КСБ-СОФТ

Positive Technologies и Центр мониторинга SOCRAT – непрерывная безопасность как современный метод защиты информации

- **Виктор Еременко**
  Лидер продуктовой практики NAD, Positive Technologies
- **Александр Кирий**
  Руководитель центра мониторинга SOCRAT, КСБ-СОФТ
- **Дмитрий Чирков**
  Руководитель регионального направления, КСБ-СОФТ

Время вебинара ~1 час

Обменивайтесь сообщениями
во вкладке «Чат»

Запись вебинара направим
всем участникам на указанный
при регистрации e-mail
в течение 2-3 рабочих дней

Задавайте вопросы во вкладке
«Вопросы»

Среди заданных вами вопросов, каждый Эксперт выберет лучший, на его взгляд, вопрос, и мы наградим 2-х авторов фирменным мерчем!

КСБ-СОФТ

Системный интегратор в сфере информационной безопасности и импортозамещения информационных технологий

Входим в ГК «Кейсистемс»

Лицензиат ФСТЭК России

Лицензиат ФСБ России

Проекты компании курируют опытные ИБ-специалисты, аккредитованные по международным сертификациям OSCP, CISM, CGEIT и CISA.

80+

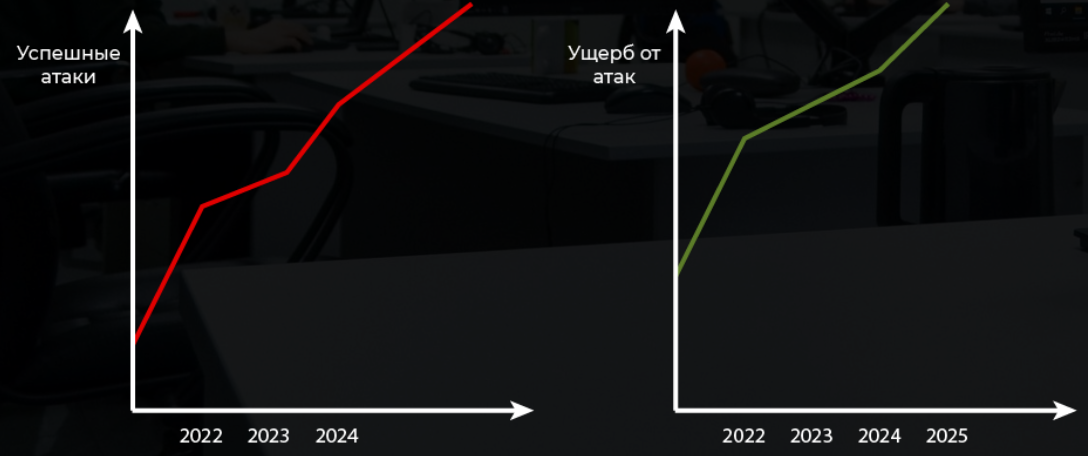
регионов внедрения

4000+

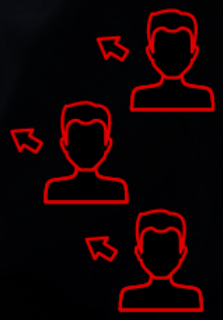
реализованных проектов

Информационная безопасность остается актуальной

Рост количества успешных атак



Смещение целей атак в сторону нарушения бизнес-процессов



Почему безопасность должна быть непрерывной?

Общее направление в части изменения НПА в сторону выстраивание процессов

Постоянно появляются новые угрозы безопасности

Естественная деградация инфраструктуры и системы защиты (неподдерживаемые вендором версии ПО и ОС, устаревшие СЗИ, неактуальные базы, текущие средства защиты не защищают от современных атак)

Какие процессы необходимы?

ИТ

- Периодическая инвентаризация (актуализация и учет активов сети)
- Обновление версий ПО и ОС (особенно установка пакетов безопасности)
- Проверка корректности бэкапирования критичной информации

И другие

ИБ

- Управление уязвимостями
- Мониторинг и реагирование на инциденты ИБ
- Повышение осведомленности сотрудников

И другие

Какие процессы необходимы?

PT NAD

Система анализа трафика (NTA) для выявления атак

MaxPatrol VM

Система нового поколения для управления уязвимостями

MaxPatrol SIEM

Выявление инцидентов ИБ в реальном времени

MaxPatrol EDR

Защитит конечные точки от сложных и целевых атак во всех популярных ОС, включая российские

Как организовать процессы?

Процессы

Ответственное лицо

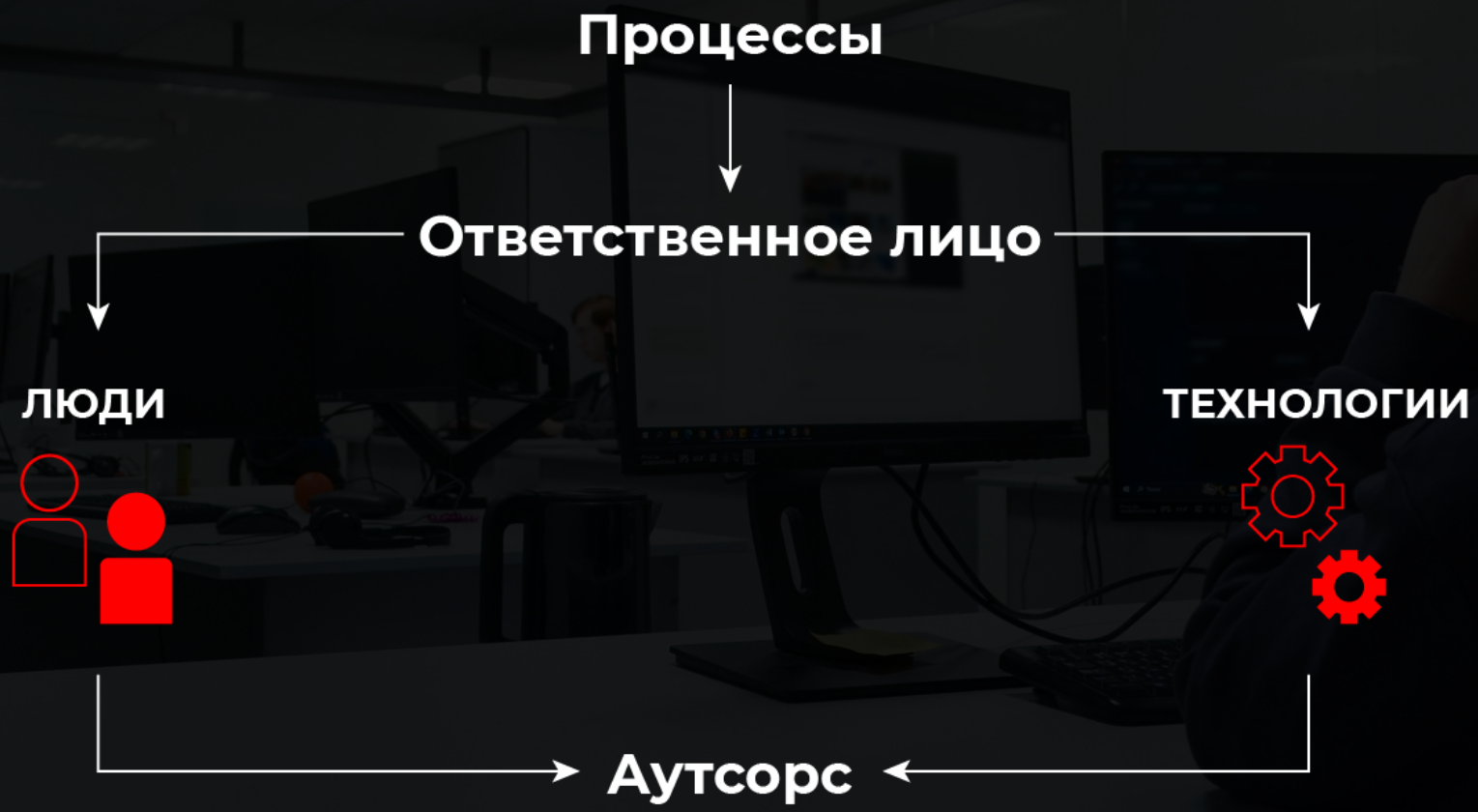
ЛЮДИ

- Подбор команды
- Регламентация процессов
- Внедрение процессов
- Контроль за реализацией
- Пересмотр и модернизация

ТЕХНОЛОГИИ

- Подбор решений
- Стендирование
- Внедрение решений
- Настройка/адаптация под изменения
- Пересмотр

Как организовать процессы?



SOC RAT
SECURITY OPERATION CENTER RUSSIAN ANALYTICS TEAM

SOCRAT – ЭТО ЦЕНТР МОНИТОРИНГА

Режим работы 24x7

Корпоративный центром ГосСОПКА

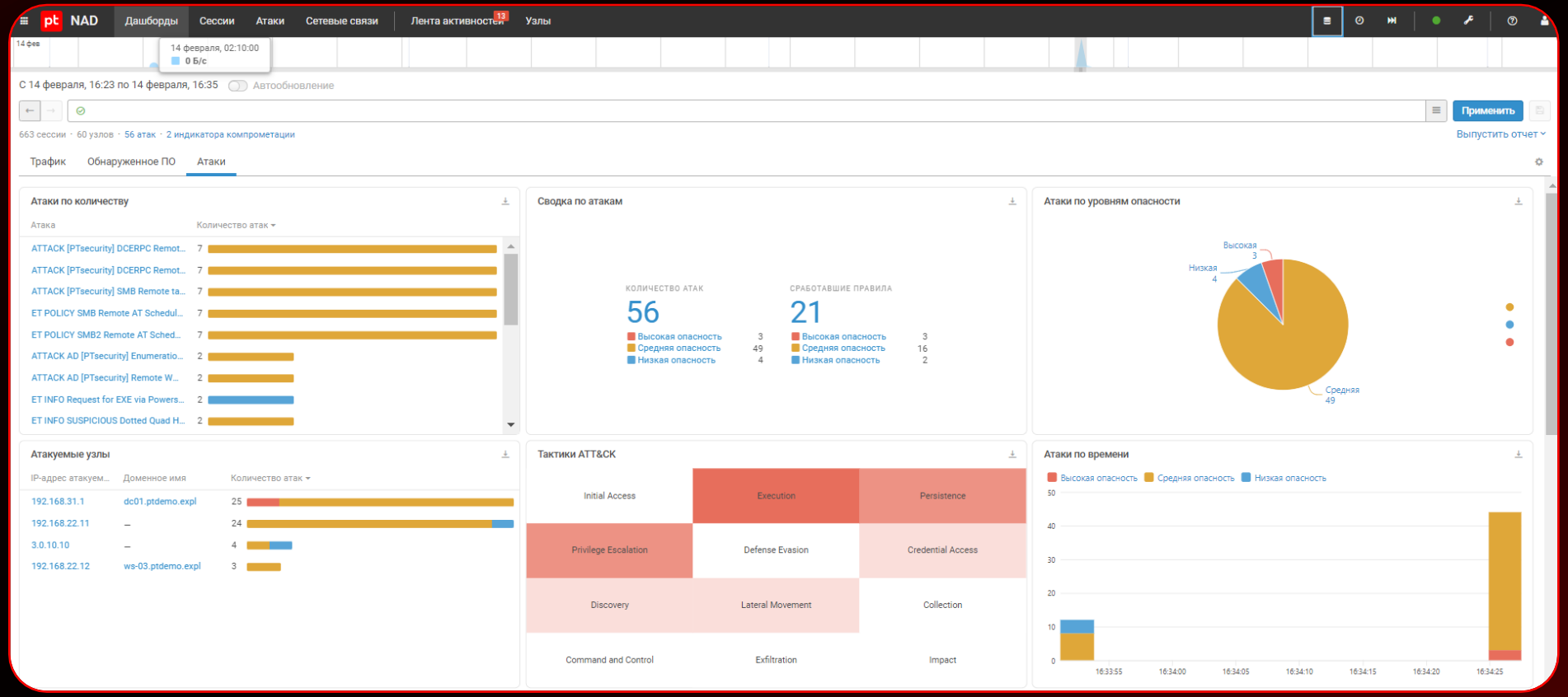
Инвентаризация
Анализ Уязвимостей
Тестирование на проникновение

Пакетная система предоставления услуг (выбор только необходимого)

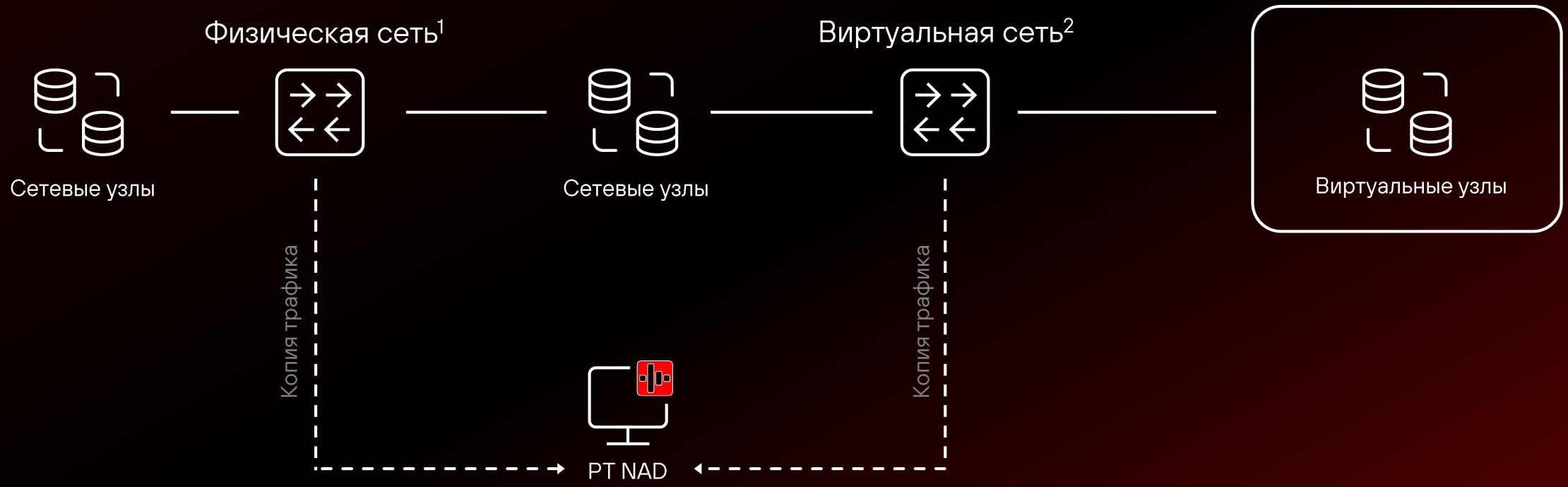
Год создания: 2020

PT Network Attack Discovery

Система поведенческого анализа сетевого трафика для обнаружения скрытых кибератак
Точно обнаруживает действия злоумышленников в сети, упрощает расследование инцидентов и помогает в проактивном поиске угроз



Варианты подключения PT NAD к сети



[1] Брокер сетевых пакетов, TAP-устройства, коммутаторы (SPAN, GRE, ERSPAN).

[2] Брокер сетевых пакетов, vTAP (виртуальный TAP), виртуальные коммутаторы (GRE, ERSPAN).

Как работает PT NAD

Методы анализа трафика

Классический	Глубокая экспертиза	ML
Сигнатурный анализ	Обнаружение новых активов	Пользовательские правила профилирования
Репутационные списки	Экспертные модули	Анализ шифрованного трафика
Интеграция с PT Sandbox	Детектирование приложений и сервисов	Поиск DGA-доменов

Какие техники MITRE ATT&CK выявляет PT NAD

Подробнее о том, какие техники покрывает PT NAD и как он их выявляет:

mitre.ptsecurity.com

Выявляет 180 техник и тактик атакующих, включая хакерский инструментарий и модифицированное вредоносное ПО

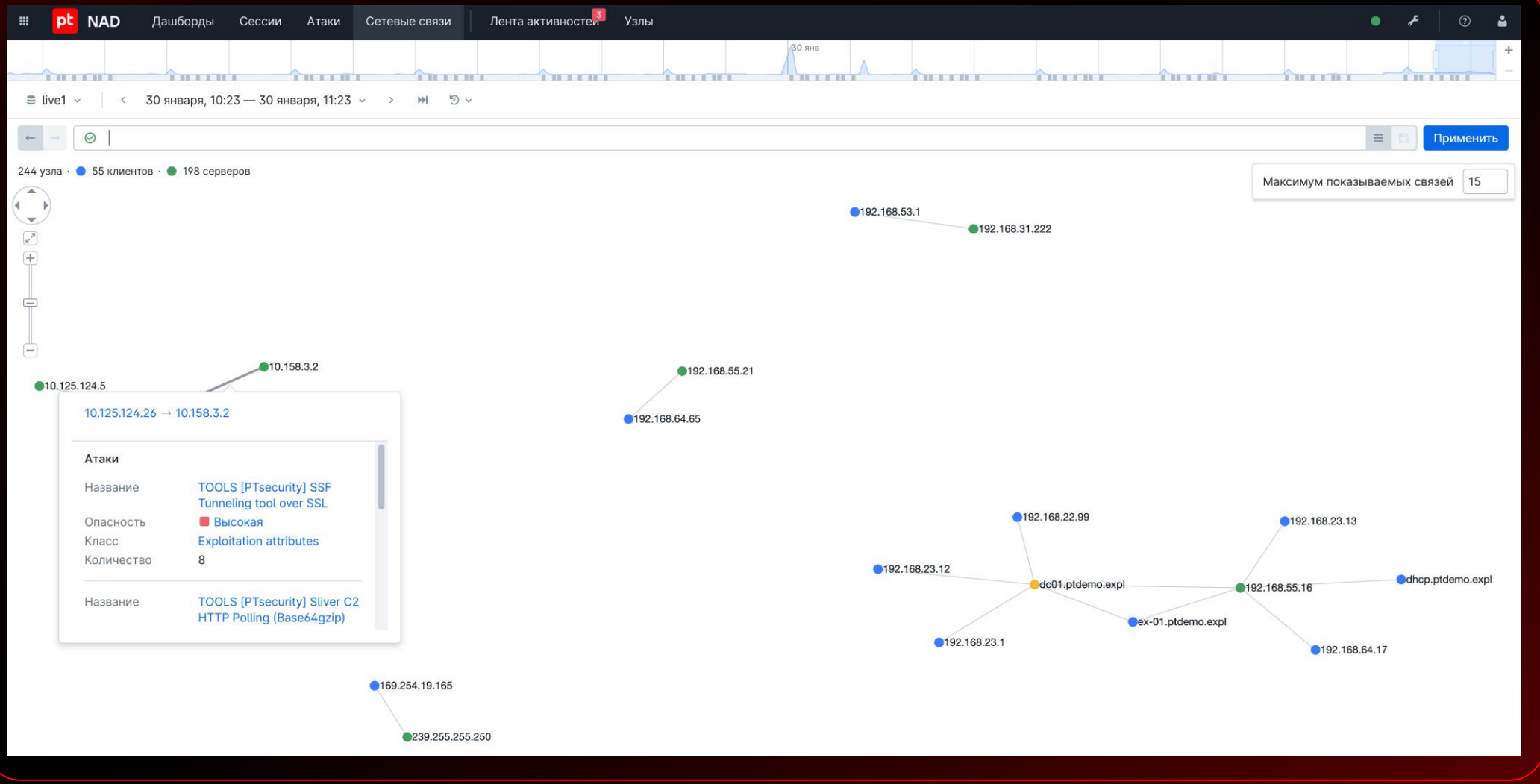
Сценарии использования

- Контроль соблюдения регламентов ИБ
- Выявление атак и аномалий в сети
- Обнаружение некорпоративных ОС и ПО
- Обнаружение средств удаленного администрирования

PT NAD

- Обнаружение теневой инфраструктуры
- Расследование атак
- Проверка сетевых узлов
- Проактивный поиск угроз

Сетевые связи



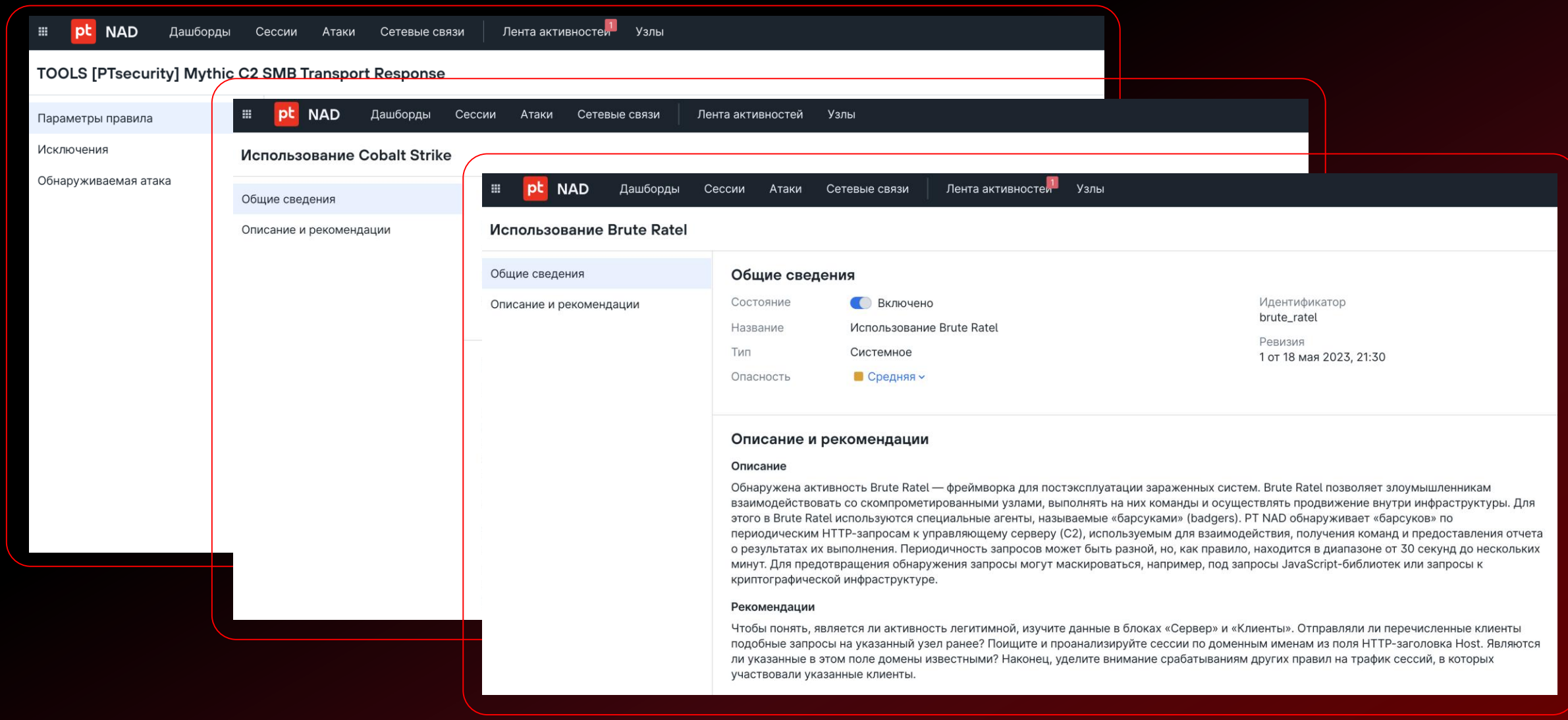
Результативность

BDU:2024-08422

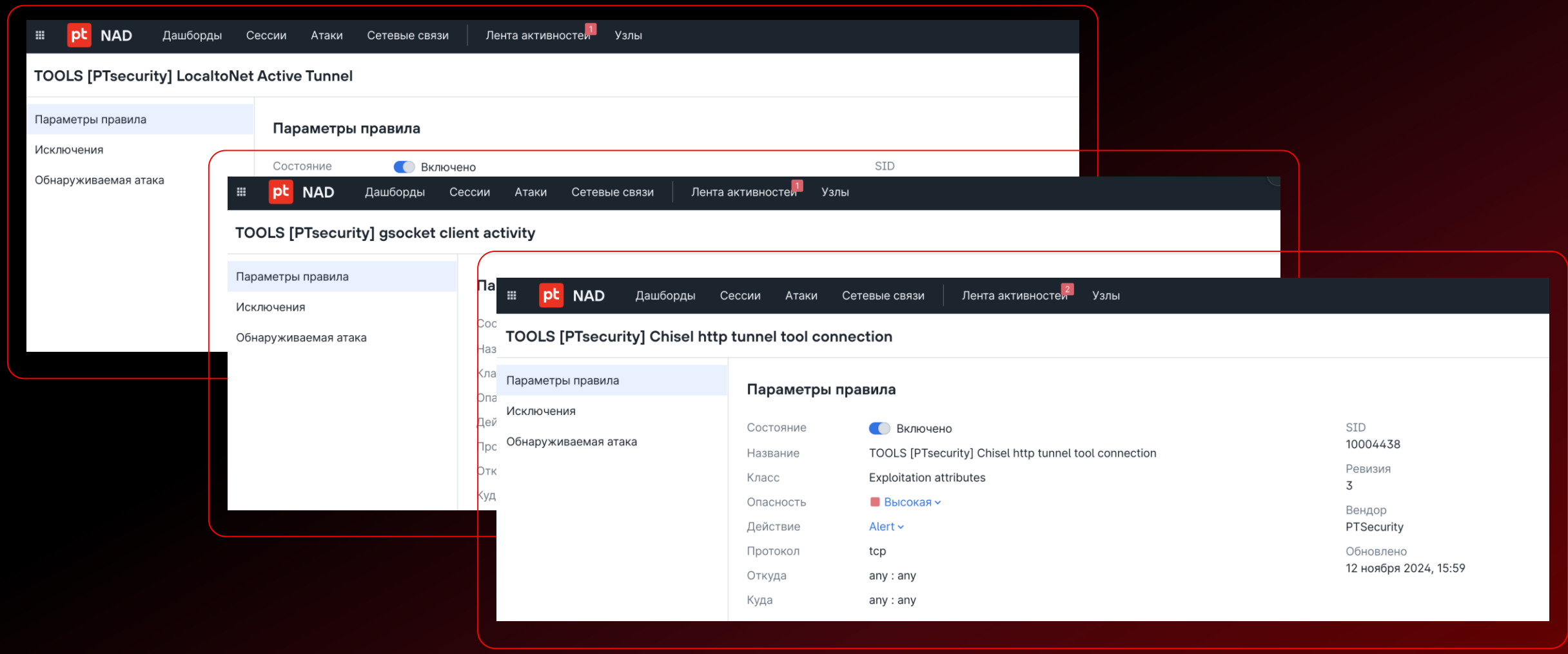
BDU:2024-08421

Ссылка

Детектирование хакерского инструментария



Детектирование коннекта с C2




NTA/NDR
Анализ сетевого трафика
SOC
EDR
Анализ активности на конечных устройствах
SIEM
Сбор журналов, анализ событий

С ЧЕГО НАЧАТЬ?

КСБ-СОФТ

ПИЛОТНОЕ ПОДКЛЮЧЕНИЕ

Вы можете бесплатно оценить качество предоставляемых услуг **SOCRAT**

Мониторинг: **8x5**

Время реагирования – **24 часа** с момента обнаружения

Ограниченный состав подключаемых ресурсов

Длительность пилота – **1 месяц**

Демостенд

Пилот

Серверы

Консультации

positive technologies

ПИЛОТНОЕ ПОДКЛЮЧЕНИЕ

Вы можете бесплатно оценить **PT NAD**

PT NAD

Система анализа трафика (NTA) для выявления атак

РАБОТАЙТЕ С НАМИ!

ksb-soft.ru

Телеграм-канал
«Мнение Интегратора»

Подкаст
«Голос Интегратора»

info@ksb-soft.ru

8 800 3333-872

428000, г. Чебоксары,
пр-т Максима Горького,
18 Б, пом. 9