SIEM и атаки «нулевого дня»

ООО «Солидекс»

Ровнов Павел

6 октября 2017 г.

Содержание

Solidex

- Характеристика SIEM
- Характеристика атак TPA
- Есть ли шанс обнаружить атаку?
- Что можно было бы предпринять?
- Выводы

Характеристика систем SIEM

- **Источники сообщений**
- **Данные**
- **Правила**

Характеристика SIEM

- **Источники сообщений**
  - **Сенсоры, работающие по сигнатурам**
    - **IPS/IDS**
    - **AV**
    - **AntiSpam**

Характеристика SIEM

Solidex

- **Данные**
  - **Сообщения о событиях**
    - **Наименование атаки**
    - **Поля: IP, TCP/UDP port**
  - **Метаданные, детали (pcap) остаются на сенсоре**

Характеристика SIEM

- **Правила**
  - **Правила-фильтры**
    - **Трансляция в точности сообщений сенсора**
    - **Контекст события не важен**
  - **Корреляция**
    - **Шаблоны, выявляющие атаки**
    - **Атаки, известные аналитику**

Содержание

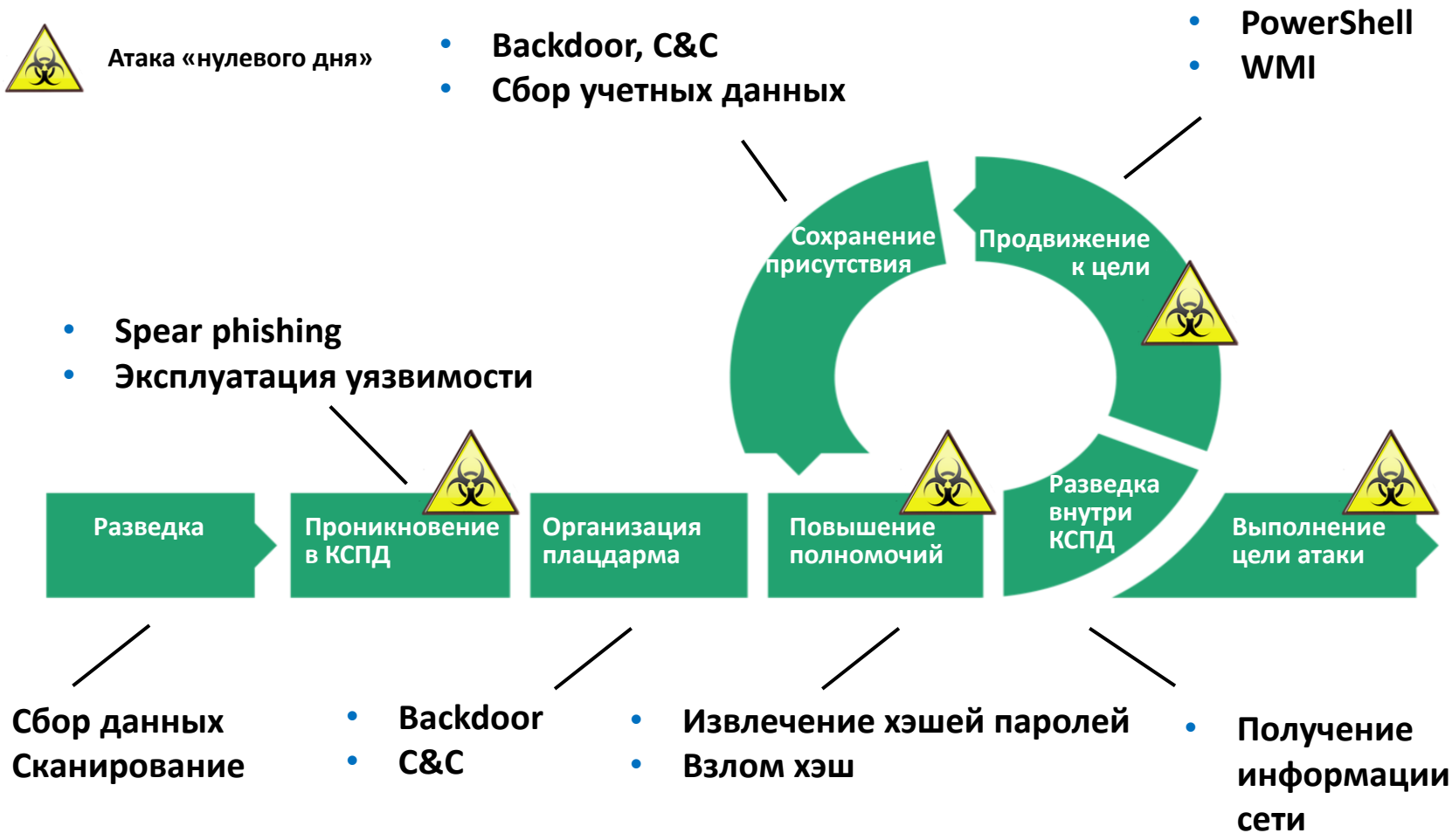
- Характеристика SIEM
- Характеристика атак TPA
- Есть ли шанс обнаружить атаку?
- Что можно было бы предпринять?
- Выводы

Характеристика Targeted Persistent Attack (TPA)

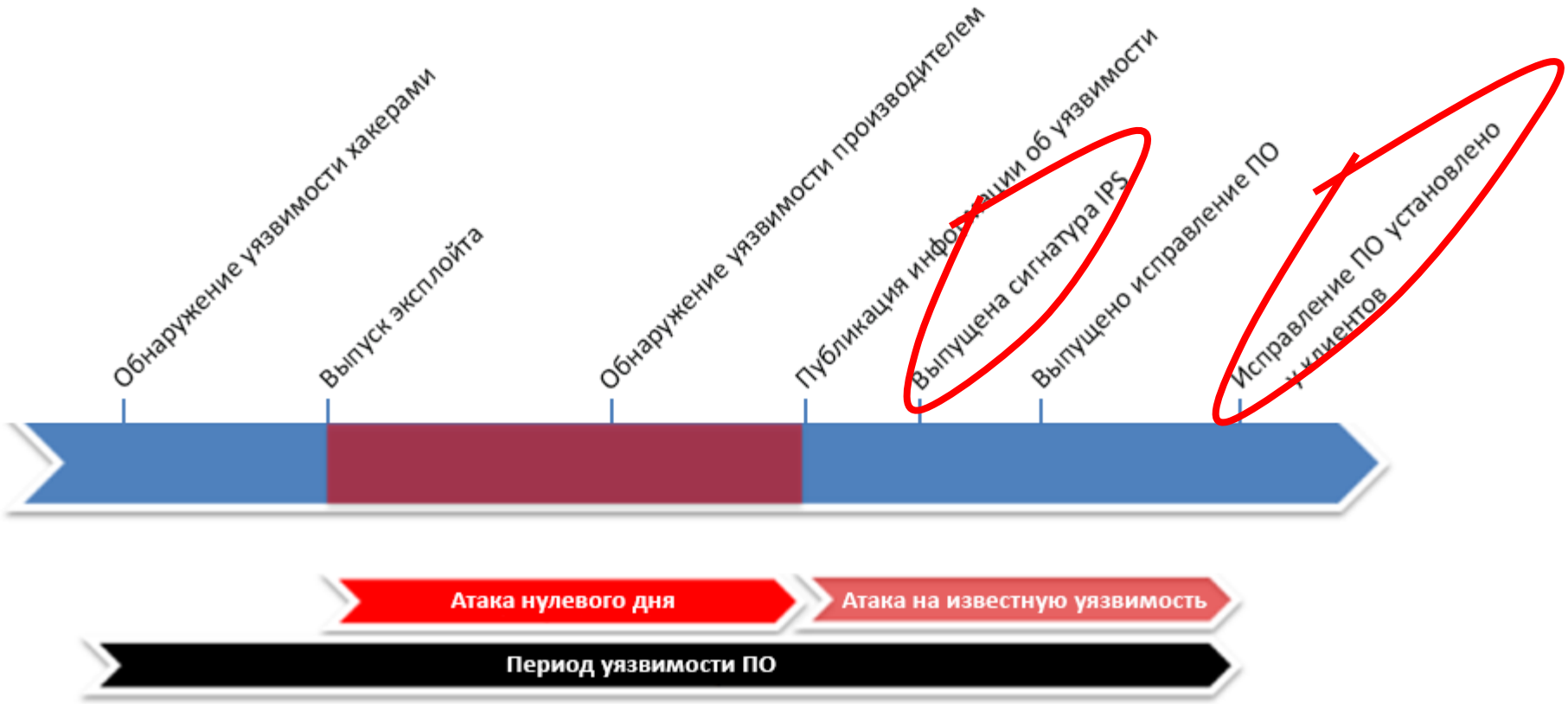
- **Targeted – заказная цель (организация), возможно, уникальные инструменты**

- **Persistent – устойчивость к попыткам обнаружения, при необходимости – смена вектора атаки**

Характеристика Targeted Persistent Attack (TPA)



Атака «нулевого дня»



- **Время жизни уязвимости ~ 6.9 лет**
  - **Время, в течение которого атака будет незаметна**

Содержание

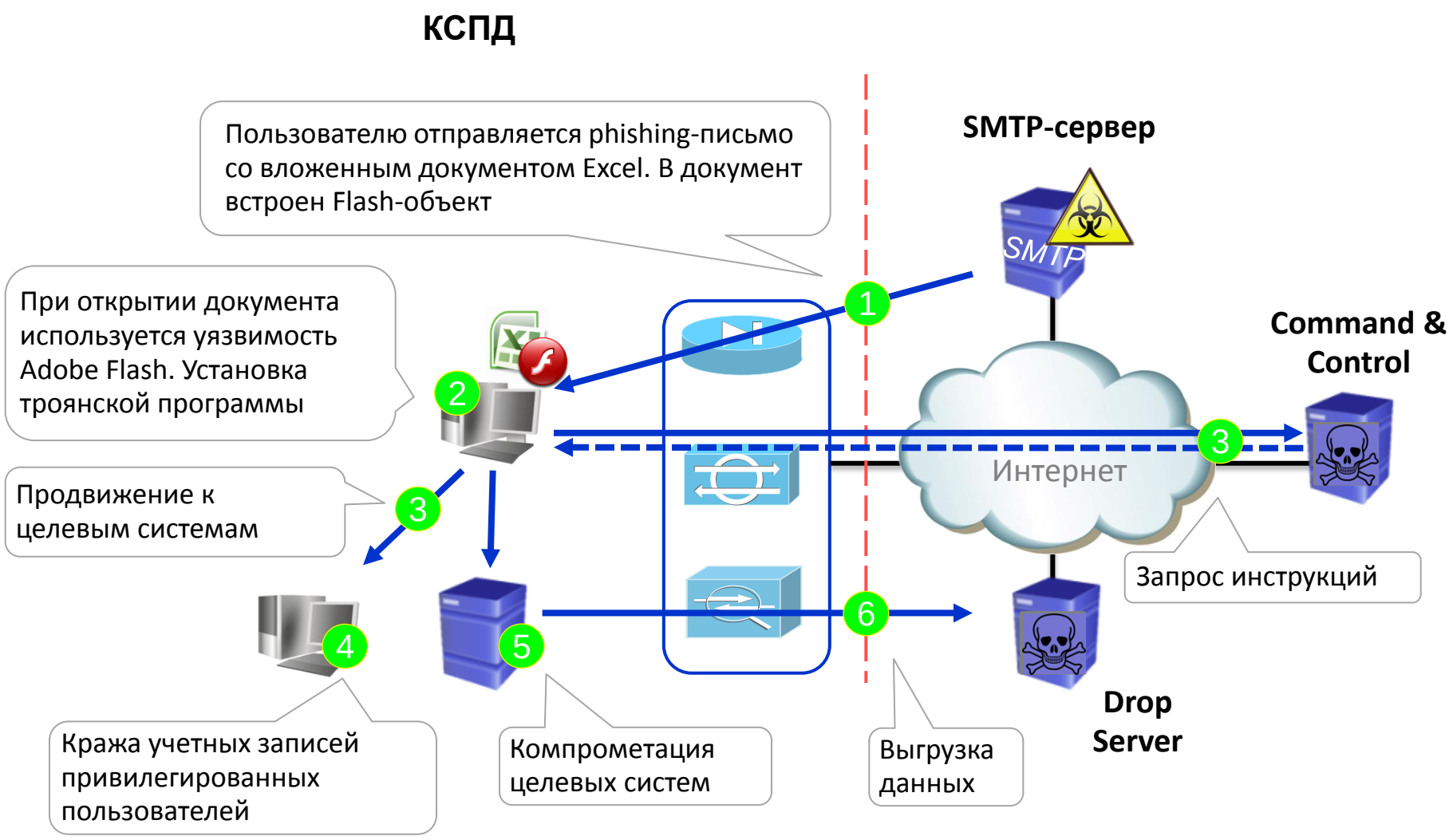
- Характеристика SIEM
- Характеристика атак TPA
- Есть ли шанс обнаружить атаку?
- Что можно было бы предпринять?
- Выводы

Как происходит обнаружение атак на практике?

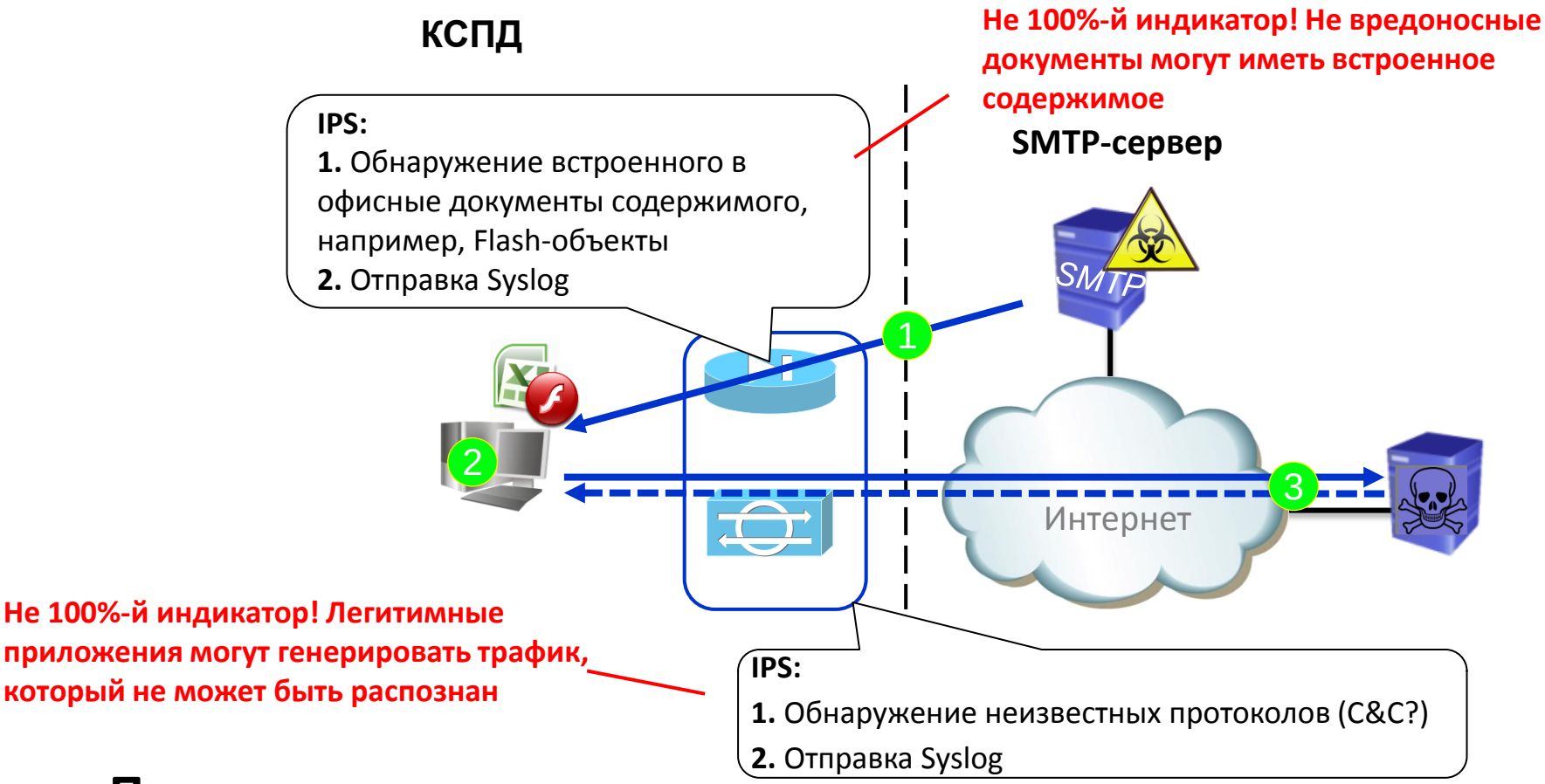
Solidex

- **Схема атаки**
- **Сценарий обнаружения атаки, правила**
- **Результаты**

Механика атаки



Сценарий обнаружения атаки



- **Правило:**
  - **Атака, если за событием «загрузка файла с встроенным содержимым» следует событие «установление C&C»**

Результаты

- **Обнаруженные атаки**
  - **Тестовые атаки (при испытаниях) обнаружены**
  - **А реальные?**

Известные атаки могли бы быть выражены в правилах

Вывод

- **Атака будет обнаружена, если:**
  - **Известно, каким способом будет производится атака**
  - **Вы – хакер:**
    - **Как работает атака?**
    - **Какие индикаторы сообщают об атаке?**
    - **Как описать атаку правилами SIEM?**

Содержание

- Характеристика SIEM
- Характеристика атак TPA
- Есть ли шанс обнаружить атаку?
- Что можно было бы предпринять?
  - Выявление аномалий поведения
  - Машинное обнаружение атак
- Выводы

Что можно предпринять?

Solidex

- **Заменить источники сообщений**
  - IPS, которые анализируют метаданные потоков, поведение
  - Пример обнаружения C&C в HTTPS (SSL-инспекции):
    - В каком направлении преобладает трафик?
    - Как часто клиент запрашивает сервер?
- **Данные**
- **Правила**

Что можно предпринять?

- **Заменить источники сообщений**
  - **Honeypot**
  - **Пример: OpenCanary**
    - **См. Семинар 2016б, «ЦОД. Контроль потоков данных» , goo.gl/L7UUML**

- **Данные**
- **Правила**

Что можно предпринять?

- **Источники сообщений**
- **Данные**
- **Заменить правила**
  - **Использовать математические алгоритмы**
    - **Исключить аналитика из процесса обнаружения атак**

Содержание

- Характеристика SIEM
- Характеристика атак TPA
- Есть ли шанс обнаружить атаку?
- Что можно было бы предпринять?
  - Выявление аномалий поведения
  - Машинное обнаружение атак
- Выводы

Механизмы TPA. Эксплуатация учетных записей

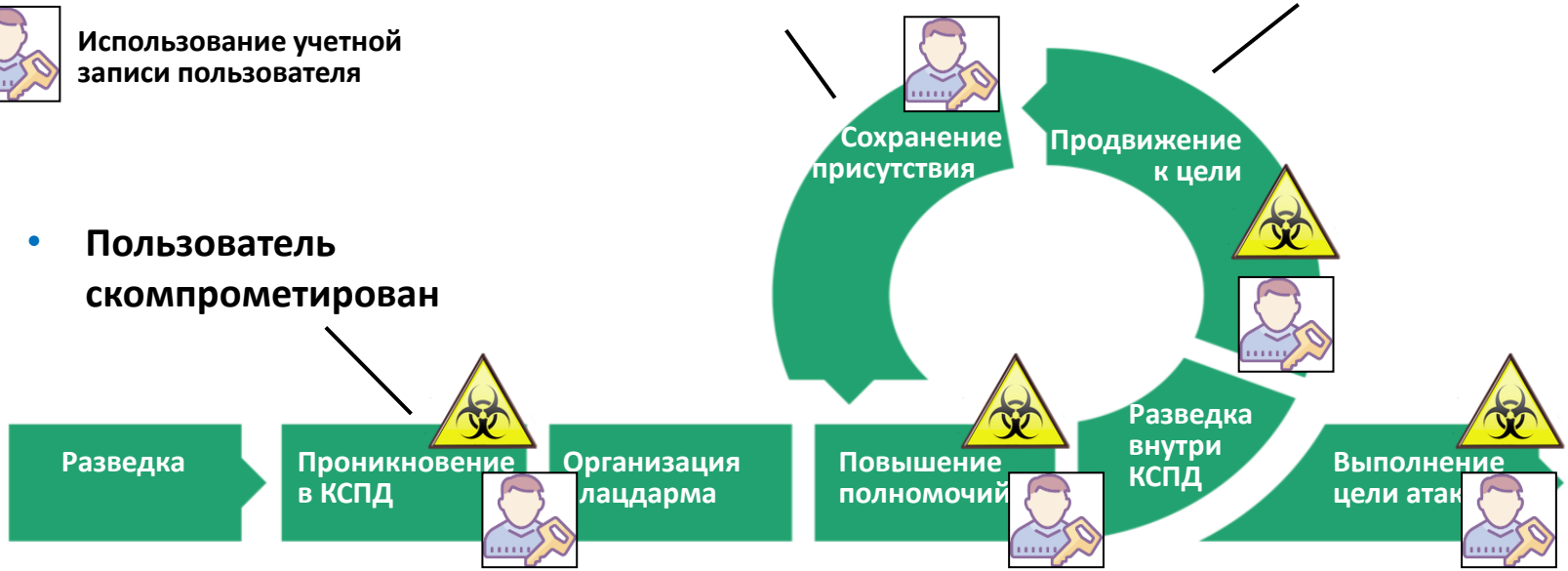
Атака «нулевого дня»

Использование учетной записи пользователя

- Получение доступа VPN
- Маскировка

- Использование учётной записи для доступа к другим системам

- Пользователь скомпрометирован



- Захват привилегированной четной записи

Как ведет себя учётная запись?

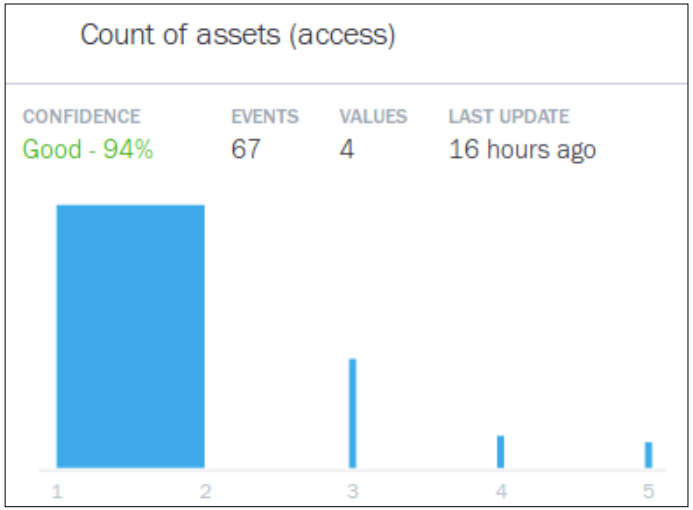
Solidex

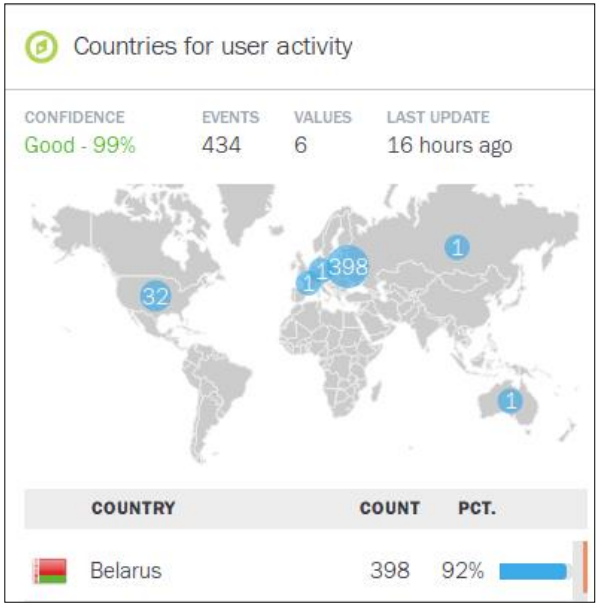
- **VPN-подключения:**
  - **Из-за пределов страны** ← **Первый раз для этого пользователя**
  - **По 12 часов в день** ← **Среднее длительность подключения – 1 час**
- **Доступ к активам:**
  - **К файловому хранилищу** ← **Первое обращение для группы пользователей**
  - **Чтение файлов** ← **Первый доступ для группы пользователей**
- **Использование приложений**
  - **Облачный файловый сервис Box** ← **Первое использование для данного пользователя**

Моделирование нормального поведения

Solidex

- **Типы событий:**
  - Аутентификация
  - Запуск приложений, процессов
  - Доступ к активам
  - События безопасности
  - …
- **Атрибуты:**
  - Время
  - Страна
  - Частота
  - …



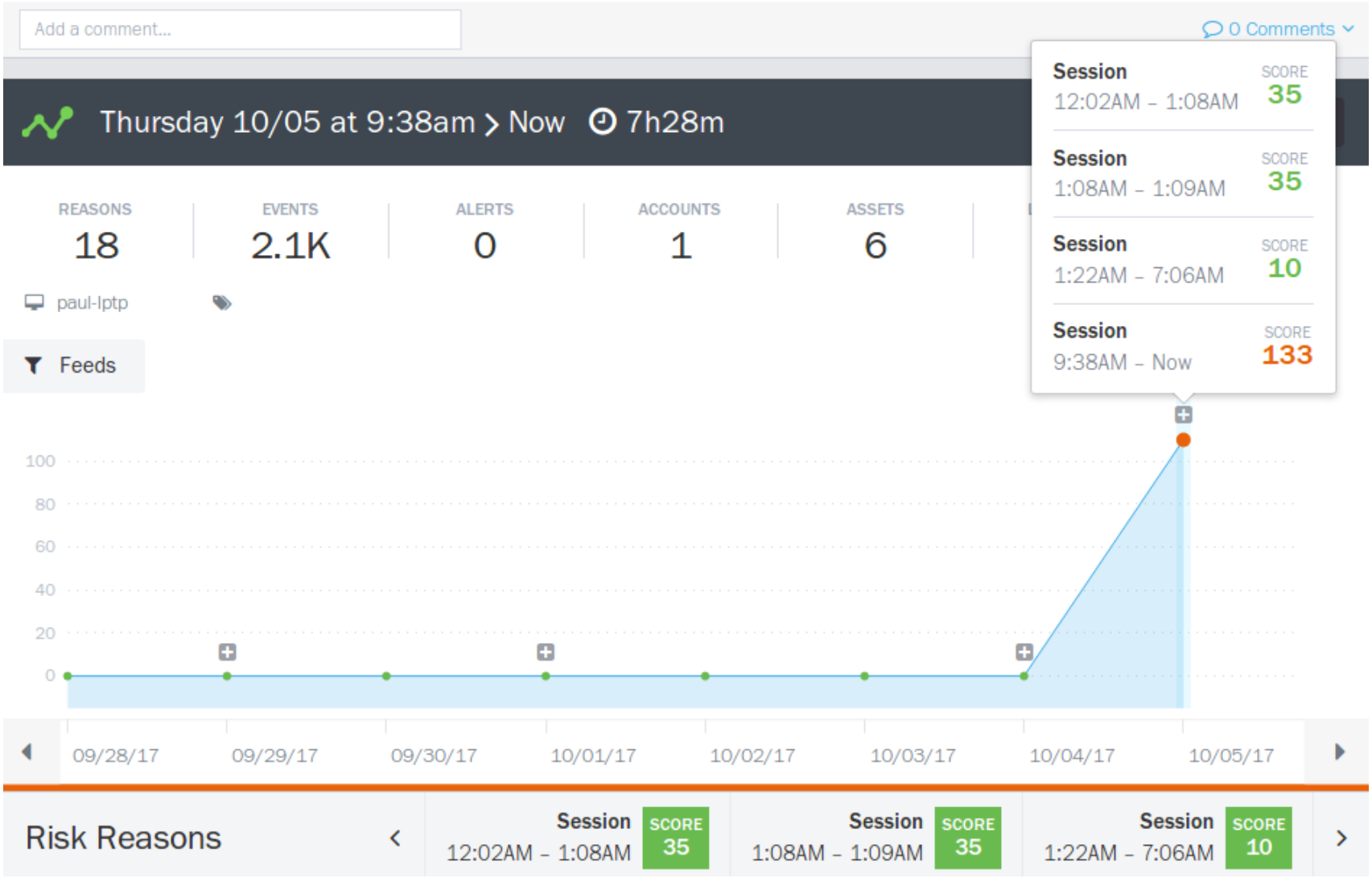


Определение аномального поведения

- **Варианты точек отсчёта:**
  - **История пользователя**
  - **Пользователь vs. Группа пользователей**
  - **Пользователь vs. Организация**

- **Аномально:**
  - **Что ранее никогда не происходило**
  - **Что отличается от предыдущего поведения**
  - **Что отличается от того, что обычно наблюдается для группы, организации в целом**

Демо!


Add a comment...
0 Comments
Thursday 10/05 at 9:38am > Now
7h28m
REASONS
18
EVENTS
2.1K
ALERTS
0
ACCOUNTS
1
ASSETS
6
paul-lptp
Feeds
Session
12:02AM – 1:08AM
SCORE
35
Session
1:08AM – 1:09AM
SCORE
35
Session
1:22AM – 7:06AM
SCORE
10
Session
9:38AM – Now
SCORE
133
100
80
60
40
20
0
09/28/17
09/29/17
09/30/17
10/01/17
10/02/17
10/03/17
10/04/17
10/05/17
Risk Reasons
Session
12:02AM – 1:08AM
SCORE
35
Session
1:08AM – 1:09AM
SCORE
35
Session
1:22AM – 7:06AM
SCORE
10

Подводные камни

- **Объем исходных данных**
  - **Достаточно ли данных, чтобы выявить что есть нормальное поведение пользователя?**
- **Выбор точки отсчёта:**
  - **Используется ли в качестве точки отсчета «нормальное» поведение пользователя?**
- **Как обрабатываются ложные срабатывания?**
  - **Пример: что-то что происходит впервые, но не является атакой?**

Что требуется для реализации?

- **Подход Big data**
  - **Анализ накопленных данным**
- **Моделирование, выявление аномалий**
  - **Статистические инструменты вычисления среднего, отклонения**
- **Группировка событий в сессии**
  - **Не только аномалий, но и событий безопасности**
  - **Контекст: что было до, что после события X**
  - **Рассмотрение цепочки событий**

Бонус. Упрощение расследований

Привычный подход

- **Поиск сообщений:**
  - **Просмотр логов, накопленных SIEM**
  - **Netflow/sflow, *.pcap**
  - **Исследование APM**
  - **…**
- **Построение цепочки событий**
- **Что в цепочке пошло не так?**

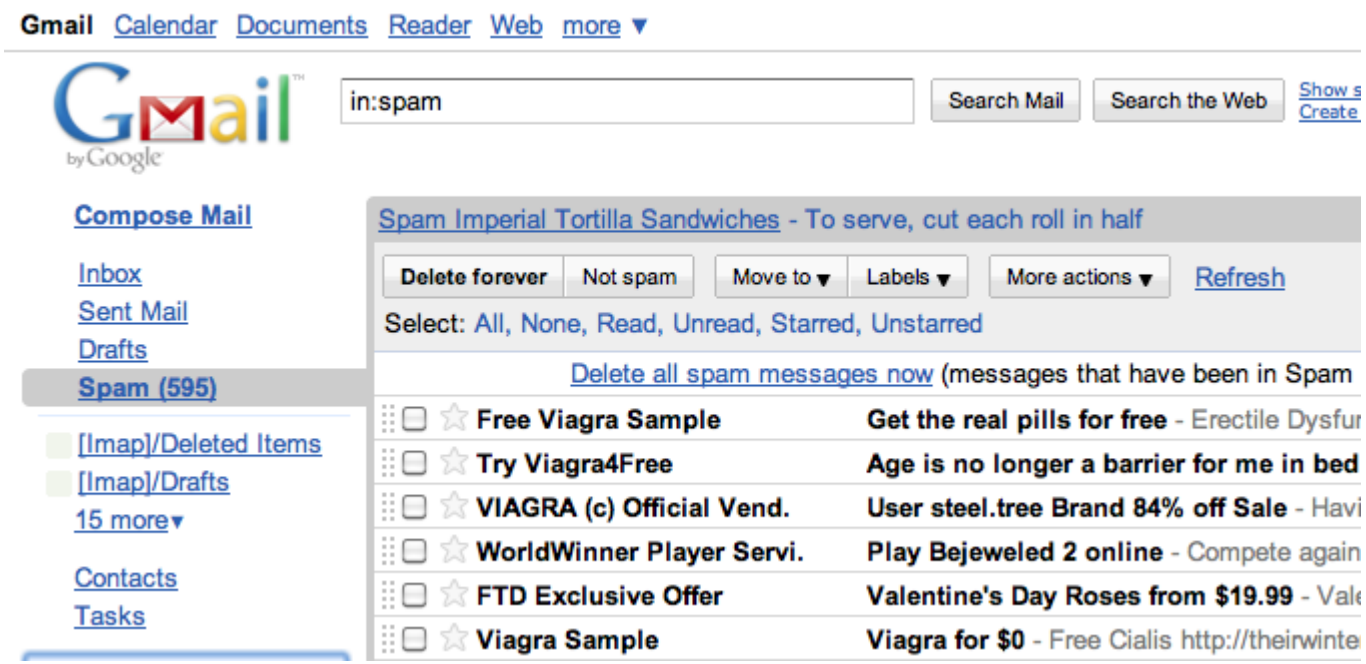
Алгоритмы сразу сообщают ответ!

Содержание

Solidex

- Характеристика SIEM
- Характеристика атак TPA
- Есть ли шанс обнаружить атаку?
- Что можно было бы предпринять?
  - Выявление аномалий поведения
  - Машинное обнаружение атак
- Выводы

Пример алгоритма фильтрации SPAM



- **Как часто «виагра» встречается**
  - **В спам-сообщениях?**
  - **В сообщениях, которые не являются спамом?**

Описание алгоритма фильтрации спам

- **Обучение**
  - Сообщения с маркерами «спам», «не-спам»
  - Определить «спамовую вероятность» слов:
    - Как часто слово X встречается в спам, не-спам?
- **Применение**
  - Поступает новое сообщение
  - Анализ слов; определение вероятность, что письмо, составленное из таких слов – спам
- **В случае, если спам прошёл:**
  - Перенаправление пользователем спам-письма с маркером «спам» для уточнения классификации

Машинное обнаружение атаки

- **Какую задачу требуется решить?**
- **Есть ли алгоритм, который бы решить задачу?**
  - **Универсального ответа на все вопросы, конечно, нет**
- **Как хорошо алгоритм справился с задачей?**

Некоторые задачи

Solidex

- **Обнаружение C&C, malware**
  - **Алгоритм Random Forest**
- **Обнаружение кражи учётной записи пользователя**
  - **Алгоритм K-means**

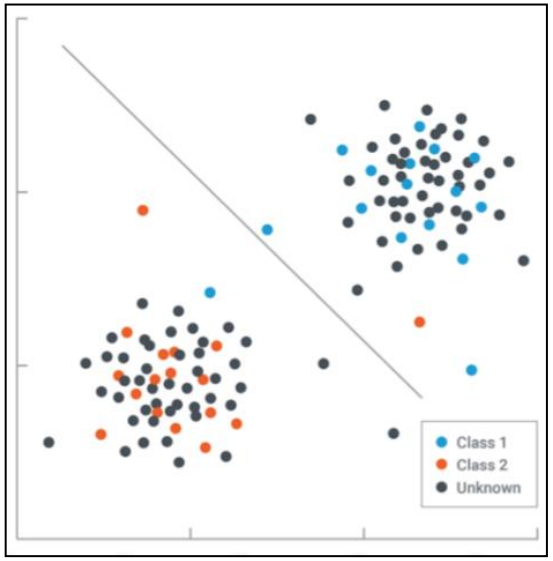
Задача обнаружения C&C. Постановка

- **Обнаружить АРМ, которые находятся под контролем злоумышленника и управляются через соединения C&C**

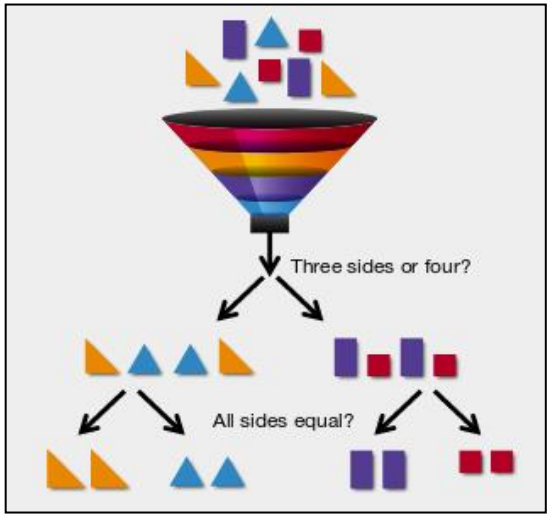
- **Исходные данные:**
  - **Использовать логи HTTP-запросов пользователей**
  - **См. логи в SIEM**

Задача обнаружения C&C

- **Задача разделении на классы:**
  - **В нашем случае классы:**
    - **C&C**
    - **Не C&C**



- **Алгоритм Random Forest:**
  - **Данные маркированы**



Вопросы

- **Где получить маркированные данные?**
  - **Трафик C&C**
    - **Вариант: наборы данных в публичном доступе в Интернете – логи заведомо зараженных хостов**
  - **Трафик, соответствующий нормальному поведению АРМ**
    - **Набор данных #1: Набор данных из Интернет соответствующих «заведомо чистой сети»**
    - **Набор данных #2: Трафик нашей сети (предполагаем, что если количество зараженных хостов есть, то оно не существенно)**

Вопросы

- **Выбор атрибутов**
  - **Как по каким признакам отличать трафик C&C от легитимного трафика?**
    - **user_agent**
    - **uri**
    - **referrer**
    - **host**
    - **subdomain**
    - **method**
    - **status_code**
    - **…**

Результат: набор данных 1

Solidex

```
% ./train_flows_rf.py -o data/http-malware.log http-training.log
Reading normal training data
Reading malicious training data

Building Vectorizers

Training

Predicting (class 0 is normal, class 1 is malicious)
class  prediction
0      0             12428
       1                15
1      0                19
       1              9563
dtype: int64
F1 = 0.998225469729
```

Фактический класс

Предсказание алгоритма

Случай ложной классификации как C&C

Случаи ложного не распознавания C&C

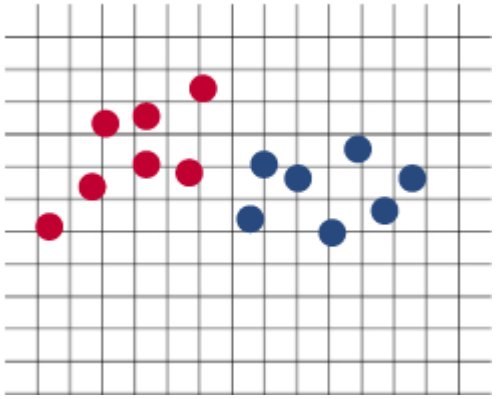
Результат: набор данных #2

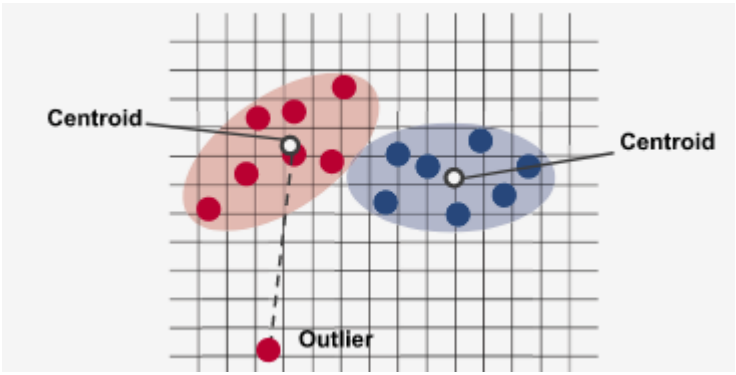
- **Обучение было невозможно!**
  - **В качестве одного из атрибутов алгоритм использовал поле лог-сообщения user_agent**
  - **В лог-сообщениях, которые формировал сенсор в нашей сети, поле user_agent отсутствует (не заполняется)**

Кража учётной записи. Постановка задачи

- **Обнаружить кражу учётной записи пользователя, через обнаружение изменения поведения**
  - **Информация о нормальном поведении, или аномальном априорно не известна**

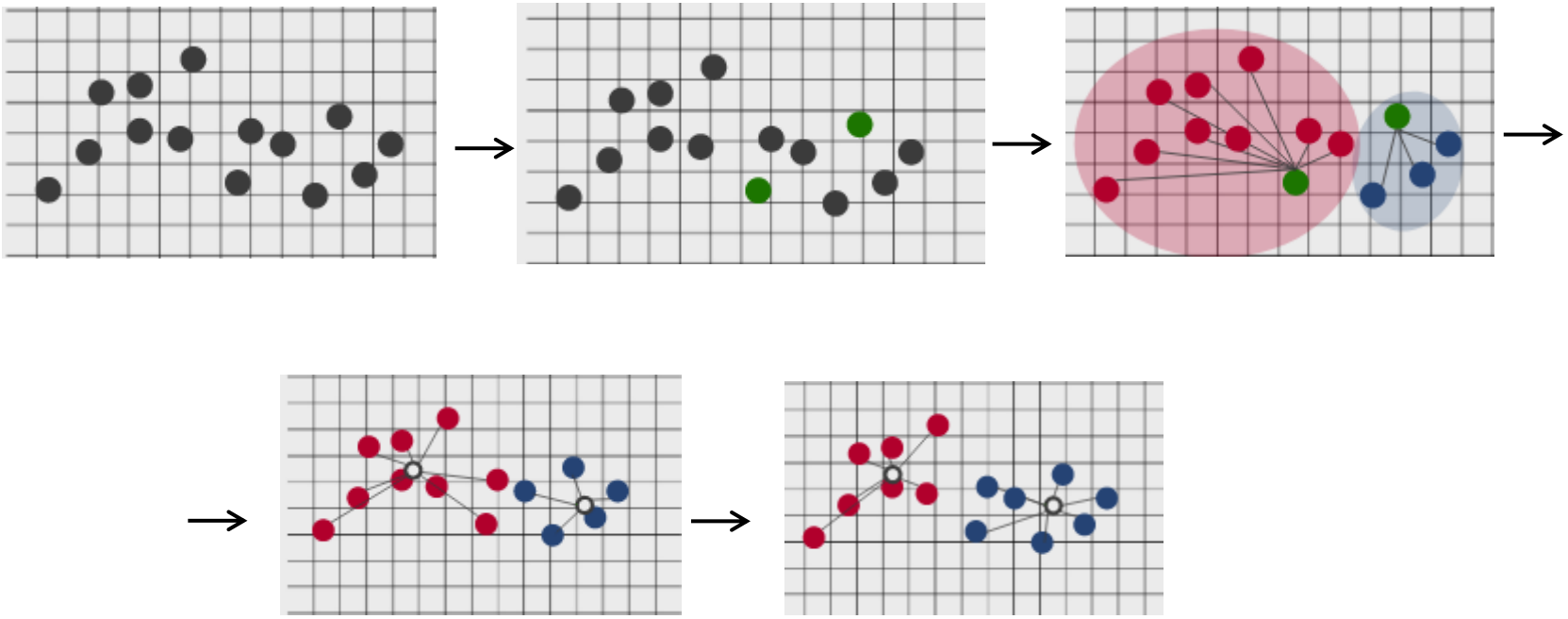
Определение аномалии





- **Аномалия в том, как далеко значение отстоит от группы**
- **Вопрос:**
  - **Как выполнить разделение на группы?**

Определение групп (K-means)



Подводные камни использования алгоритмов

- **Весь набор задач не может быть решен одним алгоритмом**
  - **Какие задачи решает система?**
  - **Какие алгоритмы используются и для чего?**

- **Есть ли данные, требуемые алгоритму для работы?**
  - **Может ли источник событий выдать такие атрибуты?**

Подводные камни использования алгоритмов

- **На сколько релевантны данные, которые используются на этапе обучения**
  - **Что, если в примере с C&C и malware: зараженные хосты были бы представлены логами для Windows, а «чистые» хосты – логами для Linux?**

- **Защита исходных данных**
  - **Не может ли злоумышленник влиять данные, которые используются при обучение алгоритма?**
  - **Может ли злоумышленник повлиять выбираемые для анализа на атрибуты?**

Вывод

- **Средствами алгоритмов можно:**
  - **Обнаружить атаки, за счет детектирования аномалий в поведении**
  - **Обнаружить общие черты атак, что в свою очередь позволяет детектировать:**
    - **Атаки, идентичные изученным**
    - **Новые атаки, которые все еще наследуют изученные ранее черты**
- **При обнаружении атаки средствами алгоритмов участие аналитика, возможно, необходимо только для устранения последствий инцидента**

Solidex

Ваши вопросы?