НТЦ ВУЛКАН

Реализация Use case-ов

SOC Forum 2017

Александр Кузнецов, CISM

Руководитель направления информационной безопасности

22.11.2017

www.ntc-vulkan.ru

СОДЕРЖАНИЕ

Что такое Use case?

- Определенное условие или событие (обычно относящиеся к конкретной угрозе) для обнаружения или реагирования средствами защиты информации

Gartner

- Типовой для конкретного SOC сценарий функционирования, включающий набор действий или шагов, позволяющих соответствующим ролям/членам команды SOC достигать поставленных целей (обнаружение утечки информации, обнаружение внутренних нарушителей, обнаружение APT и т.п.)

CISCO

- Описание ситуации, которую требуется наблюдать, отслеживать и предпринимать определенные действия в случае обнаружения

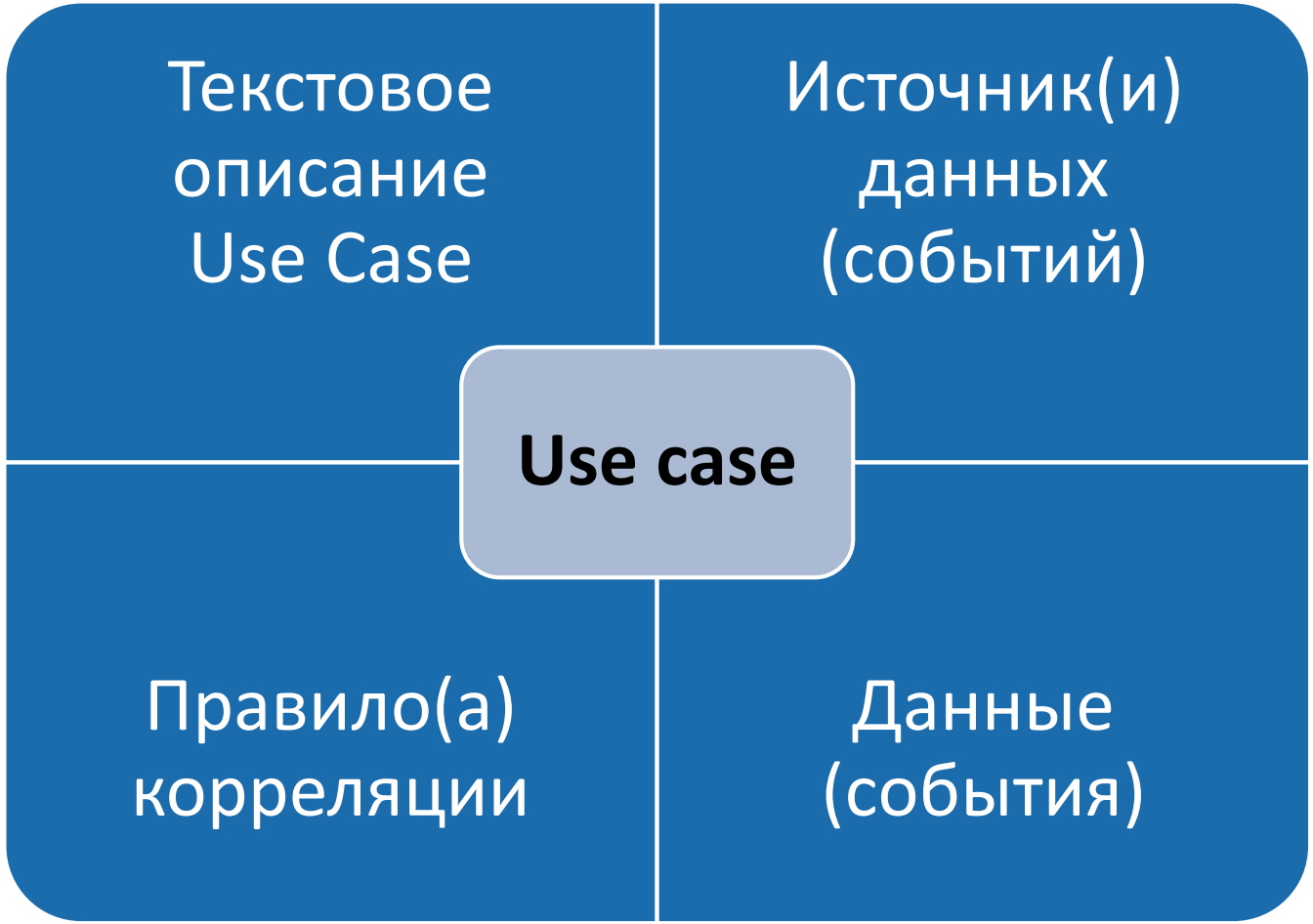
IBM

- **Андрей Прозоров** Посто Use cases сами по себе - это именно сценарии использования

Жизненный цикл Use case-ов

- Область рассмотрения в рамках настоящей презентации

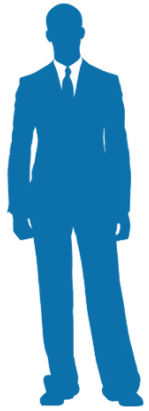
Составные части Use case



В рамках области рассмотрения настоящей презентации

Действующие лица

- Дизайнер Use case-ов



  - Своя терминология: *объект атаки*
  - Инструментарий: *Word/Excel*
  - Сценарий: *текст*

- Администратор SIEM-системы

  - Своя терминология: *источник событий*
  - Инструментарий: *консоль SIEM*
  - Сценарий: *корреляционные правила*

- Администратор СрЗИ

  - Своя терминология: *инсталляция*
  - Инструментарий: *консоль СрЗИ*
  - Сценарий: *нажать какие-то кнопки*

- Системный администратор

  - Своя терминология: *экземпляр БД*
  - Инструментарий: *консоли ПО*
  - Сценарий: *нажать какие-то кнопки*

Примеры Use case-ов

intel Security

Use Cases

- Multiple changes from administrative accounts.
- Unauthorized user access to confidential data.
- Unauthorized subnet access to confidential data.

RSA White Paper

Tracking user actions across disparate systems

Security incident response, compliance as well as Human Resources (HR) requirements call for investigating user activities across multiple information systems.

scenarios we are looking to detect: *Suspicious logins should be monitored to detect suspicious logons and attempted logons of privileged accounts.*

SECURITY USE CASES USING SPLUNK |

Use Case 2: Acceptable Use Monitoring

Acceptable Use Monitoring covers a basic questions, i.e. what resource is being accessed by whom and when. Organizations generally publish policies for users to understand how they can use the organization's resources in the best way. Organizations should develop a baseline document to set up threshold limits, critical resources information, user roles, and policies, and use that baseline document to monitor user activity, even after business hours, with the help of the SIEM solution.

Многочисленные неуспешные попытки получения доступа к файлам/директ

Неуспешные многочисленные попытки изменения прав доступа на директо

Массовое успешное изменение прав доступа на директориях

Отдельно взятый пример описания Use case

Многочисленные попытки несанкционированного доступа привилегированных пользователей к критичным данным в течение короткого промежутка времени

- **Привилегированные пользователи**
- **Критичные данные**
- **Многочисленные**
- **В течение короткого промежутка**
- **Попытки несанкционированного доступа**

О чём Вы подумали?

- **Привилегированные пользователи**
  - *Domain Admins (администраторы домена)*
  - *Root (супер пользователь в *nix)*
  - *ntc-vulkan.ru\Ivan.Ivanov*
  - *Admin_**
- **Критичные данные**
  - *C:\Windows*
  - *C:\Users\User_Name\Documents*
  - *X:\Business_Data*
  - Все файлы *.dbv
- **Многочисленные**
  - *2 раза*
  - *10 раз*
  - *100 раз*
  - *1000 раз*
- **В течение короткого промежутка**
  - *5 секунд*
  - *5 минут*
  - *55 минут*
  - *5 часов*

Источники данных (событий)

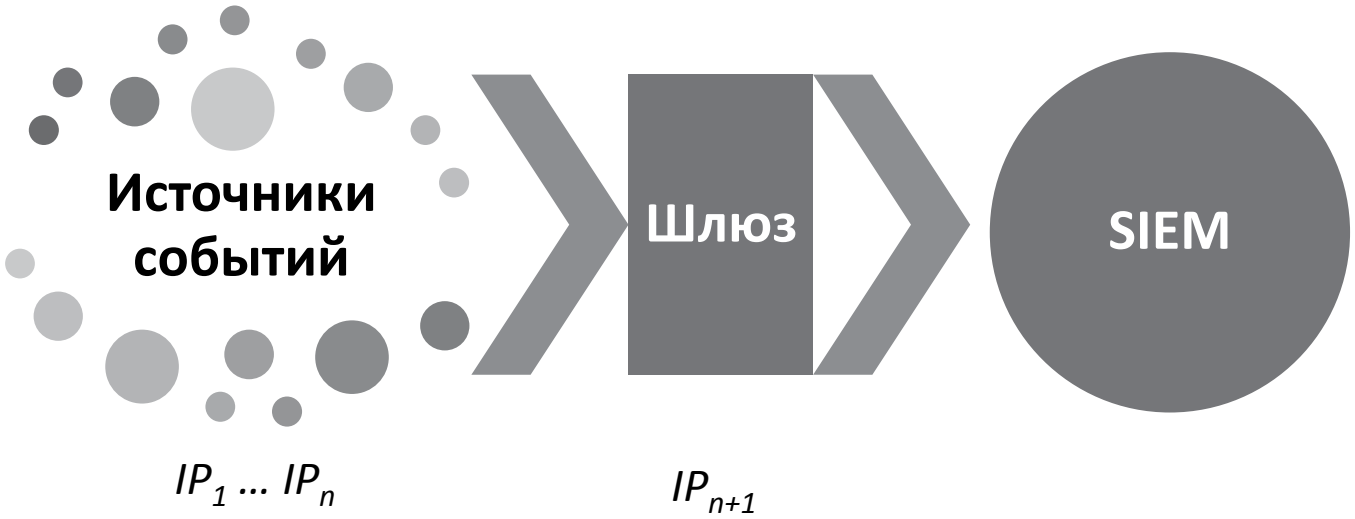
1-ый вопрос: есть или нет?

2-ой вопрос: какой именно источник данных?

- Операционная система (*локально или на контроллере домена*)
- Сторонний программный агент
- Промежуточные устройства

3-ий вопрос: какой адрес источника данных?

- Непосредственно адрес источника данных
- Адрес промежуточного шлюза



Данные (события)

Необходимые условия

- Возможность зарегистрировать событие
- Возможность предоставить доступ к зарегистрированному событию

Данные (события)

Необходимые условия

- Возможность зарегистрировать событие
- Возможность предоставить доступ к зарегистрированному событию

«Достаточные условия»

- Читаемость события

	CG_NAME	SL_CATEGORY	SL_TIMEGENERATED	SL_DATASHORT
1	ЦУС	40	2016-02-12 07:10:13.000	0x540000000100000000000000000000000200000080D0C028...
2	ЦУС	40	2016-02-12 07:38:56.000	0x5E0000000000000C2F1F2F0EEE5EDEDFBE920E0E4ECE8E...
3	КШ с ЦУСом	35	2016-02-12 07:40:35.000	0x6D000000C2F1F2F0EEE5EDEDFBE920E0E4ECE8EDE8F1F2...
4	ЦУС	40	2016-02-12 07:42:55.000	0x540000000100000000000000000000000200000090E0C028...
5	КШ с ЦУСом	40	2016-02-12 07:42:13.000	0x540000000100000000000000000000000525649534F52000000...
6	ЦУС	35	2016-02-12 07:45:27.000	0xD0000000C2F1F2F0EEE5EDEDFBE920E0E4ECE8EDE8F1F2...
7	ЦУС	40	2016-02-12 07:58:00.000	0x5F0000000000000C2F1F2F0EEE5EDEDFBE920E0E4ECE8E...
8	ЦУС	40	2016-02-12 08:15:26.000	0x5E0000000000000C2F1F2F0EEE5EDEDFBE920E0E4ECE8E...
9	КШ с ЦУСом	35	2016-02-12 08:19:08.000	0x74000000C2F1F2F0EEE5EDEDFBE920E0E4ECE8EDE8F1F2F...

Данные (события)

Необходимые условия

- Возможность зарегистрировать событие
- Возможность предоставить доступ к зарегистрированному событию

«Достаточные условия»

- Читаемость события
- Наличие необходимых данных в событии

Windows Security Log Event ID 567

567: Object Access Attempt

```
Object Access Attempt:
Object Server:Security
Handle ID:144
Object Type:File
Process ID:3156
Image File Name:C:\WINDOWS\system32\notepad.exe
Accesses:WriteData (or AddFile)
AppendData (or AddSubdirectory or CreatePipeInstance)
Access Mask:0x6
```

	CG_NAME	SL_CATEGORY	SL_TIMEGENER
1	ЦУС	40	2016-02-12 07:1
2	ЦУС	40	2016-02-12 07:3

```
nId: "2248675" EventId: "000003fd"
EventDesc: "Тип события:     Обновлены не все компоненты
Результат:     Обновлены не все компоненты
Пользователь:     NTC-VULKAN\xxx (Активный пользователь)
Дата выпуска:     14.xx.2017 17:27:00" DeviceTime: "2017-xx-
14 14:41:48.0" SourceInt: "16777xxxx" wstrPar1: "null" wstrPar2: "nul
l" wstrPar3: "null" wstrPar4: "null" wstrPar5: "null" wstrPar6: "null
" wstrPar7: "null" wstrPar8: "null" wstrPar9: "null"
```

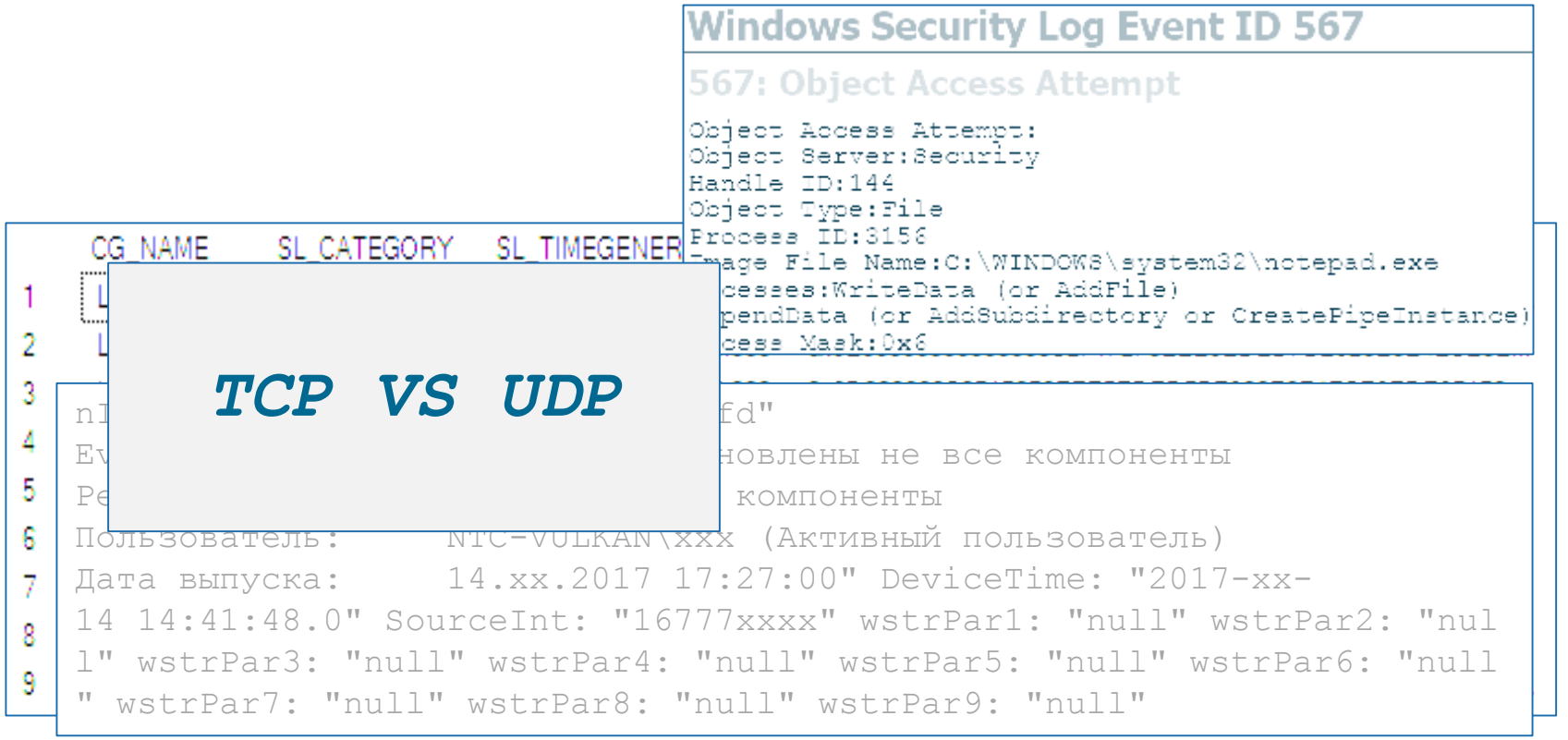
Данные (события)

Необходимые условия

- Возможность зарегистрировать событие
- Возможность предоставить доступ к зарегистрированному событию

«Достаточные условия»

- Читаемость события
- Наличие необходимых данных в событии
- Гарантированная доставка события



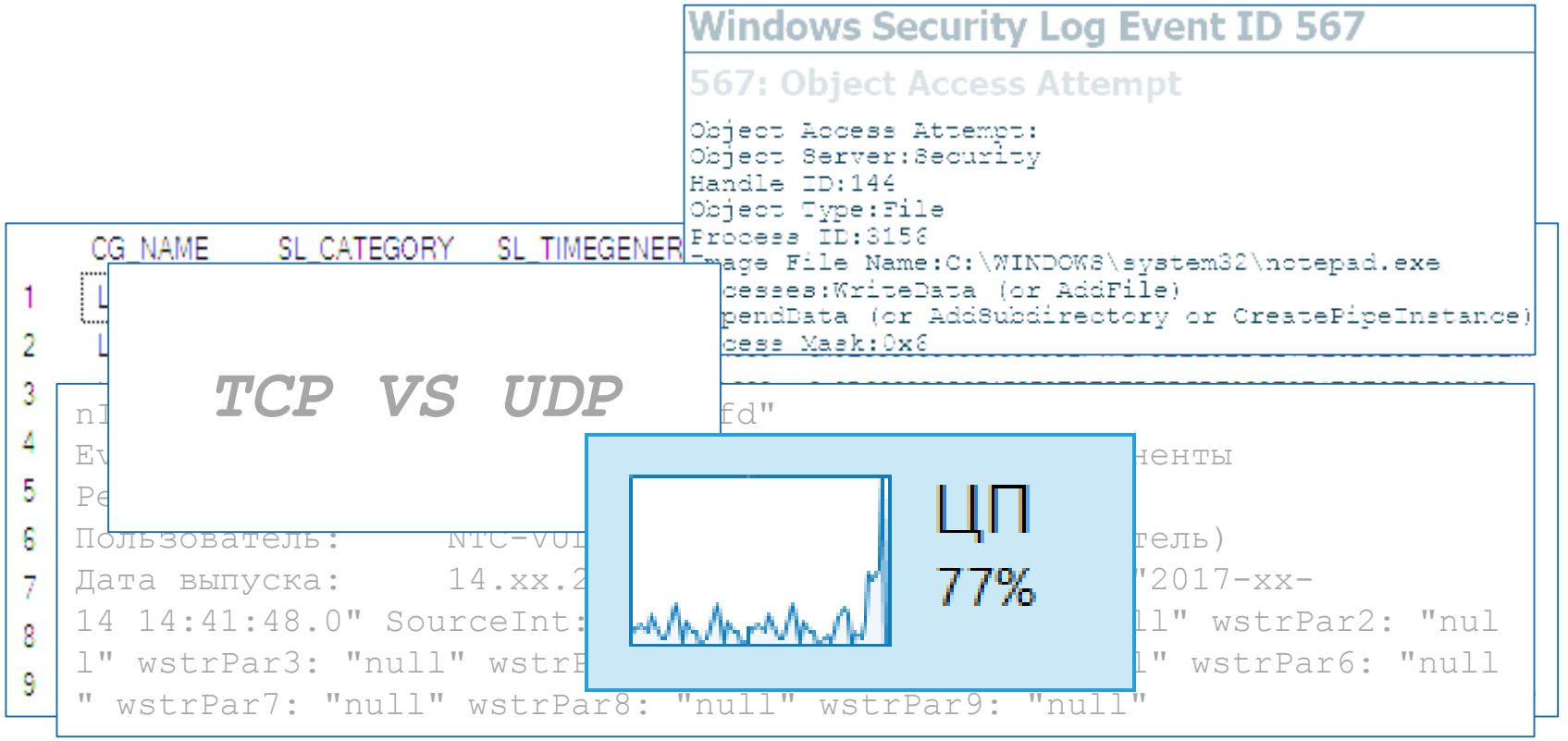
Данные (события)

Необходимые условия

- Возможность зарегистрировать событие
- Возможность предоставить доступ к зарегистрированному событию

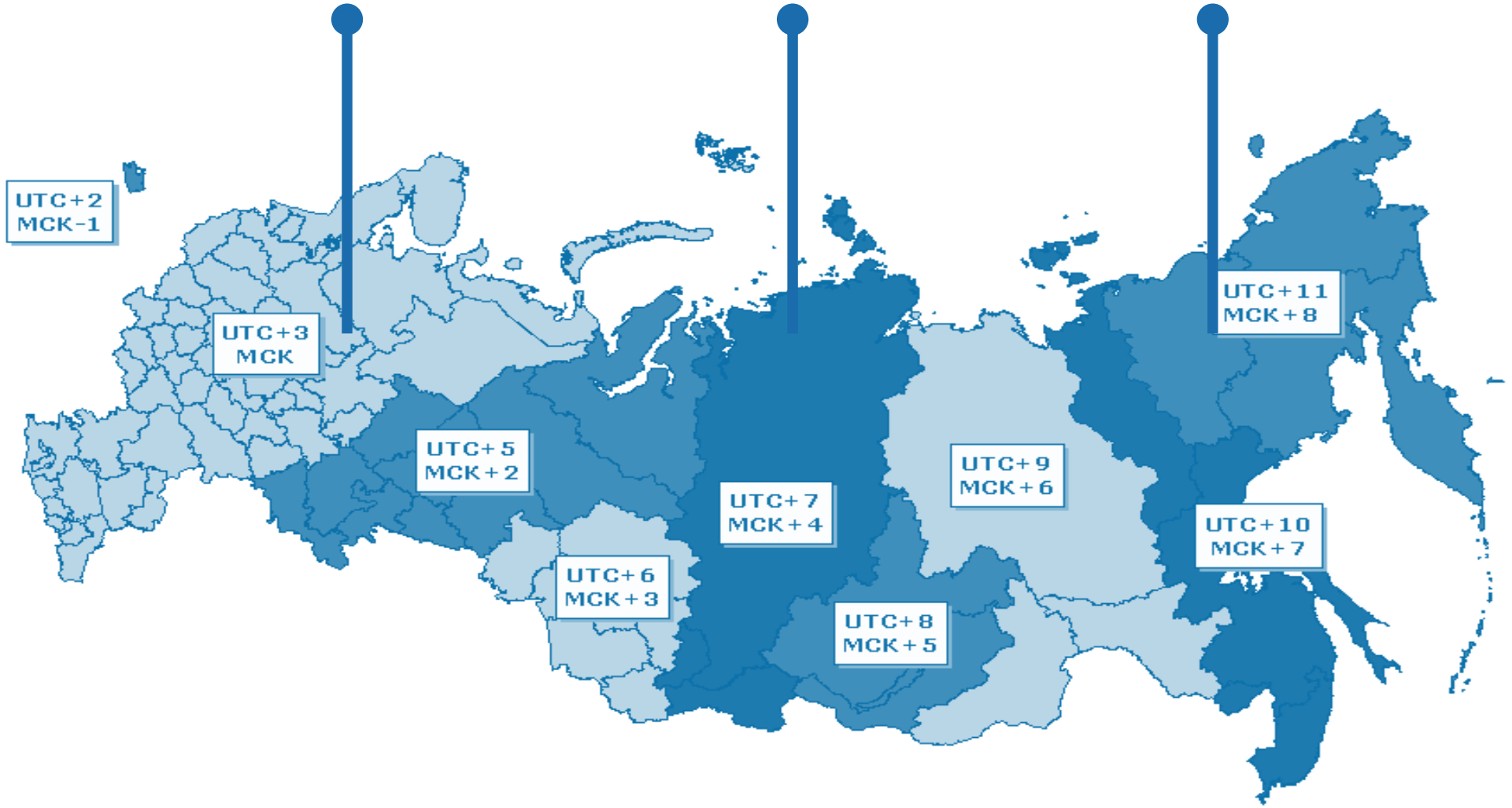
«Достаточные условия»

- Читаемость события
- Наличие необходимых данных в событии
- Гарантированная доставка события
- Влияние регистрации событий на произво -дительность источника данных



Время события

Δt между событиями: 0 мин. +1 мин. +2 мин.



Время события

Δt между событиями: 0 мин. +1 мин. +2 мин.

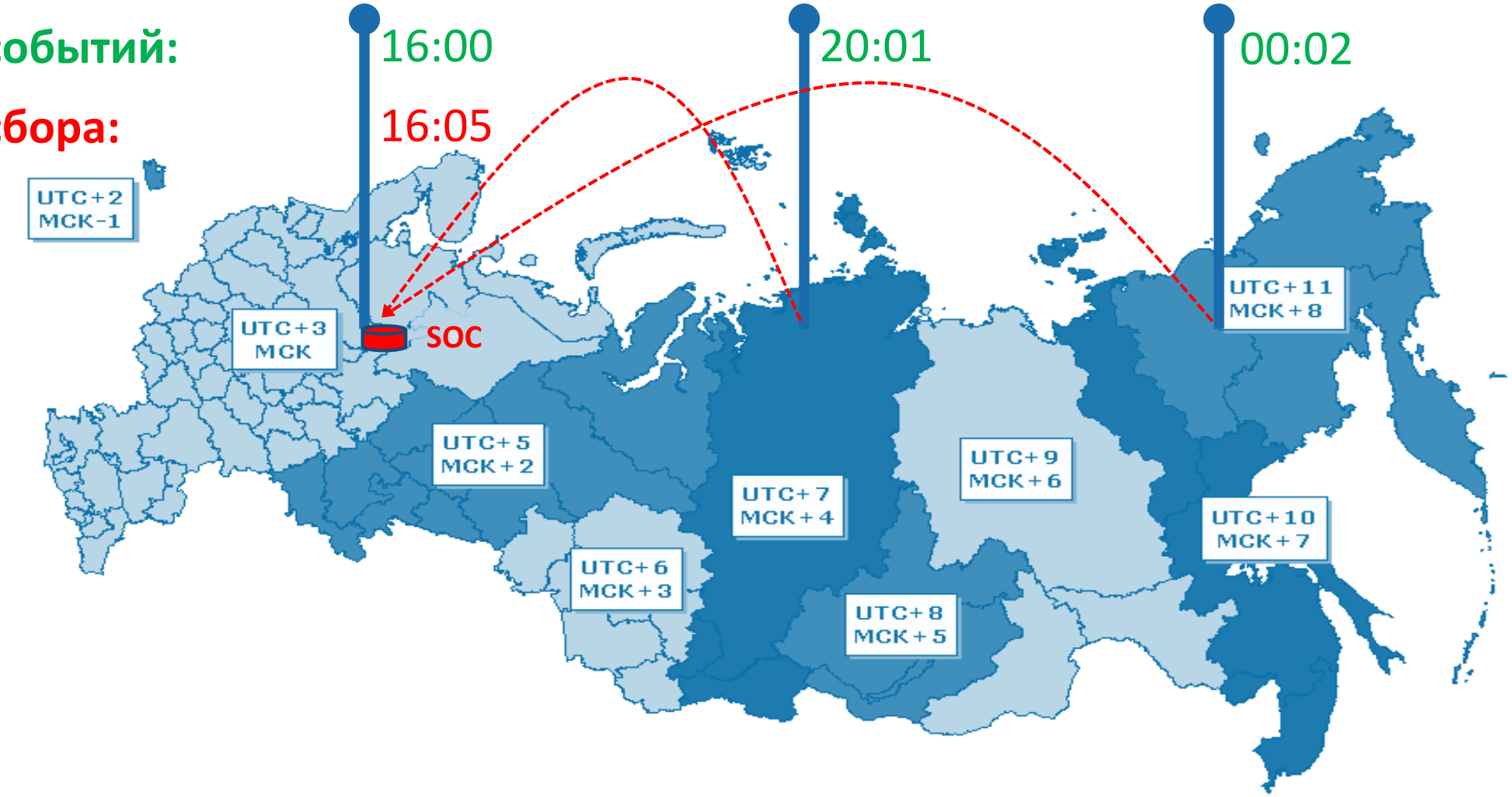
Время событий: 16:00 20:01 00:02

Время события

Δt между событиями: 0 мин. +1 мин. +2 мин.

Время событий: 16:00 20:01 00:02

Время сбора: 16:05



Время события

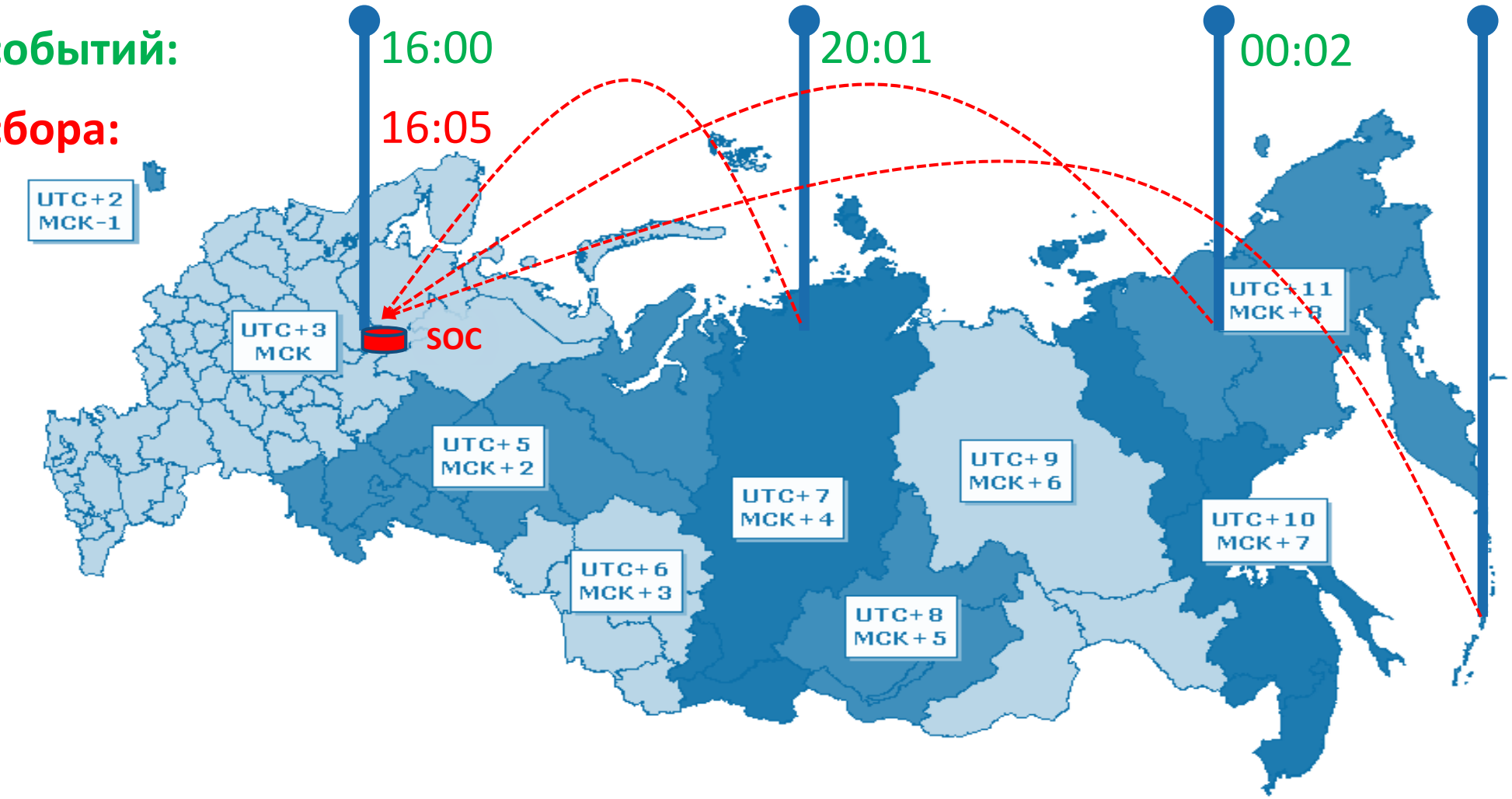
Δt между событиями: 0 мин. +1 мин. +2 мин.

Время событий: 16:00 20:01 00:02

Время сбора: 16:05

Пачка событий

00:01
00:02
...
23:58
23:59



Правила корреляции

- Ограничение на время окна корреляции (*в лучшем случае это «часы»*)
- Ограничения на логические конструкции (*например, отсутствие «ИЛИ»*)
- Ограничения на вложенность логических конструкций друг в друга
- Ограничения на применение всех логических конструкций ко всем полям событий

Правила корреляции

- Ограничение на время окна корреляции (*в лучшем случае это «часы»*)
- Ограничения на логические конструкции (*например, отсутствие «ИЛИ»*)
- Ограничения на вложенность логических конструкций друг в друга
- Ограничения на применение всех логических конструкций ко всем полям событий

Wizard
GUI

Esper + Event Processing Language (EPL)
Ariel Query Language (AQL)
Python

Тестирование Use case-ов

- Проверка работоспособности (*troubleshooting*)
- Выявление false positive
- Выявление false negative
- Выявление «тяжелых» Use case-ов (*QA*)

- Попробуй протестировать DDoS или угрозы, связанны с 0-day уязвимостями ☺

Измерение реализации Use case-ов

- **Общий показатель:**
  - Количество Use case-ов
  - Количество уточненных сценариев
  - Количество корреляционных правил в SIEM

- **Полезные соотношения:**
  - Количество реализованных правил/ количество спроектированных правил
  - Количество протестированных правил/ количество всех реализованных правил
  - Количество эксплуатируемых правил/ количество всех спроектированных правил

А в попугаях я значительно длиннее!

Заключение

- «Use cases are in the core of security monitoring activities» (*Dr. Anton Chuvakin*) Gartner
- Однозначно интерпретируйте описание Use case-ов
- Думайте о возможности тестирования Use case уже на стадии его дизайна
- Соблюдайте последовательность:
  - Описание Use case
  - Источник данных (событий)
  - Данные (события)
  - Конструкция правила корреляции
- Используете информативные метрики для оценки реализации Use case-ов

СПАСИБО ЗА ВНИМАНИЕ!

Александр Кузнецов, CISM

Руководитель направления ИБ

+7 (495) 777-13-10

a.kuznetsov@ntc-vulkan.ru

www.ntc-vulkan.ru