Новое в версии ViPNet TIAS 3.8

Светлана Старовойт
руководитель продуктового направления

infotecs

План вебинара

- Система ViPNet IDS 3
- Решение ViPNet TDR
- Новое в версии ViPNet TIAS 3.8
- Планы развития

ViPNet IDS 3

Система обнаружения компьютерных атак (вторжений) ViPNet IDS 3

ViPNet IDS NS

ViPNet TIAS

ViPNet IDS MC

Обязательный компонент

Не обязательные компоненты

Система обнаружения компьютерных атак класс В

Система обнаружения вторжений уровня сети 4 класс

Требования доверия безопасности 4 уровня

Сертифицированные версии продуктов

Сертифицированные версии:

- ViPNet IDS NS 3.6.1 + 5 патчей обновления
- ViPNet TIAS 3.5.1 + 1 патч обновления
- ViPNet IDS MC 1.6 + 2 патча обновления

Завершается контроль изменений:

- ViPNet IDS NS 3.8
- ViPNet TIAS 3.7.1
- ViPNet IDS MC 1.8

ФЕДЕРАЛЬНАЯ СЛУЖБА БЕЗОПАСНОСТИ РОССИЙСКОЙ ФЕДЕРАЦИИ

СЕРТИФИКАТ СООТВЕТСТВИЯ

№ СФ/СЗИ-0394

СИСТЕМА СЕРТИФИКАЦИИ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ

СЕРТИФИКАТ СООТВЕТСТВИЯ

№ 4329

НАЧАЛЬНИК 2 УПРАВЛЕНИЯ ФСТЭК РОССИИ

ViPNet TDR

ViPNet Threat Detection & Response

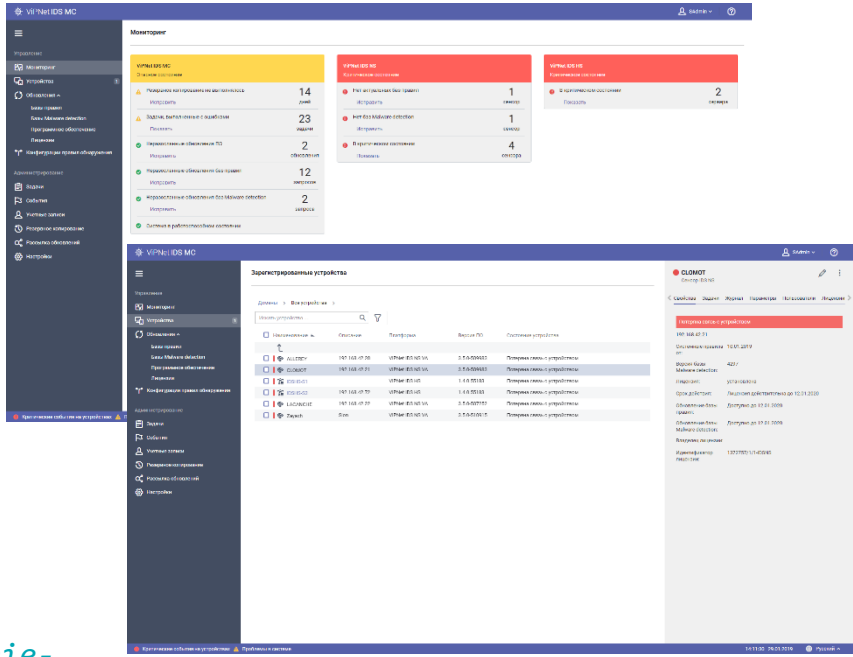
infotecs

Решение по обнаружению и предотвращению компьютерных атак

Управление	ViPNet IDS MC
Анализ	ViPNet TIAS
Обнаружение	ViPNet IDS NS ViPNet IDS HS
Обнаружение и предотвращение	ViPNet xFirewall ViPNet EndPoint Protection

ViPNet IDS MC

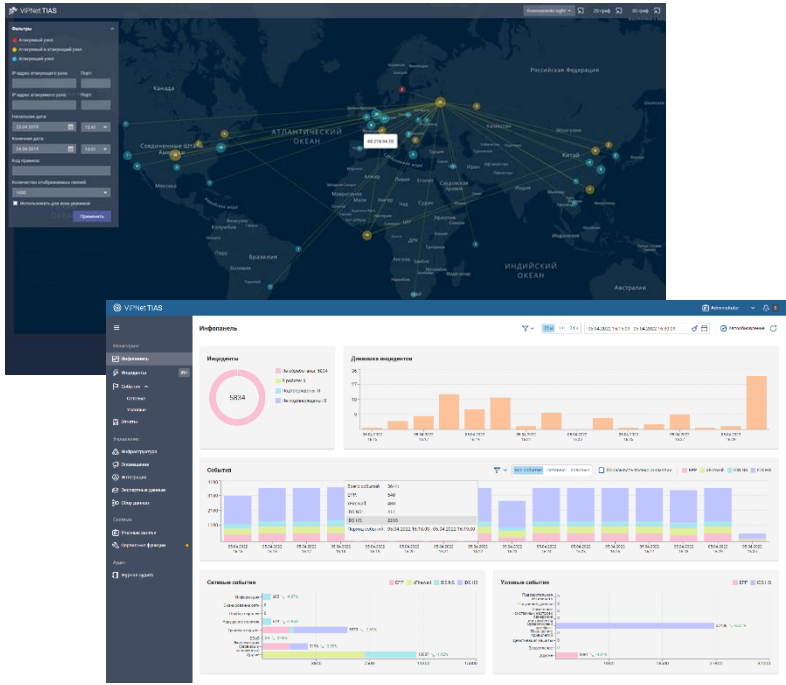
- Ввод в эксплуатацию сенсоров IDS;
- управление инфраструктурой решения ViPNet TDR;
- управление конфигурациями правил на устройствах.
- обновление:
  - баз решающих правил
  - сигнатур вредоносного ПО
  - экспертных данных
  - программного обеспечения устройств
  - лицензий
- мониторинг состояния устройств



https://infotecs.ru/webinars/archive/bystroe-razvorachivanie-i-vvod-v-ekspluatatsiyu-resheniya-vipnet-tdr.html

ViPNet TIAS

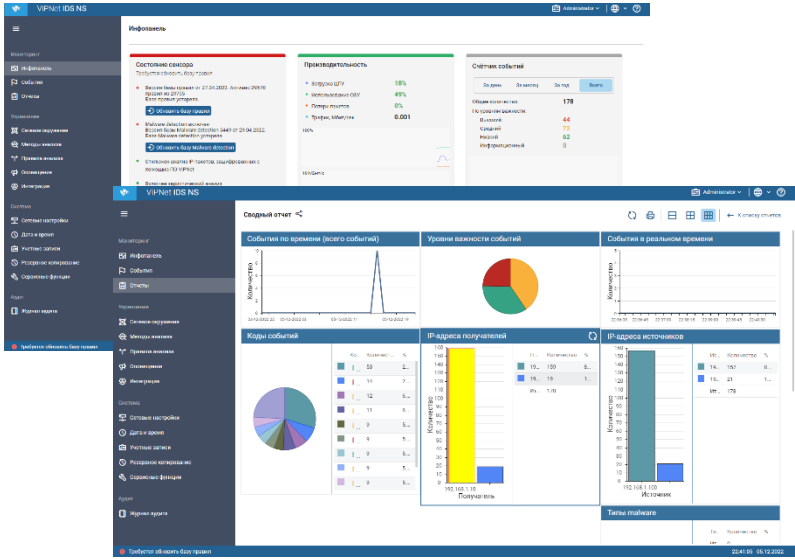
- сбор и анализ событий ИБ, поступающих от источников;
- автоматическое выявление подозрений на инциденты ИБ;
- предоставление рекомендаций по реагированию на инцидент;
- формирование отчетов по событиям и инцидентам;
- предоставление возможностей для ручного анализа событий и проведения расследований по инцидентам.



https://infotecs.ru/webinars/archive/demonstratsiya-vozmozhnostey-resheniya-tdr-v-usloviyakh-provedeniya-setevoy-ataki.html

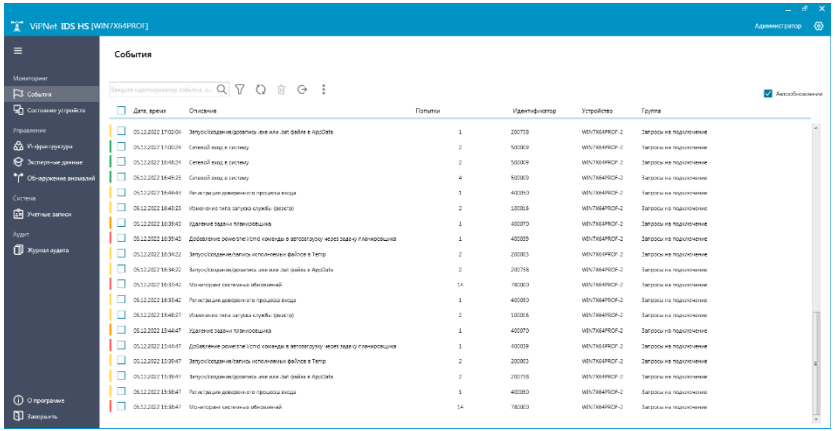
ViPNet IDS NS

- анализ сетевого трафика с помощью баз решающих правил, сигнатур вредоносного ПО и эвристических методов и выявление событий ИБ;
- хранение событий, пакетов и сессий;
- передача событий во внешние системы;
- передача во внешние системы статистики Netflow;
- пользовательские правила анализа.



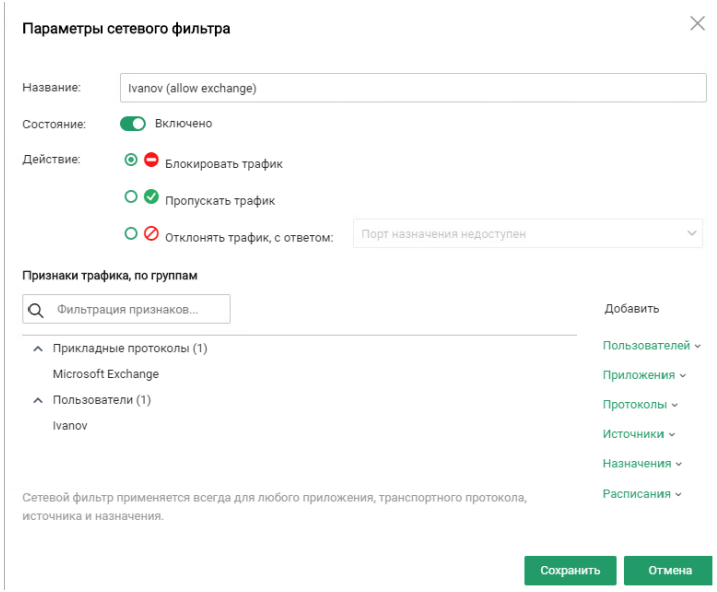
ViPNet IDS HS

- анализ сетевого трафика проходящего через узел;
- выявление подозрительной активности внутри ОС:
  - файловая активность,
  - изменения в реестре,
  - неизвестные процессы.
- выявление подозрительной активности пользователей;
- выявление вредоносного ПО.



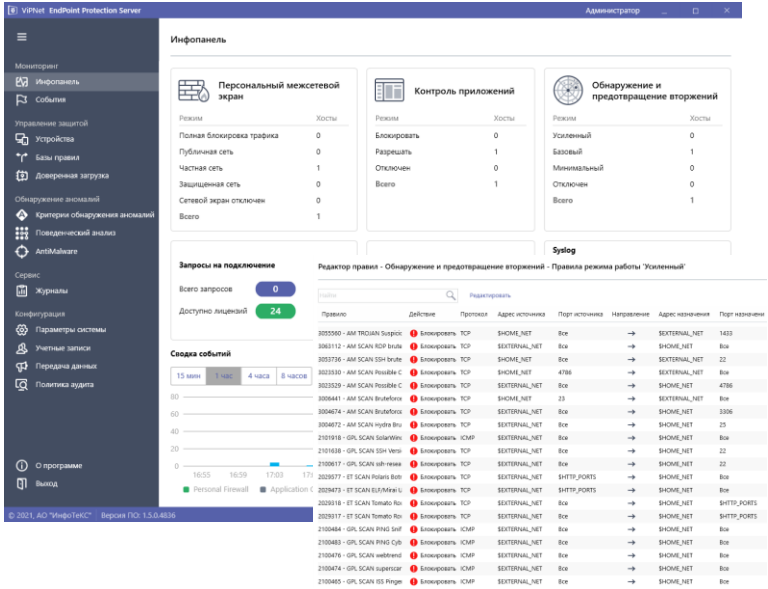
ViPNet xFirewall

- выявление подозрительной активности в сетевом трафике с помощью:
  - правил IPS;
  - эвристического и поведенческого анализа;
- блокирование компьютерных атак и подозрительных действий с помощью:
  - фильтров межсетевого экрана;
  - правил IPS + DPI;
  - фильтров контроля приложений.



ViPNet Endpoint Protection

- выявление подозрительной активности на конечных рабочих станциях с помощью:
  - правил системы обнаружения и предотвращения вторжений;
  - эвристического анализа Anti-malware;
  - обнаружения аномального поведения системных утилит;
- блокирование компьютерных атак и подозрительных действий с помощью:
  - фильтров Межсетевого экрана
  - списков ПО для Черного и Белого списка
  - правил HIPS



ViPNet TIAS 3.8

Новое в версии ViPNet TIAS 3.8

Основные улучшения и новые возможности

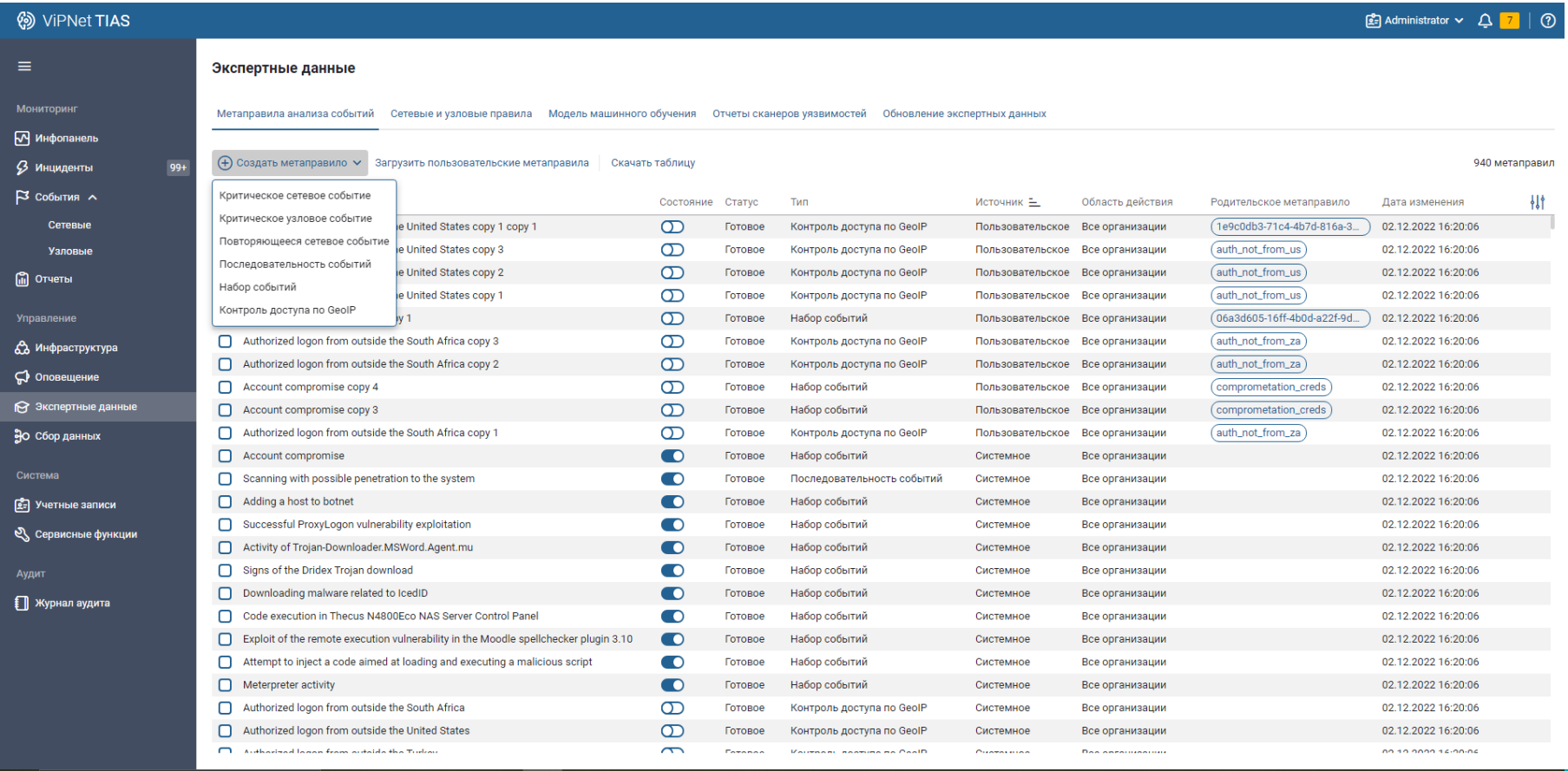
Пользовательские метаправила
возможность написания собственных правил анализа событий и выявления инцидентов

Дообучение модели
возможность дообучения модели машинного обучения как на новых экспертных данных, так и на размеченных данных пользователей

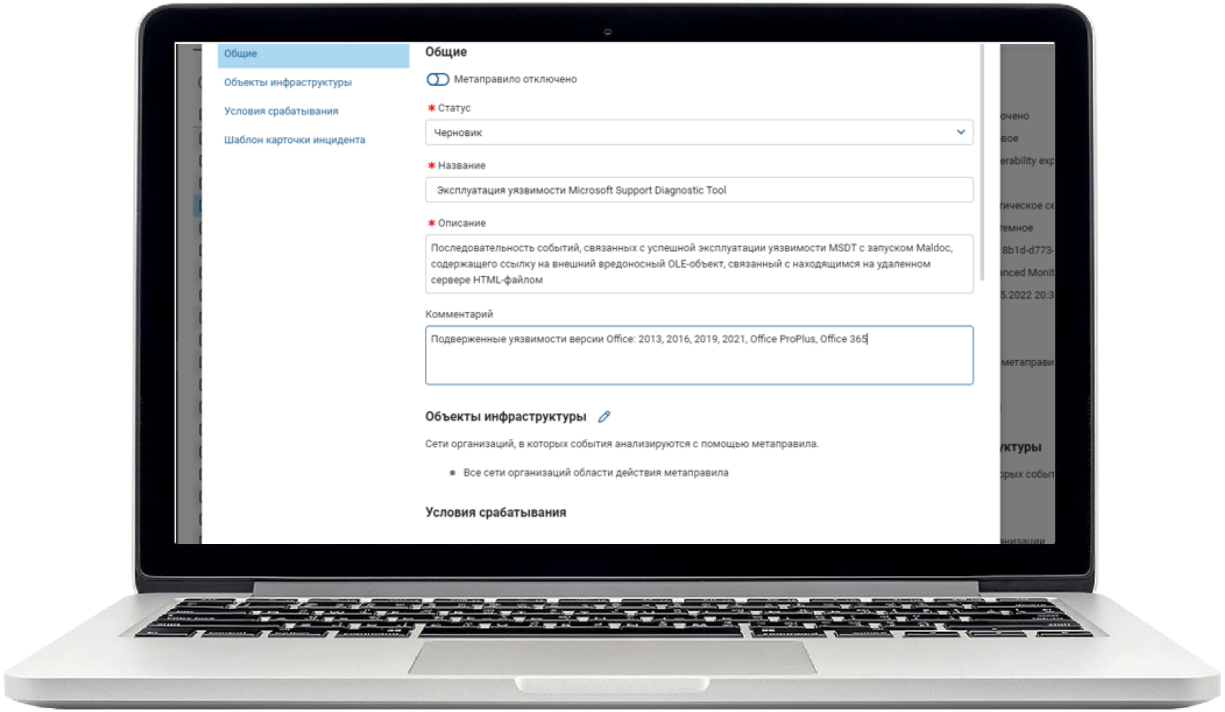
Улучшения UX
адаптация web-интерфейса под разные разрешения экранов и повышение удобства работы в ранее реализованных сценариях

Пользовательские метаправила

Управление метаправилами



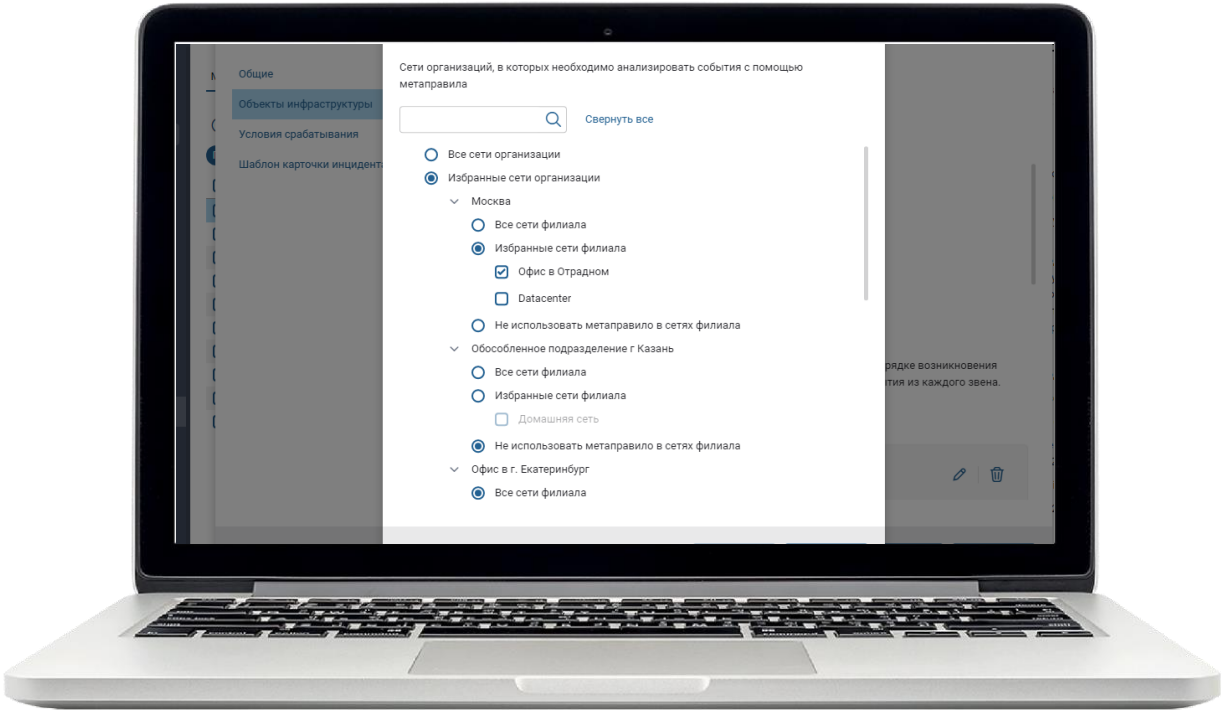
Создание нового метаправила



Шаблоны метаправил:

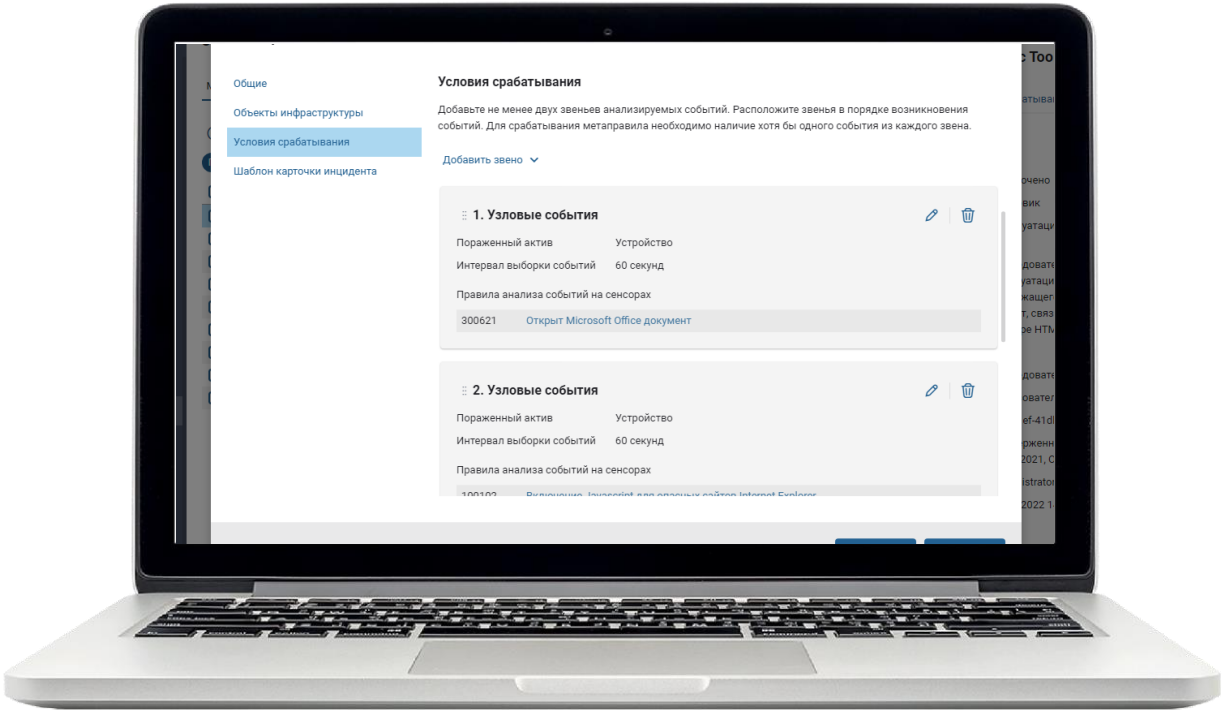
- критическое сетевое событие;
- критическое узловое событие;
- повторяющееся сетевое событие;
- последовательность событий;
- набор событий;
- контроль доступа по GeoIP.

Назначение метаправил на объекты инфраструктуры



Назначение метаправил на любой уровень инфраструктуры с точностью до подсети

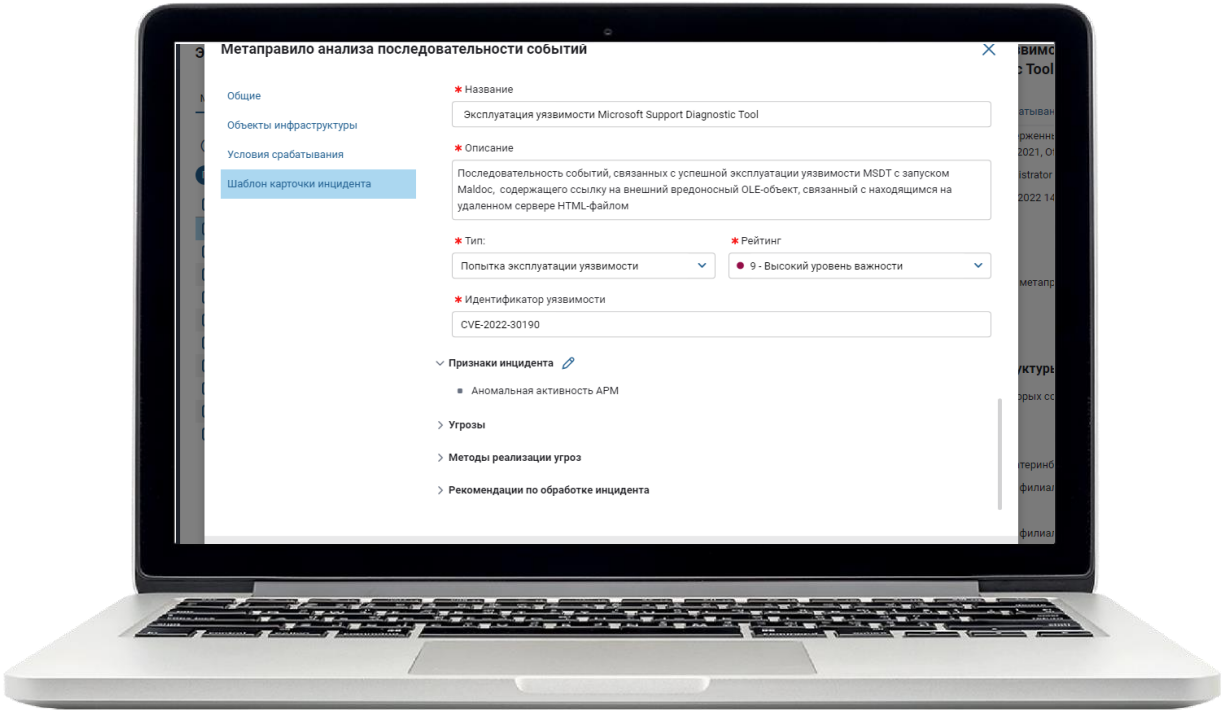
Условия срабатывания правила



Выбор условий:

- направление атаки;
- интервал выборки событий;
- порядок следования событий;
- сетевые и узловые правила.

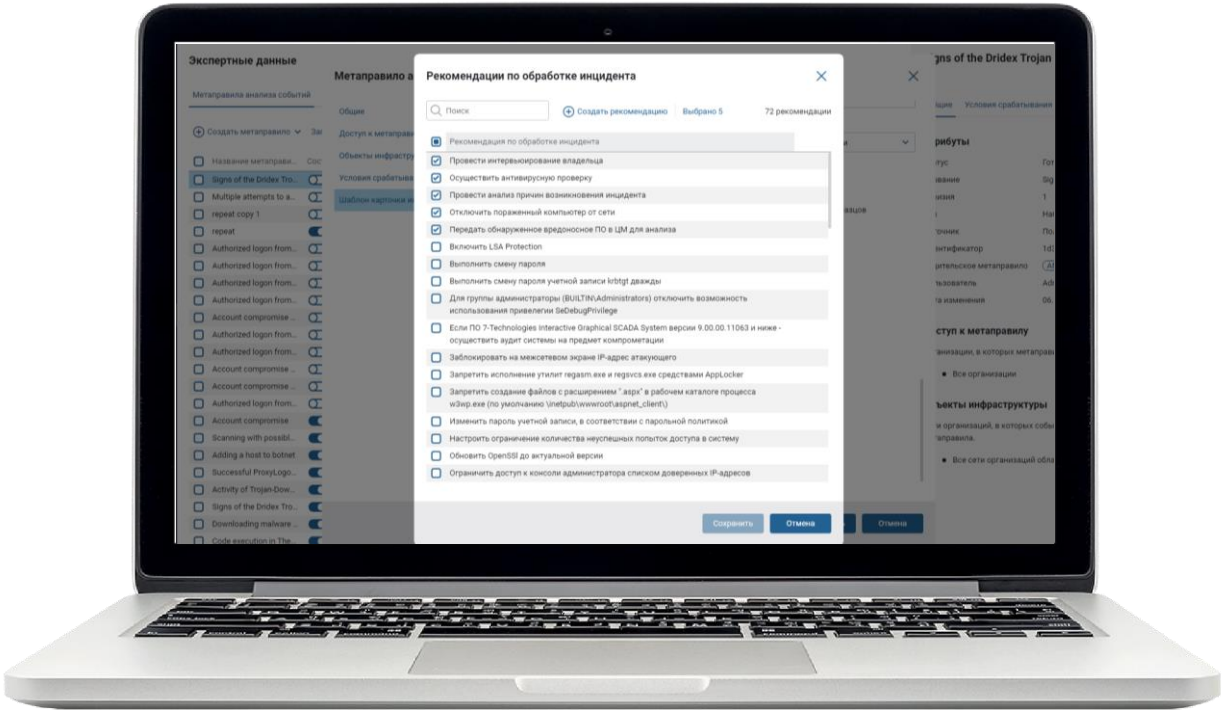
Шаблон карточки инцидента



Шаблон инцидента:

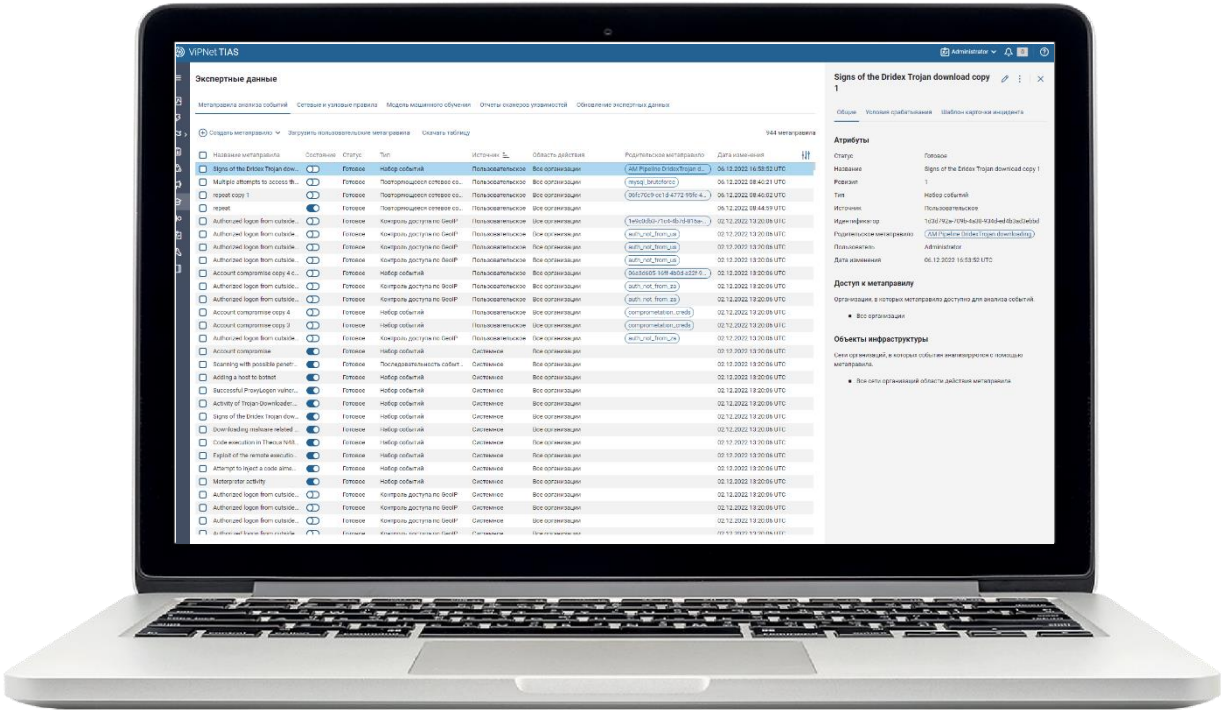
- название;
- описание;
- тип инцидента;
- рейтинг;
- идентификатор уязвимости;
- признаки инцидента;
- угрозы;
- методы реализации угроз;
- рекомендации по обработке.

Рекомендации по обработке инцидента



Выберите набор рекомендаций из представленного списка или добавьте свои

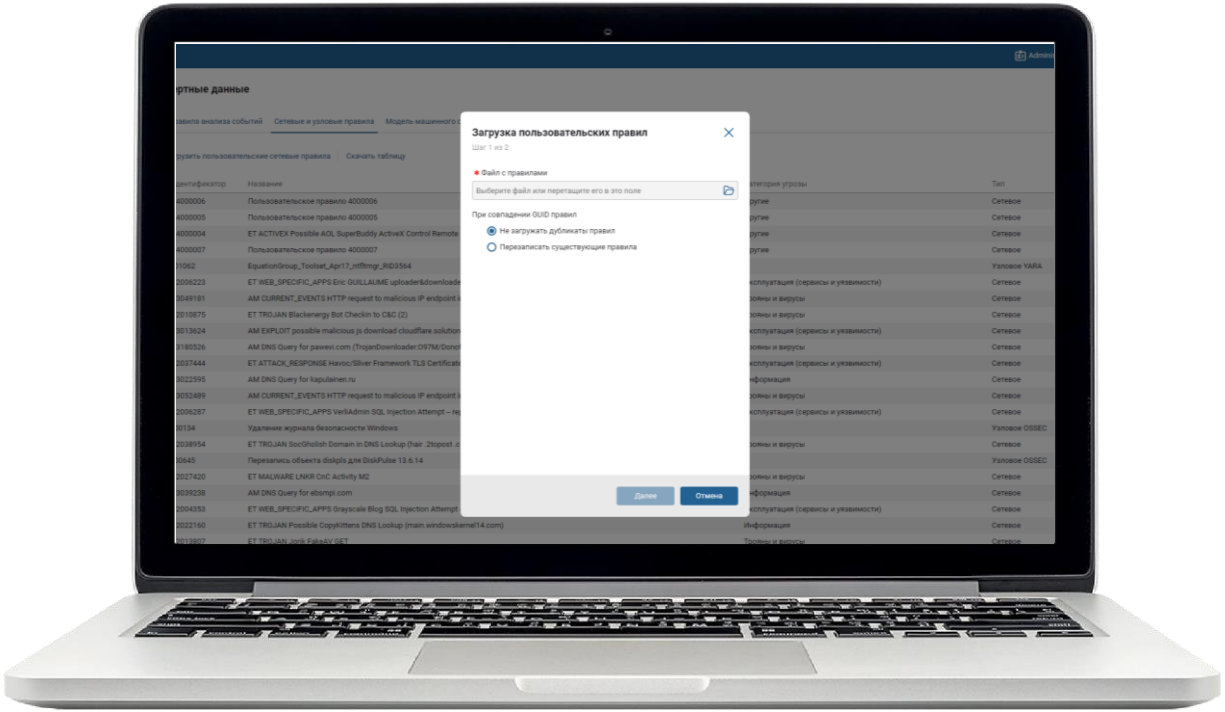
Работа с правилами



Для ввода правила в действие необходимо:

- назначить область действия правила;
- перевести из статуса «черновик» в статус «готовое»;
- включить правило

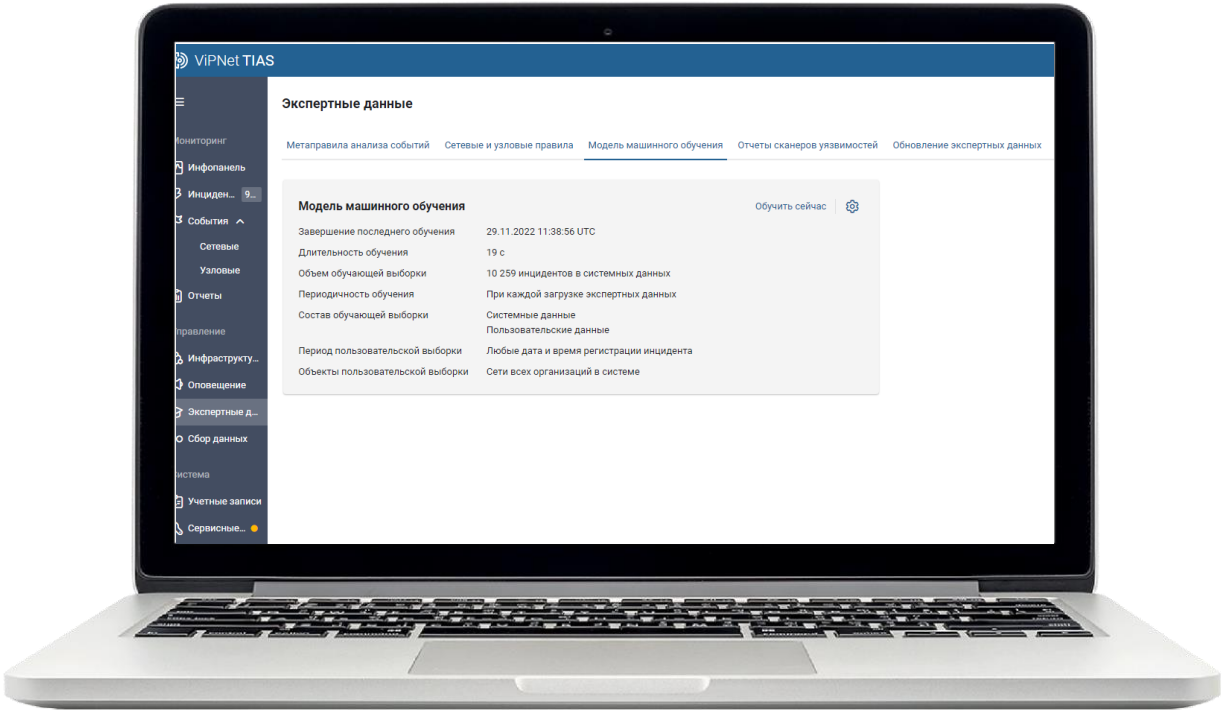
Пользовательские правила IDS NS



Для выявления инцидентов на основе событий, сработавших на пользовательские правила, необходимо загрузить пользовательскую БРП в TIAS.

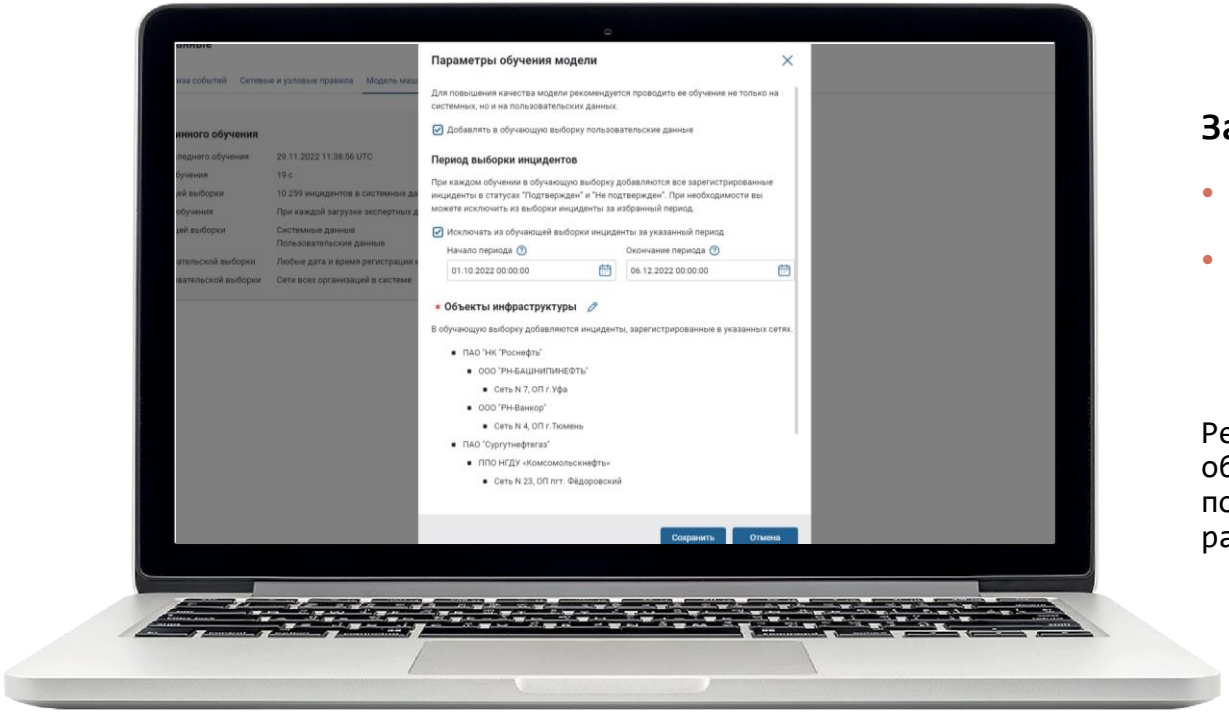
Дообучение математической модели принятия решений

Статистика обучения модели



- время завершения последнего обучения;
- длительность последнего обучения;
- объем обучающей выборки;
- периодичность обучения;
- состав обучающей выборки

Параметры обучения модели



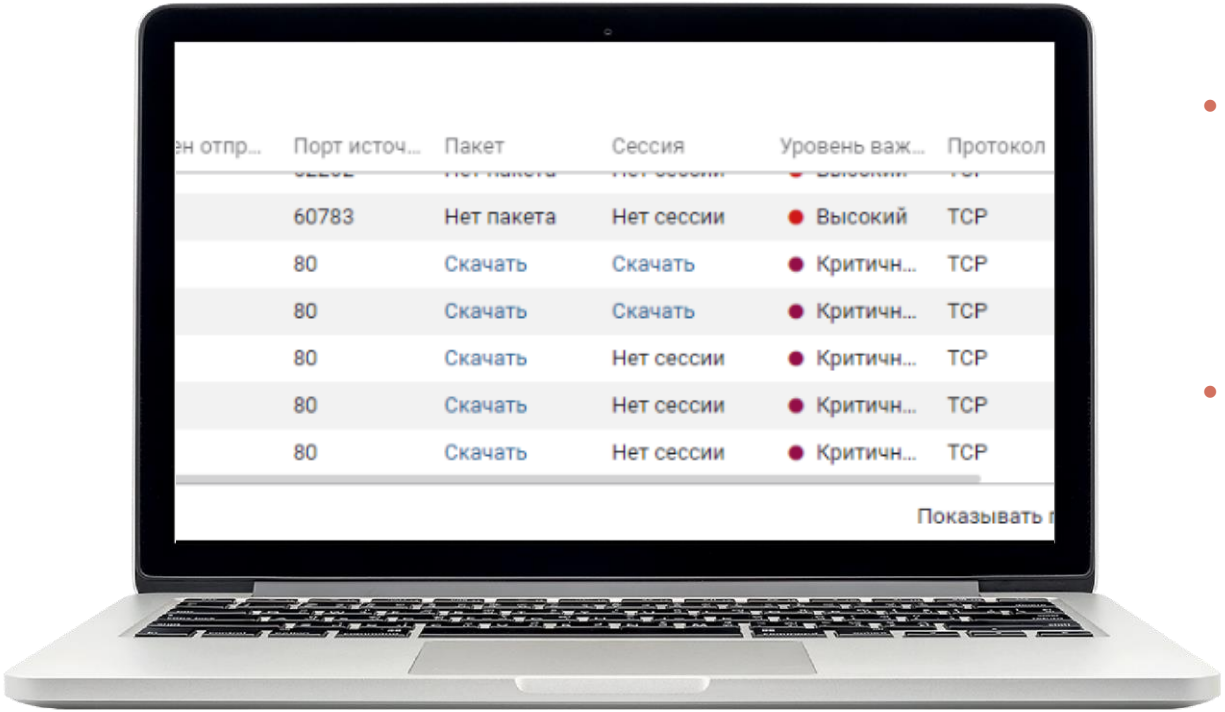
Задайте:

- Периодичность обучения
- Состав обучающей выборки

Рекомендуем добавлять в обучающую выборку пользовательские данные при размеченных статусах инцидентов

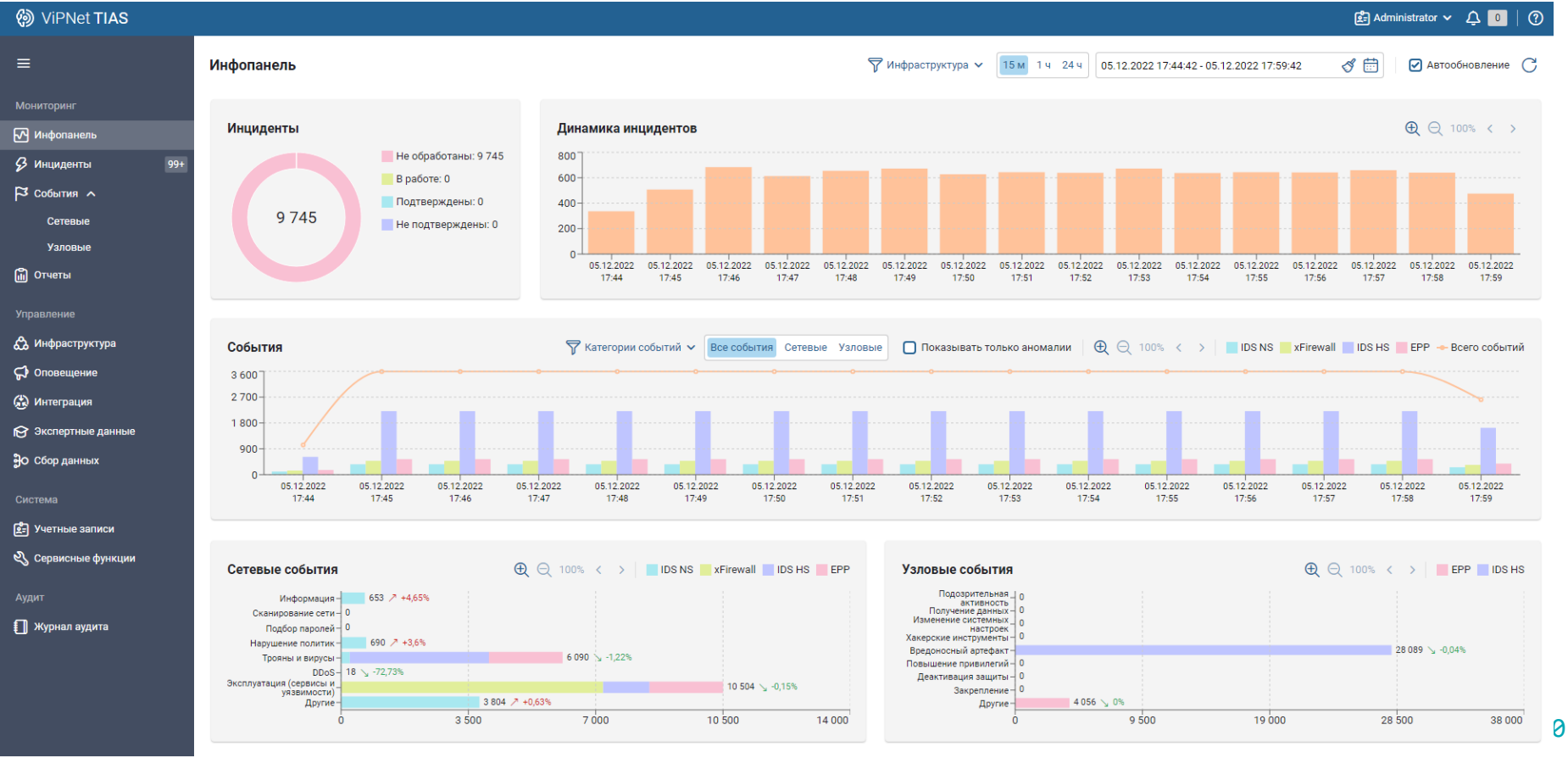
Улучшения пользовательских сценариев

Передача записи сессии из IDS NS в TIAS

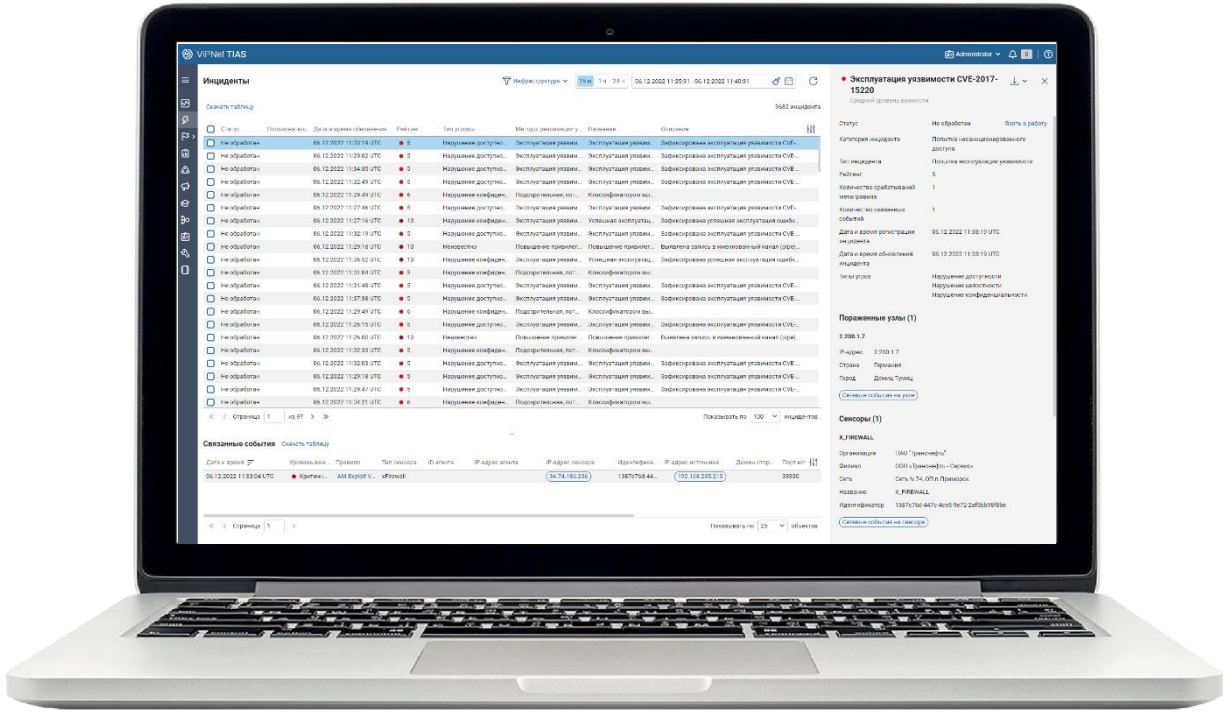


- Отображение статуса наличия пакета и сессии для скачивания по каждому событию
- Возможность скачивания с IDS NS как одного сетевого пакета, так и записанной сессии;

Главная инфопанель

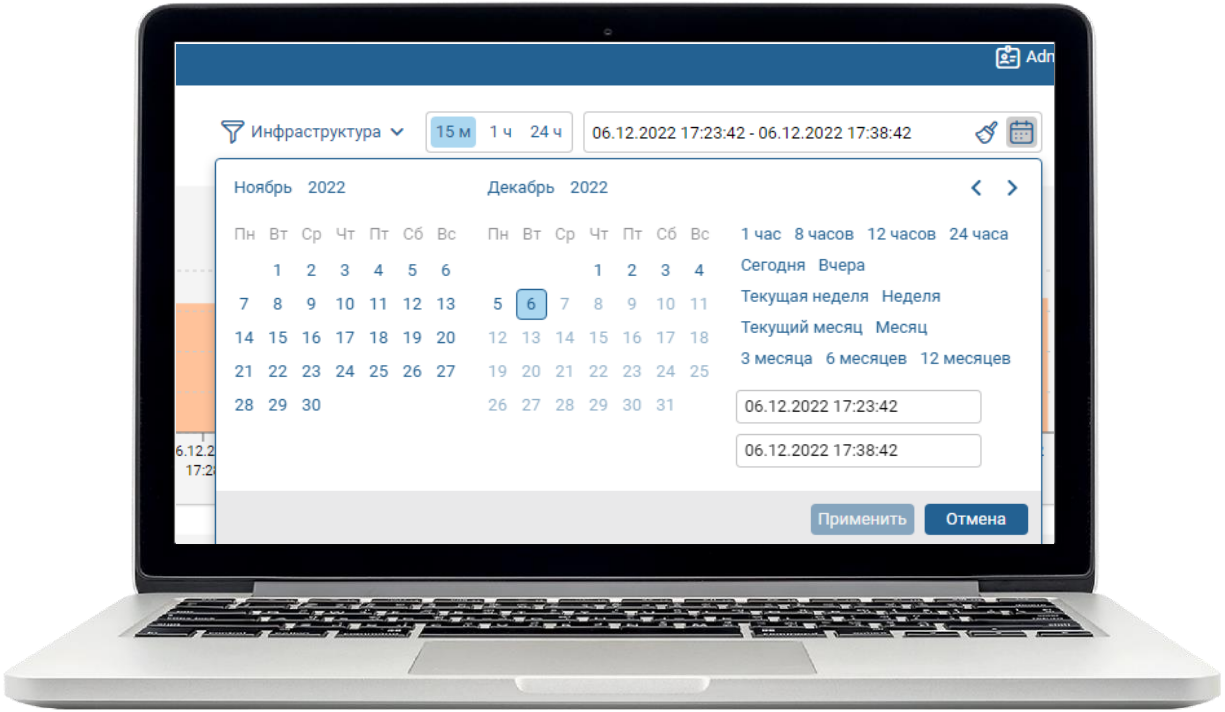


Настройка размеров отображаемых областей



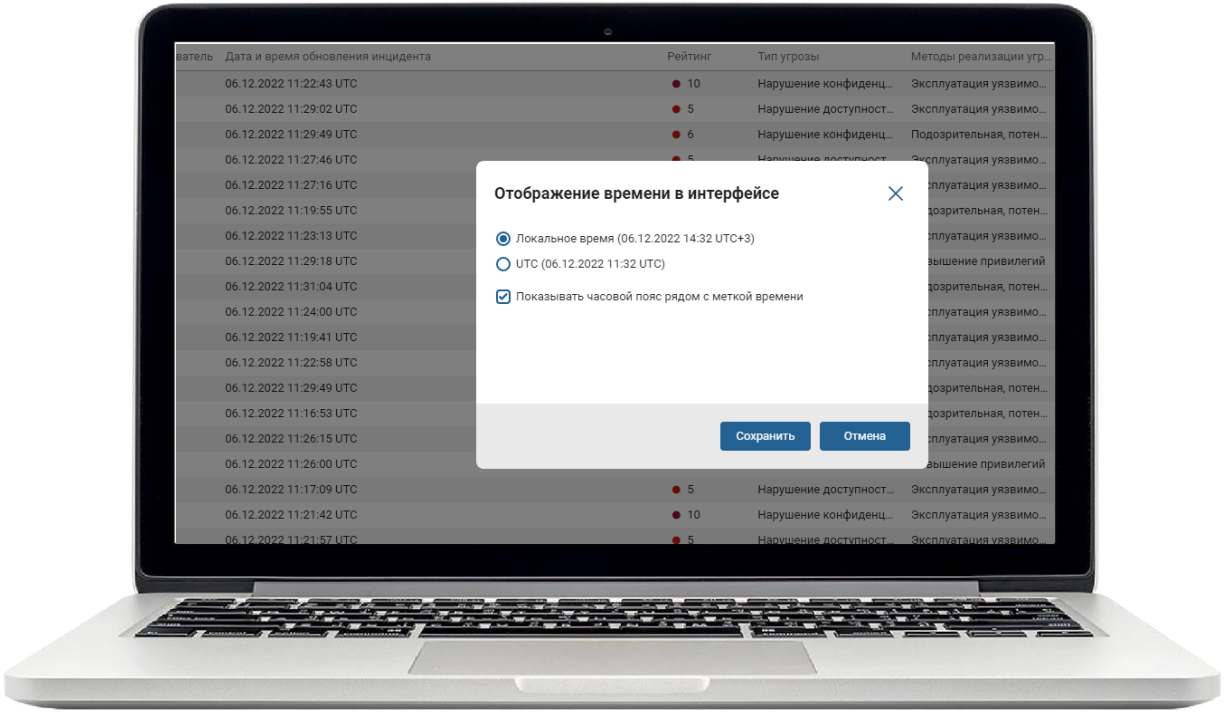
- Динамическая подстройка размеров отображаемых областей в зависимости от размера окна.
- Ручная настройка размеров фреймов

Задание глобального фильтра отображения данных



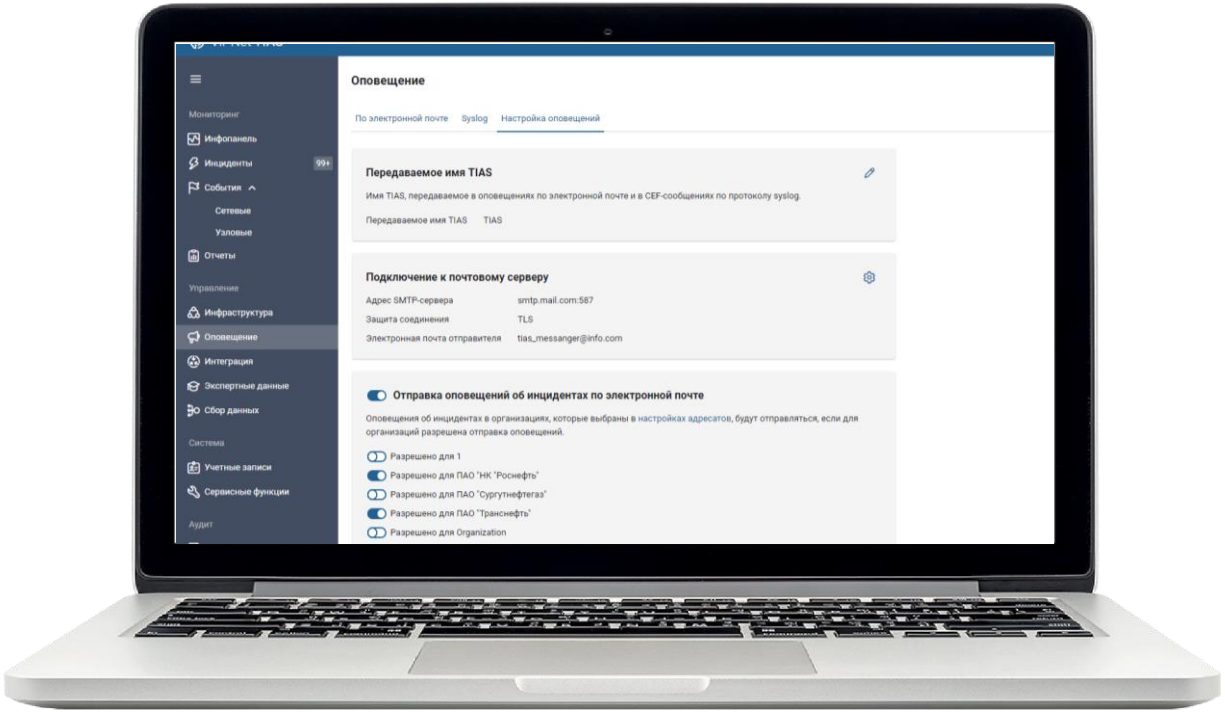
Задавайте время отображения в глобальном фильтре в один клик

Синхронизация и отображение времени



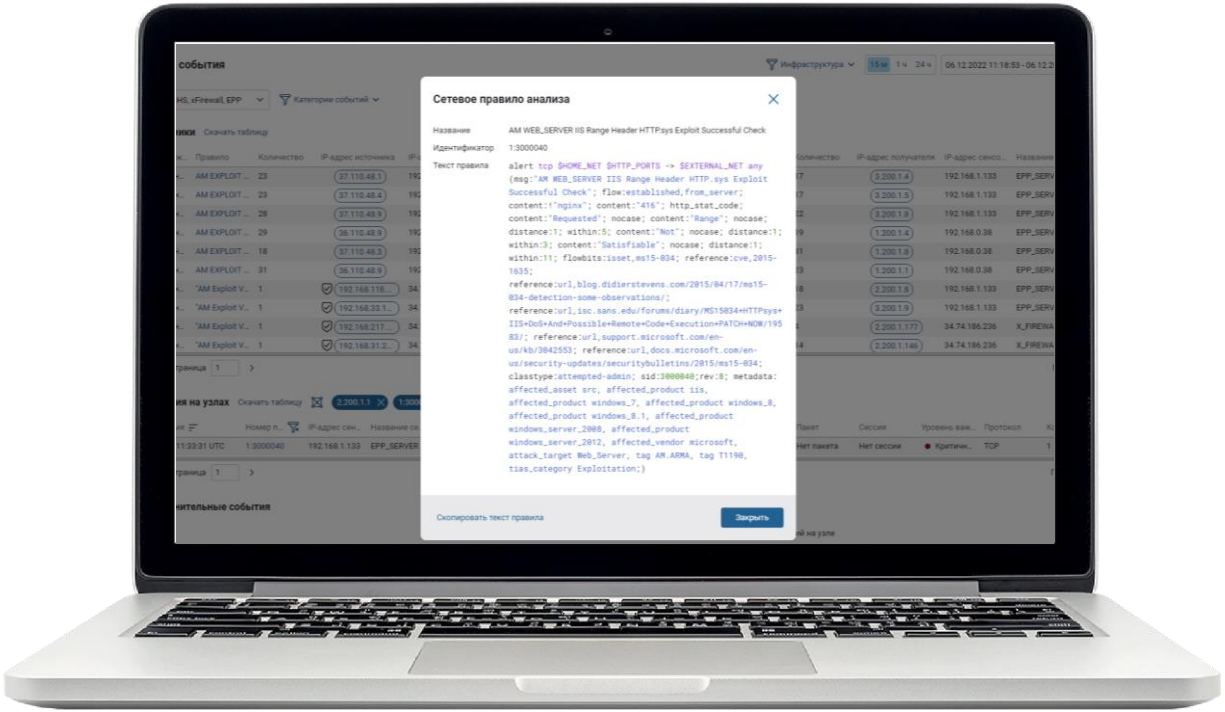
- Отображение в интерфейсе локального времени или времени в формате UTC;
- Синхронизация времени с IDS MC

Настройка оповещений



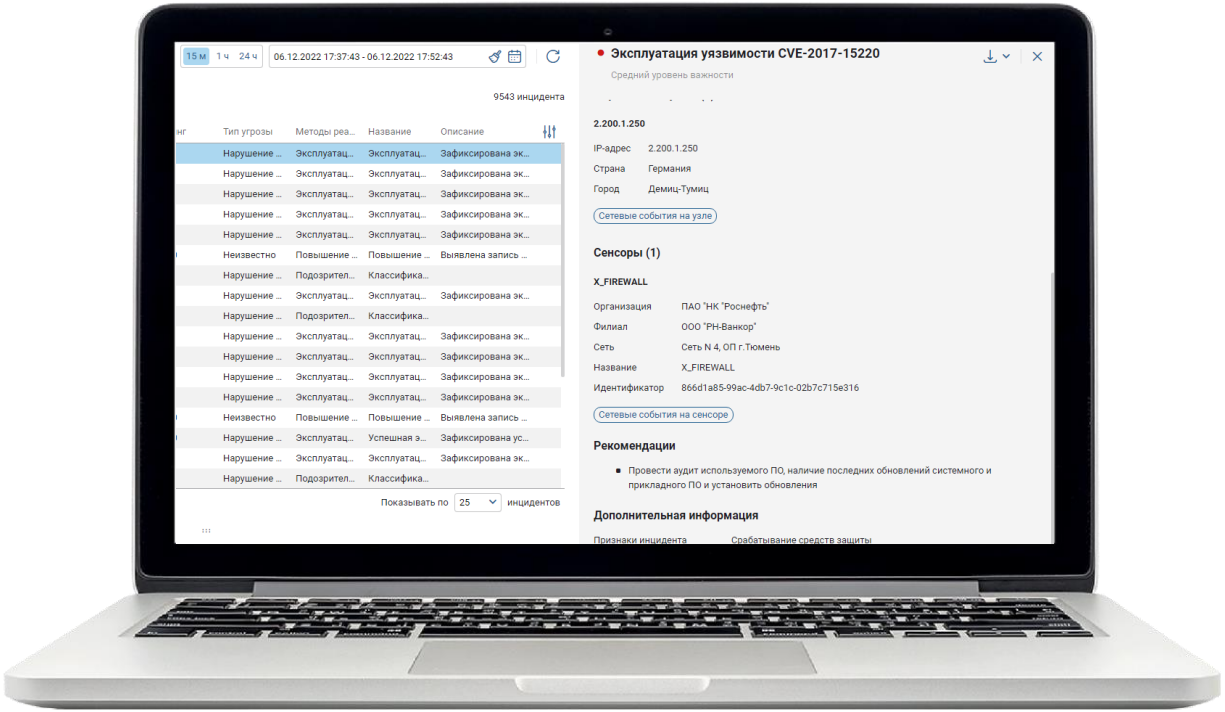
Настройка имени TIAS, передаваемого во внешние системы

Разметка правила



Отображение текста правила с цветовой разметкой

Отображение информации об инфраструктуре в карточке инцидента



- Отображение информации о принадлежности пораженных активов инфраструктуре в карточке инцидента;
- Передача всех параметров инцидента по syslog

Улучшения в IDS MC и IDS NS

ViPNet TIAS IDS MC

infotecs

Основные улучшения и новые возможности

Централизованное обновление пользовательских БРП
загрузка с IDS NS и отправка на другие сенсоры пользовательской базы решающих правил

Подключение работающего TIAS к IDS MC
передача с TIAS в IDS MC информации об инфраструктуре и подключенных устройствах

Обмен информацией об инфраструктуре между IDS MC
Инфраструктура, заведенная в IDS MC сервис-провайдера передается в IDS MC заказчика

ViPNet IDS NS

Исполнения IDS NS:

ПАК:

- ПАК ViPNet IDS NS100 X2;
- ПАК ViPNet IDS NS1000 Q3;
- ПАК ViPNet IDS NS2000 Q4;
- ПАК ViPNet IDS NS10000 Q1;

ПО:

- ViPNet IDS NS VA 100;
- ViPNet IDS NS VA 500;
- ViPNet IDS NS VA 1000;
- ViPNet IDS NS VA 2000;
- ViPNet IDS NS VA 5000;

Поддержка записи сессий на низкопроизводительных платформах

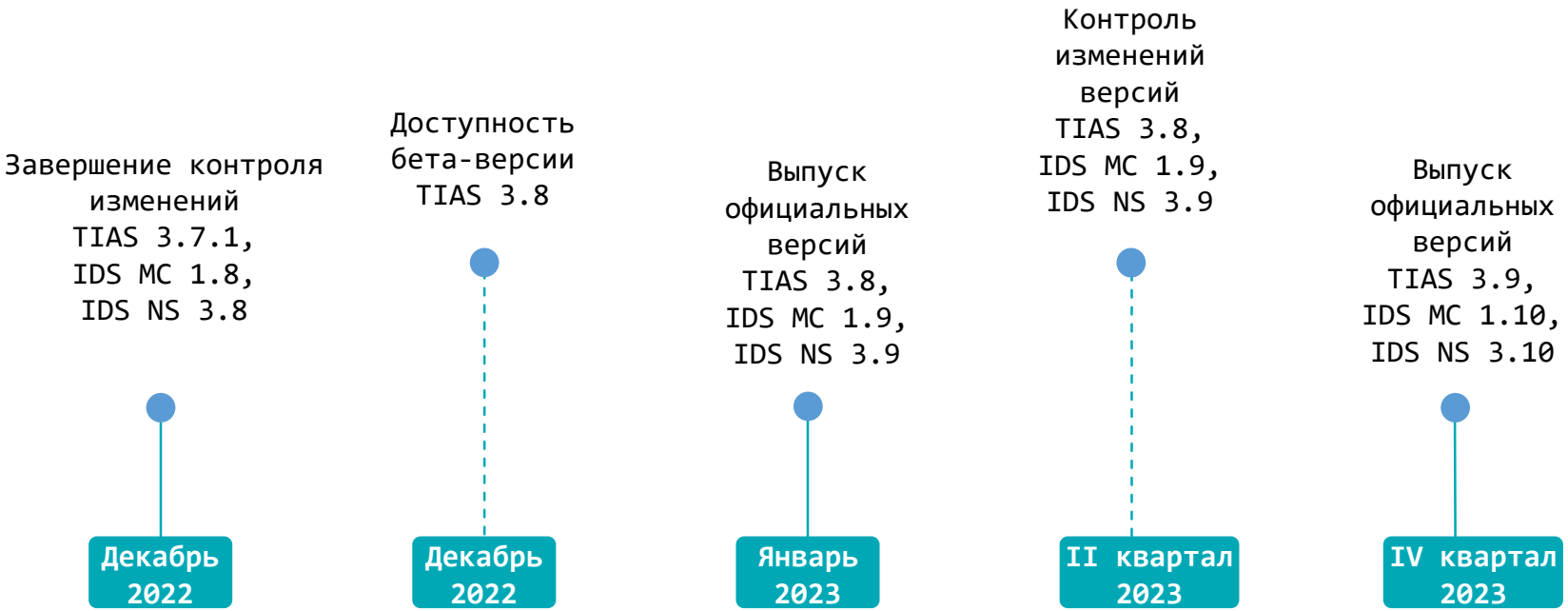
- регулирование времени записи сессии
- запись сессии с определенного IP

Математическая модель анализа Netflow
новый эвристический способ анализа аномалий в сетевом трафике

Выгрузка пользовательских БРП
возможность выгрузки пользовательских БРП для передачи в TIAS и IDS MC

Планы развития

Таймлайн выпуска версий продуктов



Планы развития на 2023 год

Новые возможности и улучшения

Ретроспективный анализ событий в TIAS
возможность поиска инцидентов в событиях, сохраненных в базе TIAS

Интеграция с ViPNet Prime

IDS MC и TIAS

Создание карточки инцидента вручную
Возможность самостоятельно заводить инциденты на основании событий в TIAS

Улучшение работы моделей TIAS и IDS NC

- новые алгоритмы работы модели TIAS;
- расширенный анализ Netflow в IDS NS

Спасибо за внимание!

Светлана Старовойт

Руководитель направления развития продуктов

e-mail: starovoytsg@infotecs.ru

Подписывайтесь на наши соцсети

vk.com/infotecs_news

t.me/infotecs_official

rutube.ru/channel/24686363