IDS vs NTA.

Чей кунг-фу сильнее?

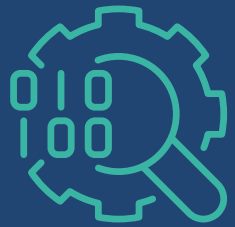
Светлана Старовойт

Руководитель продуктового направления

инфотекс ТЕХНОФЕСТ

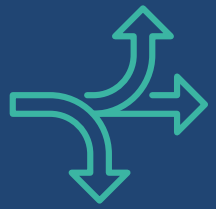
Синий поток

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

1998

IDS

Перехват сетевых пакетов и проверка на заданные критерии

2010

NextGen IPS/IDS

- DPI
- SSL Decryption
- IoC
- SendBox
- Эвристические методы анализа

2017

Gartner Top Technologies for Security

NTA – это подход, основанный на анализе сетевых потоков с акцентом на ML

2022

Network Detection and Response

NDR включают сценарии автоматического реагирования, такие как ограничение доступа к узлу или блокирование трафика

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

Выводы

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 общую картину состояния сети

А нужно ли выбирать?

Система обнаружения вторжений ViPNet IDS NS

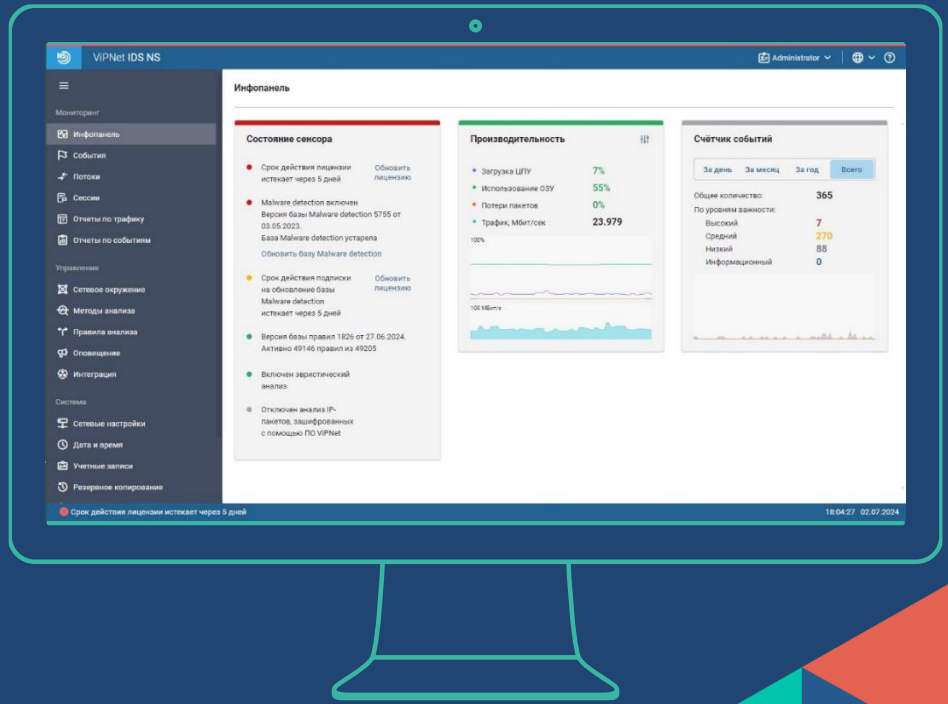
инфотекс

ViPNet IDS NS

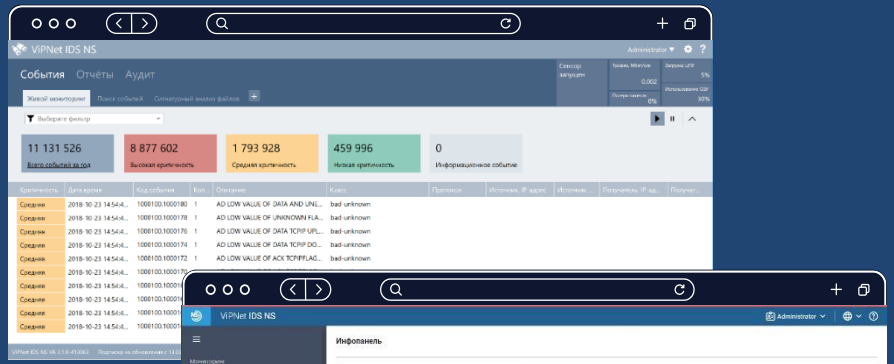
анализировать сетевой трафик

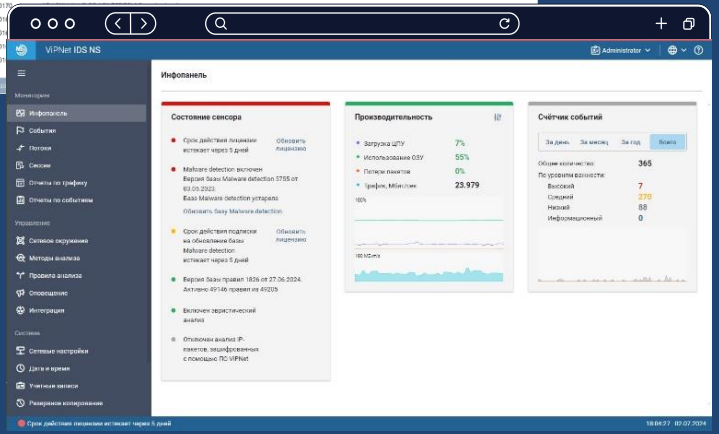
хранить события, исходные сетевые пакеты

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:

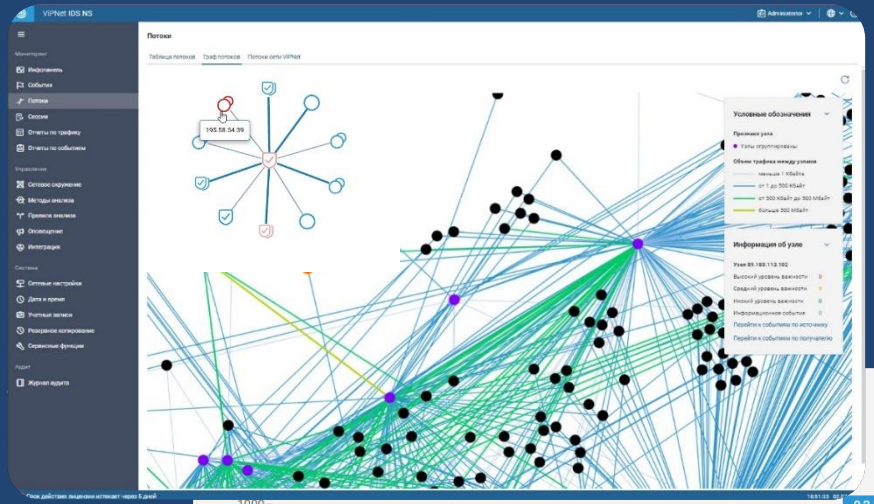
- отслеживание отклонений параметров сетевого трафика от эталонной модели
- анализ служебных полей заголовков протоколов на наличие аномалий (RPC, HTTP, SMTP, FTP, SSH, MODBUS, GTP, SIP, Telnet, TCP, SSL, IMAP, DNS, DNP3, MODBUS, POP)
- отслеживание ARP-spoofing

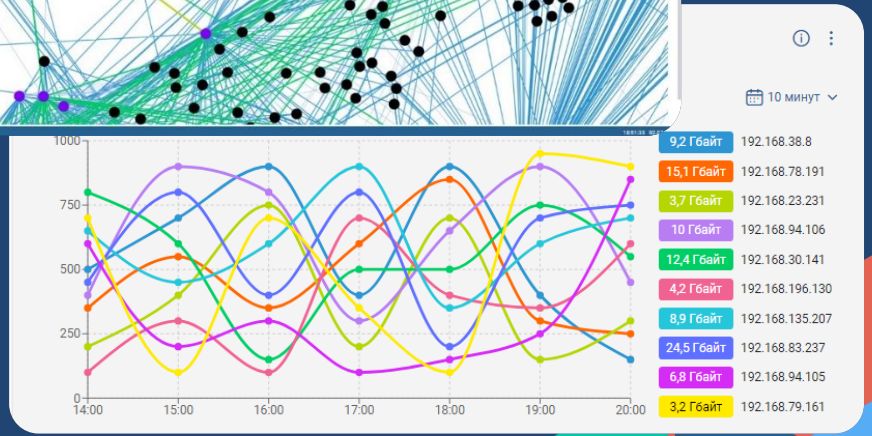
ViPNet IDS с модулем NTA

анализировать сетевой трафик с помощью моделей машинного обучения

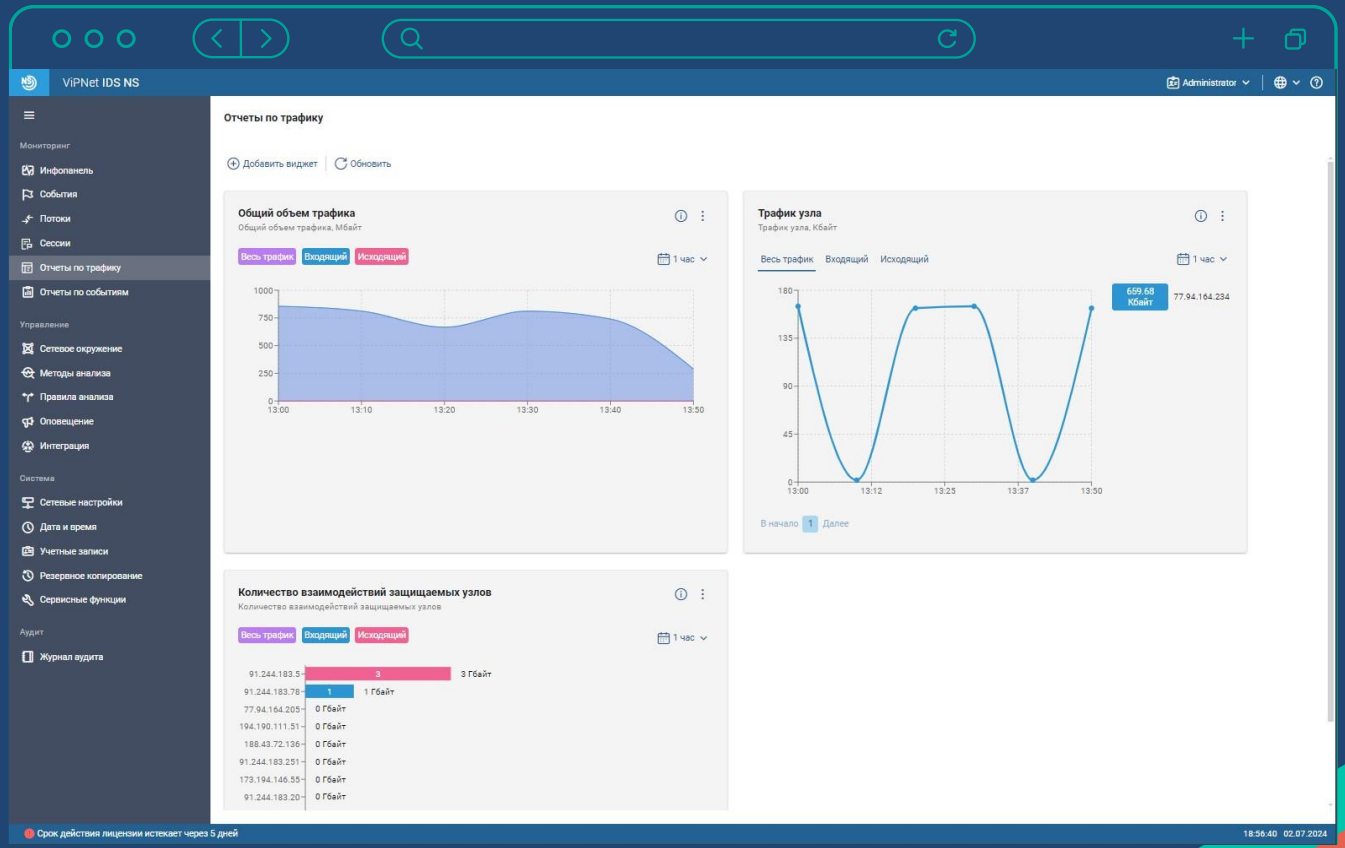
хранить статистику о сетевых потоках и сессиях

отображать информацию о сетевых потоках и сессиях



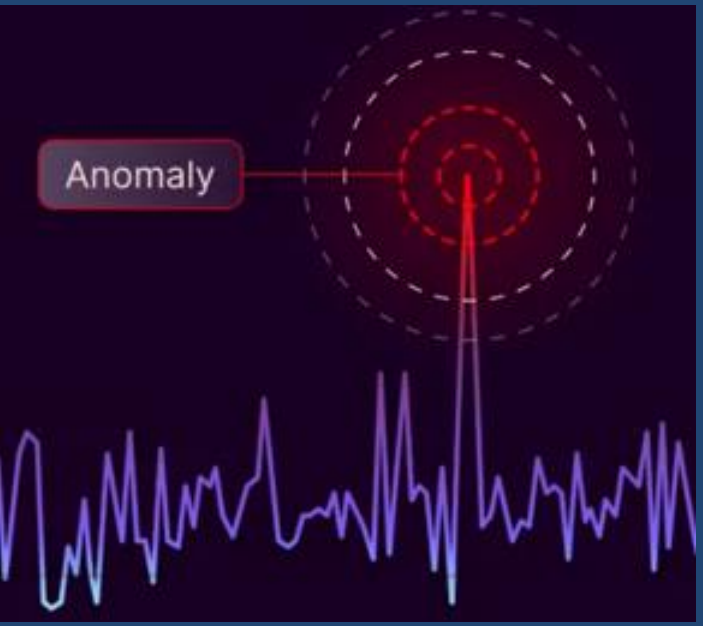


NTA Дайджесты



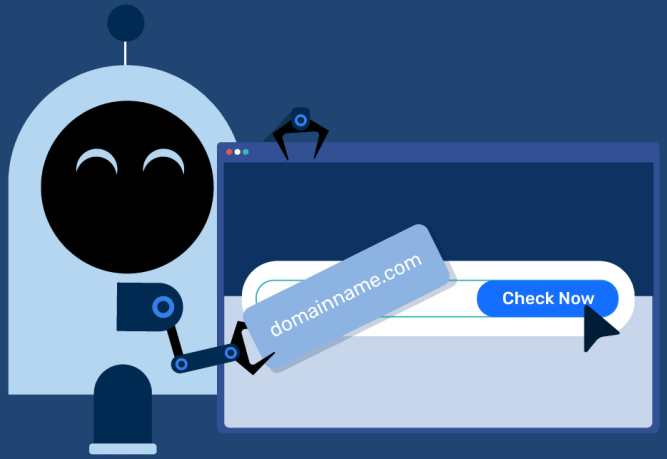
Модели машинного обучения

Выявление аномального увеличения трафика



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

Обнаружение сгенерированных доменных имен



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

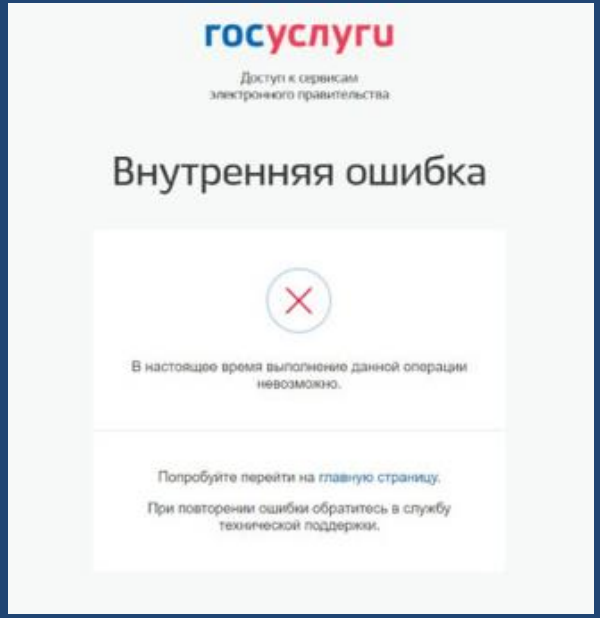
Обнаружение фишинговых доменных имен

- Анализ DNS-запросов
- Обучение на списке доверенных и фишинговых имён
- Исключения на основании пользовательского белого списка
- Определение процента схожести

Обнаружение вредоносного ПО в TLS-трафике

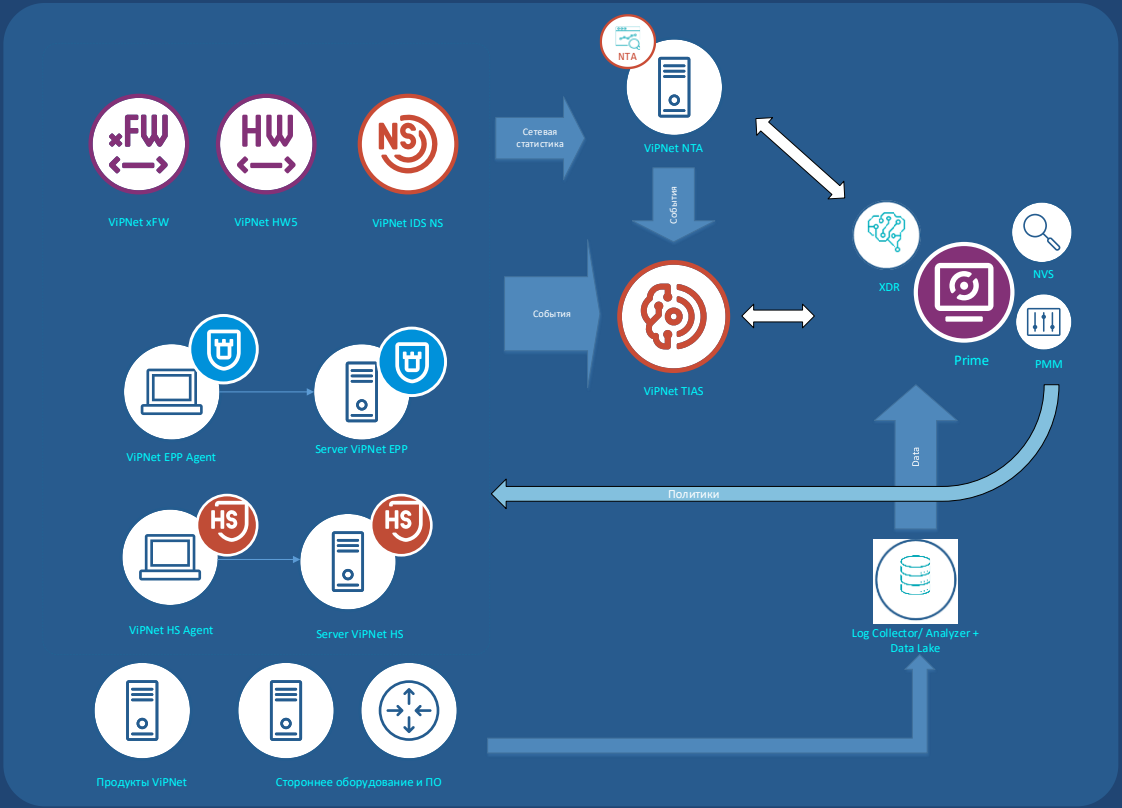
- База известных хэш-сумм JA3 входит в состав базы правил
- Метод поддерживает протоколы следующих версий:
  - TLS – 1.0-1.3.
  - SSL – 3.0.

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

САНКТ ПЕТЕРБУРГ

инфотекс

ТЕХНОФЕСТ

Академия инфотекс · Учебный центр инфотекс · AMPIRE · TELEOFIS · КОМФОРТЕЛ оператор связи бизнес-класса · РУТОКЕН компания ИНФОТЕКС · TS Solution · AXOFT

Подписывайтесь на наши соцсети