

Extended Detection and Response. Расширяем границы И ВОЗМОЖНОСТИ



техно infotecs
2023 Фест
ТЕХНИЧЕСКАЯ
КОНФЕРЕНЦИЯ

Старовойт Светлана

**Откуда взялось
и зачем это нужно?**

Краткая история концепции XDR

Происхождение термина

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

2018

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

2020

Появление на Российском рынке

Kaspersky Symphony и PT XDR

2022

2023

Настоящее и будущее XDR

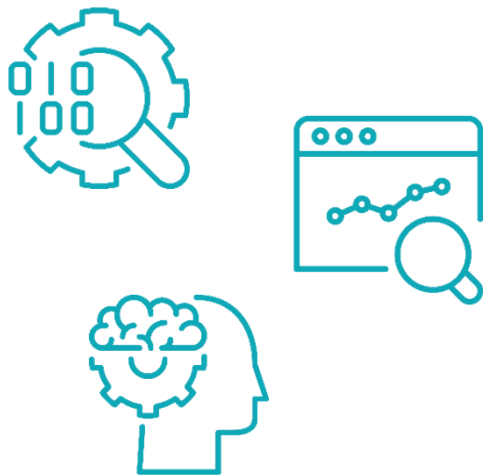
XDR в данный момент находится в первой фазе цикла, на стадии технологического прорыва, и выйдет на «плато производительности» через 5–10 лет

Проблемы



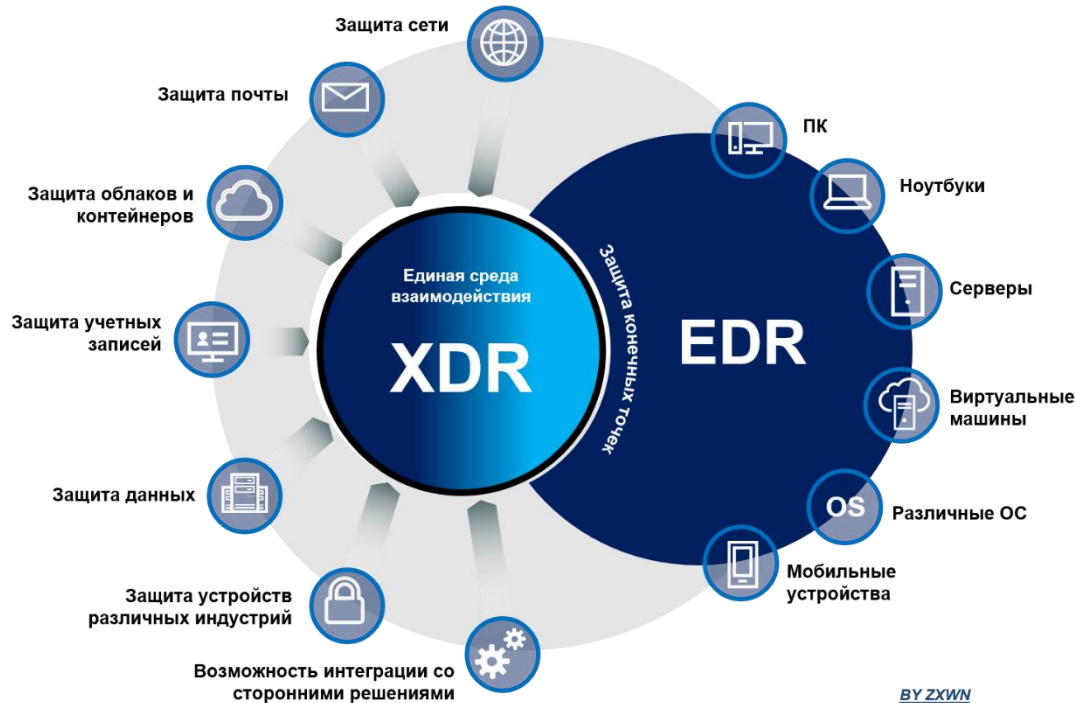
- Разрозненные не интегрированные решения;
- Недостаточная автоматизация;
- Отсутствие кросс-продуктовых сценариев;
- Низкий уровень приоритизации;
- Много ложно-положительных срабатываний;
- Плохая визуализация

Основные задачи XDR-решения



- получение основных и контекстных данных;
- нормализация данных для хранения и работы с ними;
- 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

Источники событий

EDR/EPP IDS/IPS FW SECURE GATEWAY NTA/NAD
NGFW/UTM DLP UEBA IAM/IDM WAF/TLS GATEWAY

Реагирование

Сбор

NORMALIZATION

DATA LAKE

KORELATION

AUTOMATION

Обработка

ORCHESTRATION

INCIDENT INVESTIGATION

ADVANCED ANALYTICS

POLICY MANAGEMENT

Принятие решений

Обогащение

VULNERABILITY
MANAGEMENT

THREAT
INTELLIGENT

IT ASSET
MANAGEMENT

База знаний

Архитектура решений XDR

Основные и контекстные данные

События ИБ

- События от сетевых и хостовых IDS/IPS/WF/AV
- Request logs/Traffic logs
- NetFlow статистик

Данные о пользователях и устройствах

- IT-инфраструктура
- Привязка к бизнес-процессам
- Привилегии пользователей
- Аномалии поведения

Данные об уязвимостях

- Описание уязвимостей с привязкой к устройству

TI-feeds

- IoC (IP- и URL-адреса, домены, email, Хэши, DGA, ключи реестра)
- Базы угроз (Mitre ATT&CK/база ФСТЭК)

Сбор нормализация и хранение

Протоколы передачи

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

Big Data

- структурированные или неструктурированные массивы данных большого объема
- исходные образцы трафика

Долгосрочное хранение

- требования нормативов и регламентов по срокам
- требования для computer/network forensics

Оперативное хранение

- online-обработка
- обработка запросов

Выявление взаимосвязей

Правила корреляции

- Корреляция от разных источников с привязкой к контекстным данным
- Оперативный и ретроспективный анализ

ML

- Использование алгоритмов машинного обучения
- Data Sets для обучения
- Обучение с учителем и самообучение

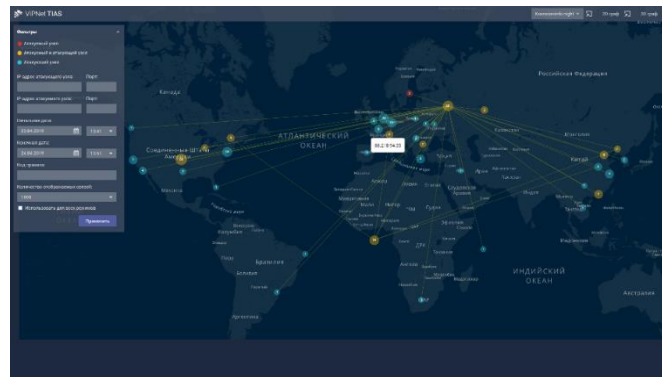
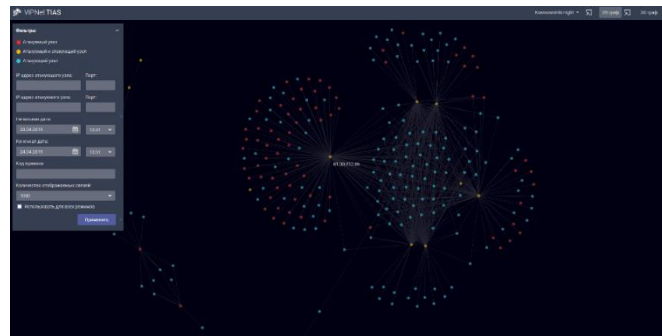
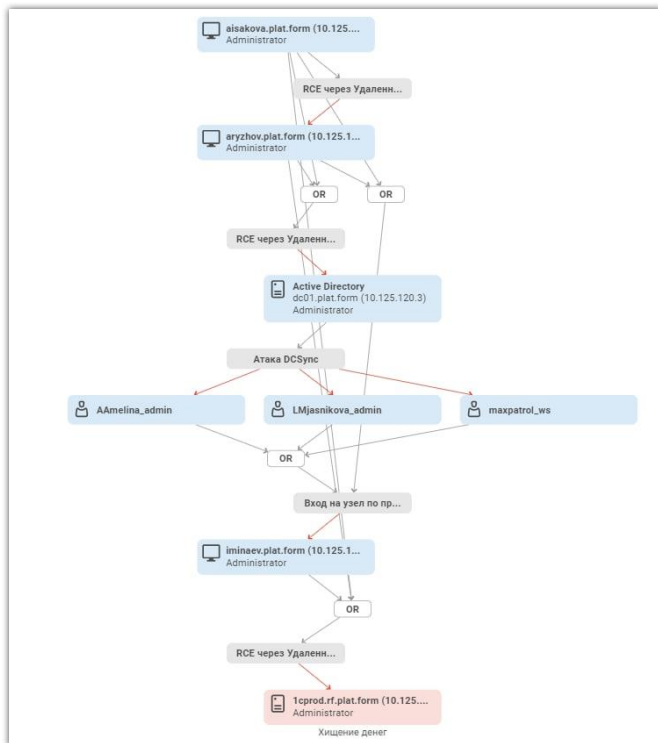
Advanced analytics

- BI
- Predictive analytics

UEBA

- Машинное обучение
- Статистический анализ

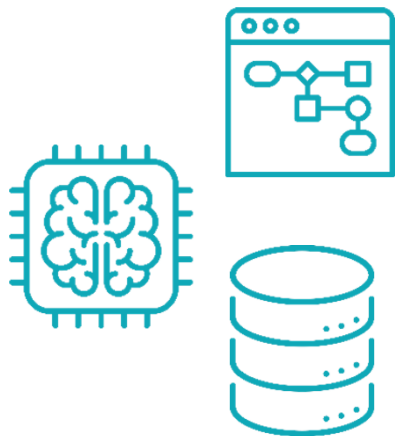
Визуализация данных



Реагирование



Технологии, используемые в решениях XDR



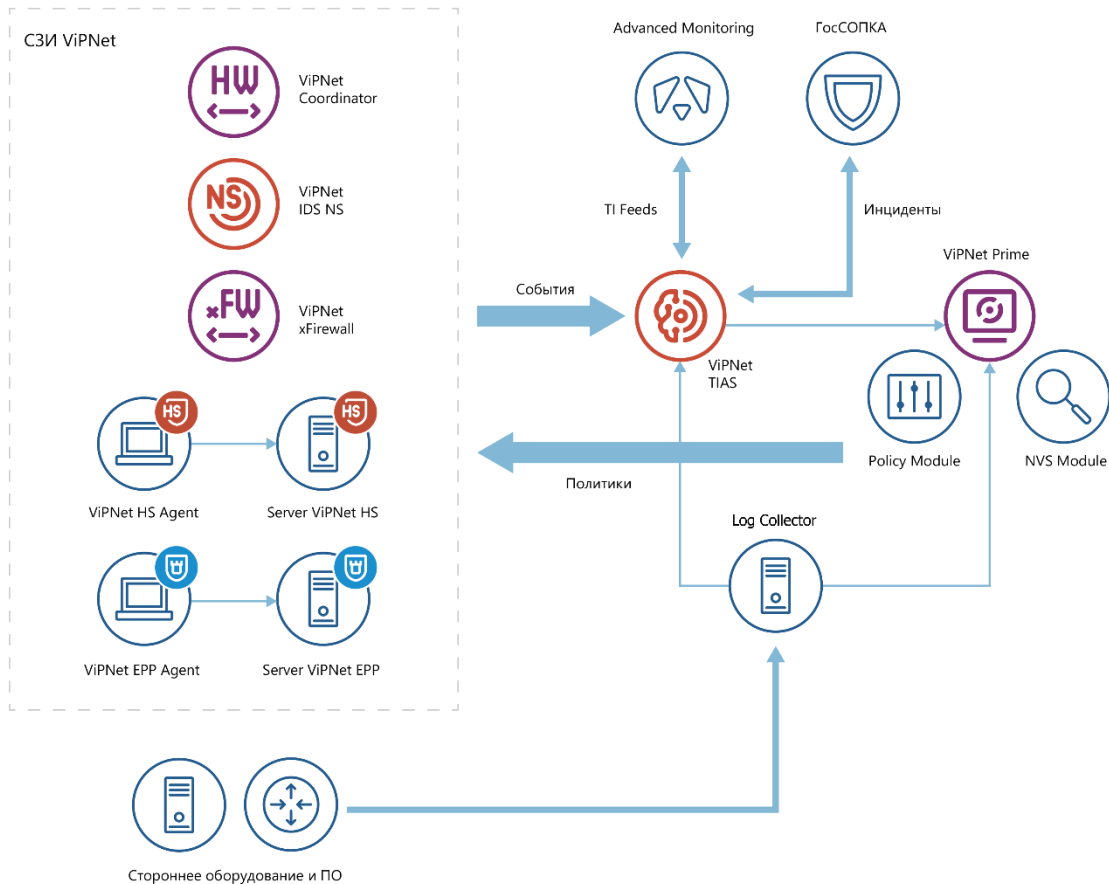
- Big Data
- Machine learning
- Business Intelligent
- On-Line Analytical Processing
- Advanced Analytics
- Visibility and Interoperability

Инструменты для построения XDR

- Log Management
- Incident Management
- Policy Management
- SIEM
- Asset Management Software
- Vulnerability management
- TI Platform
- SandBox

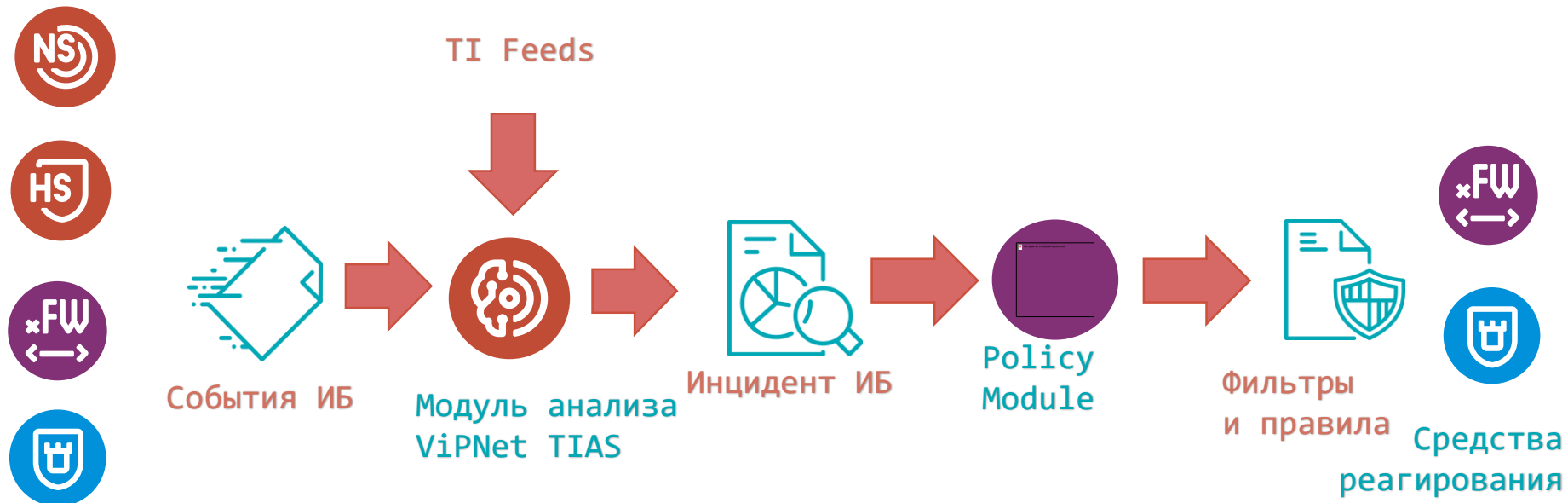


Решение ViPNet XDR



Решение ViPNet XDR

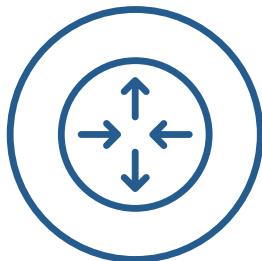
Как это работает?



Источники
событий

Сбор информации с дополнительных источников

Стороннее оборудование и ПО



Log Collector

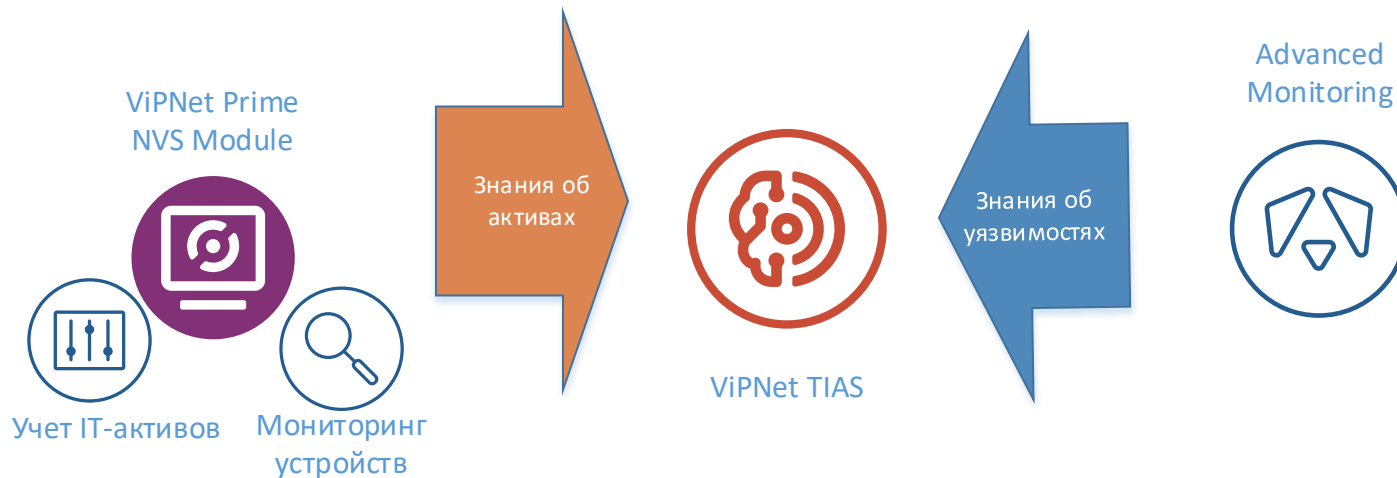
- CEF 2.0
- syslog
- NetFlow
- event log
- SNMP

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



Реагирование


ViPNet TIAS

Знания о заданных политиках



Изменения в политиках на
основе рекомендаций



ViPNet
Policy
Manager

Измененные политики



ViPNet Coordinator HW



ViPNet xFirewall

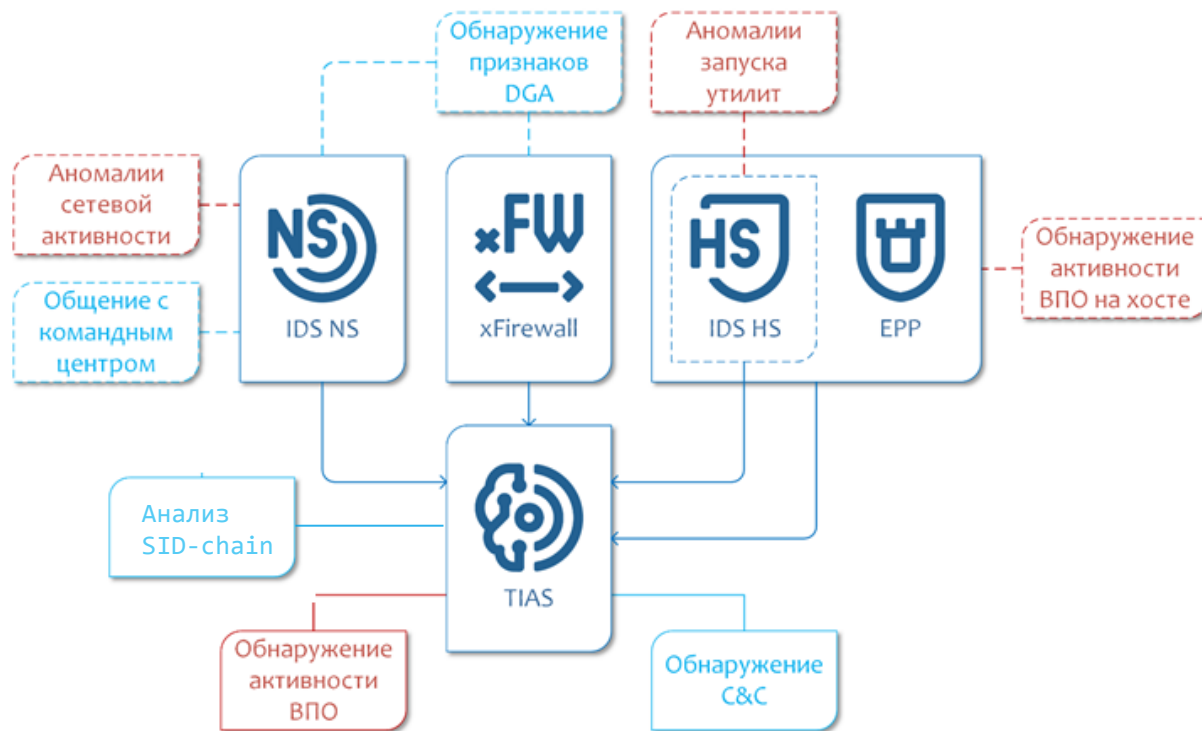


ViPNet Endpoint Protection

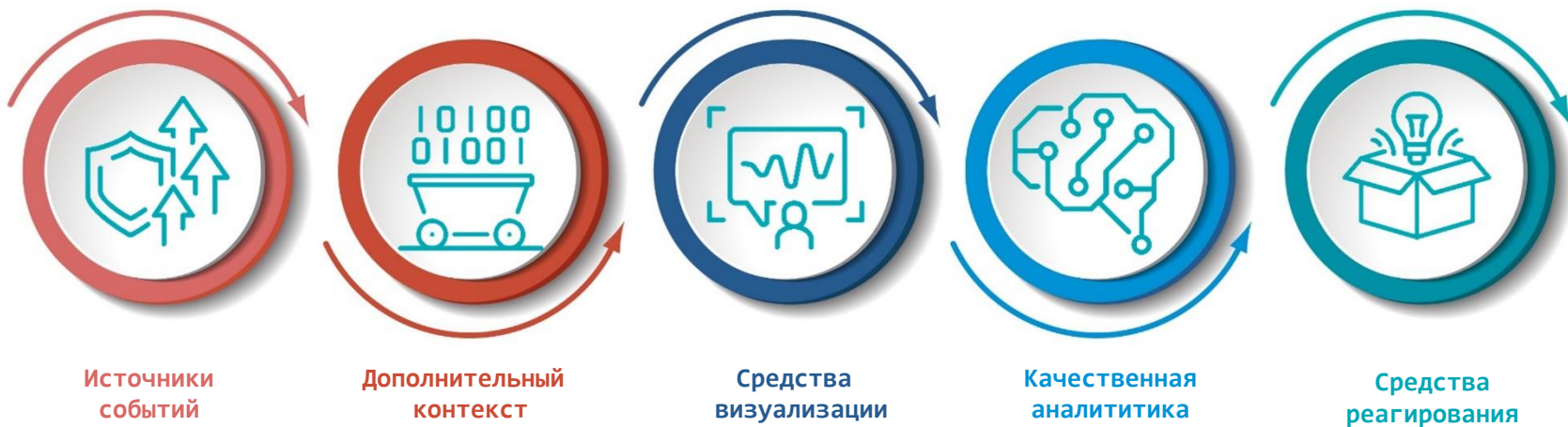


ViPNet SafePoint

Расширенная аналитика



Подведем итог, на чем строится решение XDR



техно infotecs
2023 Фест

Спасибо
за внимание!

Подписывайтесь на наши соцсети



vk.com/infotecs_news



https://t.me/infotecs_official



rutube.ru/channel/24686363