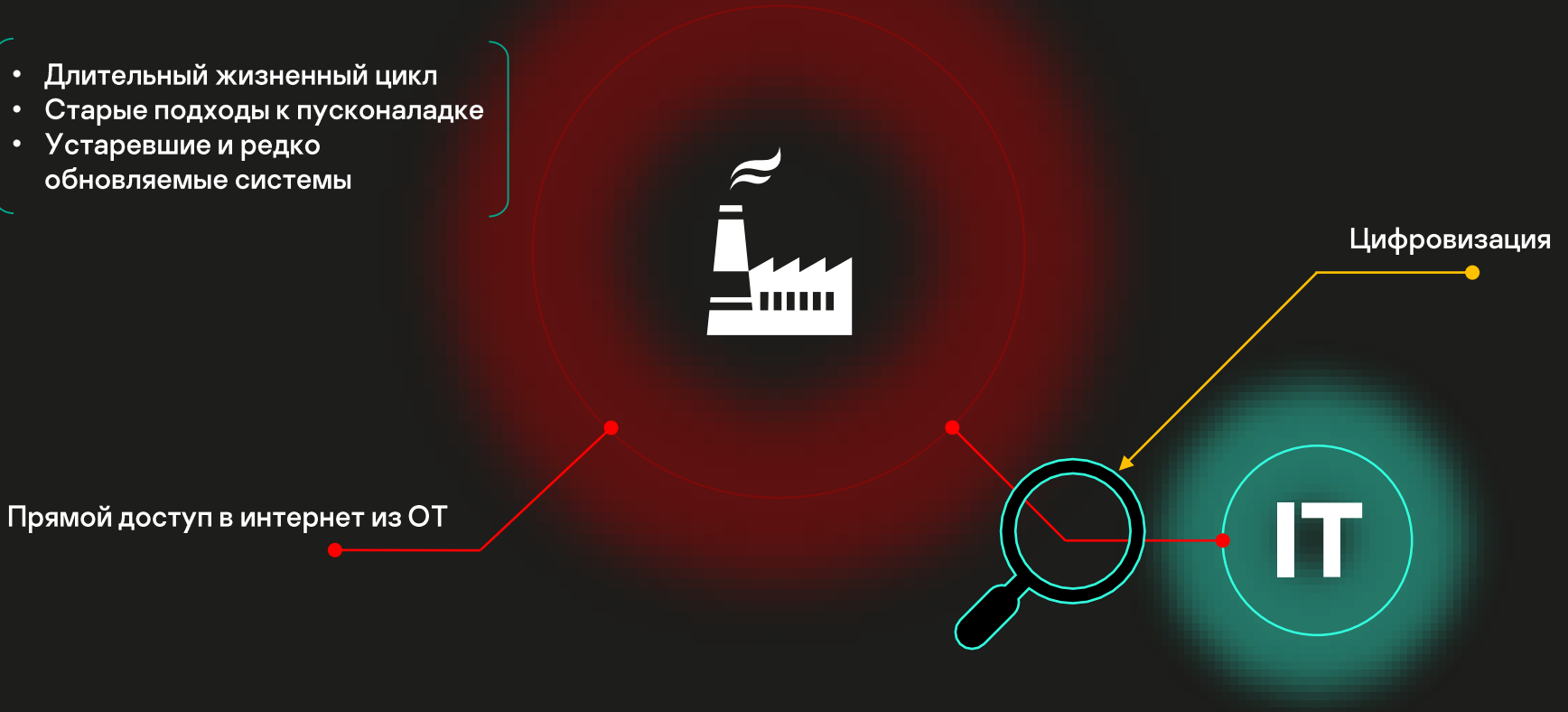
Kaspersky Industrial Cybersecurity Conference 2023

Возможности и сценарии XDR в промышленной среде

Михаил Нагорный

kaspersky

- Длительный жизненный цикл
- Старые подходы к пусконаладке
- Устаревшие и редко обновляемые системы



Наиболее частые риски ИБ

OT

- Внешние накопители
- Подключаемые модемы и телефоны
- Удаленный доступ для обслуживающих организаций

- Угрозы технологического характера, например износ оборудования
- Злонамеренное вмешательство в технологический процесс

IT

- Фишинг и социальная инженерия
- USB носители
- Зараженные web страницы
- Атака на смежную информационную систему

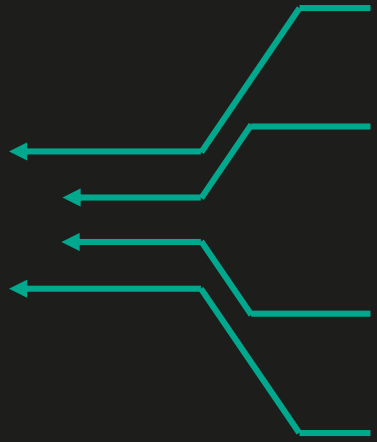
Возможные векторы атак

- Нарушение или остановка тех. процесса
- Ремонт и восстановление
- Аварийное состояние
- Переналадка оборудования
- Физическое повреждение устройств

- Нарушение цепочки «заказчик-поставщик»
- Финансовые издержки
- Ущерб репутации
- Экономический ущерб
- Влияние на экологию
- Физический ущерб

Возможные последствия

- Регулярный анализ текущей оценки защищенности (выявление и устранение рисков ИБ, планирование внедрения требуемых решений ИБ и процессов, управление уязвимостями)
- Мониторинг, выявление и предотвращение угроз на всех уровнях (рабочие станции, сервера, сетевой трафик, сетевые устройства и др.)
- Реагирование на всех уровнях
- Контроль нарушений тех. процесса

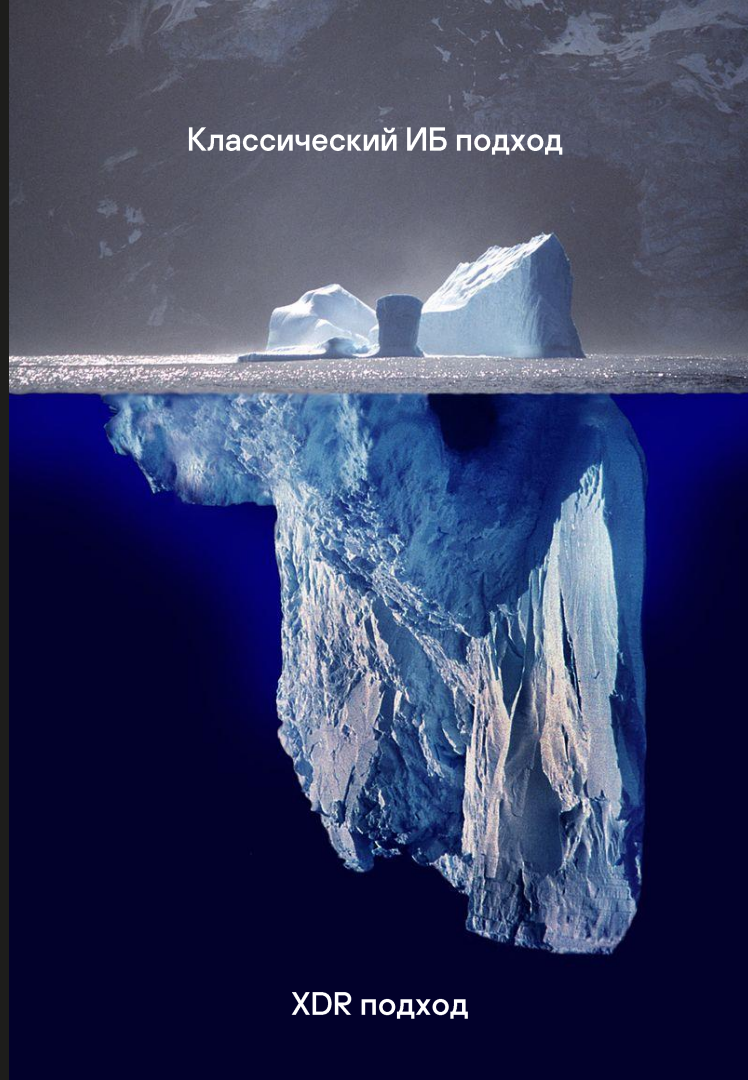


Задачи перед ИБ командой

XDR помогает упростить многие из этих задач

- Охват максимального количества информационных систем и анализ данных из множества источников
- Своевременное обнаружение и понимание источника распространения угрозы
- Комплексное реагирование с участием ИБ, IT и OT команд
- Понимание уровня защищенности в будущем
- Удобство не только для ИБ, но и OT специалиста

XDR подход



SIEM IT и OT (обогащение TI, доп. возможности по выявлению угроз)

Инвентаризация (выявление угроз, прошивок пром. софта и уязвимостей)

Выявление сетевых угроз IDS

Выявление угрозы на уровне узлов

Контроль целостности сетевых коммуникаций

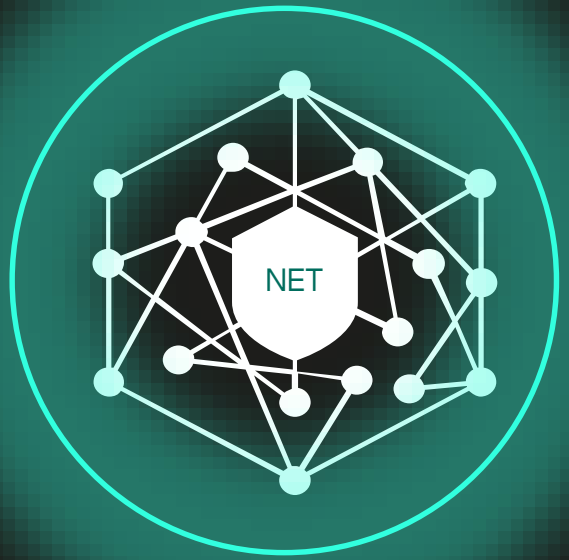
Анализ промышленного трафика DPI

Визуализация деталей угрозы - карточка инцидента

Рабочие XDR сценарии KICS. Выявление угроз

- ручная изоляция узла
- блокирование вредоносных объектов
- сканирование на IoC

HOST



- на коммутаторе – блокировка портов
- на межсетевом экране – блокировка доступа к сетевым ресурсам и протоколов взаимодействия

Рабочие XDR сценарии KICS. Реагирование

Подключение удаленных площадок SDWAN

Карта сети, включая выявление неучтенных устройств
- Модели устройств
- Версии ОС
- Прошивки ПО
- Контроль сетевых сессий
- Контроль техн. параметров

Проверка конфигураций безопасности устройств
- состав сети
- уязвимости пром. устройств

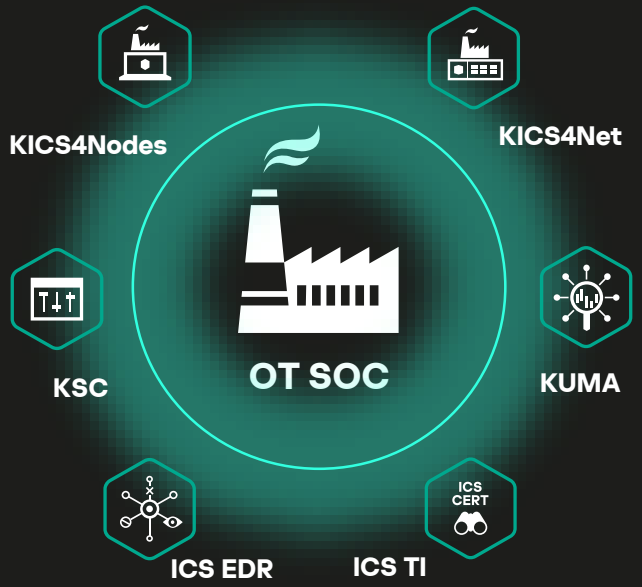
OVAL-проверки промышленного ПО

Дополнительные возможности

Информация об объекте, инфраструктуре

Информирование о защищенности

Применение необходимых мер защиты



Выявление аномалий и угроз на основе множества источников данных

Внедрение средств реагирования

Не забываем про защиту IT сегмента

Технологически XDR подход является одной из составляющих OT SOC

Спасибо!

Михаил Нагорный
mikhail.nagorny@kaspersky.com

kaspersky