GIS DAYS

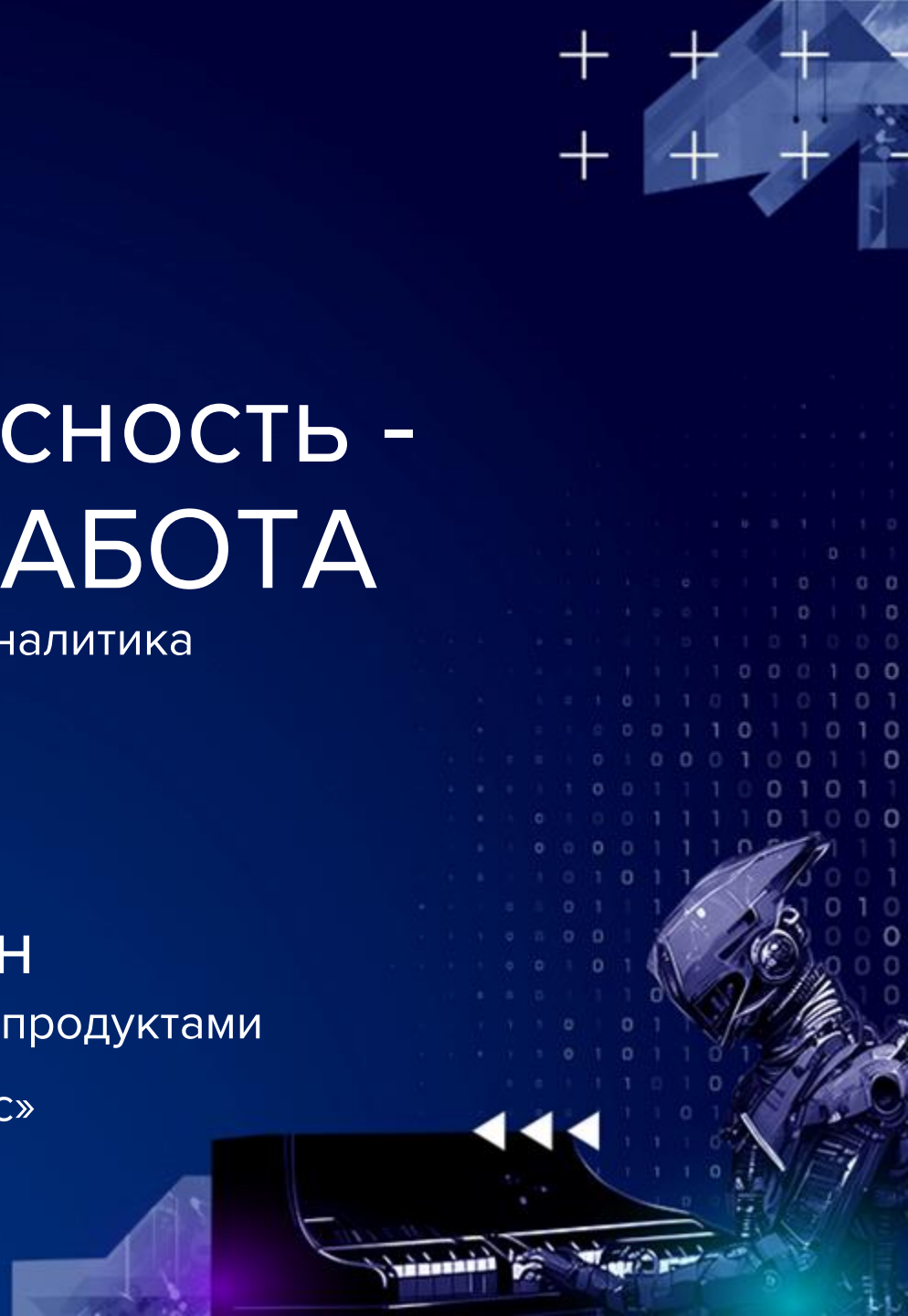
Сетевая безопасность - КОМАНДНАЯ РАБОТА

NAC, VPN, поведенческая аналитика

Сергей Никитин

Руководитель группы управления продуктами

ООО «Газинформсервис»



GIS DAYS

EFROS DEFENCE OPERATIONS

Немного статистики:

Кратный рост количества
APT-атак за последние 5 лет

MITRE

MITRE ATT&CK указывает
14 тактик и 240 техник кибератак

Актуально: как поломать NAC?

GIS DAYS

EFROS
DEFENCE OPERATIONS

Инструментарий хакера

01

Сетевой хаб

02

Портативный PoE-инжектор

03

Специализированный ноутбук

Атака: ARP-spoofing aka ARP cache poisoning

MITRE

ID: T1557.002

Sub-technique of: T1557

ⓘ Tactics: Credential Access, Collection

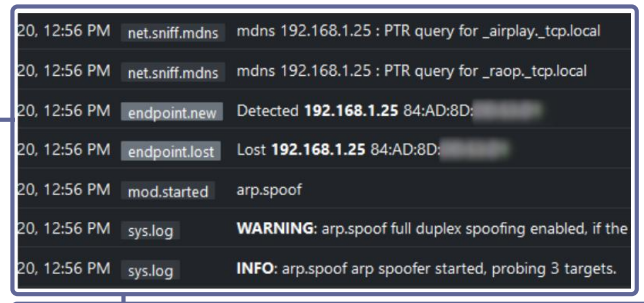
ⓘ Platforms: Linux, Windows, macOS

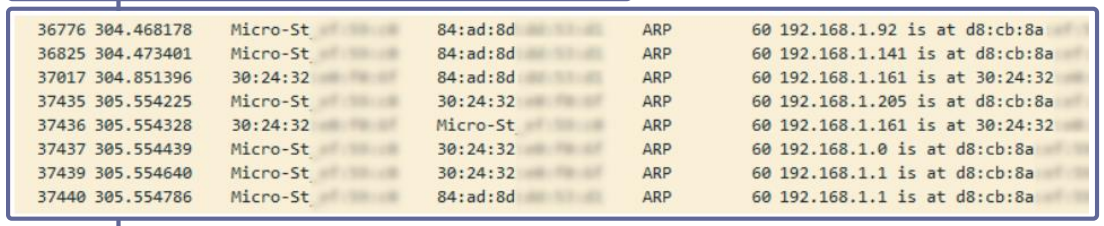
Contributors: Jon Sternstein, Stern Security

Version: 1.1

Created: 15 October 2020

Last Modified: 22 July 2022





- «Угнали» пару IP+MAC,
- Прошли аутентификацию,
- Защита не обеспечена

GIS DAYS

EFROS DEFENCE OPERATIONS

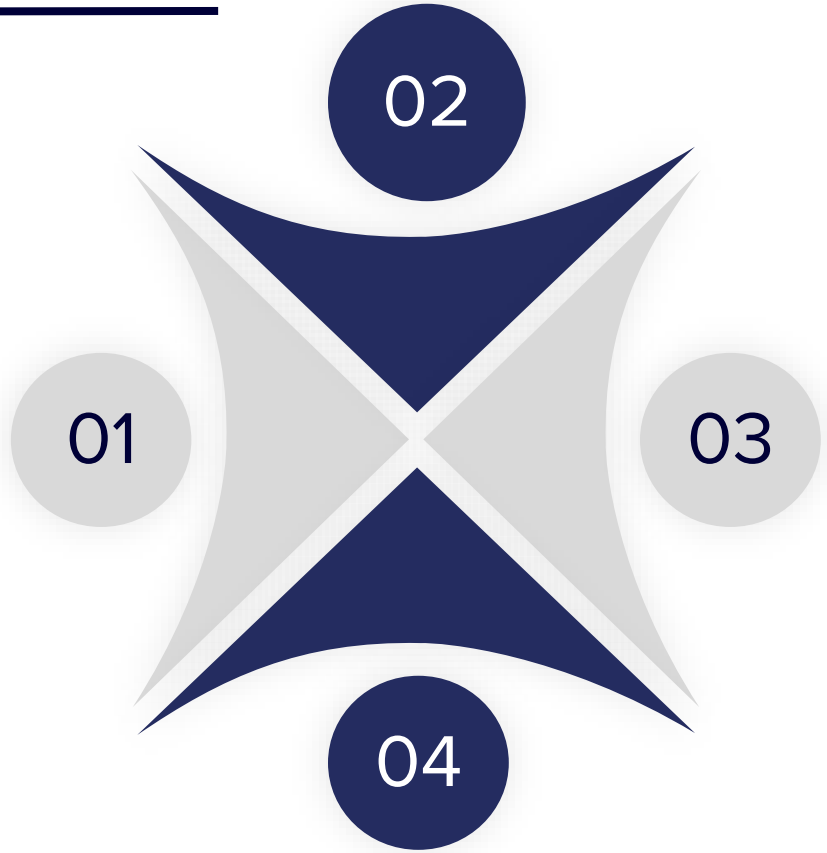
Проблематика актуальна:

01  ..... **Для интернета людей:** злоумышленник может устроиться в компанию под видом сотрудника

02  ..... **Для интернета вещей:** можно подключиться в пару с IP-телефоном, IP-камерой, IP-датчиком и т. п.

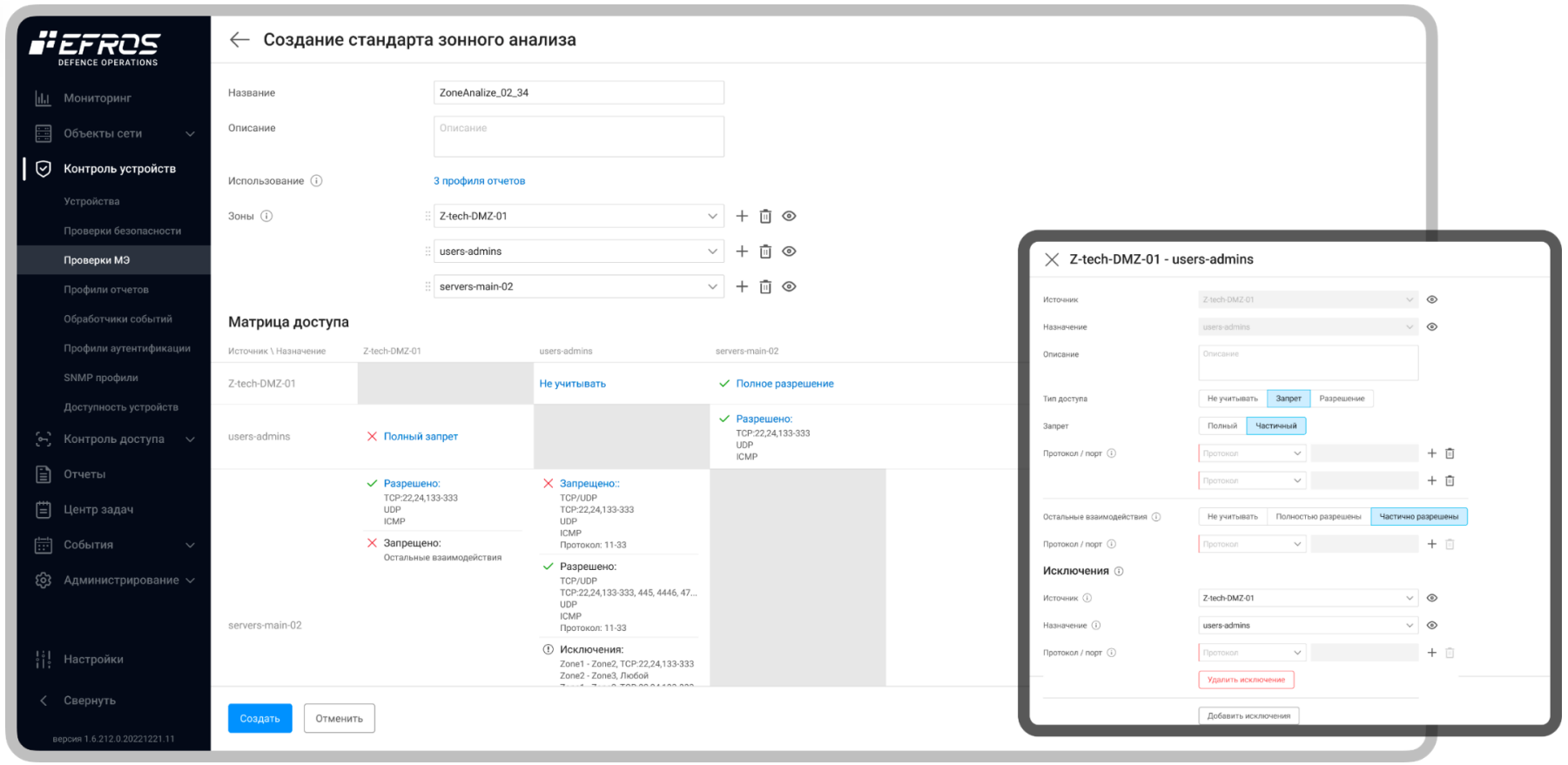
Как решается с помощью **NAC** и...

- Правильных настроек **сегментации сети**
- **VPN-туннелей** с шифрованием
- Систем **поведенческой аналитики**



Сегментация сети и постоянный аудит

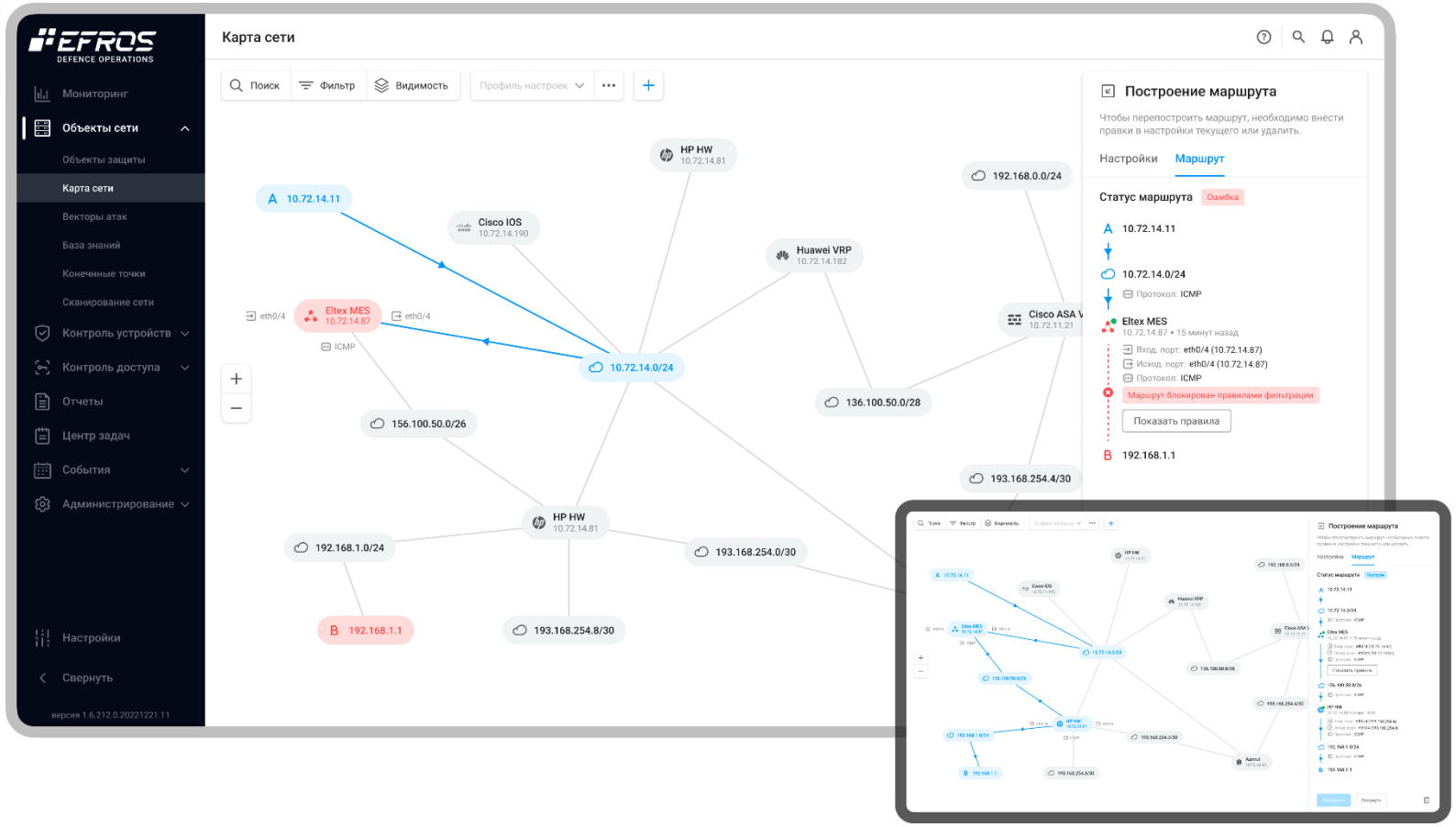
01



- Создание стандартов безопасности для сегментов сети
- Проверка соответствия правил доступа корпоративной политике

Сегментация сети и постоянный аудит

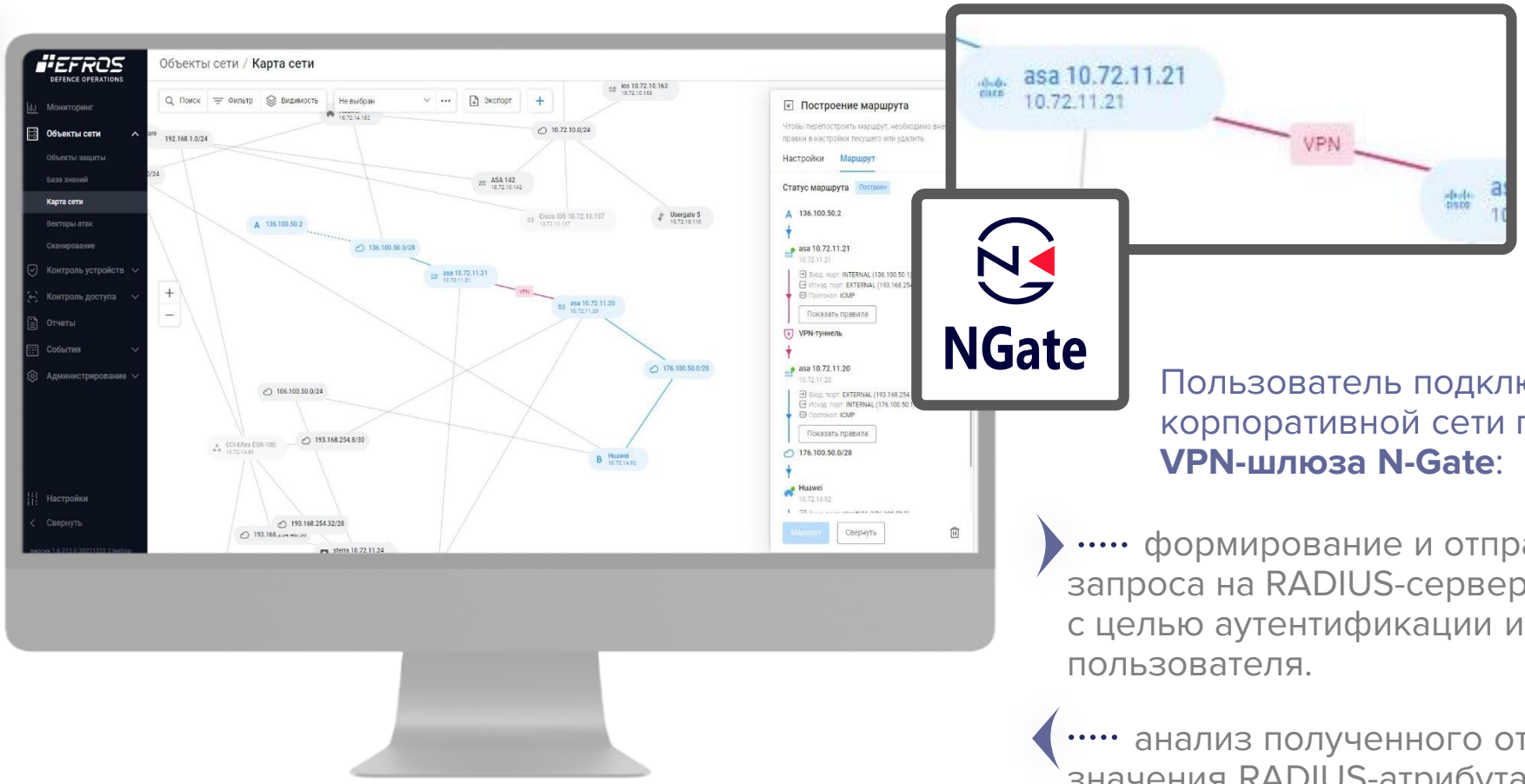
01



- Анализ связности и достижимости подсетей, выявление маршрутов распространения трафика включая VPN и NAT.
- Моделирование изменений сетевой инфраструктуры и оценка влияния вносимых изменений

Использование VPN-туннелей

02



Пользователь подключается к корпоративной сети посредством **VPN-шлюза N-Gate**:

- формирование и отправка запроса на RADIUS-сервер Efros DO с целью аутентификации и и авторизации пользователя.
- анализ полученного ответного значения RADIUS-атрибута и выбор соответствующего Access List.

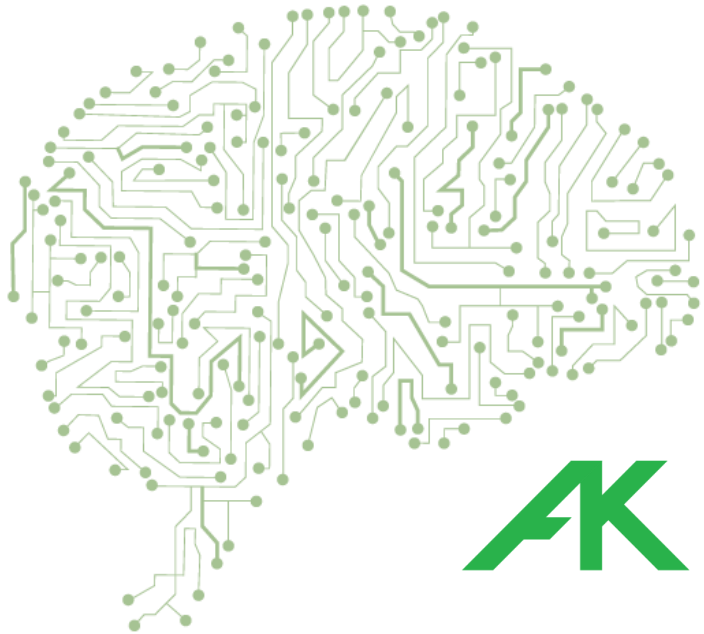
Получение доступа только к определенным сегментам корпоративной сети, что соответствует правам доступа и принадлежности к доменной группе.

Использование поведенческой аналитики

03

Выявления продолжения атаки

ARP-spoofing - задача **ASAP**



Ankey ASAP

- ····· аутентификация на нестандартном сервисе или нестандартным способом;
- ····· нетипичные команды при получении доступа;
- ····· нетипичное использование сетевых протоколов, ...

Аудит нетипичных действий на локальном хосте.

GIS DAYS

EFROS
DEFENCE OPERATIONS

Партнеры

5 дистрибьюторов

60+ интеграторов

30+ технологических партнеров

www.gaz-is.ru

GIS DAYS

СПАСИБО ЗА ВНИМАНИЕ

www. gaz-is.ru

EFROS
DEFENCE OPERATIONS