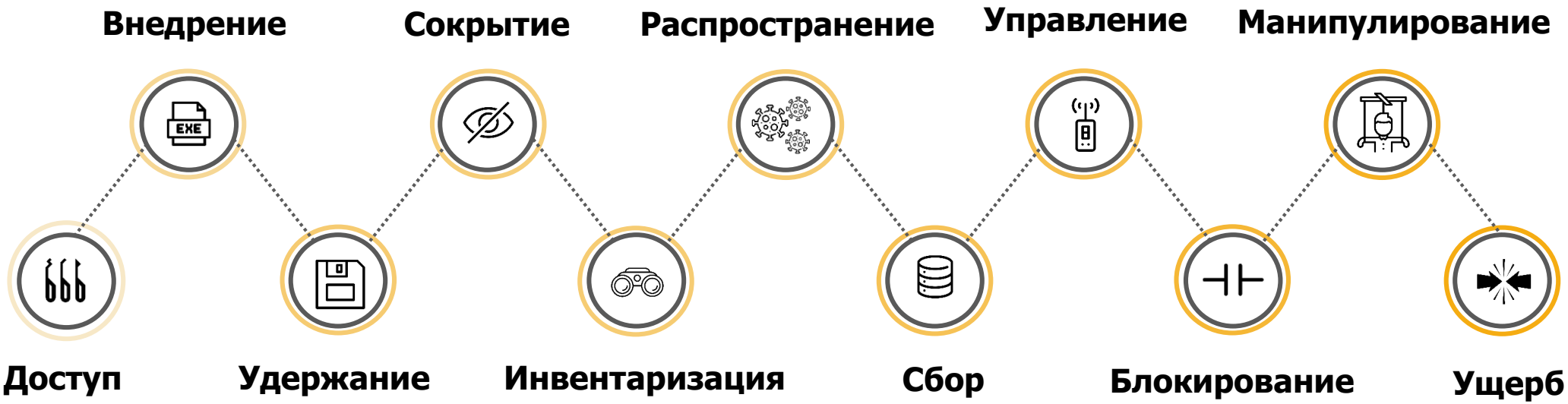
Интеллектуальный SOC: автоматизация обработки действительно большого количества событий

Николай Домуховский
Заместитель генерального директора

ИБ АСУ ТП КВО, 2022

Почему важно оперативно выявлять инциденты ИБ?

USSC



77% Компаний подвергаются успешной атаке в течение одного года

77% На столько уменьшиться ущерб, если инцидент будет выявлен в течение недели

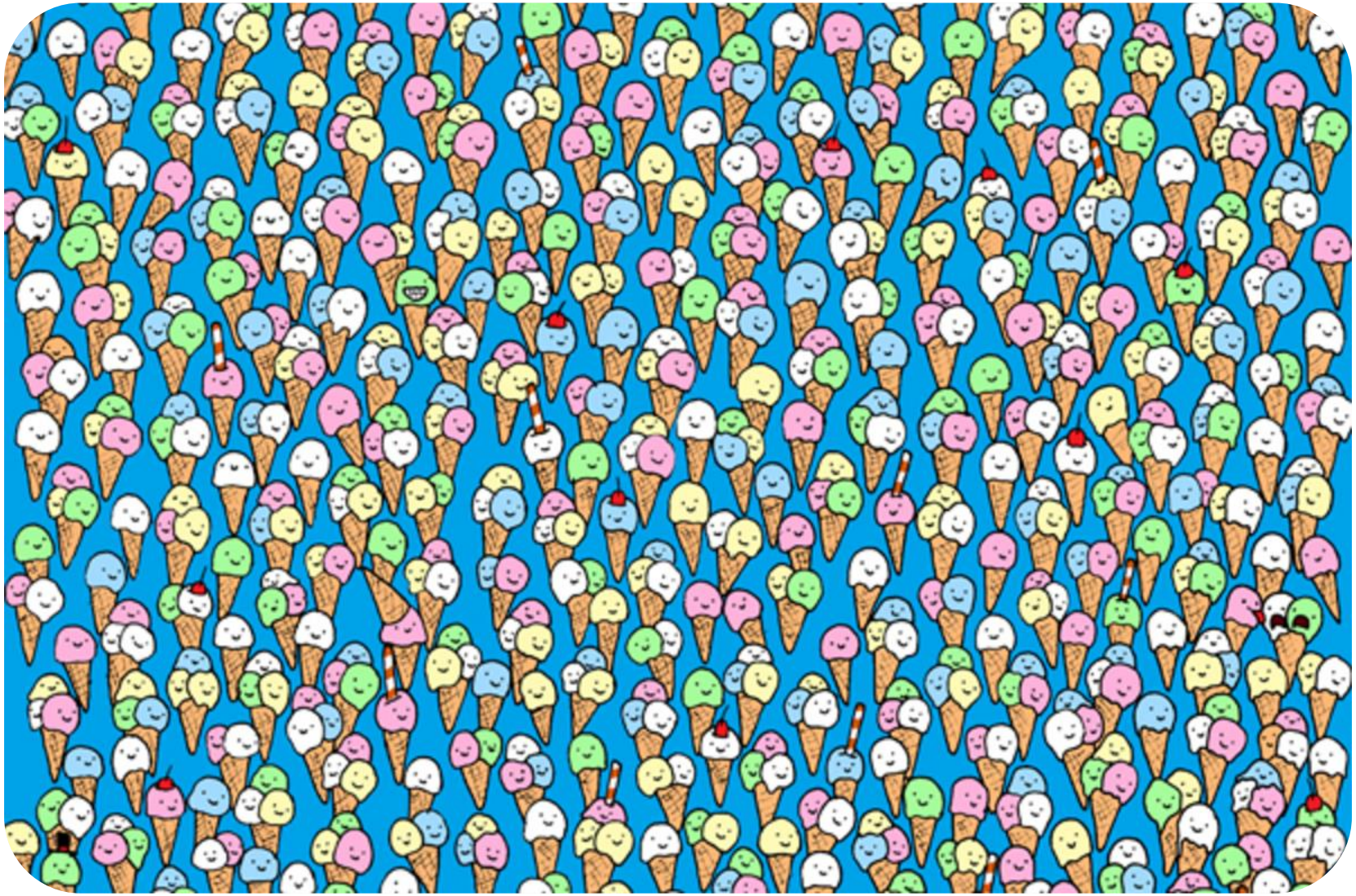
10k Оповещений получают более половины корпоративных центров управления безопасностью каждый день

101 День в среднем уходит на обнаружение инцидента

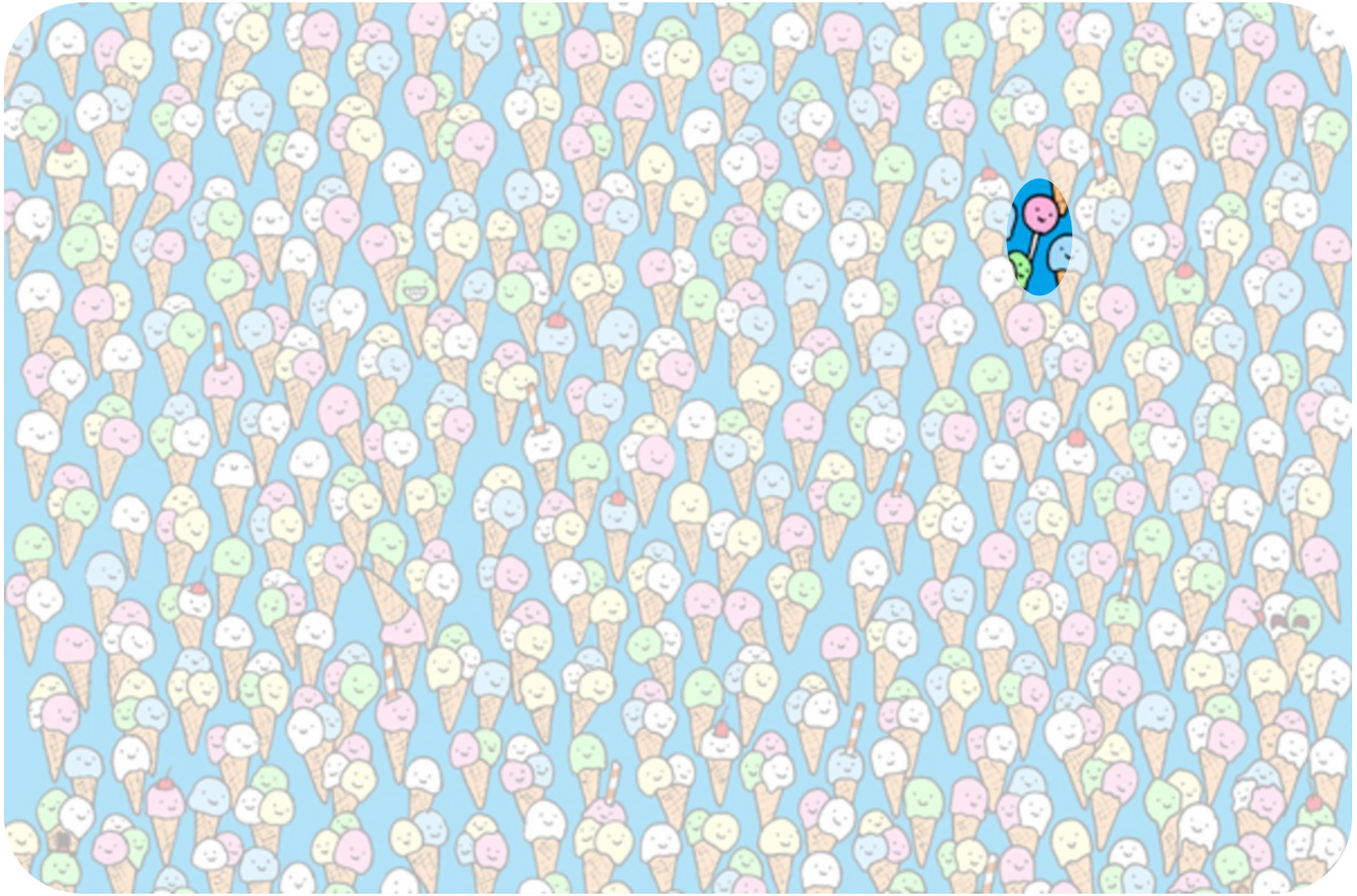
96% На столько уменьшиться ущерб, если инцидент будет выявлен в течение дня

30 Минут в среднем уходит у аналитика на обработку оповещения

Но при этом так сложно...



Но при этом так сложно...



Классическая схема работы с событиями ИБ

Сбор

- Централизованный сбор событий от множества источников
- Хранение и возможность доступа ко всему массиву событий

Нормализация

- Разбор событий от различных источников
- Приведение к единому формату

Агрегация

- Объединение однородных данных о событиях безопасности

Анализ

- Выявление признака инцидента ИБ на основе правил

По материалам ГОСТ Р № 59547-2021 Защита информации. Мониторинг информационной безопасности. Общие положения

Почему правил корреляции недостаточно?

Рассматривается только часть информации в событиях

И только конкретные типы событий

```
select  w1.event_id, w1.hostname, w1.id, w1.ip,
        w2.event_id, w2.hostname, w2.id, w2.ip
from pattern
            [
            every (w1= windows_event(event_id="140"
                    or event_id="141" or event_id="142" or event_id="106" or event_id="319") ->
                w2=windows_event(event_id="12" and w1.hostname=hostname))
            ].win:time(10 min)
```

Ограниченные возможности учета контекста

Противоречие в подходе

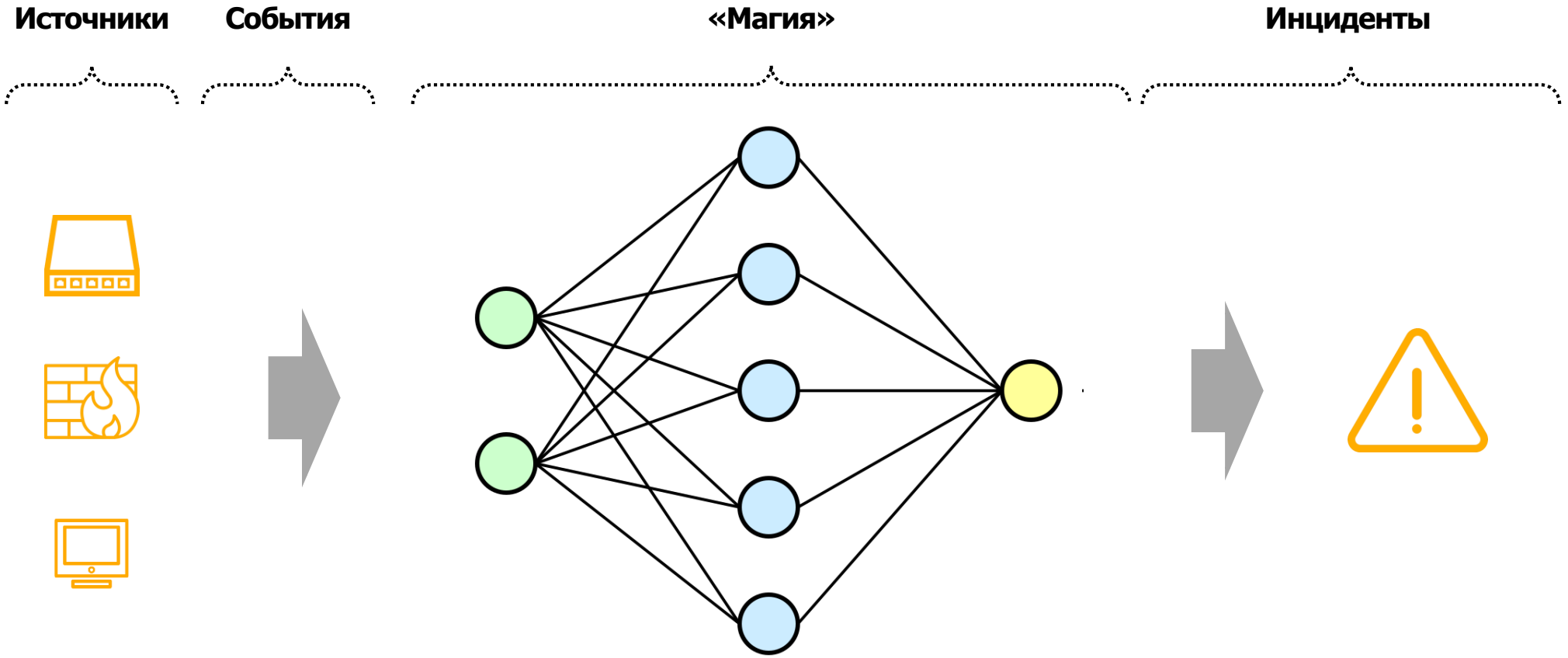
Инцидент ИБ с точки зрения правил корреляции:

1. Известный набор событий безопасности
2. Происходящих в определенной последовательности
3. Приводящий к конкретному нарушению состояния безопасности

Определение инцидента ИБ

1. Появление одного или нескольких неизвестных (неожиданных) событий ИБ
2. Значительно повышающих вероятность компрометации бизнес-операций и создания угрозы ИБ

Альтернативный подход



Но не все так просто

USSC

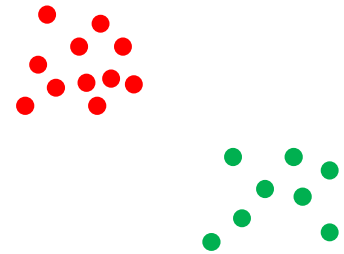
Источники | **События** | **Признаковое описание** | **Решающая функция** | **Результат распознавания**

$$X = (x_0, x_1, x_2, \ldots, x_n)$$

Как построить описание из события?

$$Y = f(X)$$

Как найти решающую функцию?



Возможности SOC

- Централизованный сбор событий от множества источников
- Хранение и возможность доступа ко всему массиву событий

- Единые правила нормализации – одинаковый набор признаков

- Все события обработаны одним набором правил
- Далее инциденты обработаны по одинаковым алгоритмам операторами

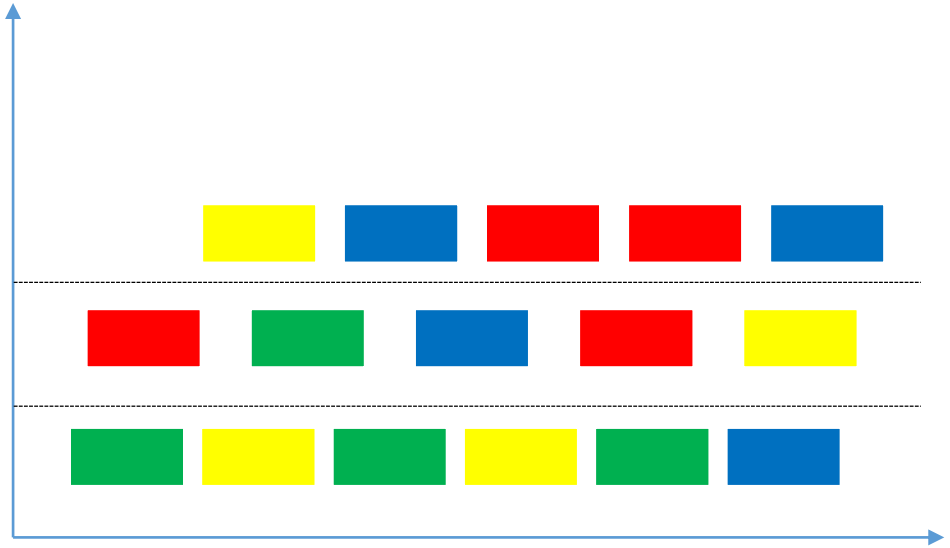
Большой объем размеченных данных для обработки с применением методов AI/ML

Метод №1: построение автоматического классификатора признаков инцидентов ИБ

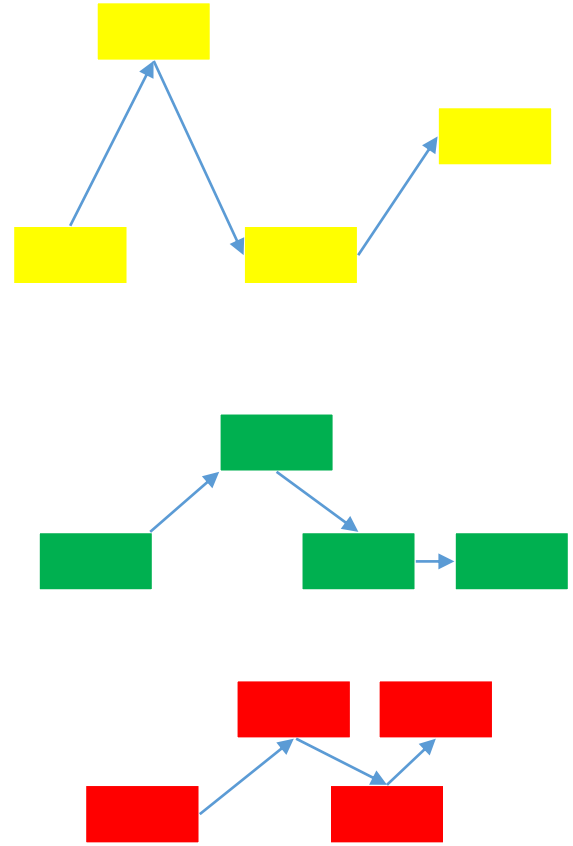
Метод №2: выявление цепочек событий, с большой вероятностью говорящих о признаке инцидента

USSC

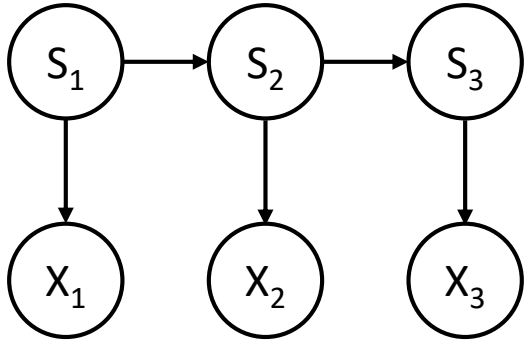
Исходный поток событий



Кластеризация на отдельные связанные события



Вероятностная модель



Достоинства и недостатки

МЕТОД №1

- \+ Простые алгоритмы обучения
- \+ В SOC есть готовые размеченные данные
- \+ Снижение нагрузки на оператора (отсеивание ложных срабатываний правил корреляции)
- — Не выявляет новые инциденты!
- — Обученную модель нельзя считать универсальной

МЕТОД №2

- \+ Не использует существующие правила
- \+ Не требует предварительной разметки данных
- \+ Способен выявить новые признаки инцидентов
- — Тяжелые алгоритмы, требующие много вычислительных ресурсов
- — Обученная модель не универсальна – надо обучать под каждую траекторию поведения
- — Требует квалифицированных аналитиков для сопровождения

USSC

СПАСИБО ЗА ВНИМАНИЕ

ВОПРОСЫ?

Николай Домуховский

Заместитель генерального директора по научно-технической работе

ООО «УЦСБ»

УРАЛЬСКИЙ ЦЕНТР СИСТЕМ БЕЗОПАСНОСТИ | USSC.RU