



Simplity

CYBERSECURITY

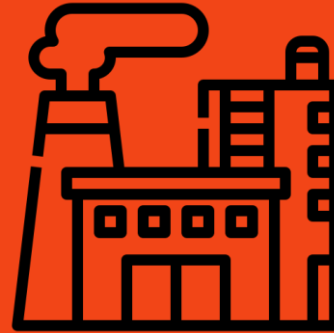
ОСНОВНЫЕ ЦЕЛИ КИБЕРАТАК НА КОМПАНИИ ГОССЕКТОРА



ШПИОНАЖ ЗА
РАЗРАБОТКАМИ
ОПК



АТАКИ НА ГИС



АТАКИ НА
ОБЪЕКТЫ КИИ



КРАЖА
ПЕРС.ДАННЫХ

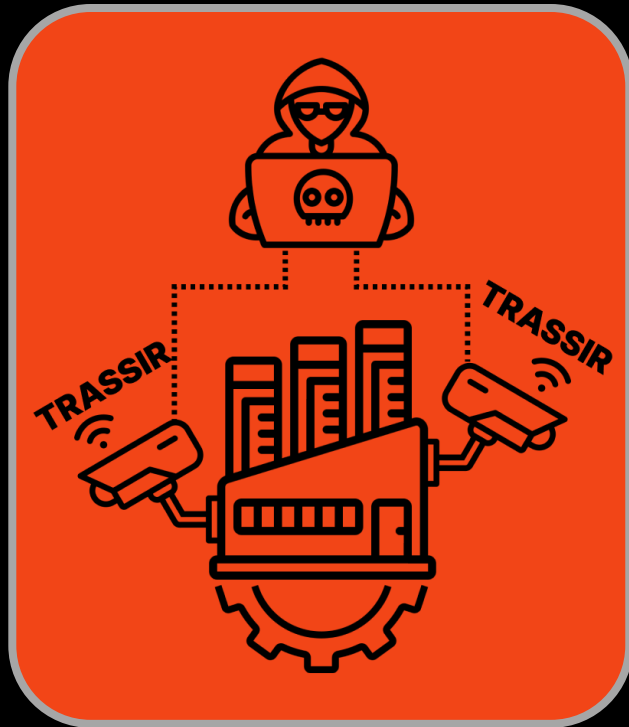
БИЗНЕС SIMPLITY- КИБЕРБЕЗОПАСНОСТЬ



Simplity – профи в тестах на проникновение, имеем собственный SOC и крутую команду инженеров и архитекторов

Лидеры логистики, финансов, промышленности, госуправления и ритейл и e-com
- с нами

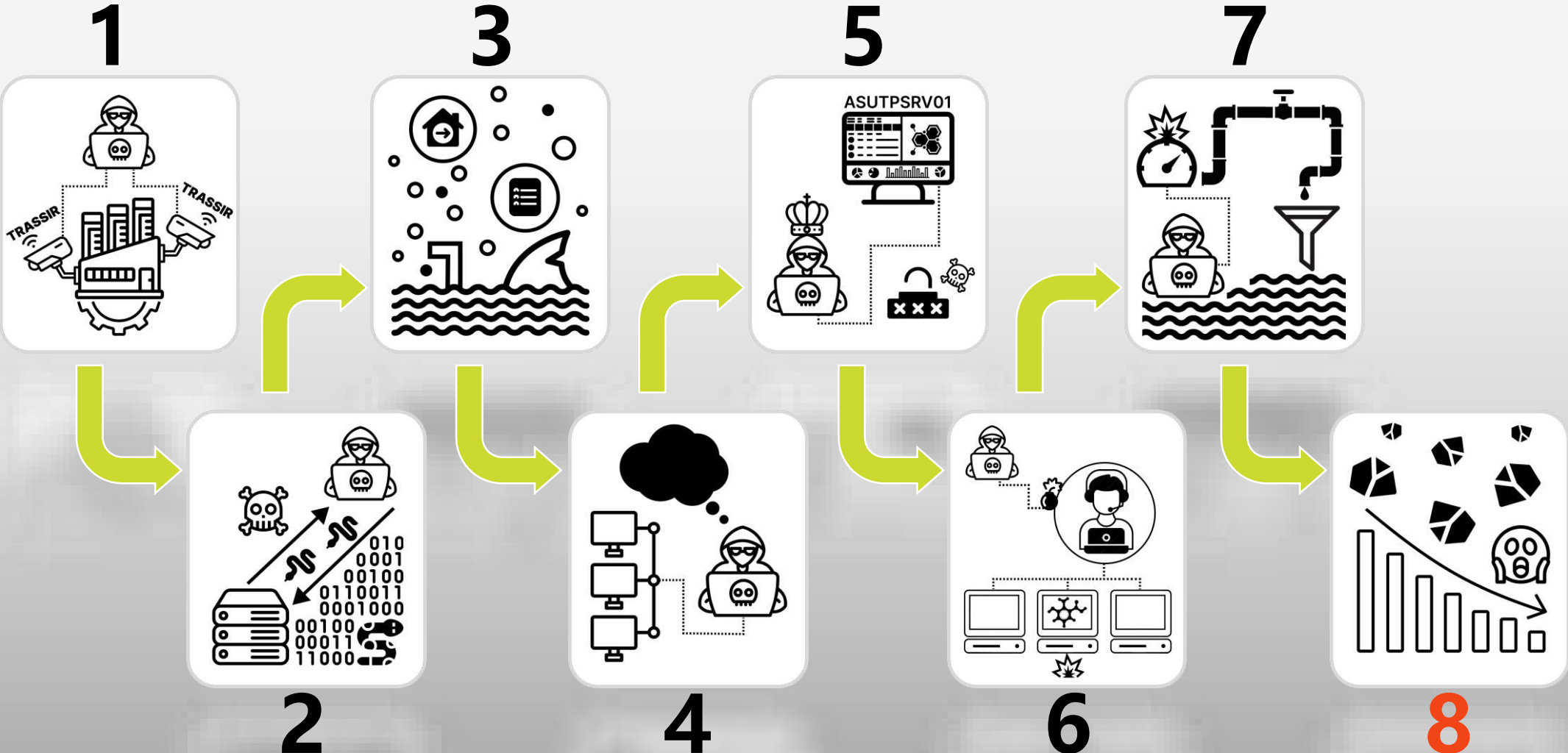
Мы за **результативный кибербез** – показываем слабые места и сразу их закрываем



ВЕКТОР 1: АТАКА НА АСУ ТП

ВЕКТОР – ЭТО ПОСЛЕДОВАТЕЛЬНОСТЬ ШАГОВ

ПРИМЕР: АТАКА НА АСУ ТП

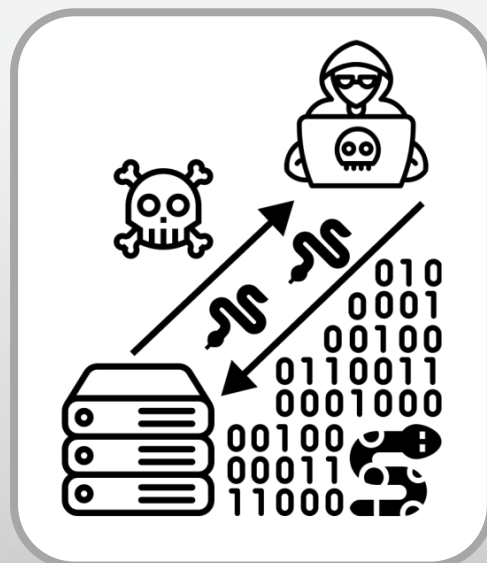
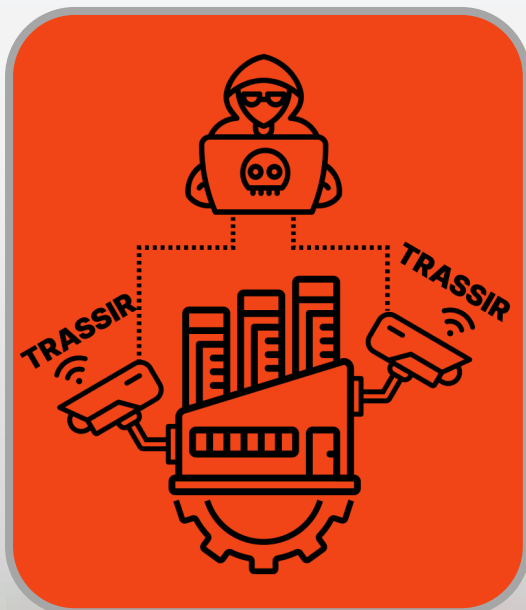


ВЕКТОР 1

АТАКА НА АСУ ТП

ОБЪЕКТ АТАКИ:

**КАМЕРА НАБЛЮДЕНИЯ ВНЕШНЕГО
ПЕРИМЕТРА ПРЕДПРИЯТИЯ**



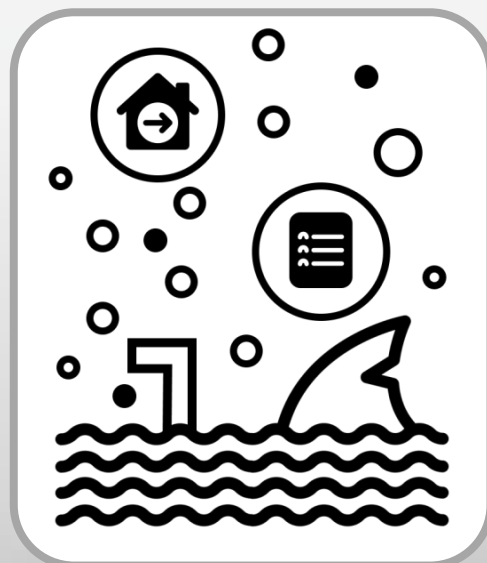
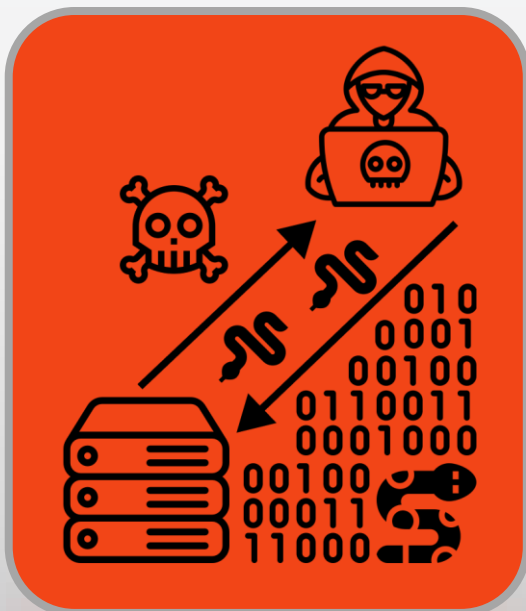
ШАГ 1: ХАКЕР ПОЛУЧИЛ ДОСТУП К КАМЕРЕ TRASSIR С ПАРОЛЕМ ПО УМОЛЧАНИЮ (admin-12345)

ВЕКТОР 1

АТАКА НА АСУ ТП

ОБЪЕКТ АТАКИ:

**КАМЕРА НАБЛЮДЕНИЯ ВНЕШНЕГО
ПЕРИМЕТРА ПРЕДПРИЯТИЯ**



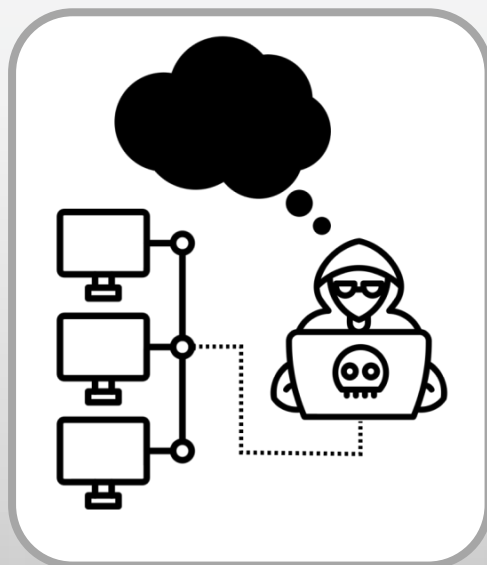
ШАГ 2: ИСПОЛЬЗОВАНИЕ ВСТРОЕННОГО ФУНКЦИОНАЛА ВИДЕОНАБЛЮДЕНИЯ ДЛЯ УДАЛЕННОГО ДОСТУПА И СОЗДАНИЯ ПРОКСИ-ТУННЕЛЯ

ВЕКТОР 1

АТАКА НА АСУ ТП

ОБЪЕКТ АТАКИ:

**КАМЕРА НАБЛЮДЕНИЯ ВНЕШНЕГО
ПЕРИМЕТРА ПРЕДПРИЯТИЯ**



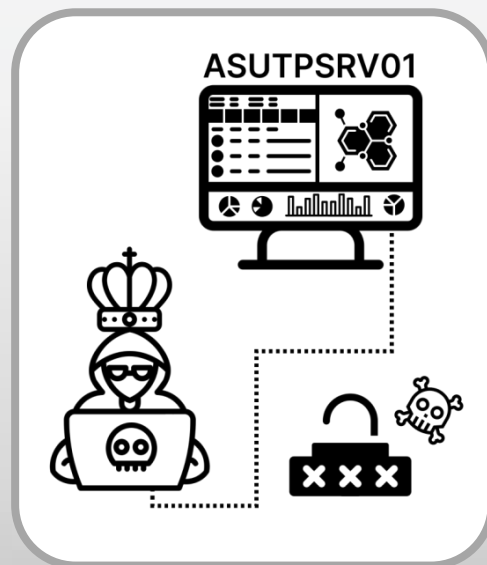
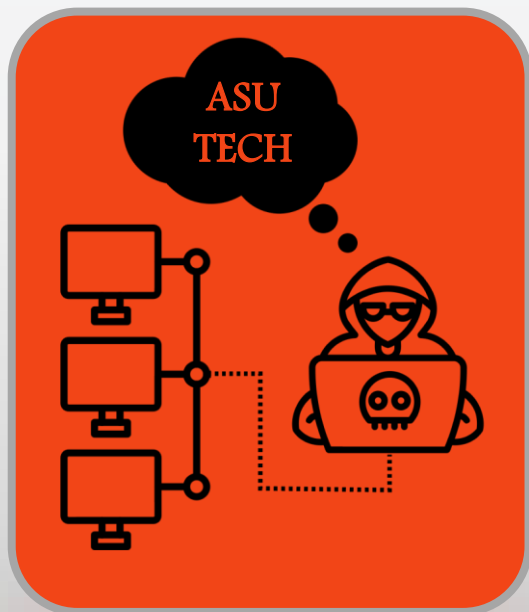
ШАГ 3: ХАКЕР УЖЕ ВНУТРИ ПРЕДПРИЯТИЯ. ПРОСЛУШИВАНИЕ ТРАФИКА, ПОЛУЧЕНИЕ ВНУТРЕННЕЙ УЧЕТНОЙ ЗАПИСИ И СПИСКА КОМПЬЮТЕРОВ

ВЕКТОР 1

АТАКА НА АСУ ТП

ОБЪЕКТ АТАКИ:

**КАМЕРА НАБЛЮДЕНИЯ ВНЕШНЕГО
ПЕРИМЕТРА ПРЕДПРИЯТИЯ**



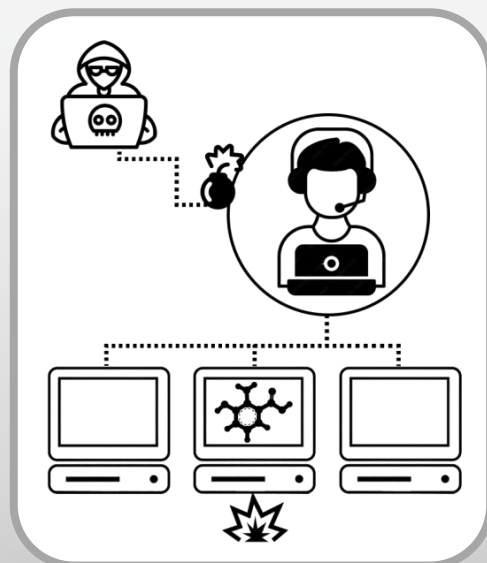
ШАГ 4: ПОИСК КЛЮЧЕВЫХ СЛОВ В НАЗВАНИЯХ КОМПЬЮТЕРОВ (ASU, TECH), ЧТОБЫ ПОНЯТЬ, ГДЕ АСУ ТП

ВЕКТОР 1

АТАКА НА АСУ ТП

ОБЪЕКТ АТАКИ:

**КАМЕРА НАБЛЮДЕНИЯ ВНЕШНЕГО
ПЕРИМЕТРА ПРЕДПРИЯТИЯ**



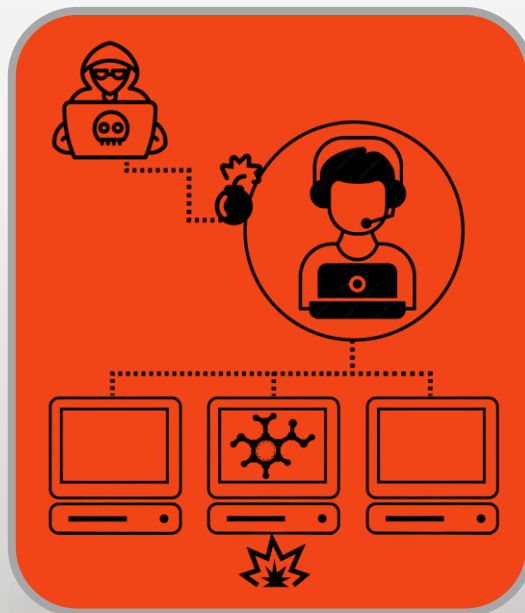
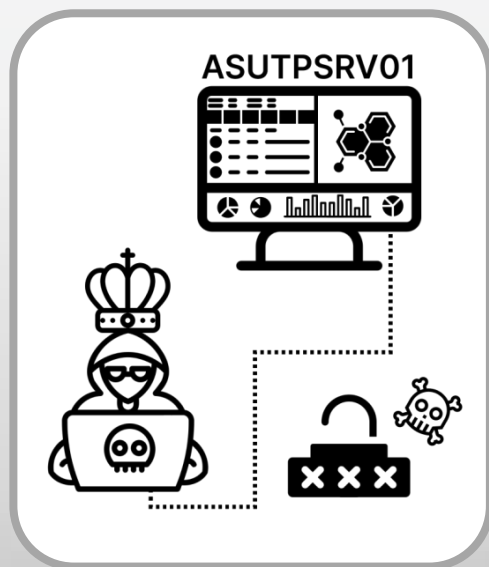
ШАГ 5: ОБНАРУЖЕНА МИСКОНФИГУРАЦИЯ В СЕТИ,
ПОЗВОЛЯЮЩАЯ ЧИТАТЬ ПАРОЛЬ ЛОКАЛЬНОГО
АДМИНИСТРАТОРА НА КОМПЬЮТЕРЕ ASUTPSRV01

ВЕКТОР 1

АТАКА НА АСУ ТП

ОБЪЕКТ АТАКИ:

**КАМЕРА НАБЛЮДЕНИЯ ВНЕШНЕГО
ПЕРИМЕТРА ПРЕДПРИЯТИЯ**

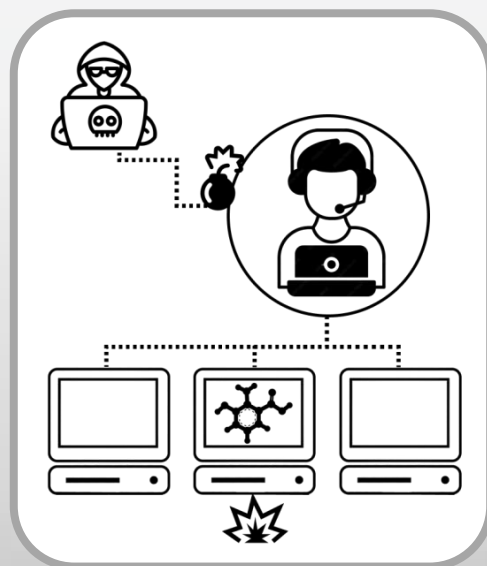
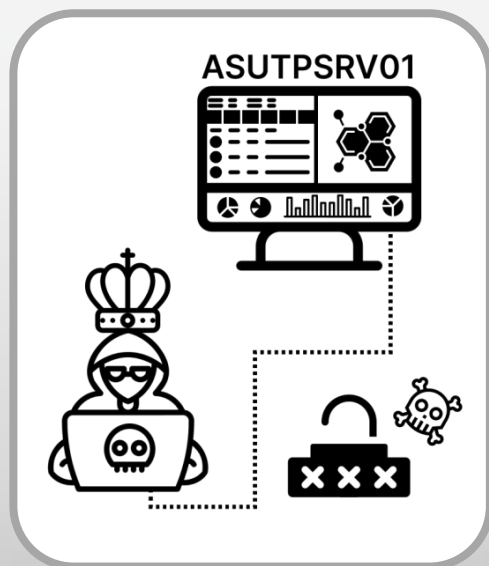


**ШАГ 6: ЗАХВАТ УЗЛА ОПЕРАТОРА С ДОСТУПОМ В
ТЕХНОЛОГИЧЕСКУЮ ПОДСЕТЬ**

ВЕКТОР 1 АТАКА НА АСУ ТП

ОБЪЕКТ АТАКИ:

**КАМЕРА НАБЛЮДЕНИЯ ВНЕШНЕГО
ПЕРИМЕТРА ПРЕДПРИЯТИЯ**



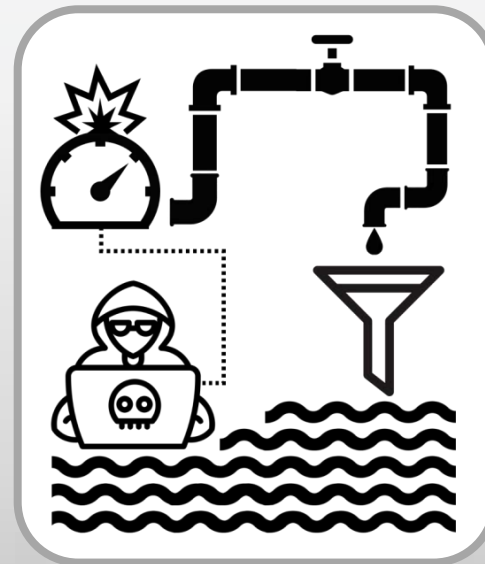
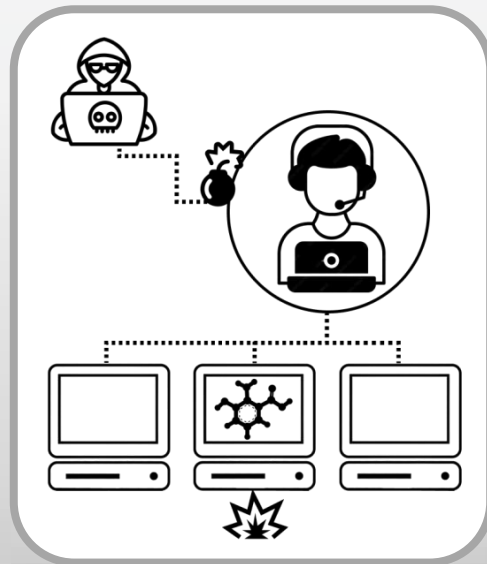
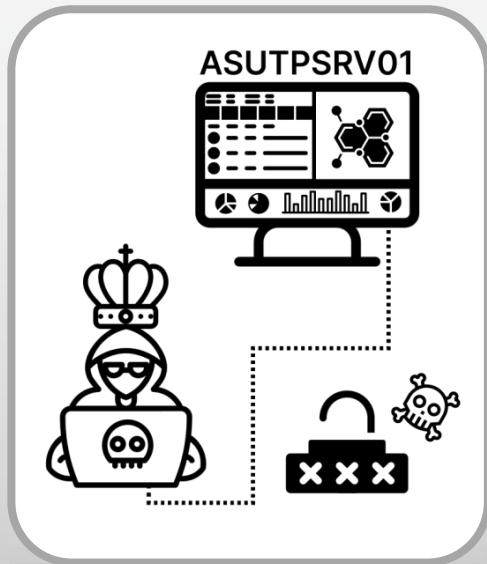
ШАГ 7: СБОР ИНФОРМАЦИИ О ТЕХНОЛОГИЧЕСКОМ ПРОТОКОЛЕ УМНЫХ ПРОИЗВОДСТВЕННЫХ УСТРОЙСТВ.

ХАКЕР ОТПРАВЛЯЕТ НЕЛЕГИТИМНУЮ КОМАНДУ, НАПРИМЕР, ДЛЯ ИЗМЕНЕНИЯ СКОРОСТИ ПОДАЧИ СЫРЬЯ

ВЕКТОР 1 АТАКА НА АСУ ТП

ОБЪЕКТ АТАКИ:

**КАМЕРА НАБЛЮДЕНИЯ ВНЕШНЕГО
ПЕРИМЕТРА ПРЕДПРИЯТИЯ**



ИТОГ: КОМПАНИЯ ВЫПУСКАЕТ БРАК И ТЕРЯЕТ ДЕНЬГИ



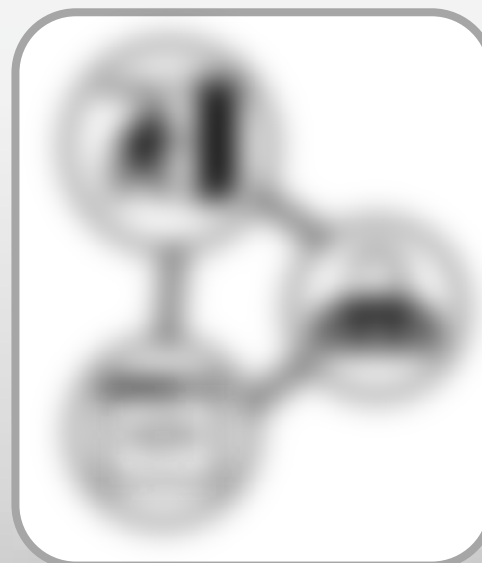
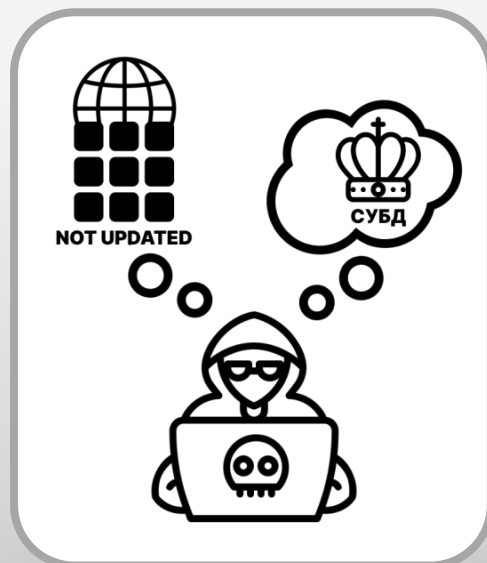
ВЕКТОР 2: ШИФРОВАНИЕ

ВЕКТОР 2

ШИФРОВАНИЕ

ОБЪЕКТ АТАКИ:

ВЕБ-ПОРТАЛ ГИС



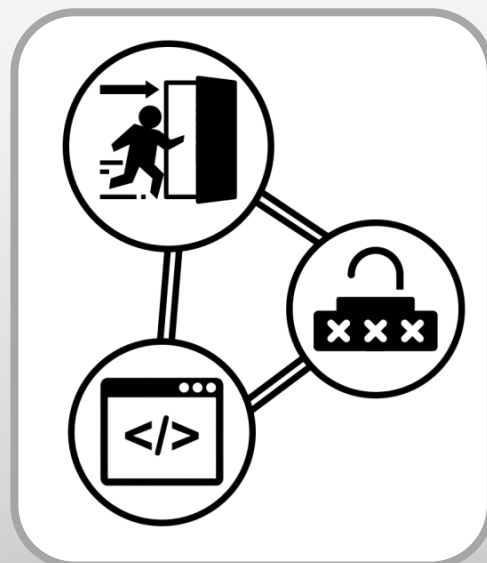
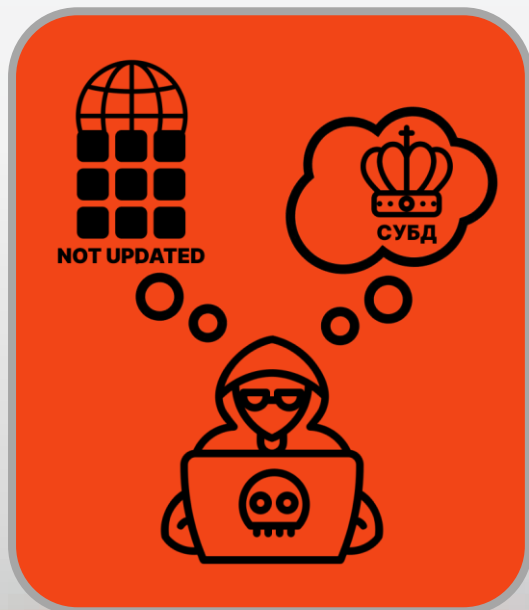
ШАГ 1: АНАЛИЗ ВНЕШНЕГО ПРИЛОЖЕНИЯ (ГИС)

ВЕКТОР 2

ШИФРОВАНИЕ

ОБЪЕКТ АТАКИ:

ВЕБ-ПОРТАЛ ГИС



ШАГ 2: ХАКЕР ОБНАРУЖИЛ НЕОБНОВЛЕННЫЕ МОДУЛИ НА САЙТЕ, КОТОРЫЕ ПОЗВОЛЯЮТ ПОЛУЧИТЬ ПАРОЛЬ АДМИНИСТРАТОРА СУБД

ВЕКТОР 2

ШИФРОВАНИЕ

ОБЪЕКТ АТАКИ:

ВЕБ-ПОРТАЛ ГИС



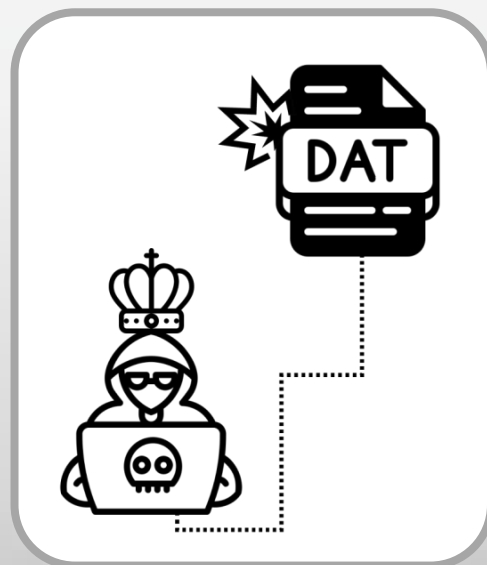
ШАГ 3: ХАКЕР ОБНАРУЖИЛ САМОПИСНОЕ РЕШЕНИЕ С ОТКРЫТЫМ ИСХОДНЫМ КОДОМ, ПРЕДНАЗНАЧЕННОЕ ДЛЯ УДАЛЕННОГО АДМИНИСТРИРОВАНИЯ СЕРВИСОВ, КОТОРОЕ МОЖНО СКАЧАТЬ НА GITHUB. ДОСТУП ОСУЩЕСТВЛЯЕТСЯ С ДЕФОЛТНЫМ КЛЮЧОМ.

ВЕКТОР 2

ШИФРОВАНИЕ

ОБЪЕКТ АТАКИ:

ВЕБ-ПОРТАЛ ГИС



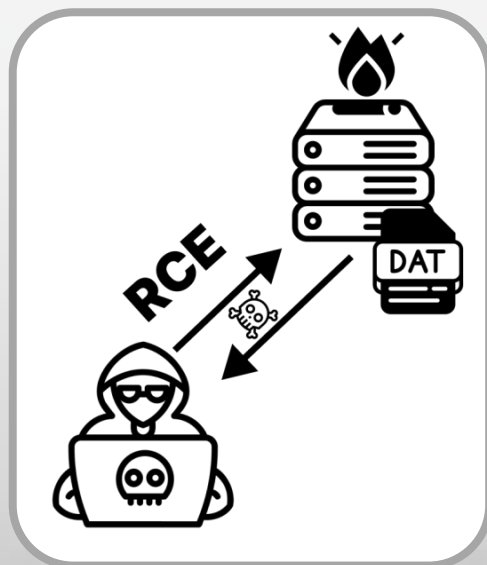
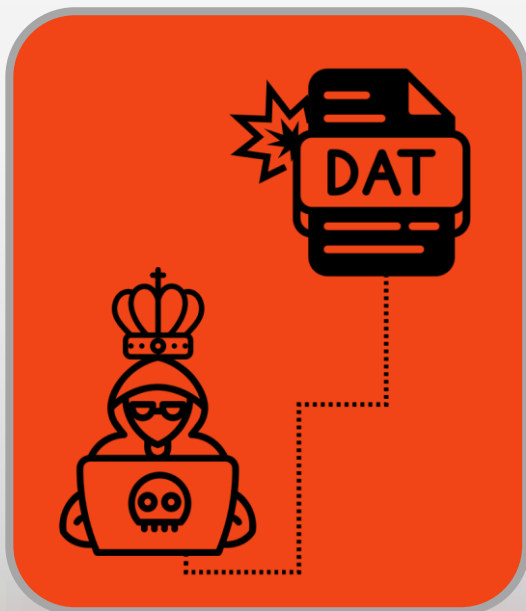
ШАГ 4: ДОСТУП В ПАНЕЛЬ АДМИНИСТРИРОВАНИЯ НА САЙТЕ
(МОДУЛЬ ДЛЯ АДМИНОВ) С ПАРОЛЕМ ПО УМОЛЧАНИЮ

ВЕКТОР 2

ШИФРОВАНИЕ

ОБЪЕКТ АТАКИ:

ВЕБ-ПОРТАЛ ГИС



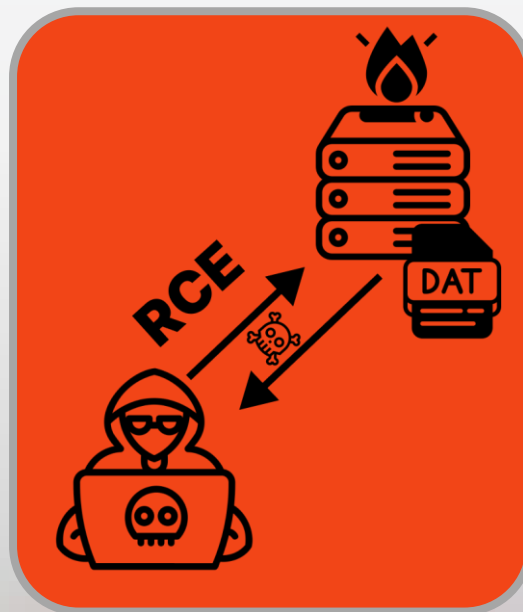
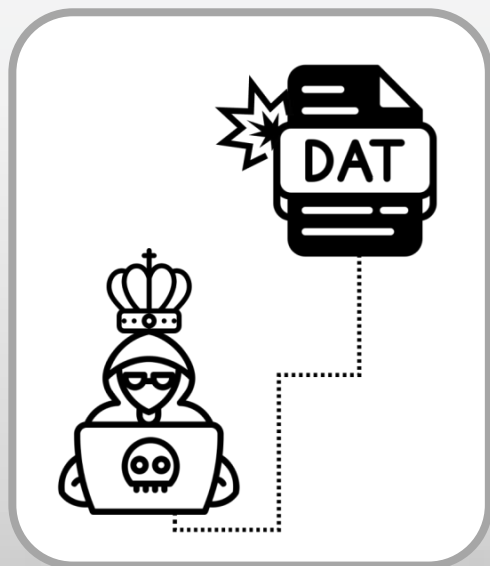
ШАГ 5: ПОДКЛЮЧЕНИЕ К БАЗЕ ДАННЫХ С ПРАВАМИ АДМИНИСТРАТОРА, ИСПОЛЬЗУЯ МОДУЛЬ АДМИНИСТРИРОВАНИЯ

ВЕКТОР 2

ШИФРОВАНИЕ

ОБЪЕКТ АТАКИ:

ВЕБ-ПОРТАЛ ГИС



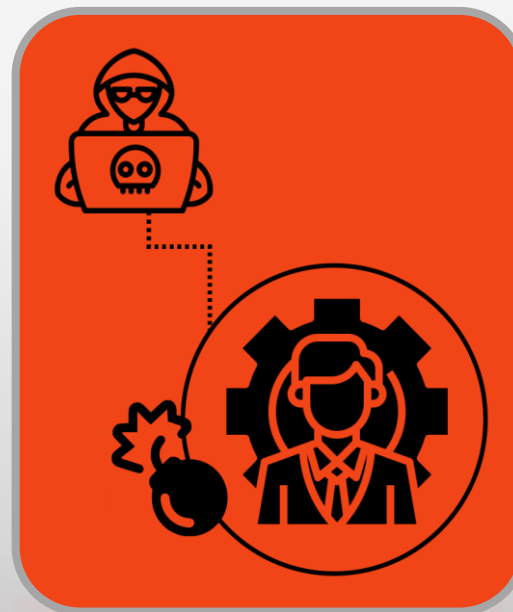
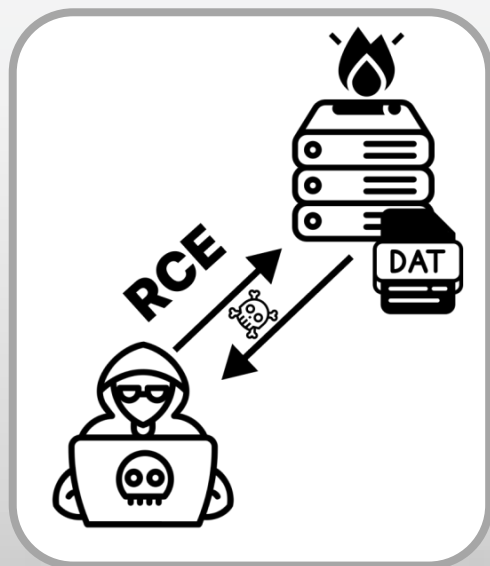
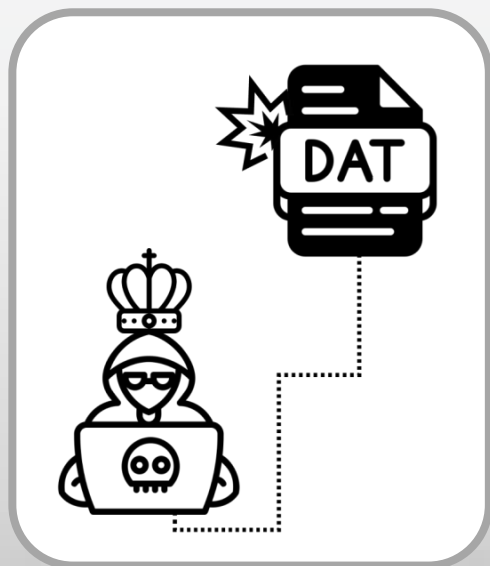
ШАГ 6: УДАЛЕННОЕ ИСПОЛНЕНИЕ КОДА НА СЕРВЕРЕ БАЗЫ ДАННЫХ И ЗАХВАТ СЕРВЕРА

ВЕКТОР 2

ШИФРОВАНИЕ

ОБЪЕКТ АТАКИ:

ВЕБ-ПОРТАЛ ГИС



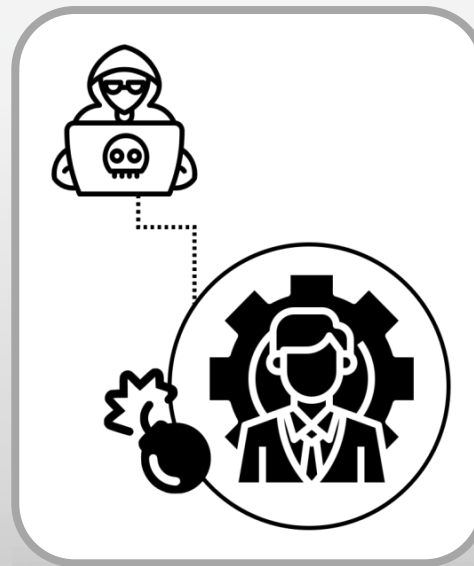
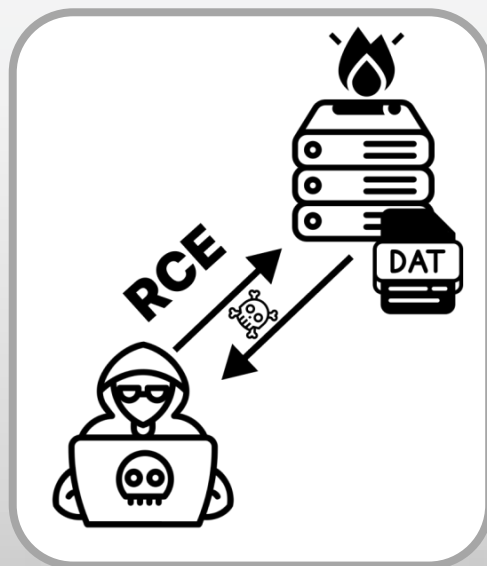
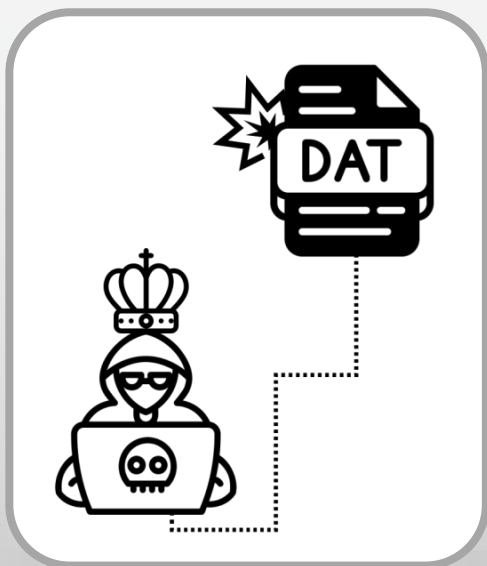
ШАГ 7: ЗАХВАТ ЛОКАЛЬНОЙ УЧЕТНОЙ ЗАПИСИ АДМИНИСТРАТОРА

ВЕКТОР 2

ШИФРОВАНИЕ

ОБЪЕКТ АТАКИ:

ВЕБ-ПОРТАЛ ГИС



ИТОГ: ШИФРОВАНИЕ 90% СЕТИ С ПАРОЛЕМ ЛОКАЛЬНОГО АДМИНИСТРАТОРА

ПОЧЕМУ ВЗЛОМАТЬ ТАК ЛЕГКО?

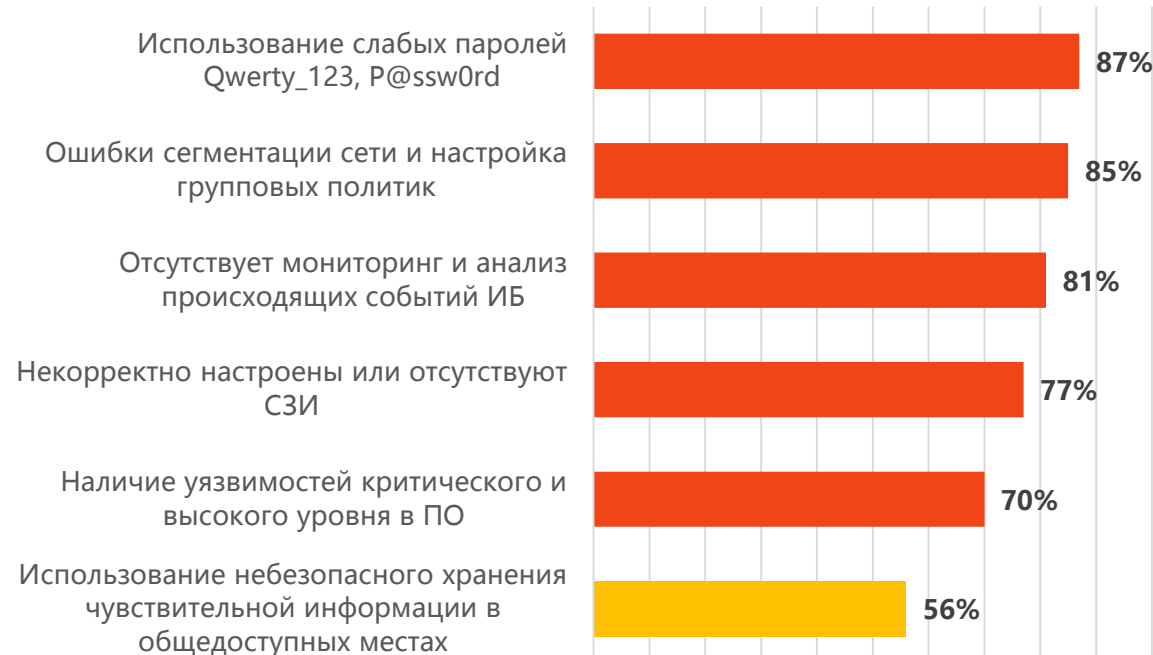
ЧТО ЧАЩЕ ИСПОЛЬЗУЕТСЯ В АТАКАХ:

Это все про
слабые пароли

ПОЧЕМУ ТАК ЛЕГКО ВЗЛОМАТЬ ПЕРИМЕТР?



ПОЧЕМУ ТАК ЛЕГКО ВЗЛОМАТЬ ВНУТРЕННЮЮ СЕТЬ?

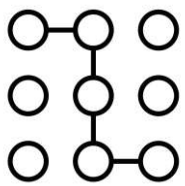


А казалось бы...



**ОБЯЗАТЕЛЬНО ПОЛУЧИТЕ СТАТИСТИКУ
У НАС НА СТЕНДЕ**

ПРЕДОТВРАЩАЕТ 9 ИЗ 10 ВЕКТОРОВ



ПРАВИЛЬНАЯ
СЕГМЕНТАЦИЯ СЕТИ И
НАСТРОЙКА ГРУППОВЫХ
ПОЛИТИК БЕЗОПАСНОСТИ



КОРРЕКТНАЯ
НАСТРОЙКА СЗИ



ДВУХФАКТОРНАЯ
АУТЕНТИФИКАЦИЯ



ПЕРИОДИЧЕСКИЙ
АНАЛИЗ
ЗАЩИЩЕННОСТИ



МОНИТОРИНГ
СОБЫТИЙ ИБ
(SOC 24/7)



ВНЕСИТЕ В CHECK-LIST



Simplity

ГОТОВЫ ОТВЕТИТЬ НА ВАШИ ВОПРОСЫ



Simplity.expert