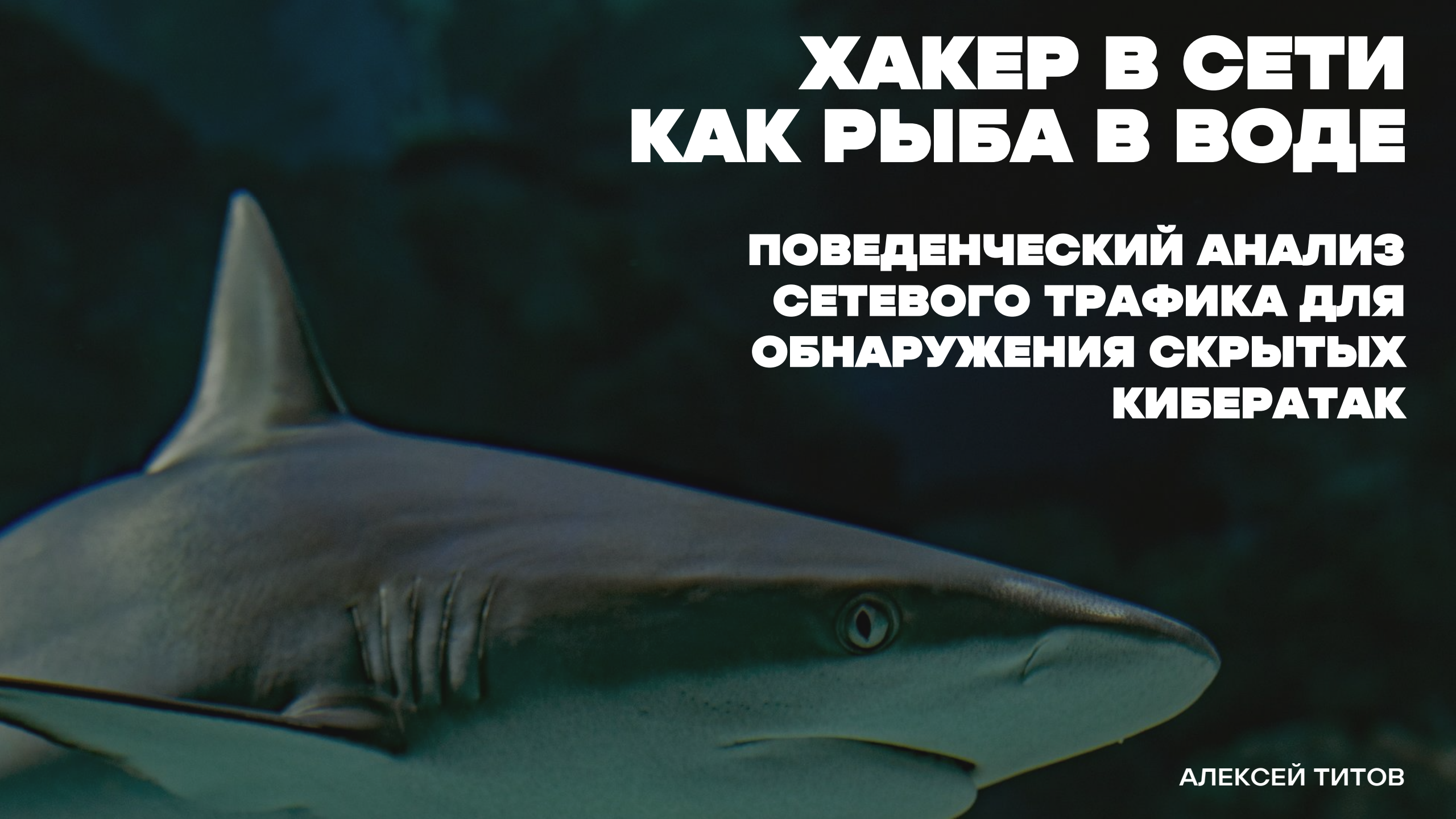


ХАКЕР В СЕТИ КАК РЫБА В ВОДЕ

ПОВЕДЕНЧЕСКИЙ АНАЛИЗ СЕТЕВОГО ТРАФИКА ДЛЯ ОБНАРУЖЕНИЯ СКРЫТЫХ КИБЕРАТАК

АЛЕКСЕЙ ТИТОВ

ЛЮБУЮ ЗАЩИЩЕННУЮ СЕТЬ МОЖНО ВЗЛОМАТЬ

96% **организаций**

не защищены от проникновения внешнего злоумышленника согласно итогов пентестов – 2022

2 часа **потребовалось**

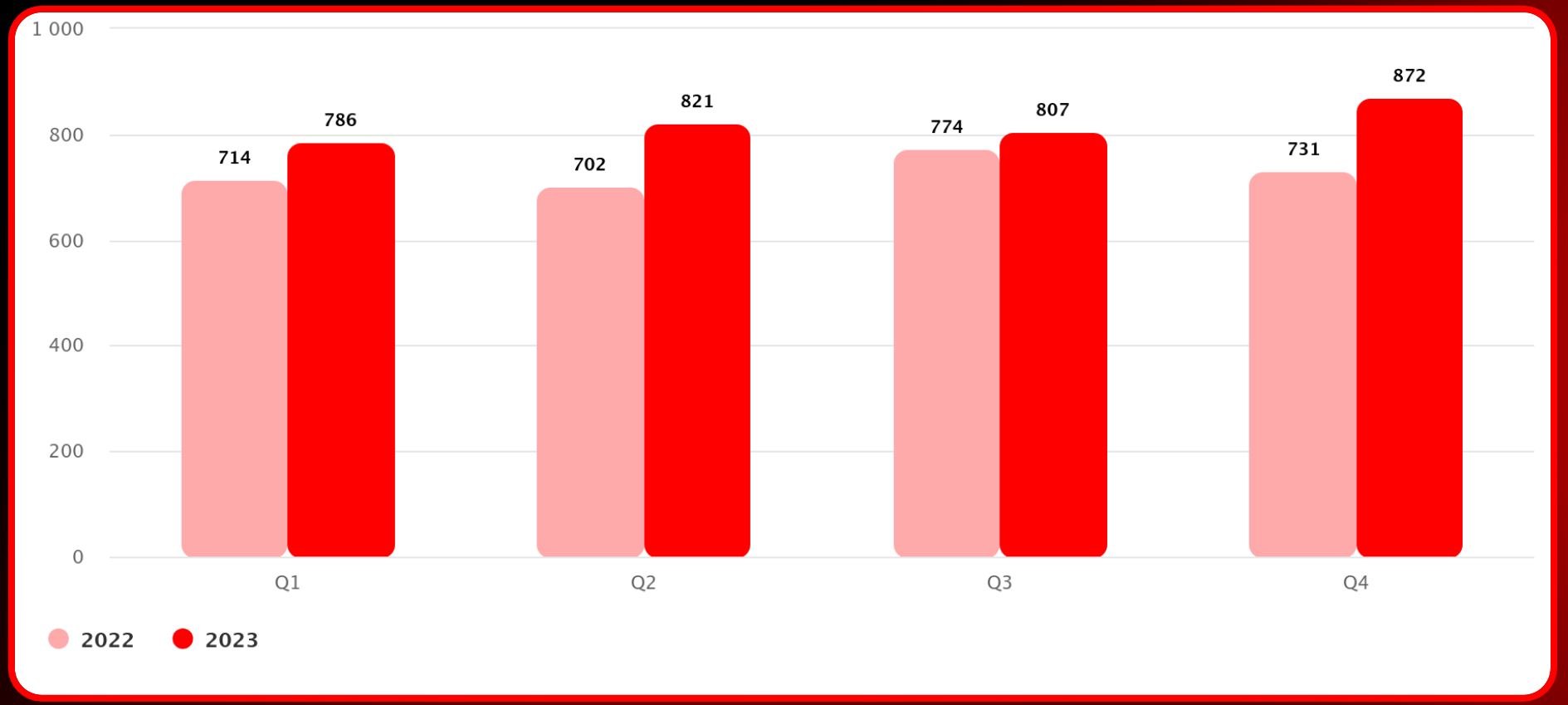
злоумышленникам на полную компрометацию инфраструктуры. Среднее время – 3-5 дней

207 дней **среднее**

время выявления незаметного присутствия злоумышленников в инфрастурктуре

ТЕОРИЯ ВЕРОЯТНОСТИ В СИЛЕ

Количество атак в 2022 и 2023 годах (по кварталам)*

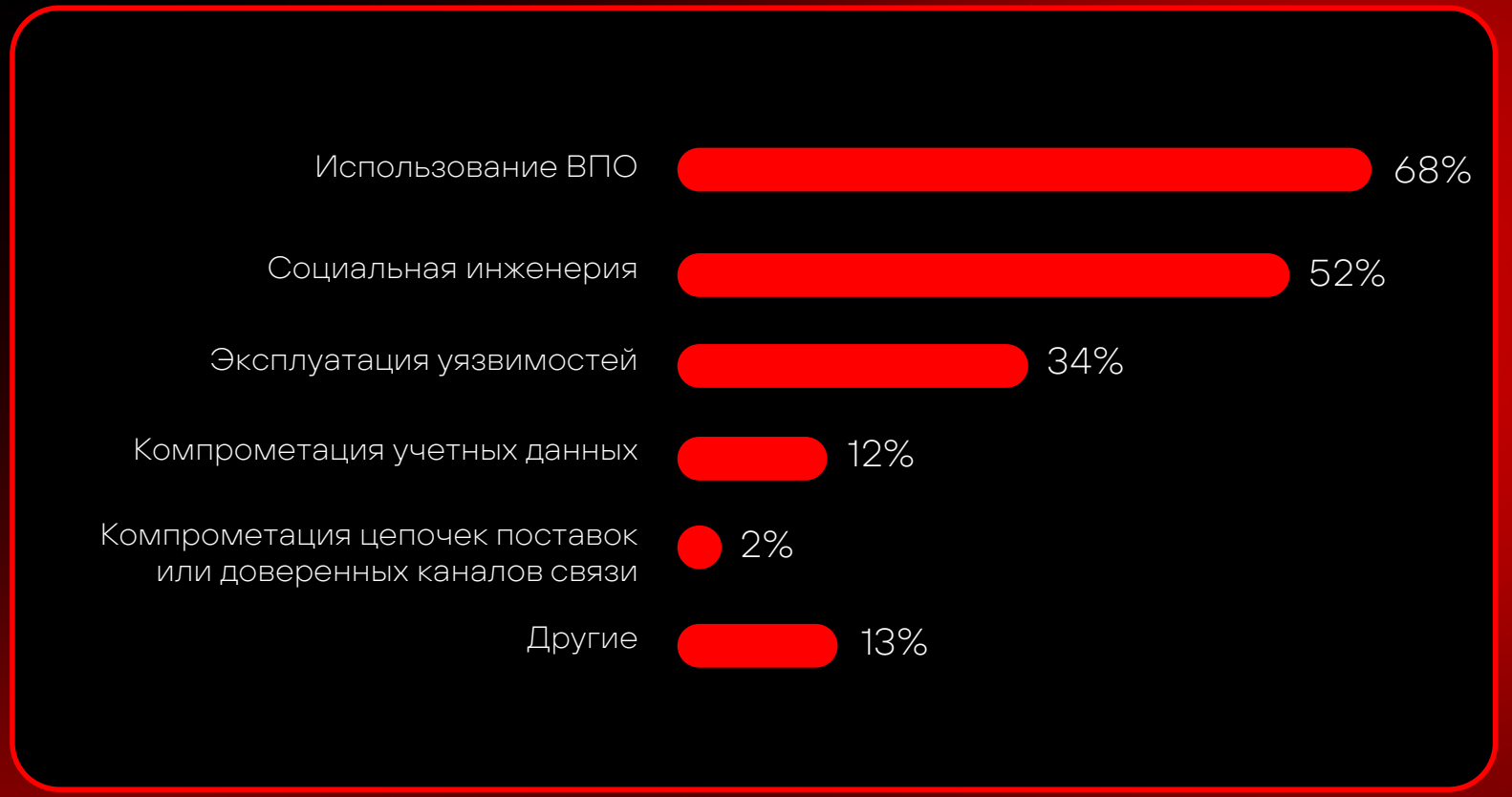


Актуальные киберугрозы: IV квартал 2023года

1-й КВАРТАЛ 2024

32%

доля атак
с использованием
RAT – ВПО для
удаленного доступа



КАК НАЧАЛСЯ 2024 В УЗБЕКИСТАНЕ

29 сайтов

в домене .uz были взломаны
с начала года

867 учеток

были скомпрометированы в
рамках атаки группировки
Lazy Koala

6 месяцев

не прекращаются
целенаправленные атаки
SugarGh0st RAT

ПОГОВОРИМ О ПОСЛЕДСТВИЯХ

Хакеры взломали сайт Lada Uzbekistan

Злоумышленники – хактивисты используя ошибки конфигурирования веб-сайта заменили интерфейс на фотографию с требованием остановить строительство АЭС

Срыв контрактных обязательств по поставке трубопроката на 3 дня

За счет нарушения функционирования технологического процесса или уничтожения системы управления цепочками поставок...

Демонстрация политических лозунгов на телевизионном канале

За счет взлома CDN или стримингового сервиса с последующим перенаправлением на ресурсы оппозиционных СМИ или подмешивание постороннего контента или взлом системы показа рекламы...

Недопуск болельщиков на матч крупного спортивного мероприятия

За счет обнуления базы болельщиков (fanid) или взлома системы контроля доступа на стадион...

ПОСЛЕДСТВИЯ ХАКЕРСКИХ АТАК БЫВАЮТ РАЗНЫЕ

АТАКИ НА ЛОГИСТИЧЕСКУЮ ОТРАСЛЬ

10 млн

активных пользователей в базе клиентов

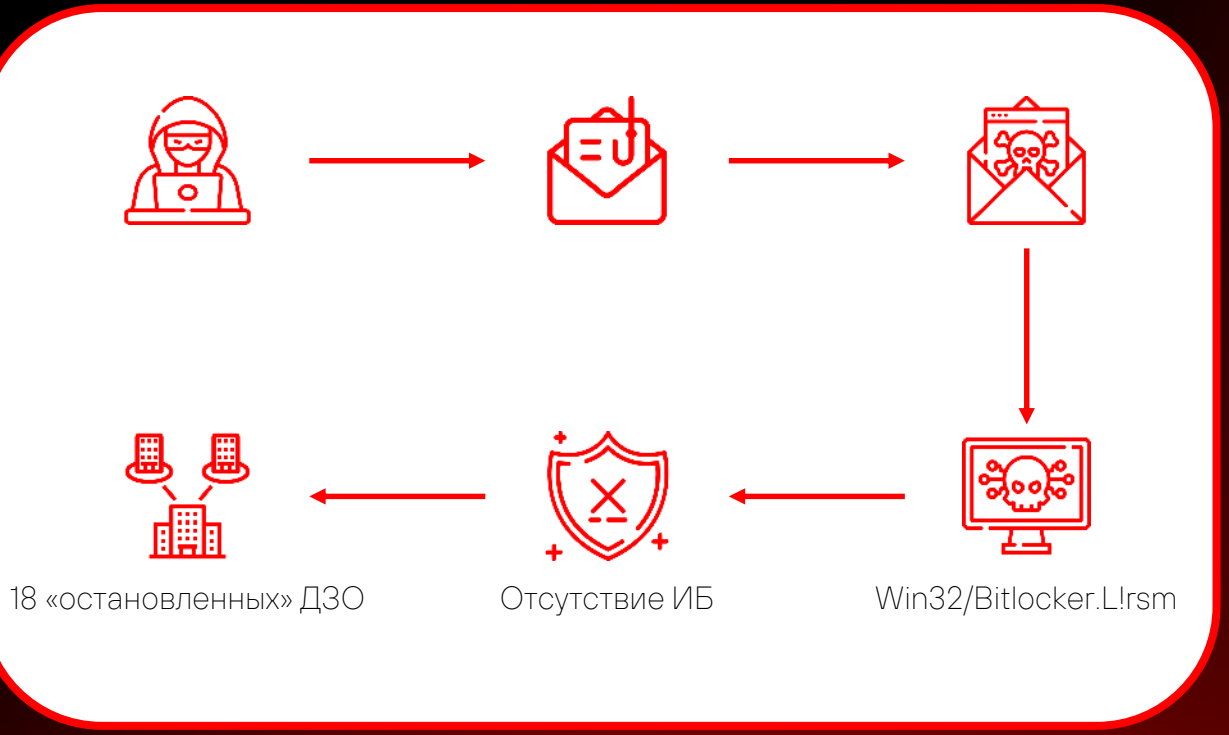
110 млн

отправлений за 2023-й год, на 128% больше чем в 2022

70 млрд

общая выручка

АТАКА НА ПИЩЕВУЮ ПРОМЫШЛЕННОСТЬ



АПХ «Мираторг» сообщает, что хакерской атаке подверглись информационные ресурсы компании

ОБЩЕСТВО Пятница, 18 март 2022, 10:51 854

АТАКА НА СТАЛЕЛИТЕЙНУЮ ПРОМЫШЛЕННОСТЬ

As you can see in the video, this cyberattack has been carried out carefully so to protect innocent individuals

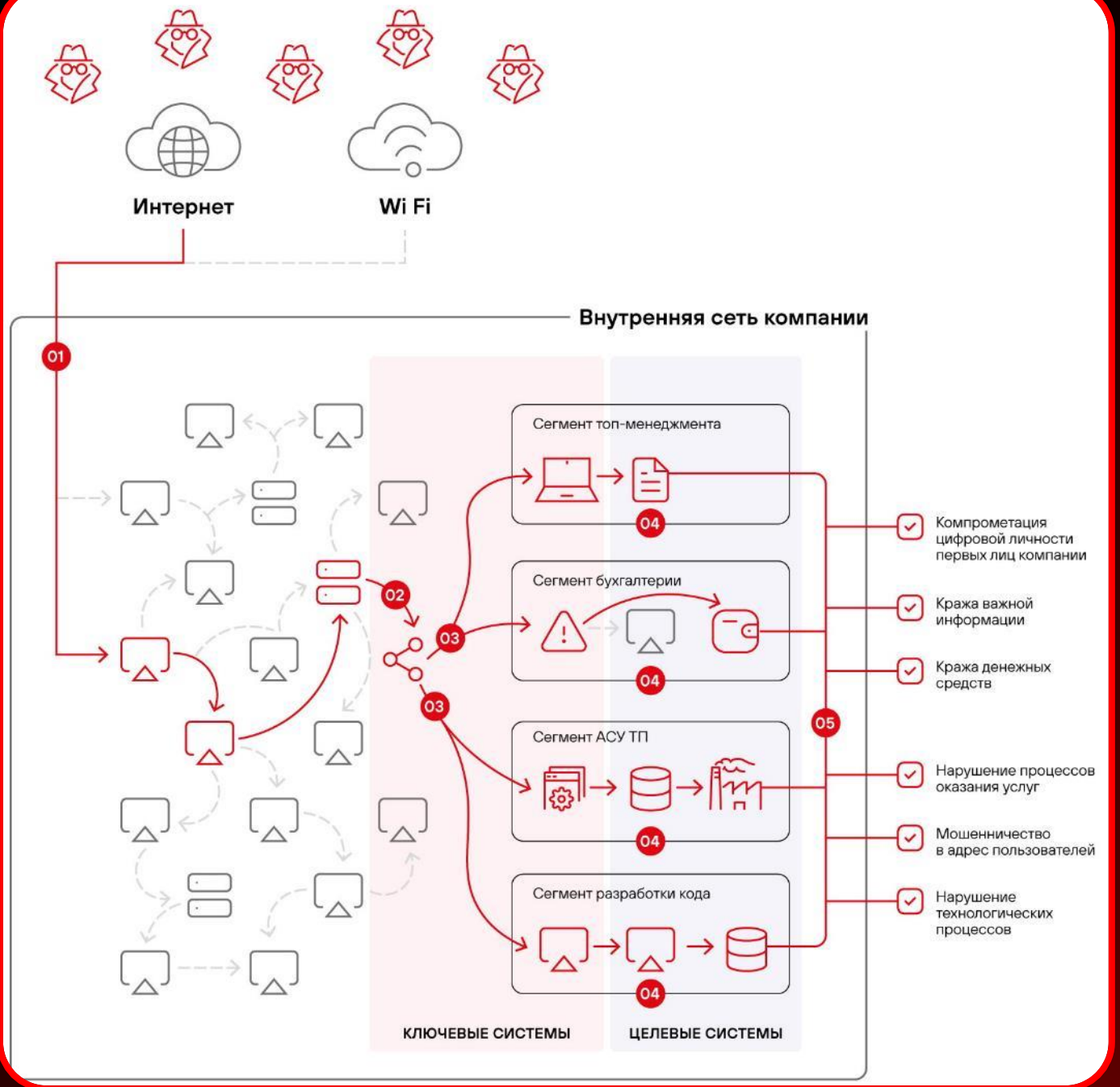
А СКОЛЬКО УСПЕШНЫХ АТАК ОСТАЛОСЬ ВНЕ ПОЛЯ ЗРЕНИЯ?

Количество доступов к инфраструктуре промышленных организаций, продаваемых в дарквебе, в 2022 году выросло на 40%.

Актуальные киберугрозы для промышленных организаций: итоги 2022 года, Positive Technologies

Что делать?

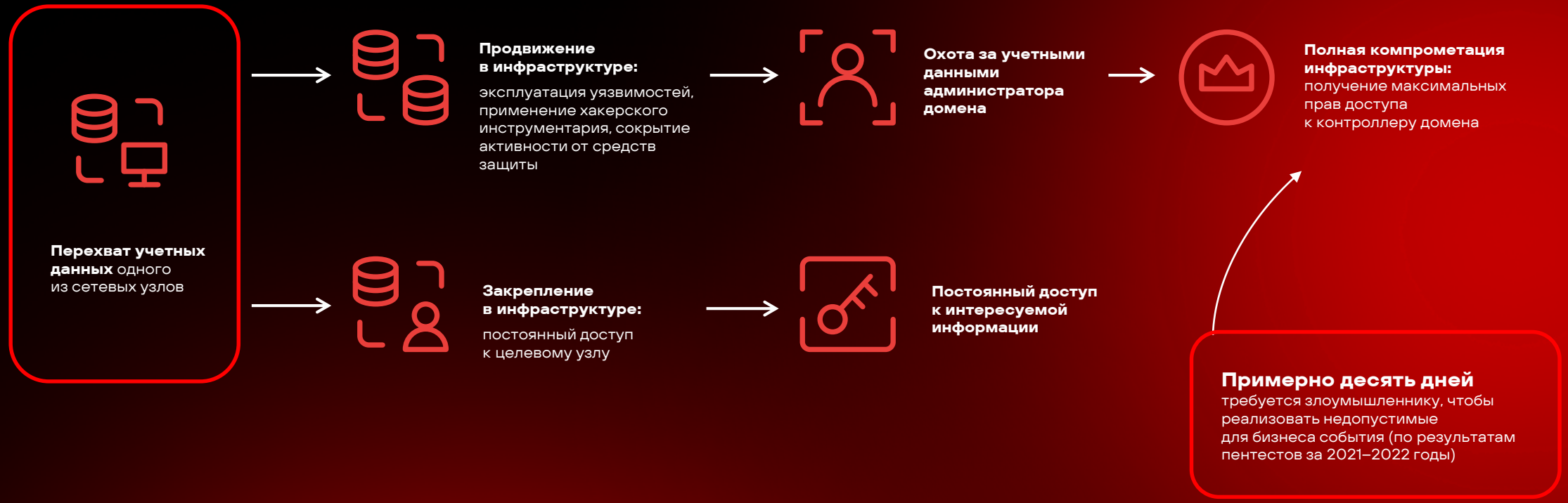
КАК ВЫГЛЯДИТ АТАКА ГЛАЗАМИ ЭКСПЕРТА



01. Преодоление сетевого периметра
02. Получение максимальных привилегий
03. Получение доступа к ключевым сегментам
04. Развитие атаки на целевые системы
05. Реализация недопустимых событий

- Аналитика по атакам 2021 года. Positive Technologies
- Как выявить атаку самому. Positive Technologies

НУЖНО ВИДЕТЬ ДЕЙСТВИЯ ХАКЕРОВ ВНУТРИ СЕТИ



По данным исследования Positive Technologies «Итоги пентестов — 2022»

PT NETWORK ATTACK DICOVERY – ЭТО NTA

Обнаружение атак и аномалий	Правила и репутационные списки	Поведенческие и статистические модули	Ретроспективный анализ	Машинное обучение
Расследование	Сетевые связи	Профилирование узлов	Импорт и экспорт сырого трафика	Воспроизведение трафика
Проактивный поиск угроз	Язык запросов	Метаданные	Сырой трафик	Извлечение объектов из трафика
Экспертиза	Исследование новейших инструментов, техник и тактик атакующих	Расследование кибератак	Мониторинг APT-группировок	
Передовые технологии	Уникальная технология DPI для детального разбора трафика			
Экосистемность	Интеграция с MaxPatrol SIEM, PT Sandbox, PT XDR, PT Threat Intelligence Feeds	Интеграция с продуктами других вендоров		

PT NAD — ДЛЯ РЕШЕНИЯ ЗАДАЧ ИБ

Контроль активов

- Инвентаризует узлы по сетевому отпечатку
- Обнаруживает нарушения регламентов ИБ

Нетипичное поведение узлов

- Находит аномалии в сетевом трафике
- Профилирует сетевые узлы и определяет приложения

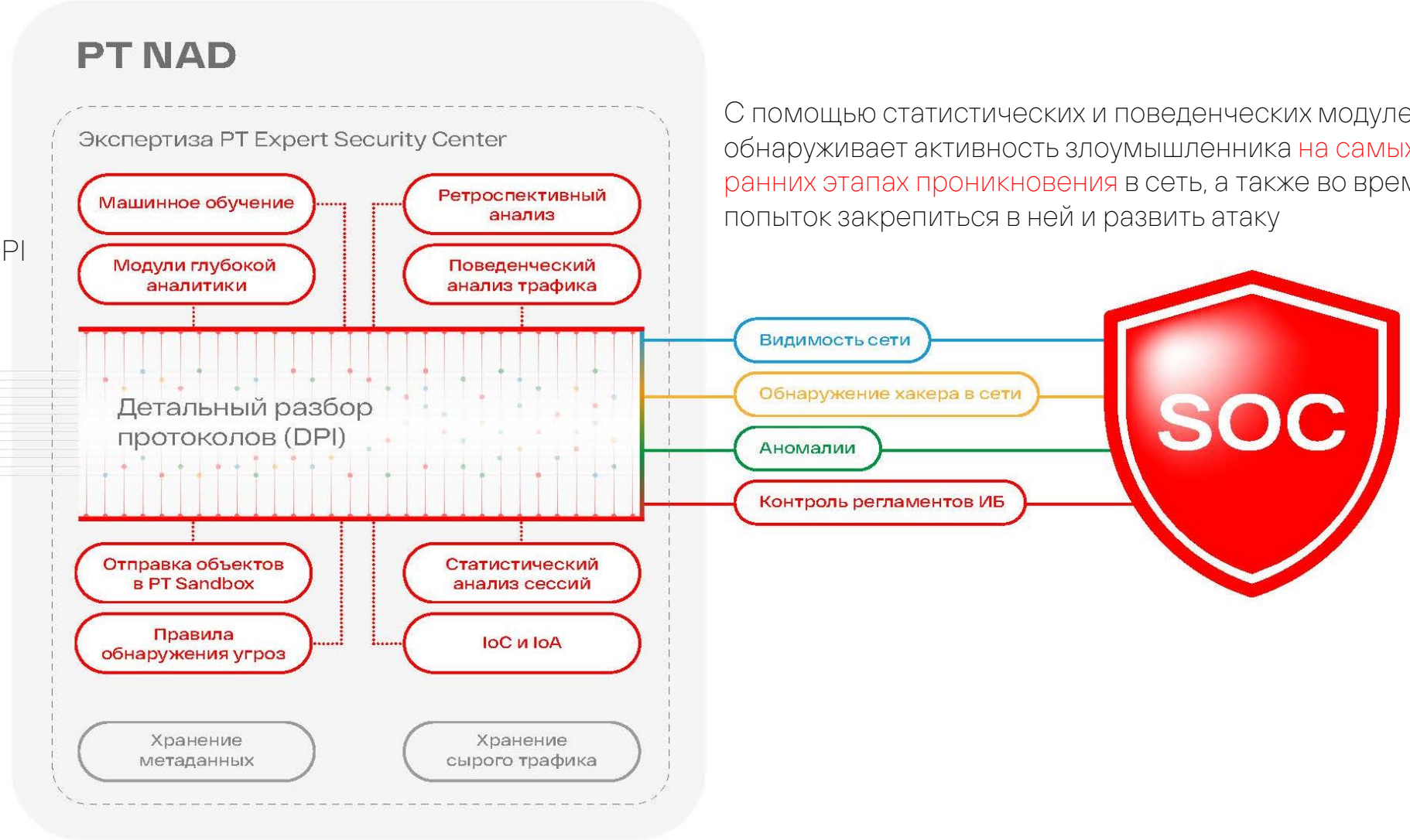
180 техник и тактик атакующих

- Обнаруживает попытки эксплуатации уязвимостей и видит факты их успешной эксплуатации
- Выявляет хакерские инструменты и перемещение атакующих внутри периметра
- Определяет угрозы в зашифрованном трафике
- Определяет зараженные узлы и подключения к C2

Какие техники MITRE ATT&CK выявляет PT NAD

КАК РАБОТАЕТ PT NAD

Захватывает, разбирает сетевой трафик на периметре и в инфраструктуре с помощью технологии DPI



С помощью статистических и поведенческих модулей обнаруживает активность злоумышленника на самых ранних этапах проникновения в сеть, а также во время попыток закрепиться в ней и развить атаку

PT NAD — ИДЕАЛЬНОЕ ДОПОЛНЕНИЕ К SIEM И EDR

- Дополняет EDR, закрывая слепые пятна на уровне сети
- Обогащает SIEM-систему сетевым контекстом и ускоряет реагирование
- PT NAD входит в тройку флагманских продуктов Positive Technologies

PT Sandbox производит анализ файлов и возвращение вердиктов, передаваемых из PT NAD, а также в почтовом, сетевом и веб-трафике.

ОТЛИЧИЯ PT NAD ОТ ДРУГИХ СИСТЕМ

В отличие от других систем, анализирующих трафик, NTA-системы сфокусированы на выявлении злоумышленников **внутри** сети.

Они глубоко анализируют сессии, сохраняют данные из них, что позволяет **проводить расследования и восстанавливать цепочку атак**.

	NTA- или NDR-система	IDS (в классическом представлении)	IPS (NGIPS)	UTM-решение	NGFW (при включении всех модулей)
Методы выявления атак	Сигнатуры, поведенческий анализ, машинное обучение, выявление аномалий	Сигнатуры	Сигнатуры, поведенческий анализ, машинное обучение, выявление аномалий	Сигнатуры, поведенческий анализ, машинное обучение, выявление аномалий	Сигнатуры, поведенческий анализ, машинное обучение, выявление аномалий
Блокировка атак или соединений	В случае интеграции с блокирующими решениями	Нет, только выявление	Да	Да	Да
Работа с шифрованным трафиком	Альтернативные методы	Отсутствует	Использование MITM («человек посередине»)	Использование MITM («человек посередине»)	Использование MITM («человек посередине»)
Глубина анализа сессий	Целиком	Первые N байт	Первые N байт	Целиком	Целиком
Анализ внешних протоколов	Да	Да	Да	Да	Да
Анализ внутренних протоколов	Да	Отсутствует	Отсутствует	Да	Да
Возможность расследований на основе метаданных и копии трафика	Полная: хранение информации о трафике, независимо от обнаружений	Отсутствует	Частичная (только в случае выявления атак)	Частичная (только в случае выявления атак)	Частичная (только в случае выявления атак)
Проверка файлов, хеш-сумм, DNS-адресов, URL	Индикаторы компрометации, DGA-домены. Извлечение и проверка файлов	Индикаторы компрометации. Извлечение и проверка файлов	Индикаторы компрометации. Извлечение и проверка файлов	Индикаторы компрометации. Извлечение и проверка файлов	Индикаторы компрометации, DGA-домены. Извлечение и проверка файлов

PT NETWORK ATTACK DISCOVERY
МОЩНЫЙ ИНСТРУМЕНТ ДЛЯ АНАЛИЗА СЕТИ

1

Точно выявляет сложные сетевые атаки и сокращает время обнаружения хакеров до 1 часа

2

Упрощает расследования инцидентов и показывает слабые точки в сети

3

Сокращает время реагирования на приоритетные угрозы службе ИБ

Давайте строить систему кибербезопасности Сегодня!