

Выявляем больше, управляем лучше!

Искусственный интеллект для выявления киберугроз и новые сценарии работы

Светлана Старовойт
Руководитель продуктового направления





Напомню о решении и некоторых важных и полезных функциях в продуктах



Расскажу об основных изменениях в новых версиях



Покажу результаты работы нейросети по выявлению аномальных объемов трафика в IDS NS



Покажу новый сценарий работы в TIAS

Система обнаружения компьютерных атак (вторжений) ViPNet IDS 3



ViPNet IDS NS

Обязательный
компонент



ViPNet TIAS

Не обязательные компоненты



ViPNet IDS MC



Система обнаружения вторжений
уровня сети 4 класс

Требования доверия безопасности
4 уровня



Система обнаружения компьютерных
атак класс В

Реестры

Единый реестр российских программ:



РЕЕСТР
ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

- **ViPNet IDS NS**
(* Программное обеспечение относится к сфере искусственного интеллекта)
- **ViPNet TIAS**
(* Программное обеспечение относится к сфере искусственного интеллекта)
- **ViPNet IDS MC**

03.14 Средства обнаружения и/или предотвращения вторжений (атак)

03.02 Средства управления событиями информационной безопасности

03.15 Средства обнаружения угроз и расследования сетевых инцидентов



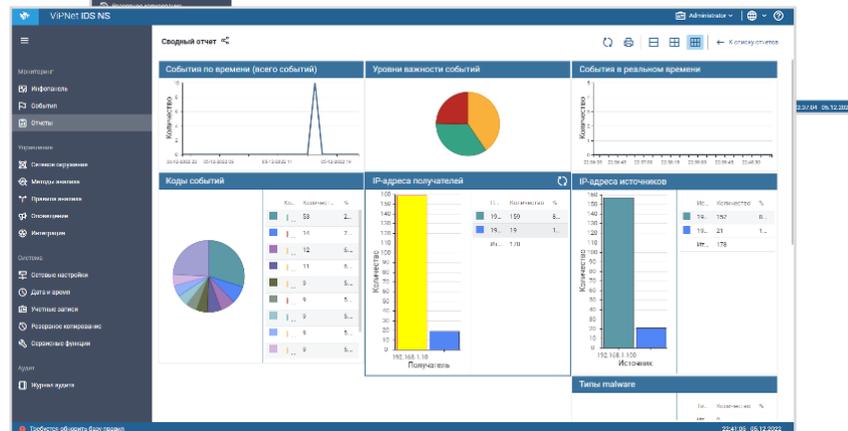
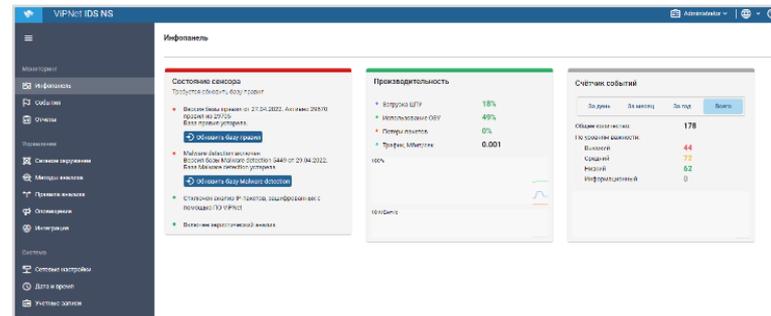
Реестр российской радиоэлектронной продукции:

- ПAK ViPNet IDS NS
- ПAK ViPNet TIAS

Подтверждение производства
продукции на территории РФ

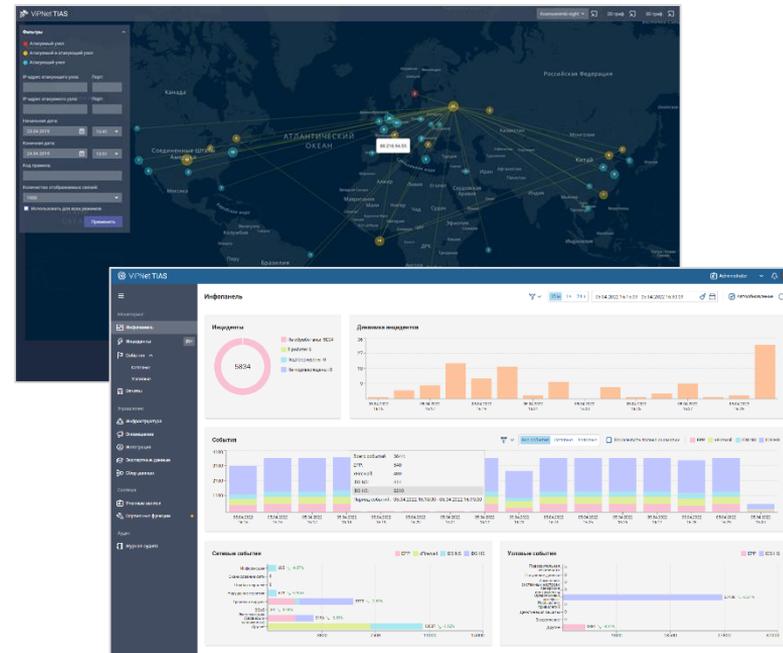
VIPNet IDS NS

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



VIPNet TIAS

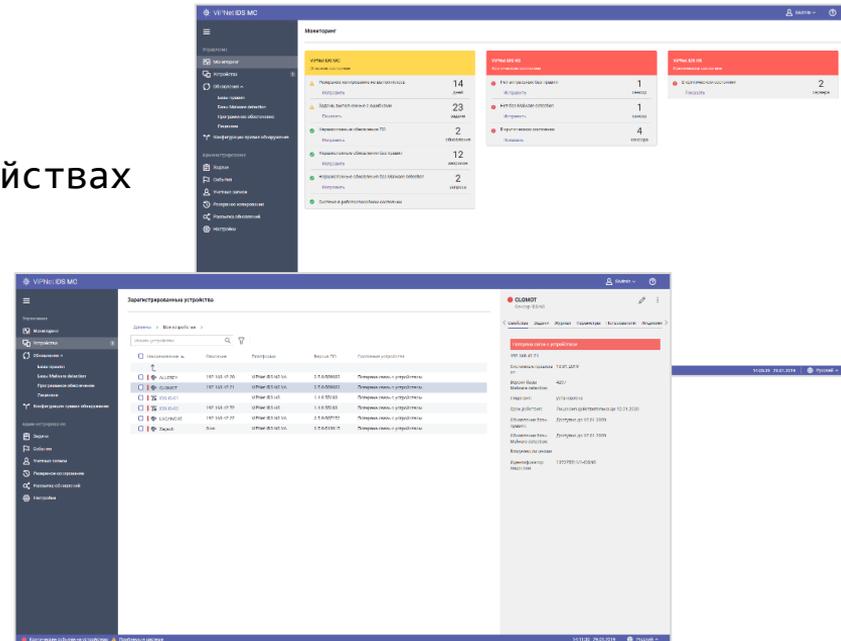
- сбор и анализ событий ИБ, поступающих от источников
- автоматическое выявление подозрений на инциденты ИБ
- предоставление рекомендаций по реагированию на инцидент
- формирование отчетов по событиям и инцидентам



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

VIPNet IDS MC

- ввод в эксплуатацию сенсоров IDS
- управление инфраструктурой ViPNet IDS 3
- 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>



Основные улучшения и новые возможности

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

Визуализация сетевых потоков

Отображение информации о сетевых потоках в графическом и табличном представлениях



Основные улучшения и новые возможности

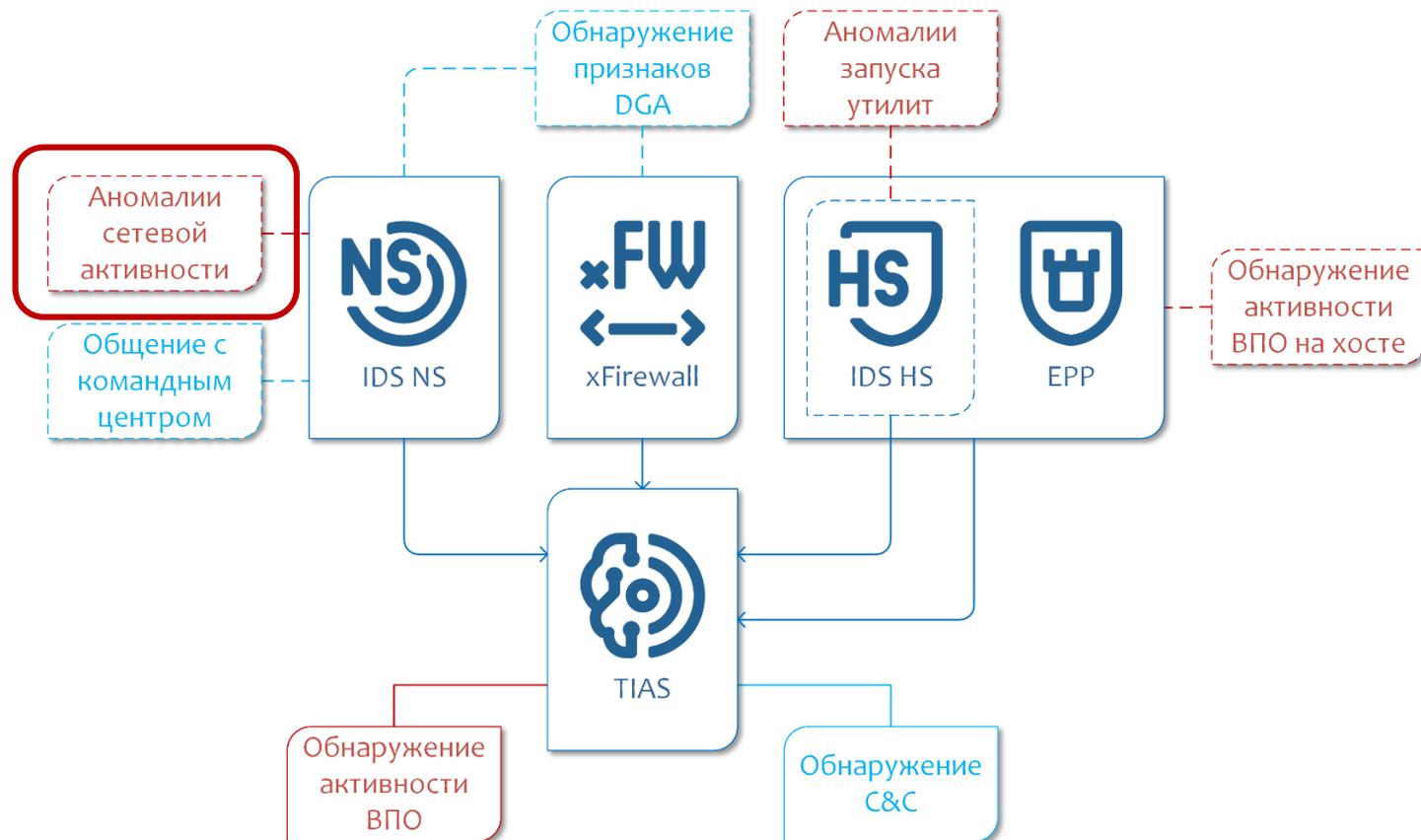
Пользовательские метаправила

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

Модели машинного обучения



Мастер-класс. Переходим к практике

техно infotecs 2024 ФЕСТ

Светлана Старойт
Руководитель продуктового направления

Подписывайтесь на наши соцсети

