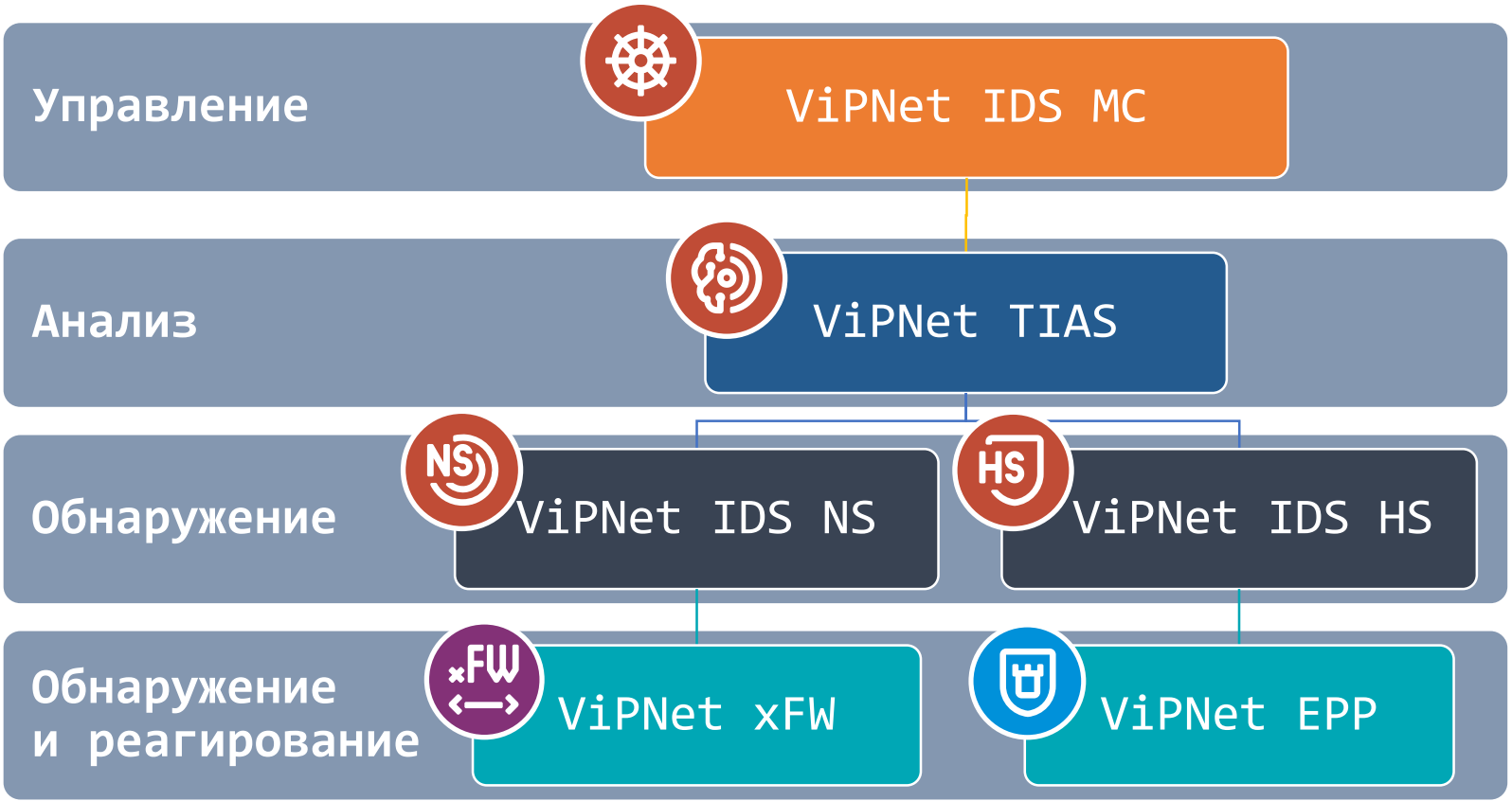
Extended Detection and Response. Расширяем границы и возможности

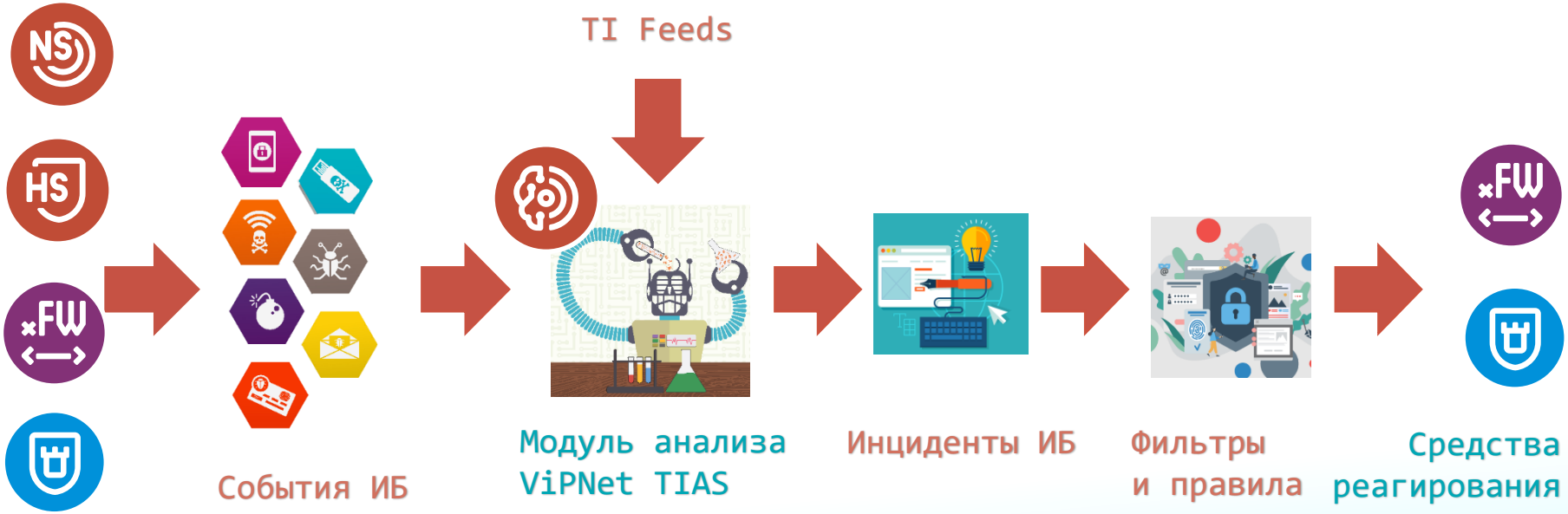
Старовойт Светлана
Руководитель продуктового направления

Что мы имеем на данный момент?

Решение ViPNet TDR



Как это работает?



Концепция XDR. Откуда взялось и зачем это нужно?

ТехноФест infotecs

Краткая история концепции XDR

ТЕХНО infotecs ФЕСТ

2018

Происхождение термина

Термин XDR был введен 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

2024

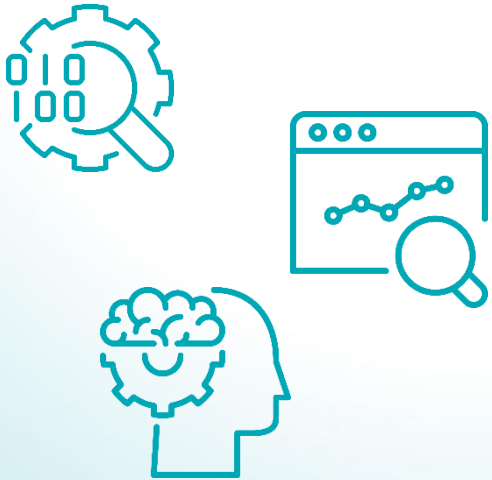
Настоящее и будущее XDR

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

Проблемы

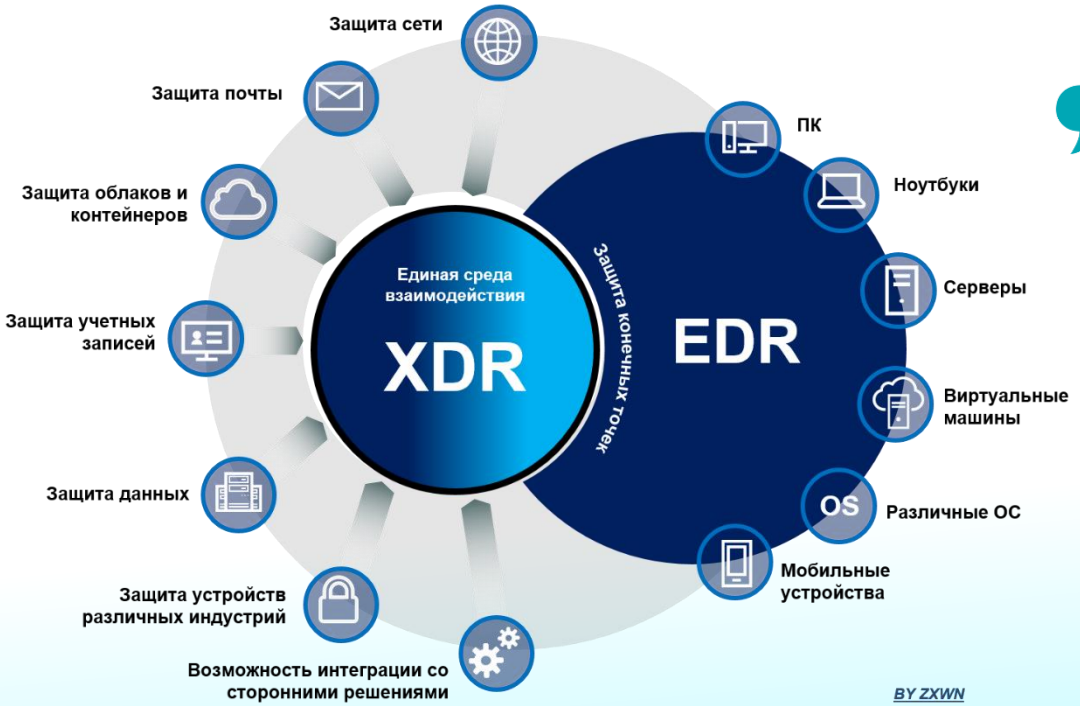
- Разрозненные не интегрированные решения
- Отсутствие кросс-продуктовых сценариев
- Недостаточная автоматизация
- Низкий уровень приоритизации
- Плохая визуализация

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)

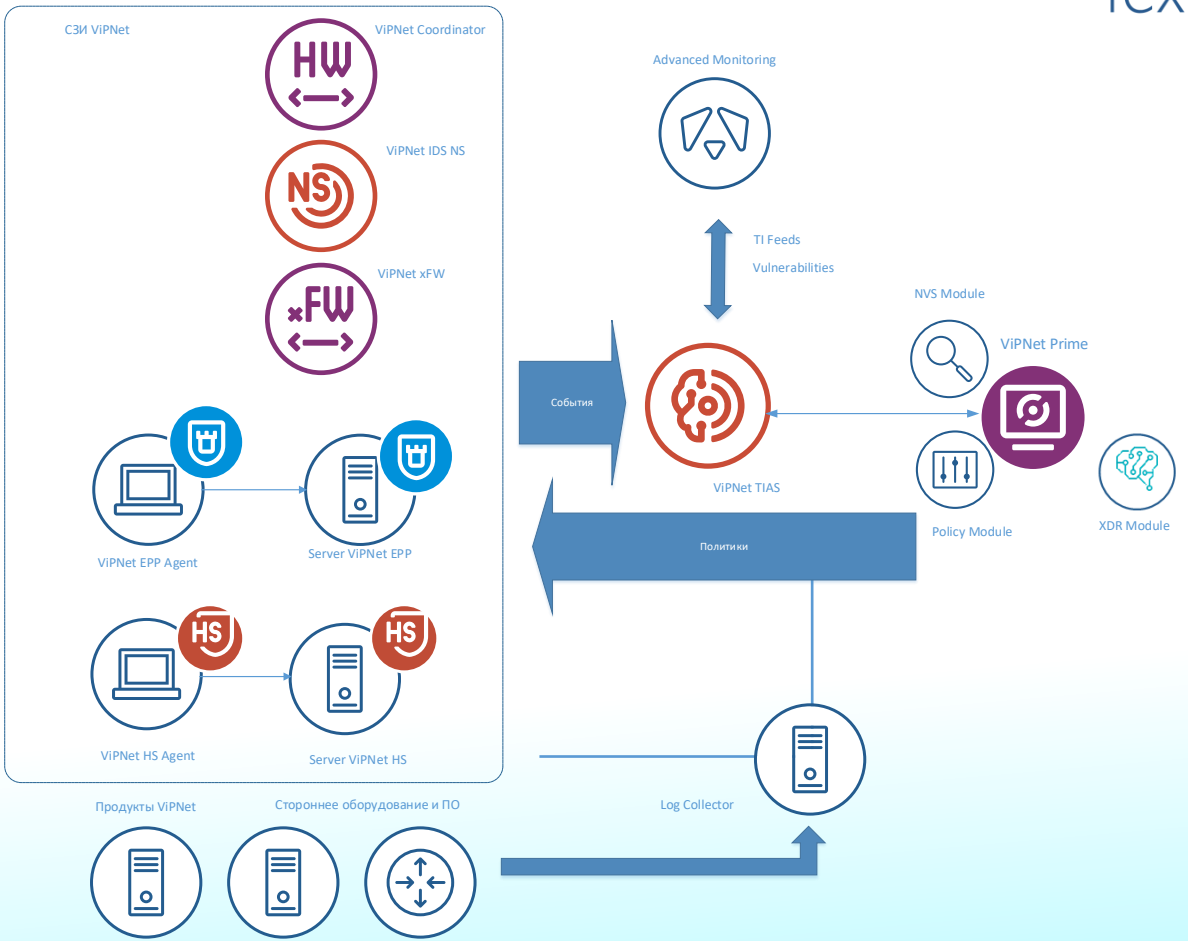


XDR – это концепция, которая представляет собой кросс-продуктовые сценарии, дополненные значимыми функциональными возможностями по реагированию на инциденты

Решение ViPNet XDR

ТЕХНО infotecs ФЕСТ

Решение ViPNet XDR



Сбор информации с дополнительных источников

Продукты ViPNet

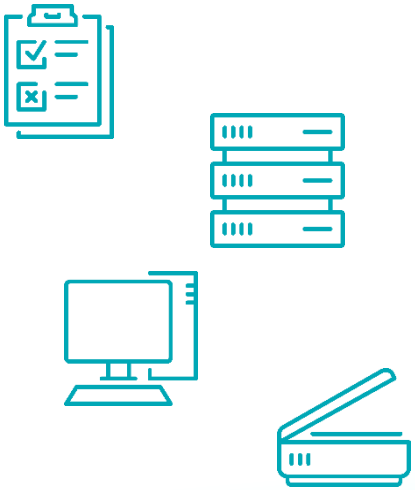
Стороннее оборудование и ПО

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

Log Collector

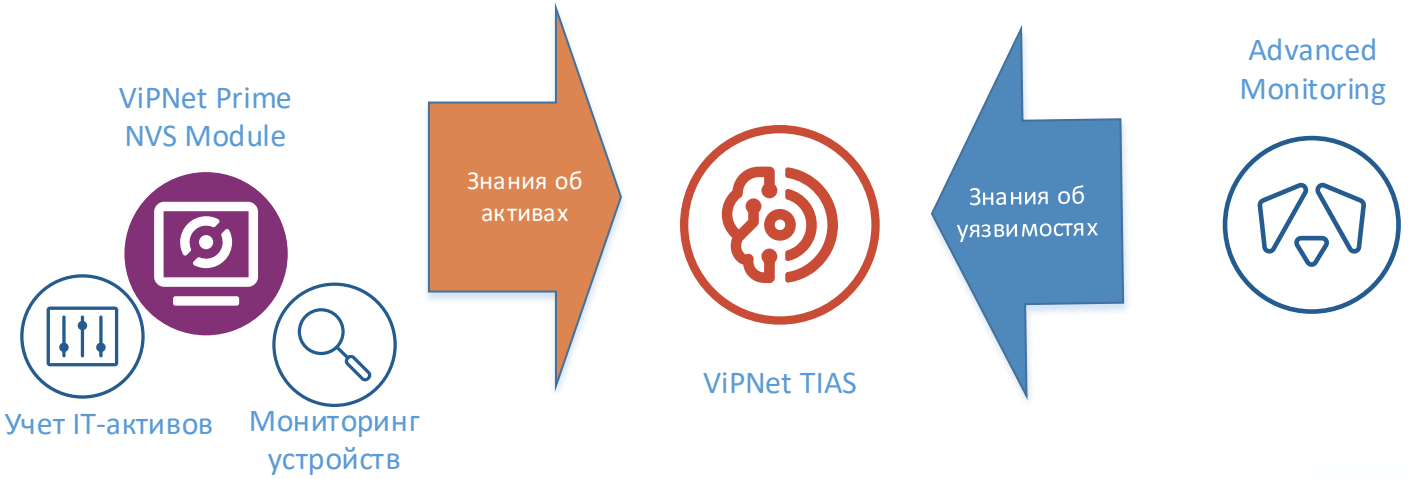
- Сбор
- Нормализация
- Хранение

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

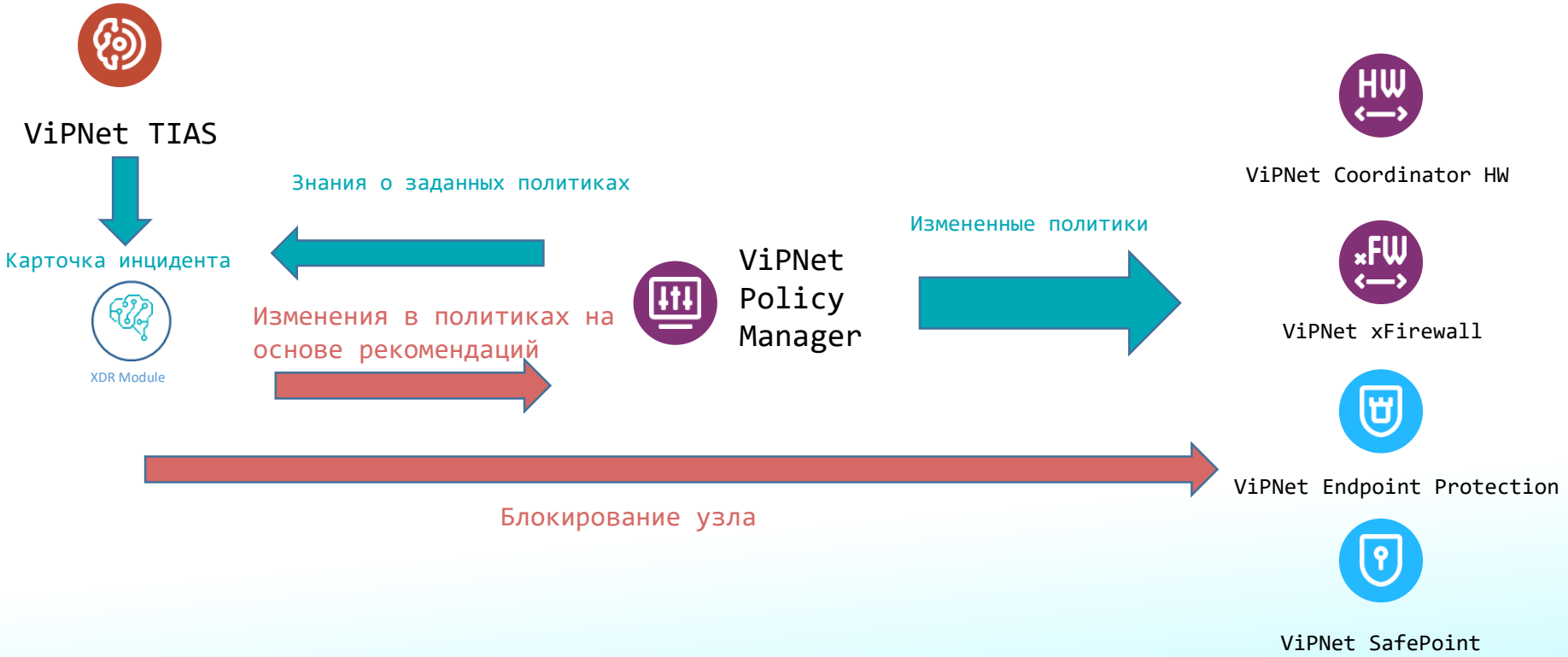
Реагирование






01	02	03	04	05	06
Блокирование атаки	Расследование	Оценка ущерба	Передача сведений	Устранение последствий	Повышение уровня защищенности
Изоляция скомпрометированного узла Правила блокировки по IoC	Выявление всех задействованных активов Способ проникновения Артефакты взлома	Финансовый ущерб Репутационные риски Влияние на внешних контрагентов	НКЦКИ ФинЦЕРТ Роскомнадзор	Восстановление системы Устранение артефактов заражения Восстановление данных	Устранение уязвимостей Изменение политик Новые правила Регламенты Обучение

Реагирование



Методы анализа

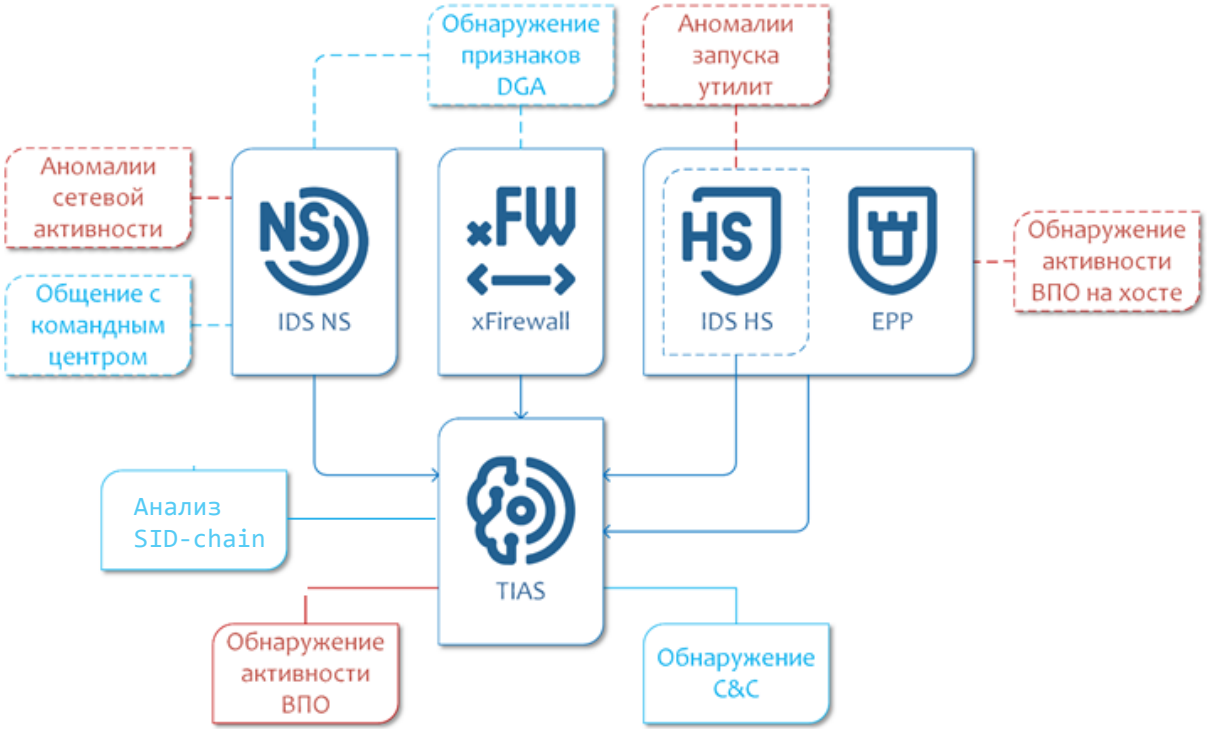
Виды анализа:

- ретроспективный анализ
- выявление потенциальных угроз
- прогнозные модели развития инцидента

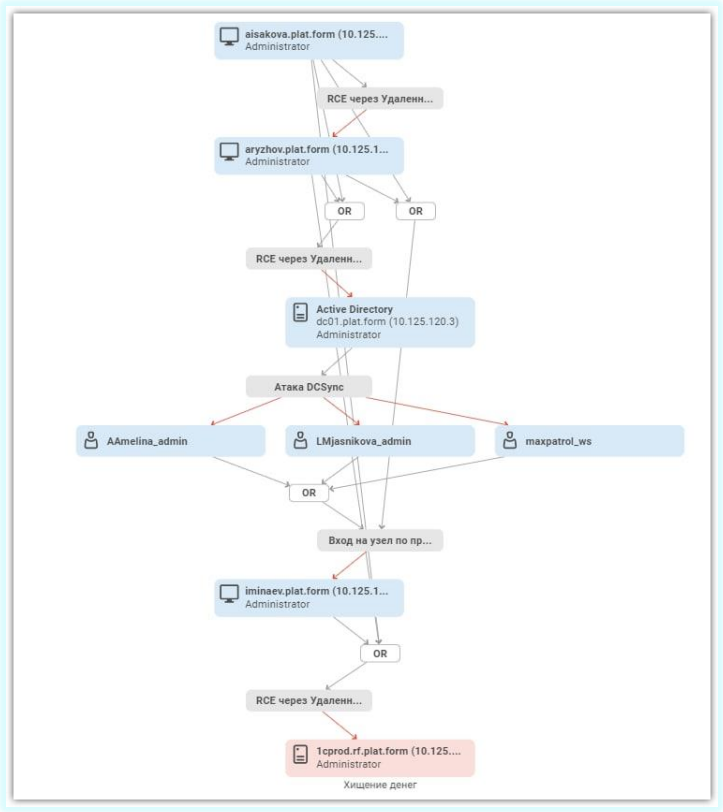
Инструменты:

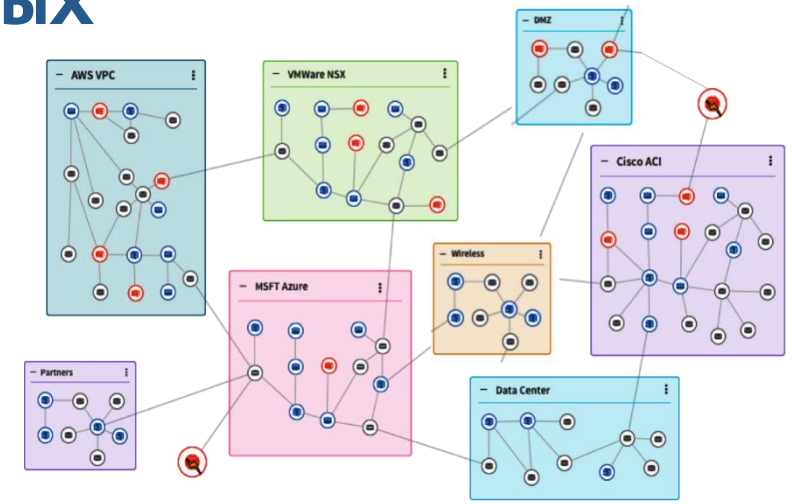
- правила
- ML-модели
- OLAP-кубы

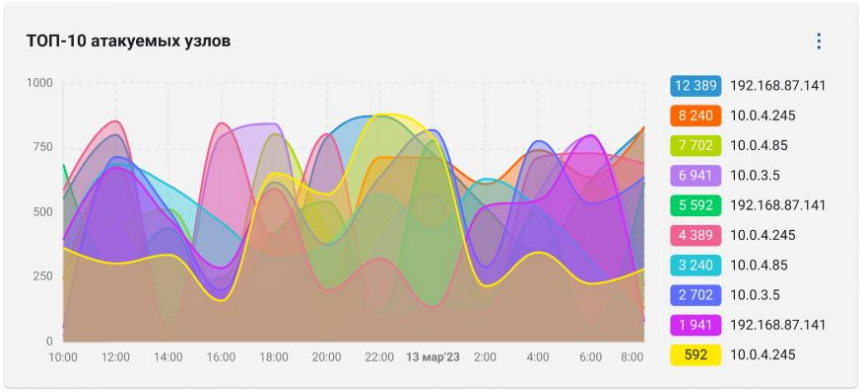
Модели машинного обучения



Визуализация данных







Подведем итог, на чем строится решение XDR

ТЕХНО infotecs ФЕСТ

Светлана Старовойт
Руководитель продуктового направления

Подписывайтесь
на наши соцсети,
там много интересного