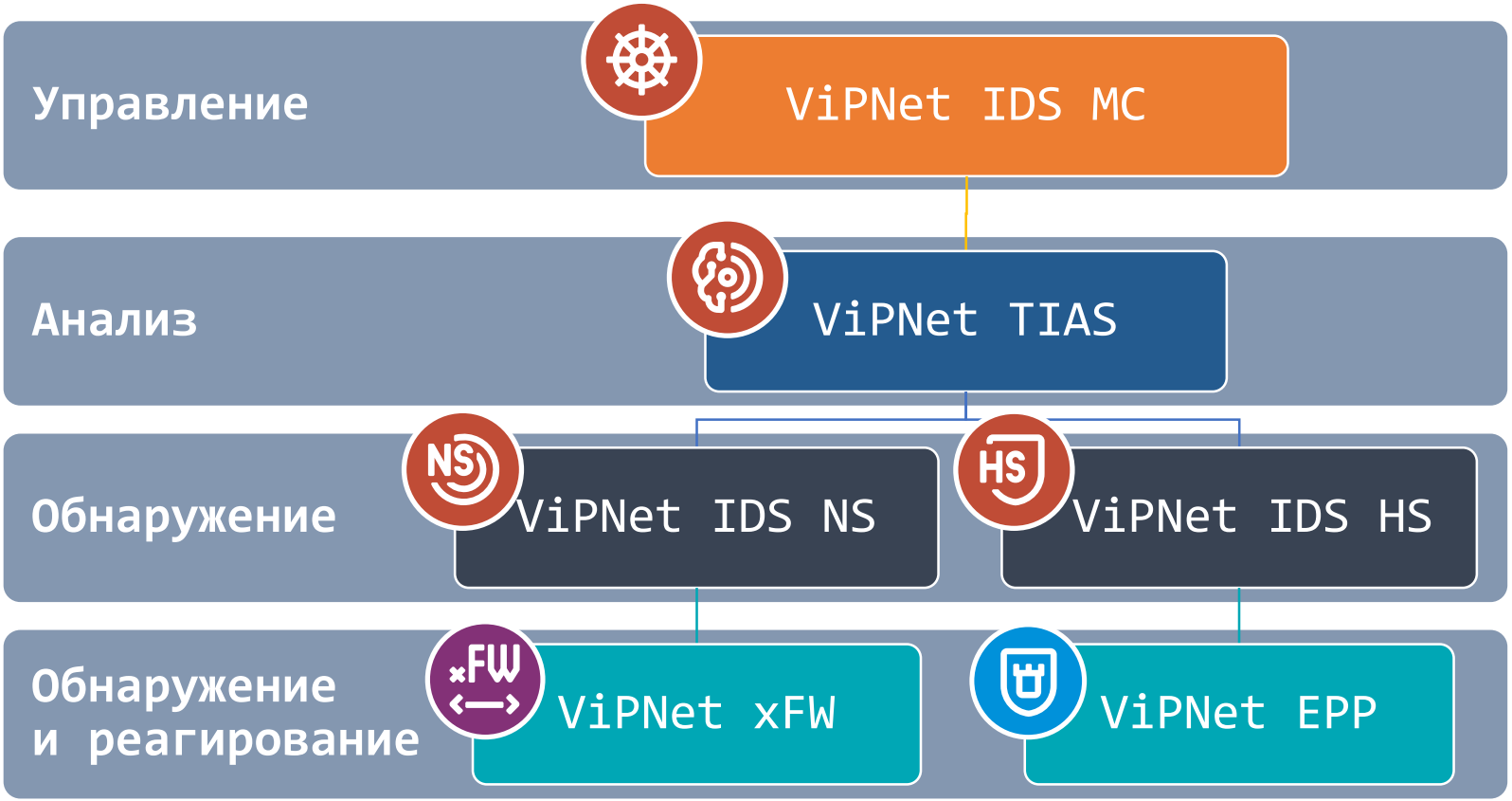
Extended Detection and Response. Расширяем границы и возможности

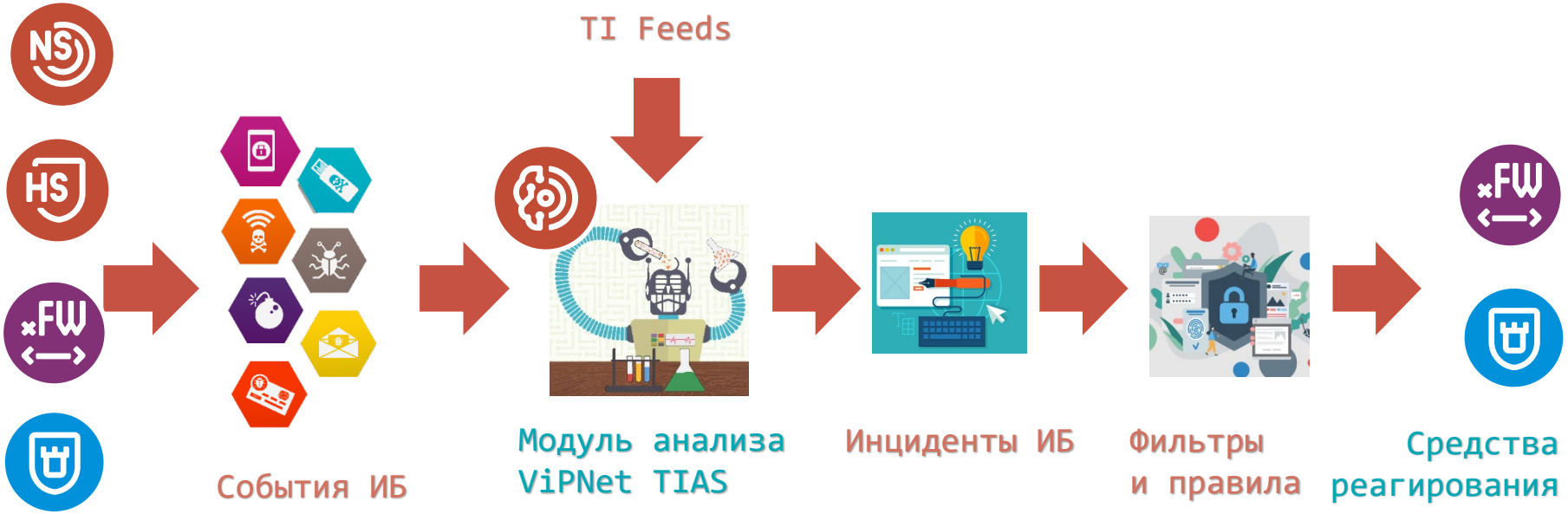
Старовойт Светлана

Что мы имеем на данный момент?

Решение ViPNet TDR



Как это работает?



Концепция XDR. Откуда взялось и зачем это нужно?

Краткая история концепции XDR

2018

Происхождение термина

Термин XDR был введён в 2018 году компанией Palo Alto.
Cortex XDR

2020

Gartner

Top 9 Security and Risk Trends for 2020
XDR – это новейшая технология, предлагающая специалистам ИБ улучшенные возможности обнаружения и предотвращения угроз и реагирования на инциденты

2022

Появление на Российском рынке

Kaspersky Symphony и PT XDR

2023

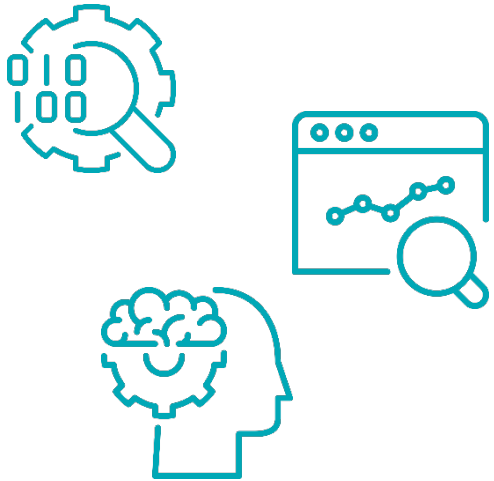
Настоящее и будущее XDR

XDR в данный момент находится в первой фазе цикла, на стадии технологического прорыва, и выйдет на «плато производительности» через 5–10 лет

Проблемы

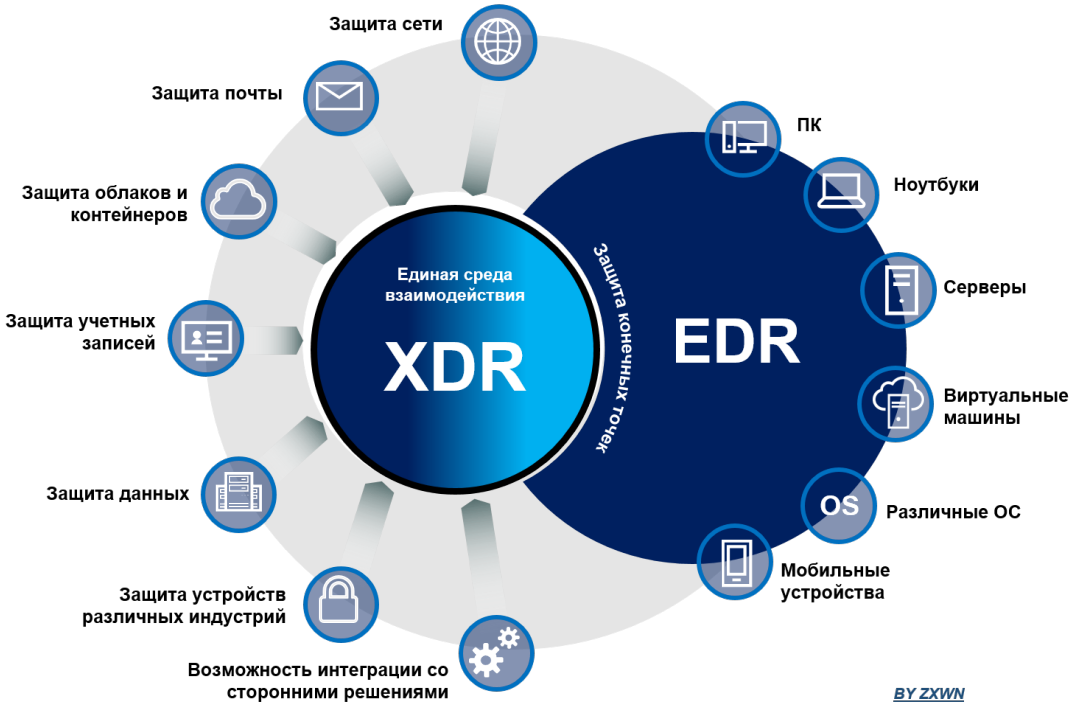
- Разрозненные не интегрированные решения
- Отсутствие кросс-продуктовых сценариев
- Недостаточная автоматизация
- Низкий уровень приоритезации
- Плохая визуализация

Основные задачи XDR-решения

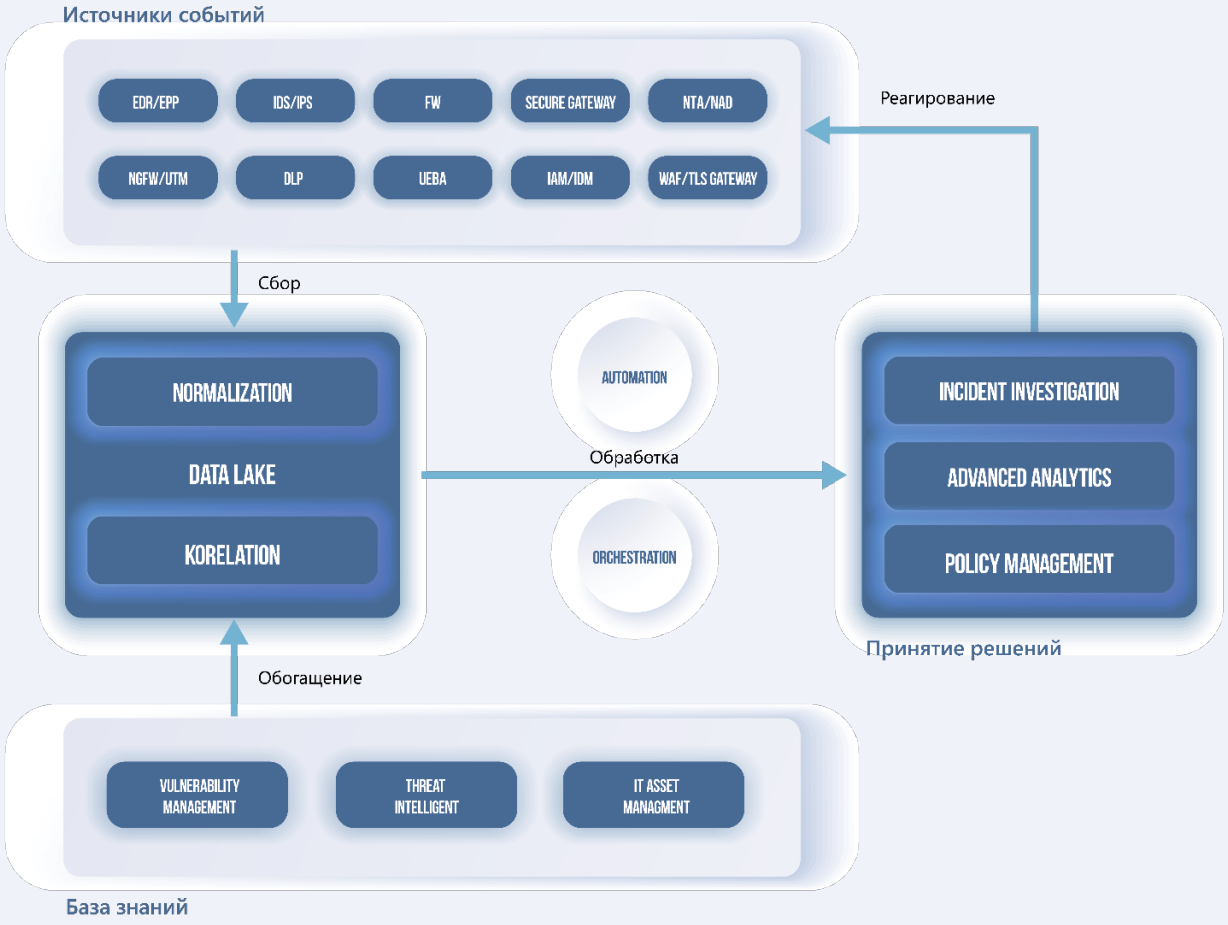


- получение основных и контекстных данных
- выявление взаимосвязей между данными контекста из различных источников
- визуализация данных в удобном для пользователя графическом представлении
- реагирование на обнаруженные взаимосвязи

Концепция Extended Detection and Response(XDR)



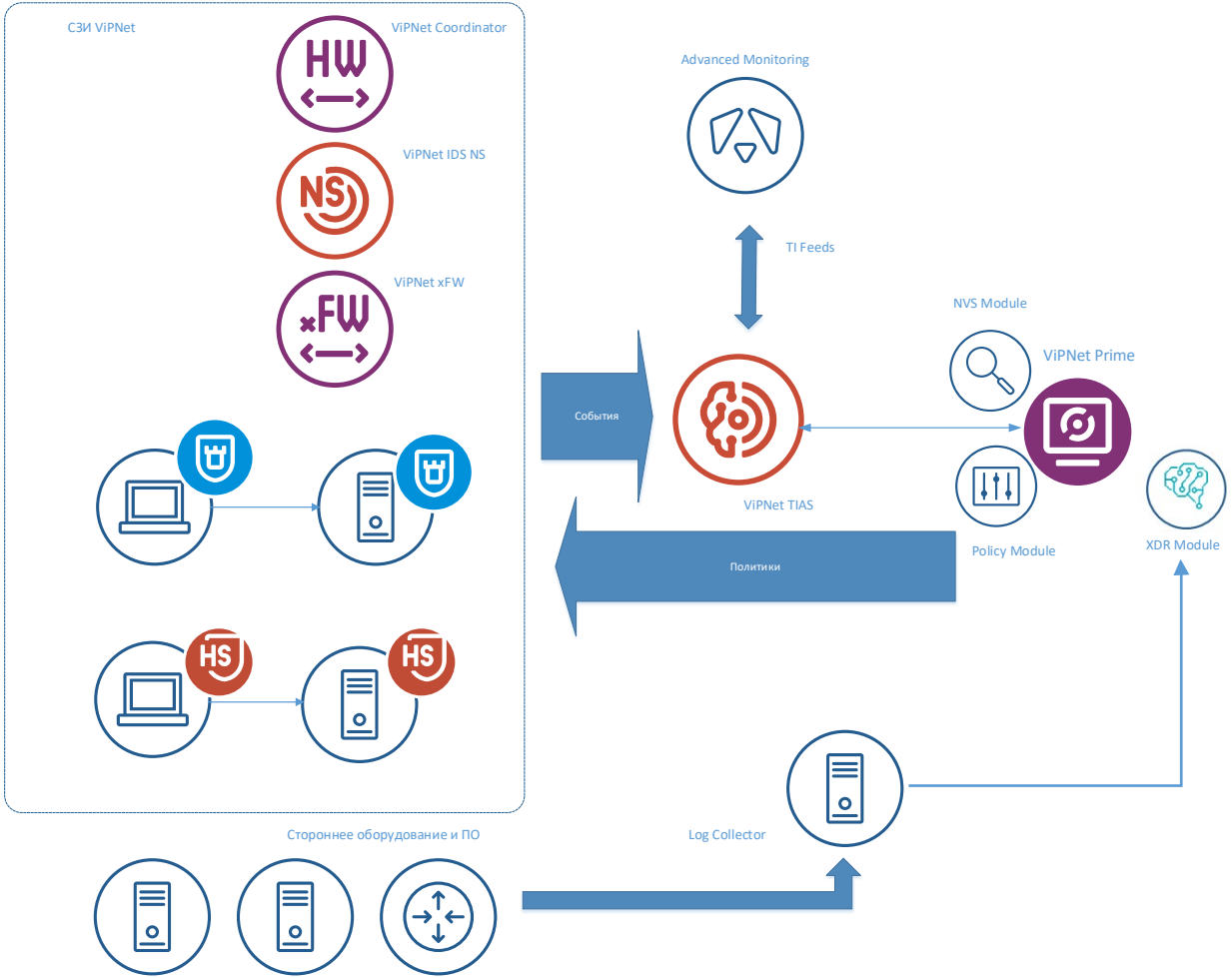
XDR – это концепция, которая представляет собой кросс-продуктовые сценарии, дополненные значимыми функциональными возможностями по реагированию на инциденты



Архитектура решений XDR

ТЕХНО 2024 infotecs ФЕСТ

Решение ViPNet XDR



Решение ViPNet XDR

Сбор информации с дополнительных источников

Продукты ViPNet

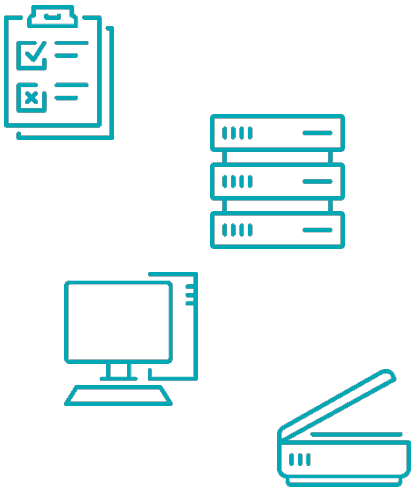
Стороннее оборудование и ПО

- CEF 2.0
- syslog
- NetFlow
- event log
- SNMP

Log Collector

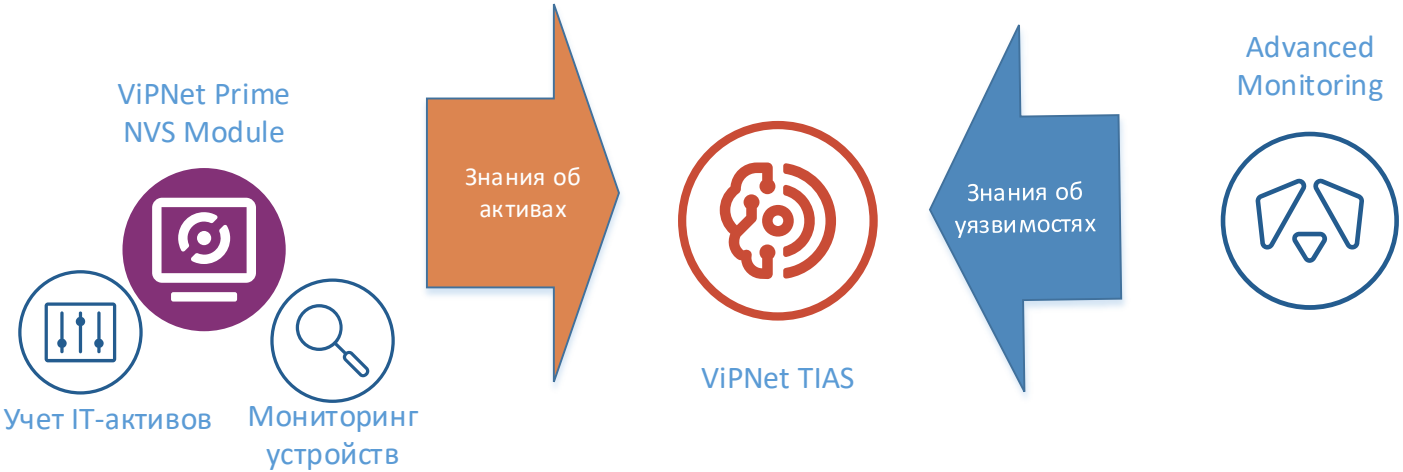
- Сбор
- Нормализация
- Хранение

Требования регуляторов к источникам сбора данных



- операционные системы
- сетевые приложения и сервисы
- прикладные сервисы
- средства обнаружения и предотвращения вторжений
- межсетевые экраны
- средства предотвращения утечек данных
- антивирусное программное обеспечение
- телекоммуникационное оборудование, в том числе активное сетевое оборудование, маршрутизаторы, коммутаторы
- средства контроля (анализа) защищенности
- средства управления телекоммуникационным оборудованием и сетями связи
- системы мониторинга состояния телекоммуникационного оборудования
- системы мониторинга качества обслуживания
- контроллеры домена
- средства (системы) контроля и управления доступом
- иные средств и систем защиты информации и систем мониторинга, эксплуатируемые владельцем информационной инфраструктуры

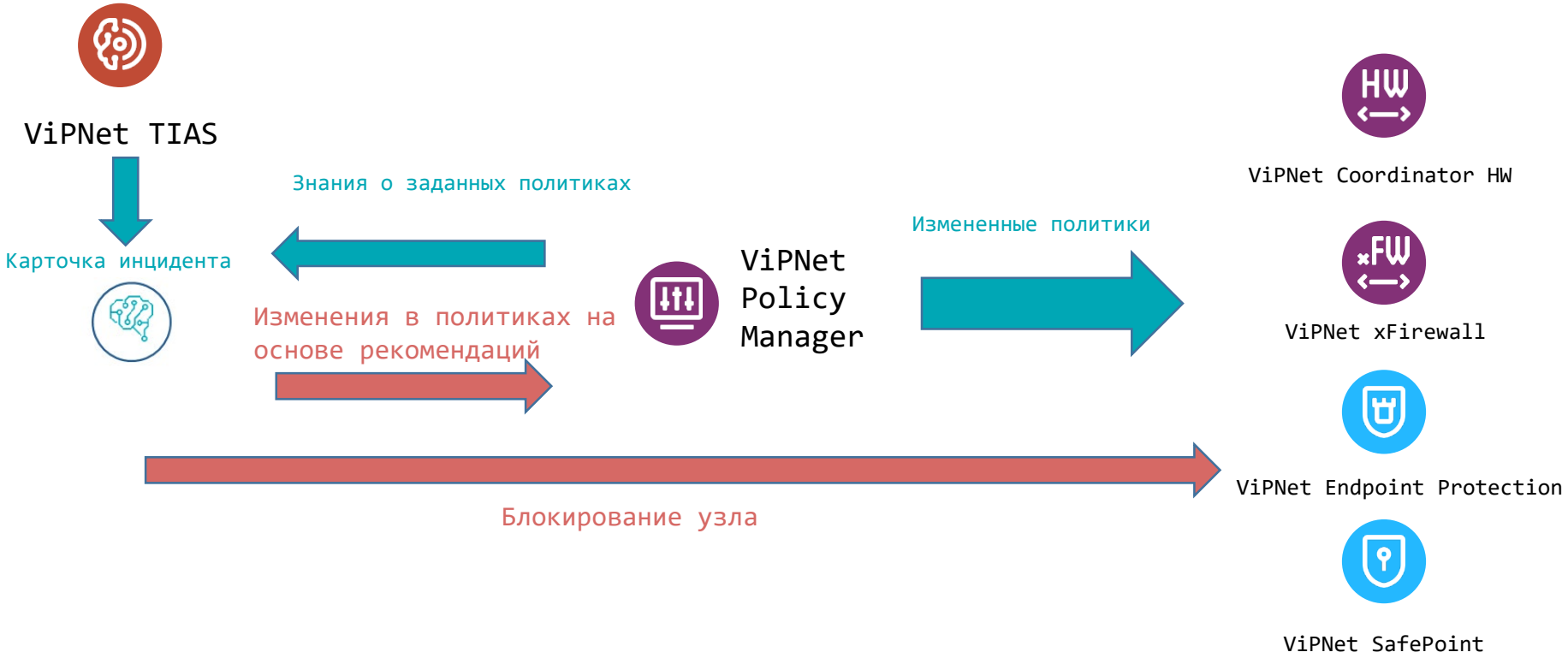
Обогащение знаниями об активах



- Тип актива
- Бизнес-ценность актива
- Принадлежность сегменту сети
- Установленное ПО и патчи

Реагирование

Реагирование



Методы анализа

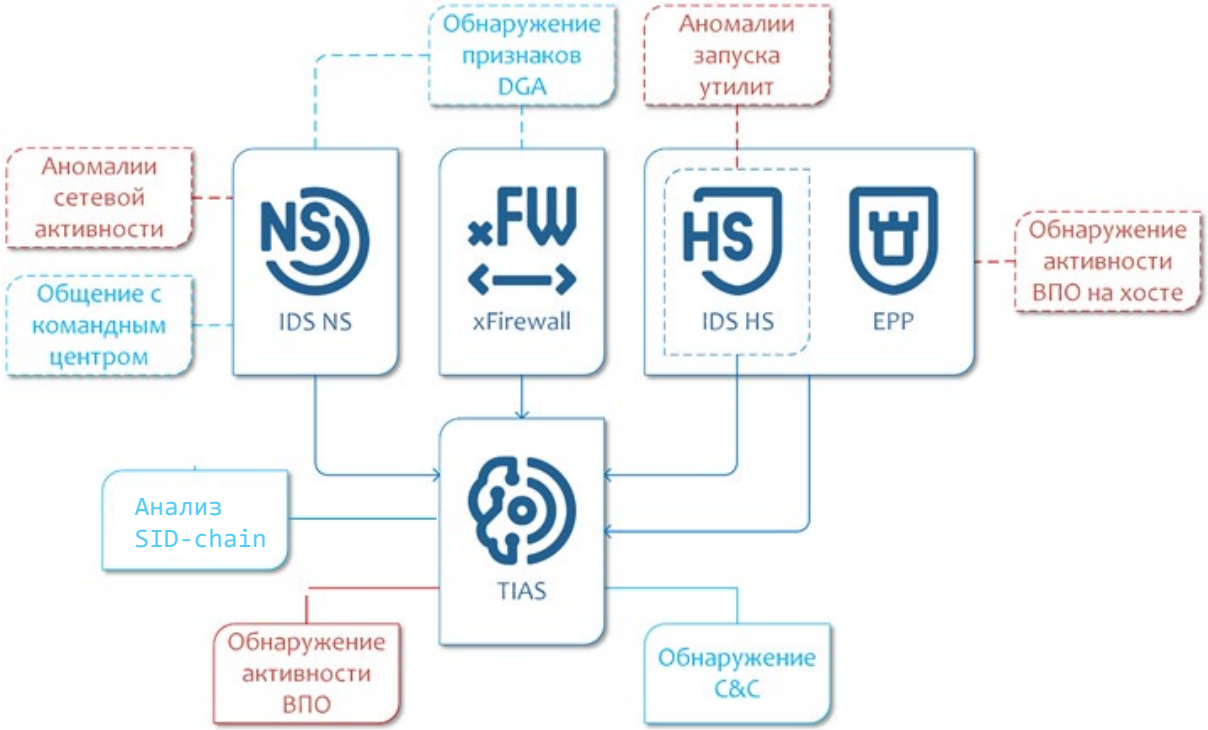
Виды анализа:

- Ретроспективный анализ
- Выявление потенциальных угроз
- Прогнозные модели развития инцидента

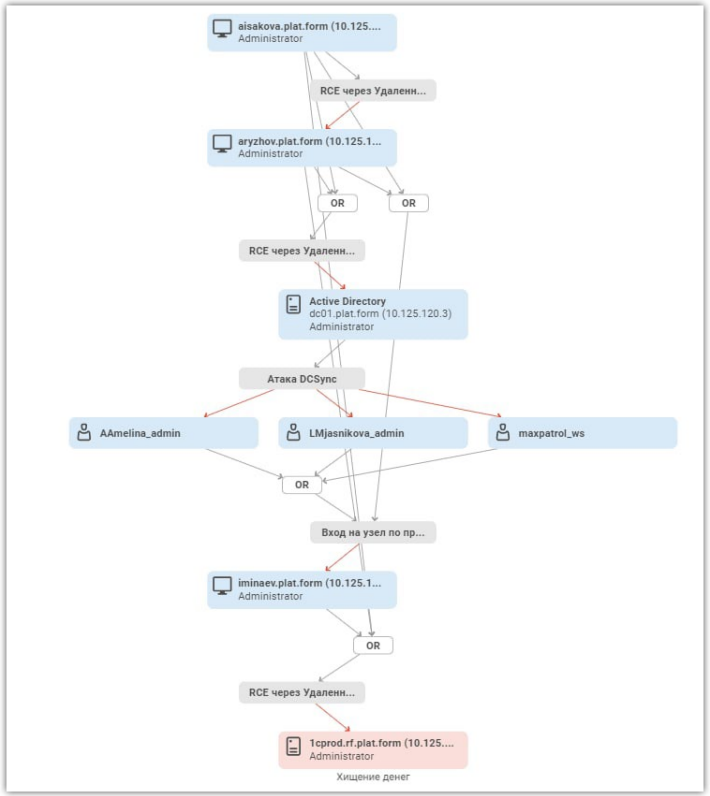
Инструменты:

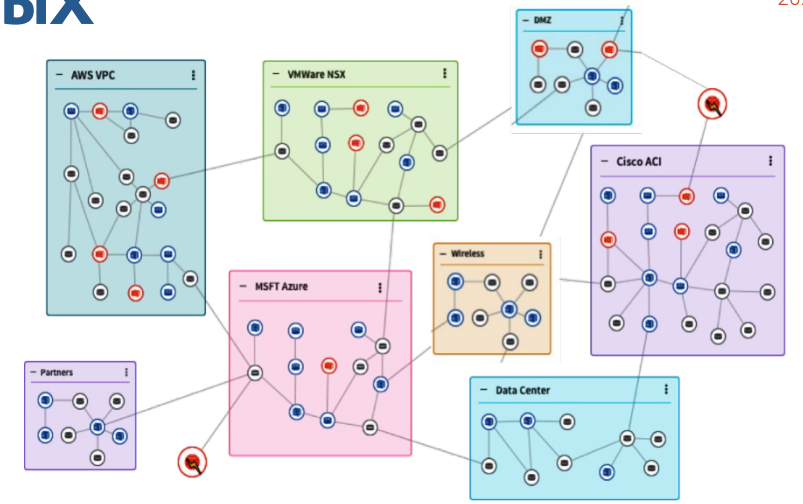
- Правила
- ML-модели
- OLAP-кубы

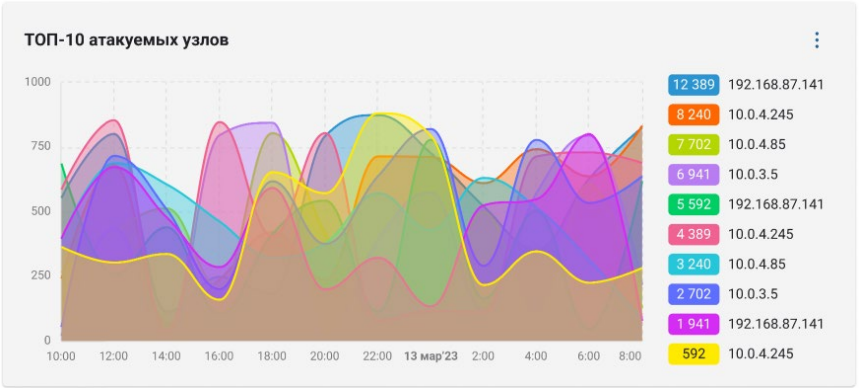
Модели машинного обучения



Визуализация данных







Подведем итог, на чем строится решение XDR

ТЕХНО 2024 infotecs ФЕСТ

Спасибо за внимание!

Подписывайтесь на наши соцсети

vk.com/infotecs_news

https://t.me/infotecs_official

rutube.ru/channel/24686363