

Ampire 360°



ПЕРСПЕКТИВНЫЙ  
МОНИТОРИНГ

# Ampire 360°

ПОЛИГОН КИБЕРБЕЗОПАСНОСТИ



Threat Intelligence

SOC & DFIR

Offensive Security

Киберучения

ИИ и киберзащита

Киберполигон Ampire



14 октября





Применение ИИ  
в системе обнаружения  
компьютерных атак.

Эффективно, безопасно,  
не дорого.

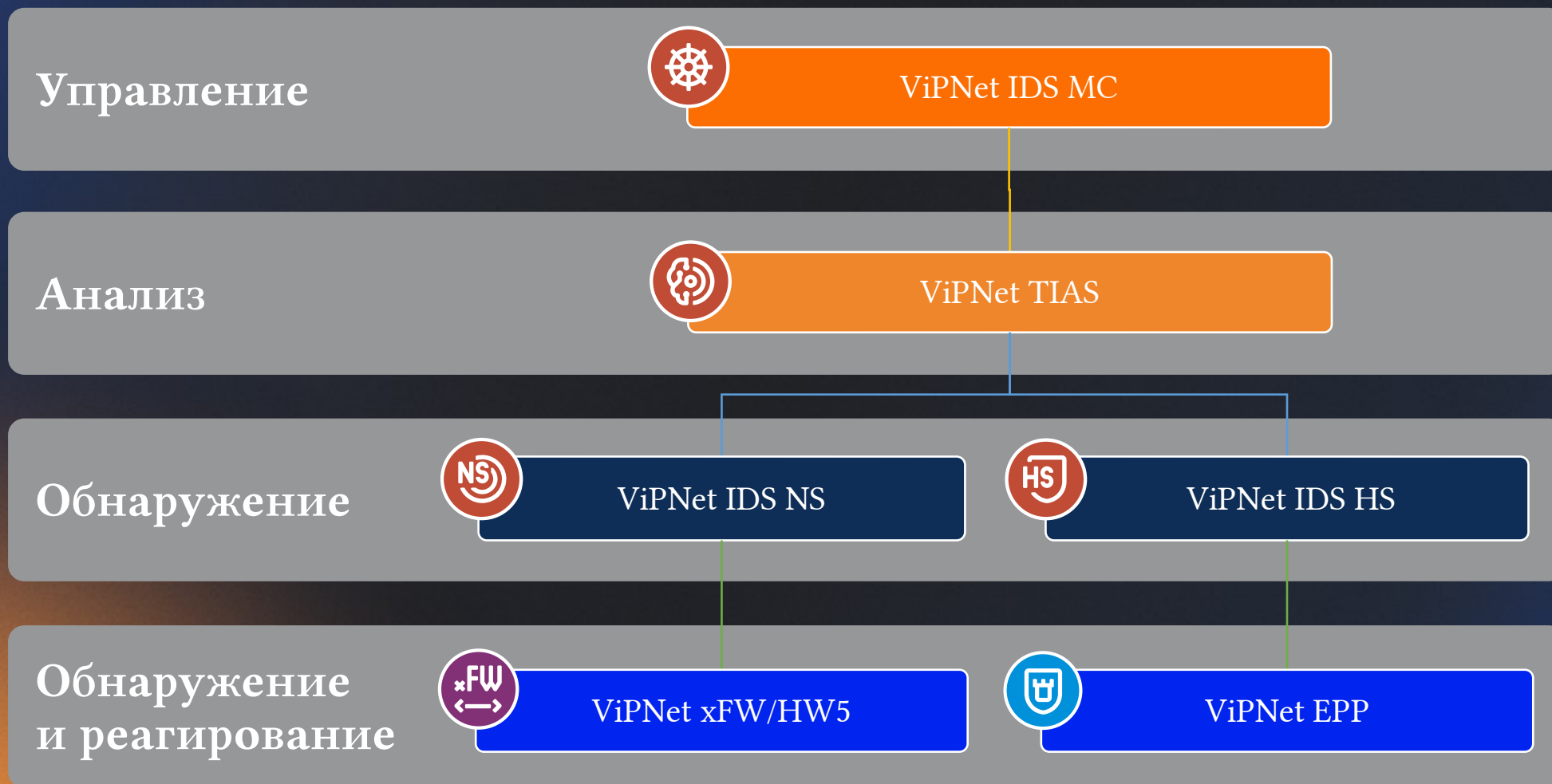
Светлана Старовойт

Руководитель направления

ИнфоТеКС



# Решение ViPNet TDR



# Продукты с ML

Ampire 360°



## Поведение на пользовательских компьютерах



ViPNet EPP

Antimalware

Аномалии PowerShell

SSDEEP

## Анализ событий ИБ



ViPNet TIAS

Retrain

SID-Chain

Поведенческие аномалии

## Анализ сетевого трафика



ViPNet IDS NS

TVA

Anti-Phishing

JA3

C&C TLS

DGA

SSDEEP

● — внедрено

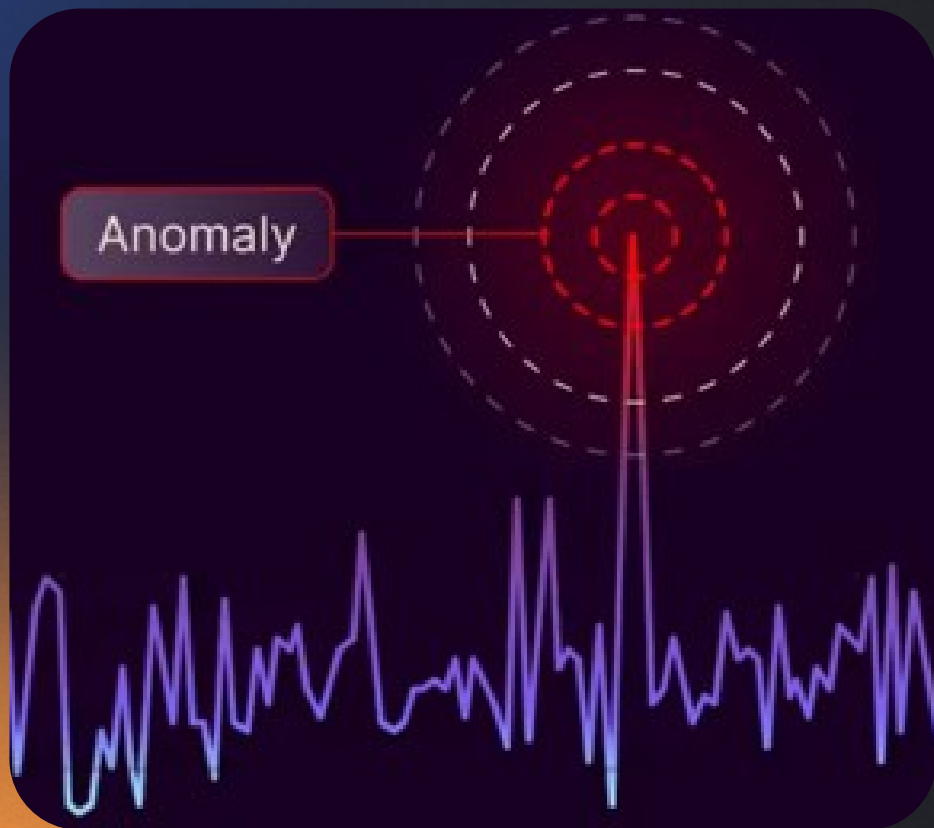
● — готовится к внедрению

● — выводится из продукта

# Анализ сетевого трафика

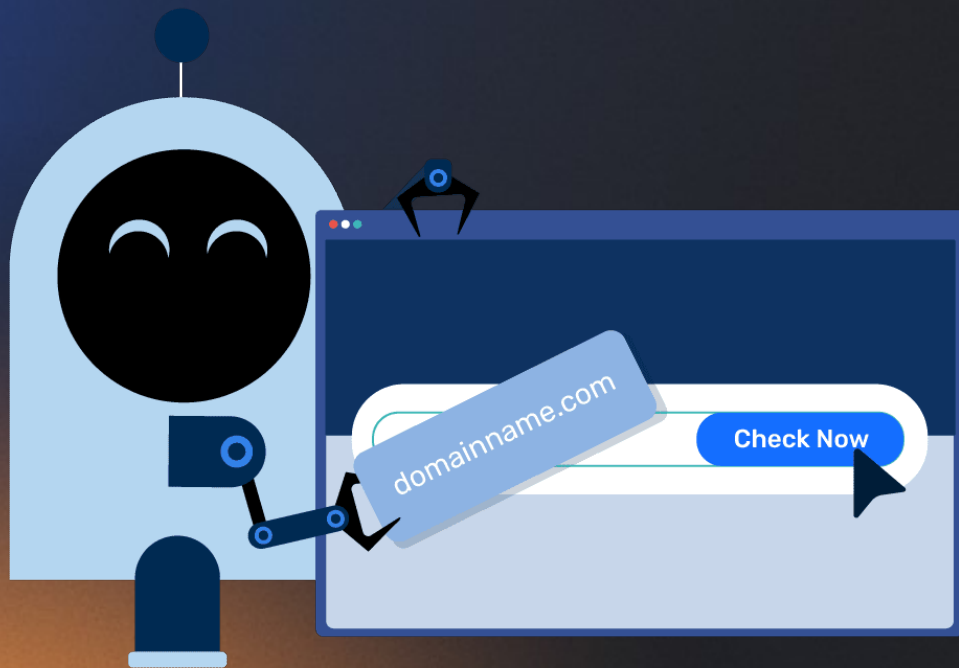


# Выявление аномального увеличения трафика



- Нейронная сеть
- Работает на статистике о потоках к homeNet-адресам
- Анализирует общий объем и размер пакетов
- 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



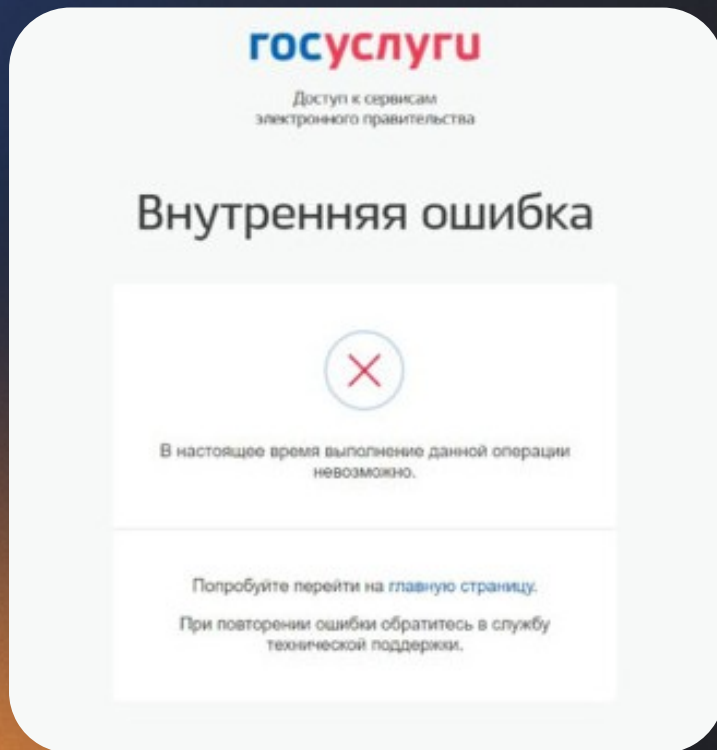
- Анализ DNS-запросов
- Обучение на списке доверенных и фишинговых имён
- Исключения на основании пользовательского белого списка
- Определение процента схожести

# 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.

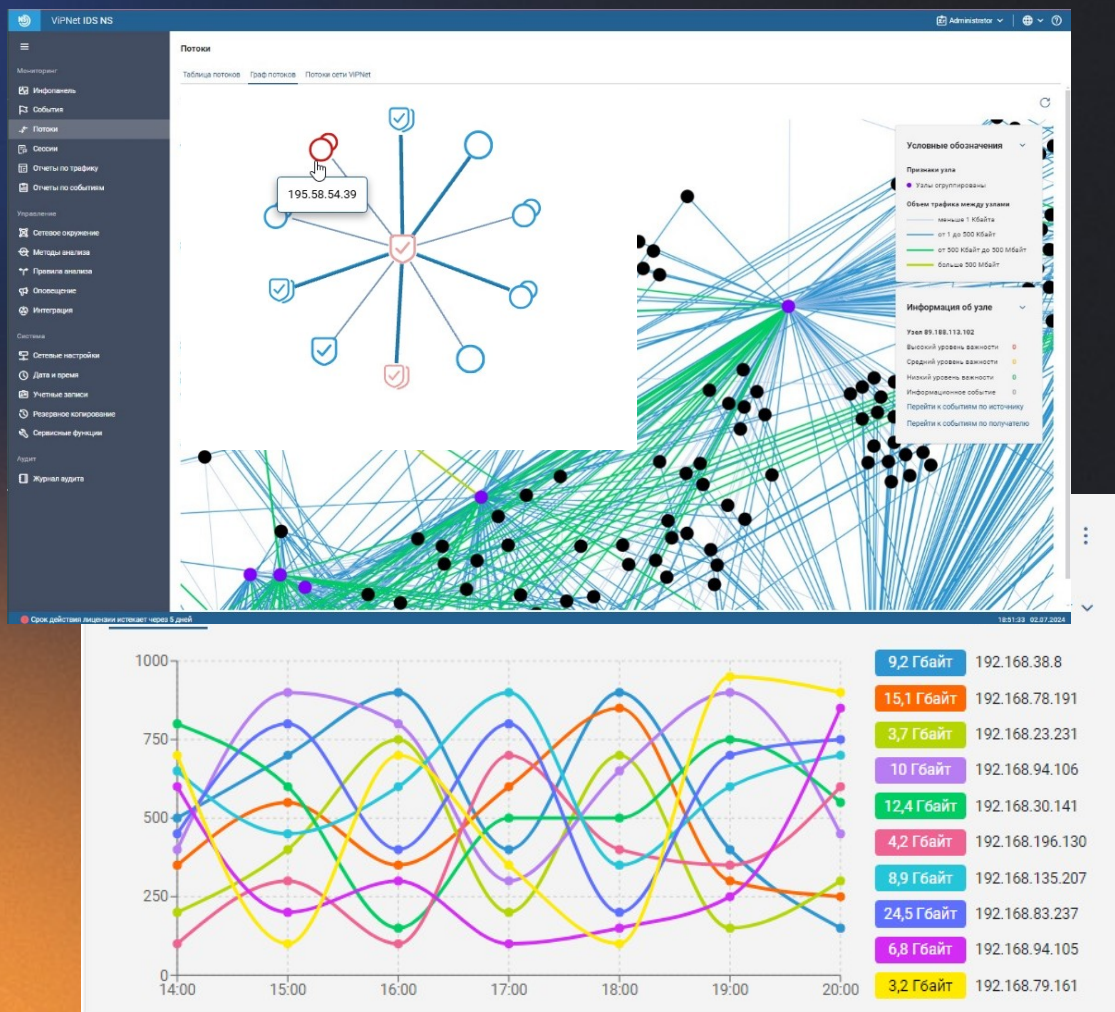
# Обнаружение низкоинтенсивных DoS-атак



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

# Дополнительные бонусы

- Предоставлять пользователю информацию о сетевых потоках и сессиях
- Строить карту сетевых взаимодействий
- Передавать метаданные о сессиях во внешние системы



# Поведенческий анализ на узлах

- Аномальный вход в систему
- Аномальные запуски системных утилит, таких как powershell, rundll32, regsrv32 и т. д.
- Аномалия в создании процесса
- Передавать метаданные о сессиях во внешние системы
- Аномалия в создании задачи планировщику



ViPNet  
EndPoint  
Protection

# Анализ событий



ViPNet TIAS

# ИИ не дорого



100%  
автономно



99%  
безопасно



На ресурсах стандартной  
аппаратной платформы



# Проблемы использования ML





- Атаки на Open Source библиотеки и на данные
- SDL или MLOps
- Передача данных третьим лицам
- Дополнительное регулирование

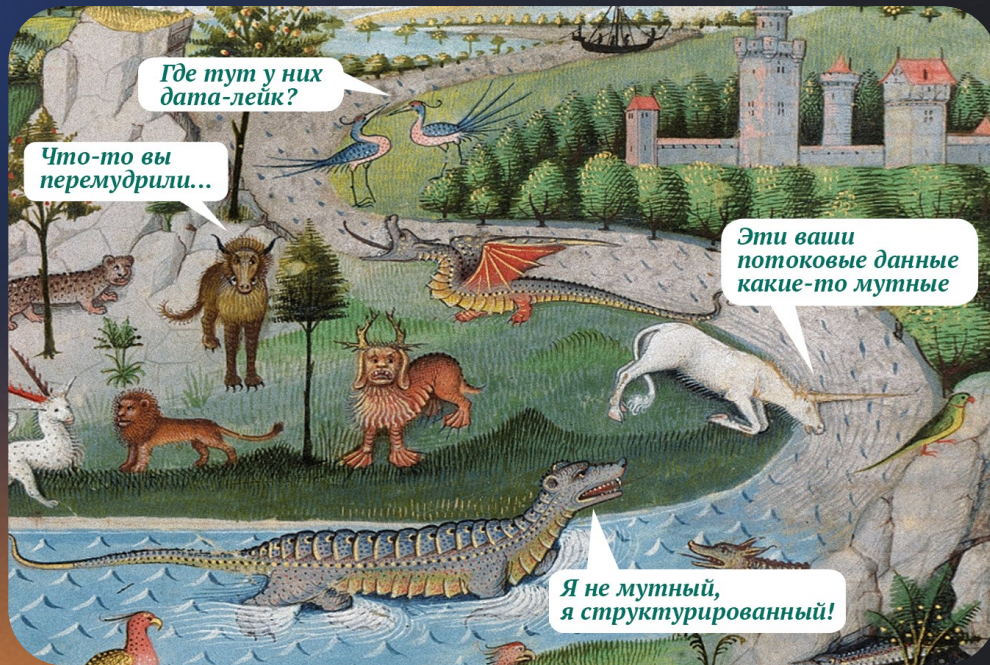
# Доверие к работе модели



- Интерпретируемость результата работы модели
- Дрейф данных
- Доверие при передаче данных



# Данные для обучения и проверки



- Синтетические данные
- Открытые источники
- Данные SOC
- Данные пользователей
- Разметка экспертами или пользователями

# Ресурсоёмкость



Где работает/  
обучается модель?

- на конечном узле
- в ЦОДе
- в облаке

Благодарю за  
внимание!



Ampire 360°