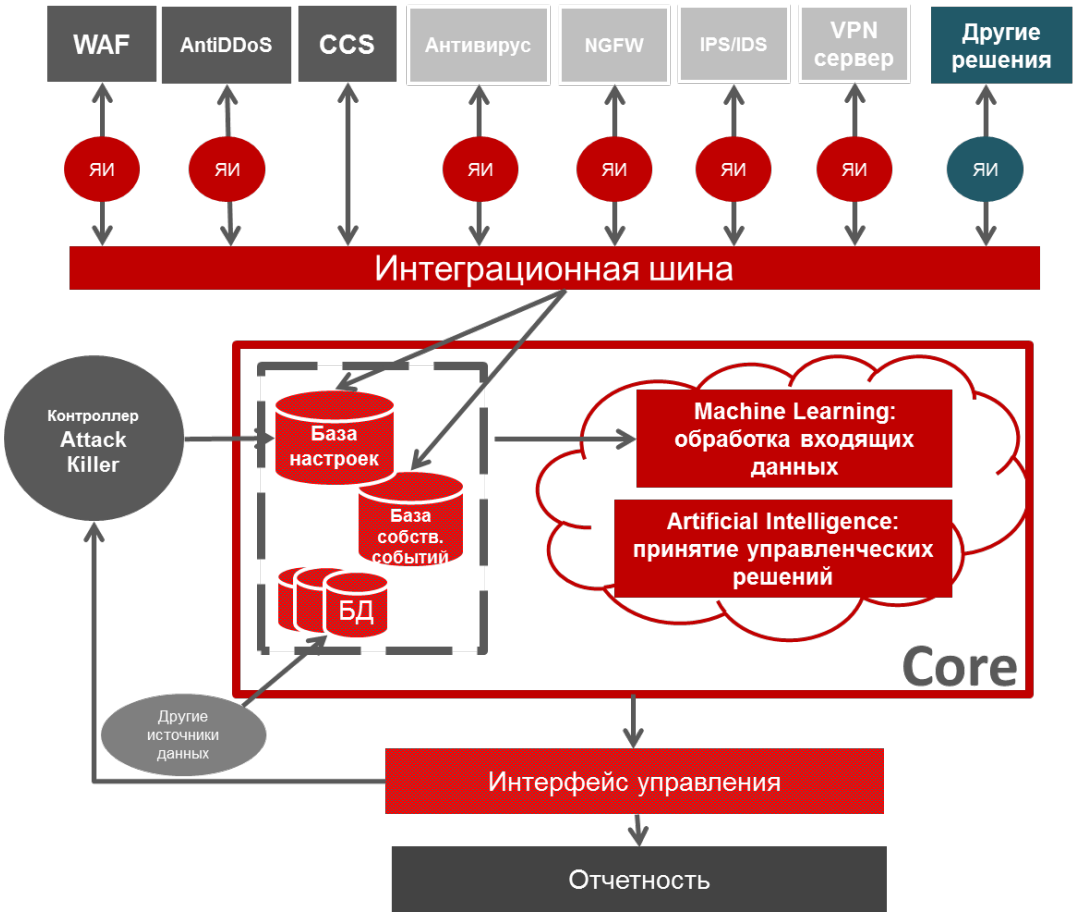
Аномалия узлов



Аномальный процесс



Архитектура RoboSOC



Уровень специализированных решений

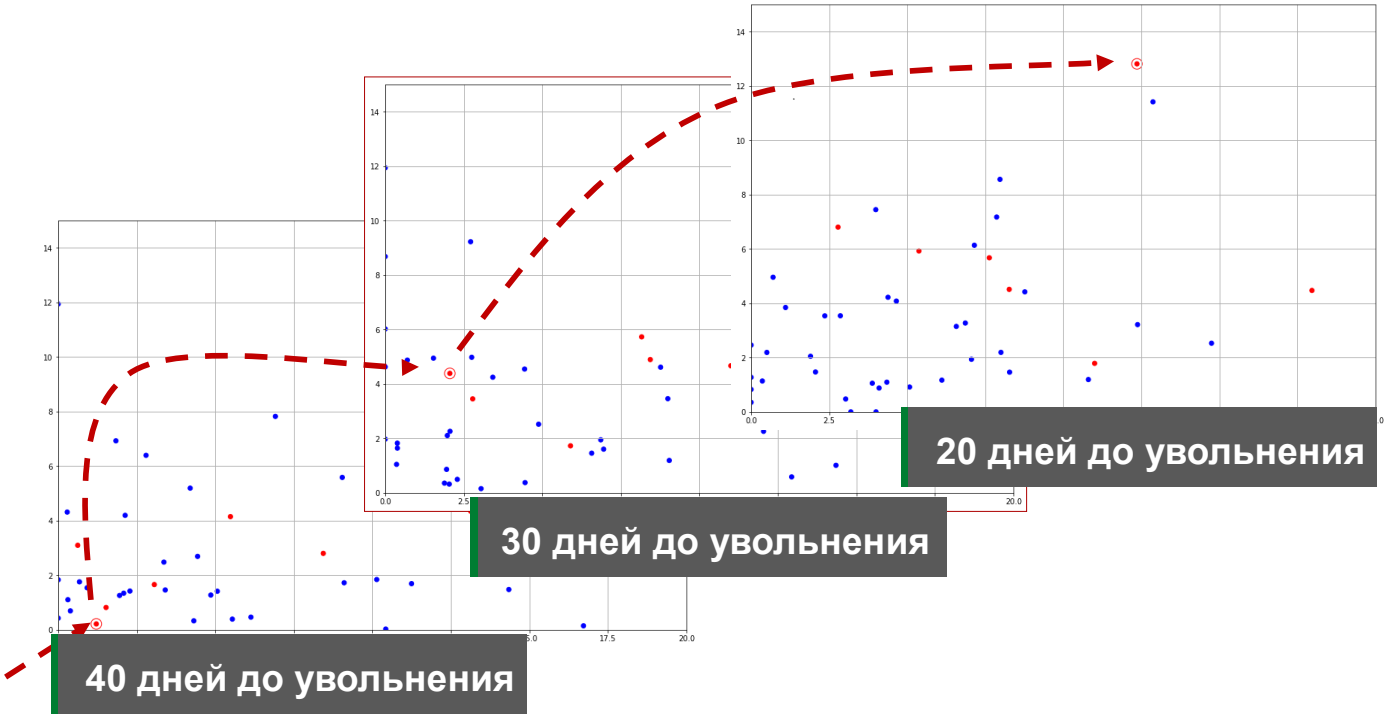
Уровень интеграции

Уровень анализа и управления

Уровень отчётности

«Уравнения умнее своих создателей» (с)

Потеря интереса к работе: миграция на периферию социального графа



«Уравнения умнее своих создателей» (с)

$$N_{\text{СМЕНА}} = F(K_{\text{ПОСЫЛОК}}) \longrightarrow M_{\text{ПРОХОДОВ}} = N_{\text{СМЕНА}} \longrightarrow S_{\text{ВЫПЛАТ}} \sim P_{\text{ПРОИЗВОД-ТЬ}} \longrightarrow C_{\text{СЕБЕСТ-ТЬ}} \sim S_{\text{ВЫПЛАТ}}$$

Уровень логики
Уровень логики
Уровень ошибок

Занимайтесь творчеством, отдайте рутину роботам

Спасибо за внимание!

Хайретдинов Рустэм
Генеральный директор
ООО «Атак Киллер»