

IDS vs NTA.

Чей кунг-фу сильнее?

Светлана Старовойт

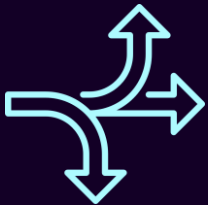
БОЛЬШОЙ
МОСКОВСКИЙ
ТЕХНО  infotecs
ФЕСТИВАЛЬ

Методы анализа сетевого трафика



Захват и анализ сетевых пакетов

- Анализ служебных полей заголовков протоколов
- Анализ содержимого пакетов



Потоковый анализ

- Статистические данные о сетевом трафике
- Поведенческий анализ

Вспомним как всё начиналось



Так в чём разница?

IDS/ IPS

1. Анализ отдельных сетевых пакетов
2. Правила анализа и сигнатуры
3. Ограниченный набор протоколов сетевого уровня
4. Отдельное событие о срабатывании правила
5. Запись отдельного сетевого пакета

NTA

Анализ сетевых взаимодействий и сетевой телеметрии

Поведенческий анализ с акцентом на ML

Анализ как сетевых так и прикладных протоколов

Метаданные о сетевых потоках и сессиях

Запись всего трафика или сессии

IDS

IDS ориентированы на определение конкретных событий, но не предоставляют полного контекста относительно происходящего в сети

NTA

собирают и анализируют данные обо всей сетевой активности, предоставляя полную картину состояния сети



А нужно
ли
выбирать?

Система обнаружения вторжений ViPNet IDS NS

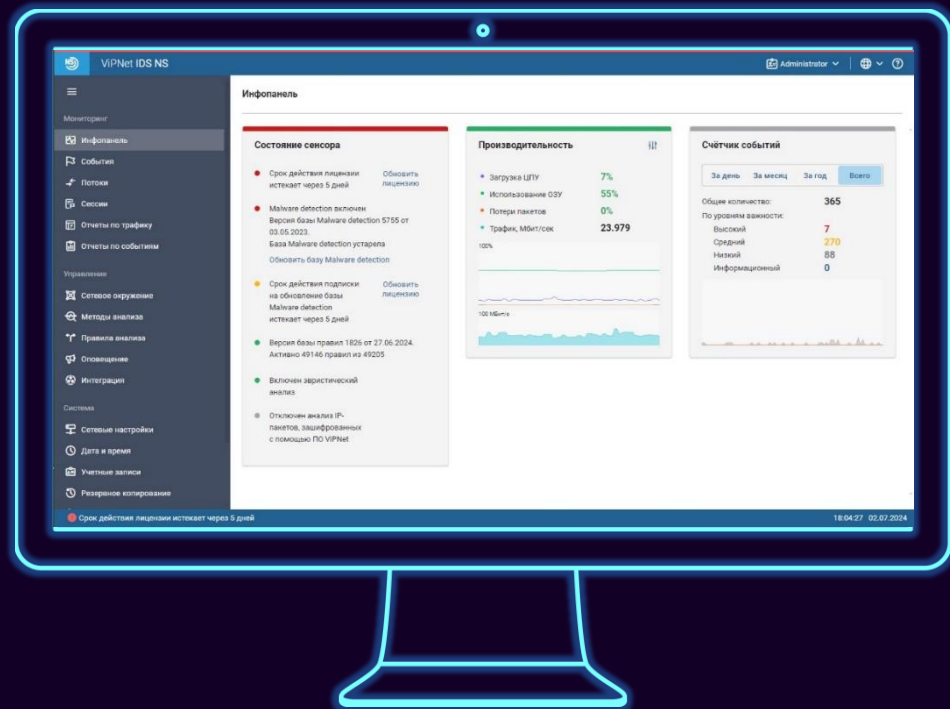


VIPNet IDS NS

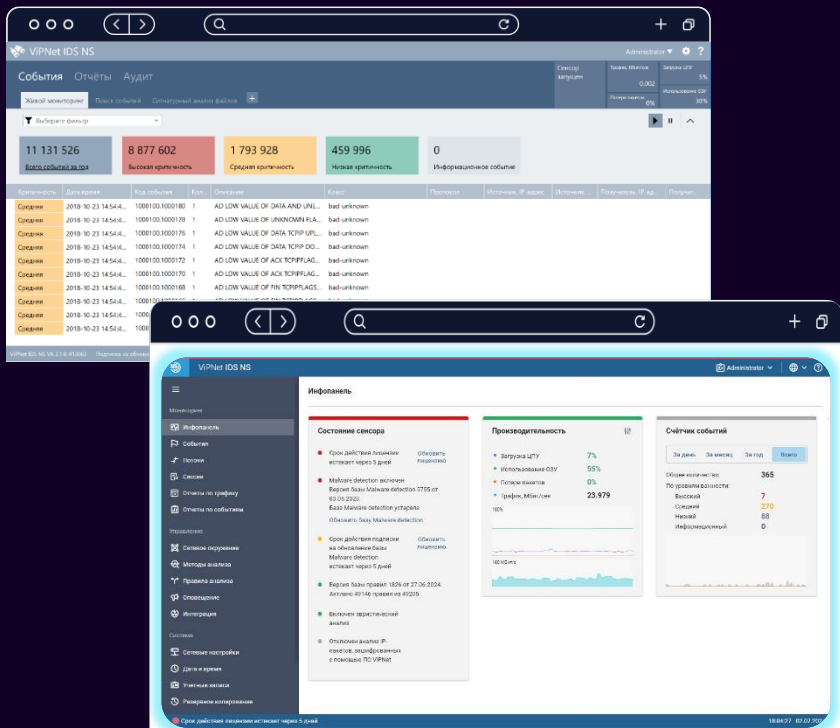
анализировать сетевой трафик

хранить события, исходные
сетевые пакеты;

передавать события
во внешние системы;



Методы анализа



Сигнатурные методы анализа:

- Анализ трафика с помощью баз решающих правил (SNORT)
- Анализ трафика на наличие вредоносных файлов (Malware detection)

Эвристический анализ:

- отслеживание отклонений параметров сетевого трафика от эталонной модели.
- анализ служебных полей заголовков протоколов на наличие аномалий (RPC, HTTP, SMTP, FTP, SSH, MODBUS, GTP, SIP, Telnet, TCP, SSL, IMAP, DNS, DNP3, MODBUS, POP)
- отслеживание ARP-spoofing

VIPNet IDS с модулем NTA

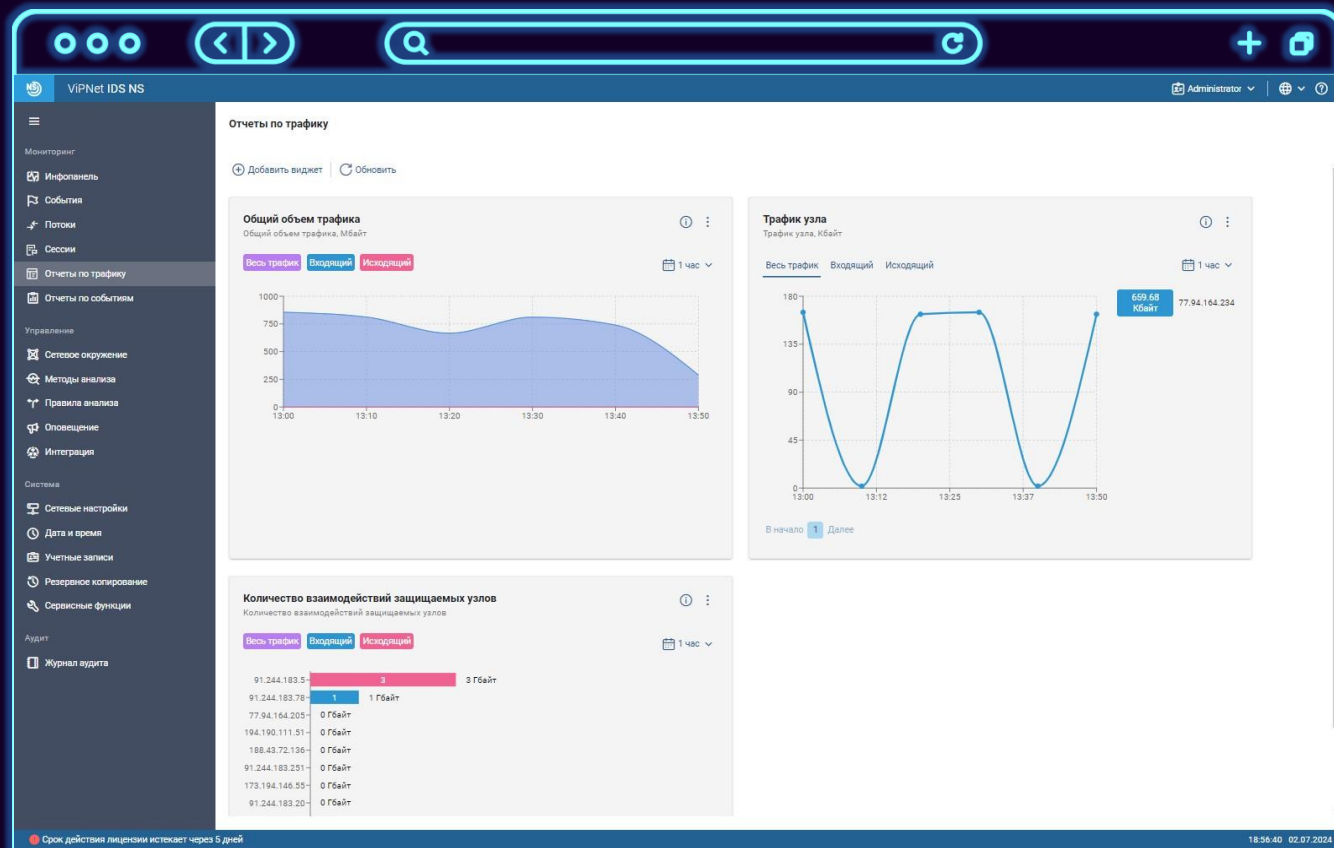
анализировать сетевой трафик
с помощью моделей машинного
обучения;

хранить статистику о сетевых
потоках и сессиях;

отображать информацию о
сетевых потоках и сессиях;

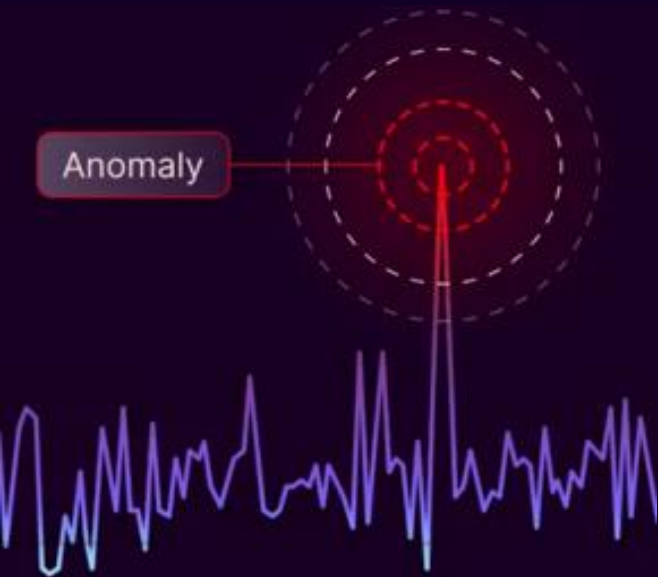


NTA Дайджесты



Модели машинного обучения

Выявление аномального увеличения трафика



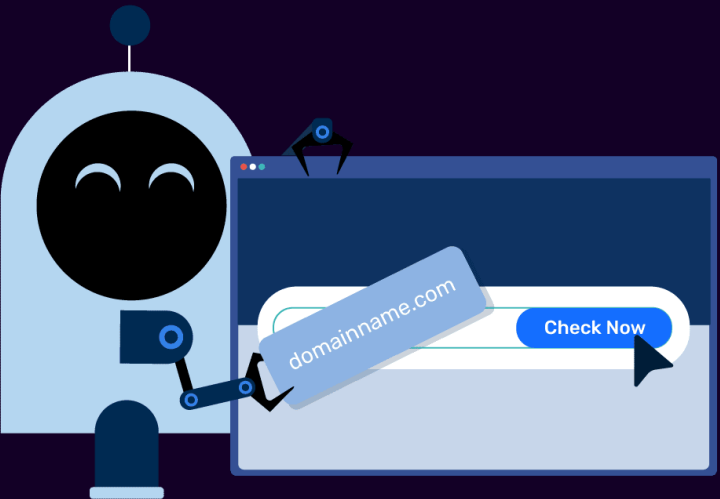
- Нейронная сеть
- Работает на статистике о потоках
- Обучается ежедневно на данных за две недели

Обнаружение вредоносного ПО в TLS-трафике



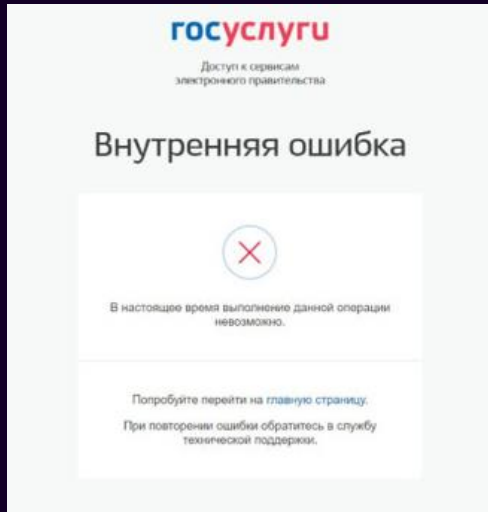
- Алгоритм RandomForest
- Работает на размерах записей в байтах в потоке TLS
- Обучается на размеченном наборе данных, где есть примеры как нормального трафика, так и трафика ВПО

Обнаружение сгенерированных доменных имен



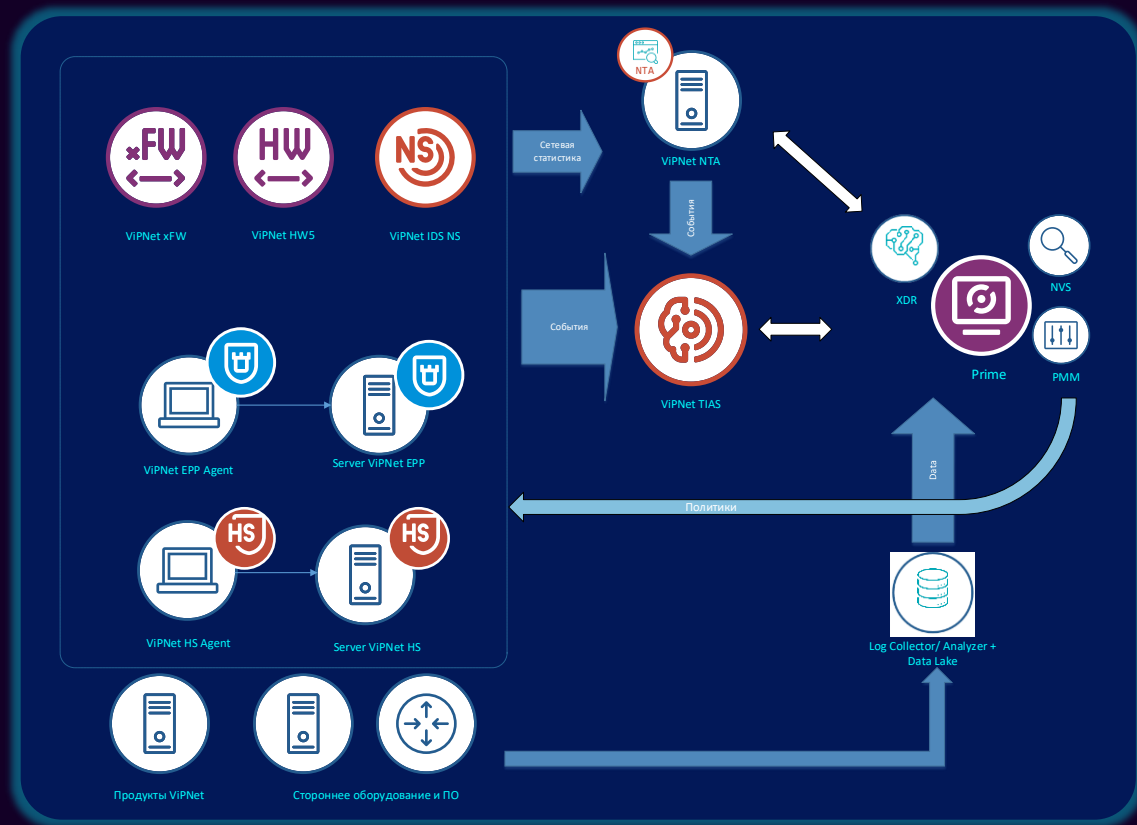
- Нейронная сеть
- Работает на данных о потоках
- Обучается на размеченном наборе данных + справочник доверенных доменных имён
- 46 миллионов доменов в сутки

Обнаружение низкоинтенсивных DoS-атак



- Нейронная сеть
- Работает на данных о количестве переданных пакетов и объеме данных (не менее 64 netflow)
- Вердикт наличия Low DoS и класс:
 - RUDY
 - Slowloris

NTA в решении XDR



- Обогащение данными об активах
- Реагирование на инциденты
- Расширенная корреляция

ТЕХНО infotecs Фест

Подписывайтесь
на наши соцсети,
там много интересного



ПЕРСПЕКТИВНЫЙ
МОНИТОРИНГ

