Kaspersky Industrial Cybersecurity Conference

Технологическое лидерство для защиты индустриальной среды

в решениях «Лаборатории Касперского»

Вениамин Левцов

Директор Центра экспертизы
по корпоративным решениям

kaspersky

Основа технологического лидерства

Понимание особенностей защищаемой среды

Технологии	Решения
Знания	Аналитика и тренинги
Экспертиза	Экспертные сервисы

В начале пути

Kaspersky Industrial CyberSecurity for Nodes

- Защита от вредоносного ПО с минимальным влиянием на систему
- PLC integrity check
- Противодействие шифровальщикам
- Контроль приложений и устройств

Kaspersky Industrial CyberSecurity for Networks

- Обнаружение в трафике передаваемых технологических параметров и их отклонений (промышленный DPI)
- Обнаружение отклонений от базовых параметров в сетевых коммуникациях
- Risk scoring событий и узлов
- Инвентаризация активов, включая данные об уязвимостях и состоянии узлов

От возможностей приложений — к задачам информационной безопасности

Kaspersky Industrial CyberSecurity for Nodes

Certified Industrial Endpoint Protection, EDR

Kaspersky Industrial CyberSecurity for Networks

ICS network monitoring, intrusion and anomaly detection

Kaspersky IoT Secure Gateway

Network segmentation (KISG)

Kaspersky ICS CERT Services

OT Services and TI

Kaspersky Unified Monitoring and Analysis Platform

SIEM KUMA

Ключевые области ИБ в индустриальной среде

- Защита от ВПО и сложных угроз
- Устройство и поддержание процессов SOC для индустриальной среды
- Кросс-продуктовые (XDR-like) сценарии реагирования
- Управление уязвимостями
- Внешние сервисы мониторинга событий ИБ
- Инвентаризация активов
- Безопасность коммуникаций с IoT
- Технологии виртуализации сетевой функции для защиты индустриальной среды

Защита от ВПО и сложных угроз

EDR функционал
для проактивного поиска
угроз

Использование данных
Threat Intelligence

Retro-scan на узлах
в течение ограниченного
периода времени

Проверка конечных точек с
ограничениями по
установке защитного ПО

Использование ICS
MITRE для обнаружения
сложных атак

Устройство и поддержание процессов SOC для индустриальной среды

Kaspersky
Unified Monitoring
and Analysis Platform

Интеграция

Тесная интеграция с решениями для защиты конечных точек и мониторинга индустриальной сети

Гибкость

Модульность и горизонтальная масштабируемость

Эффективность

Эффективность использования в изолированной среде

Детектирование

Необходимость детектирования угроз на границе сегментов (cross-segment detection and kill-chain)

ГОССОПКА

Поддержка форматов для передачи данных в ГОССОПКА

Консалтинг

Услуги SOC консалтинга

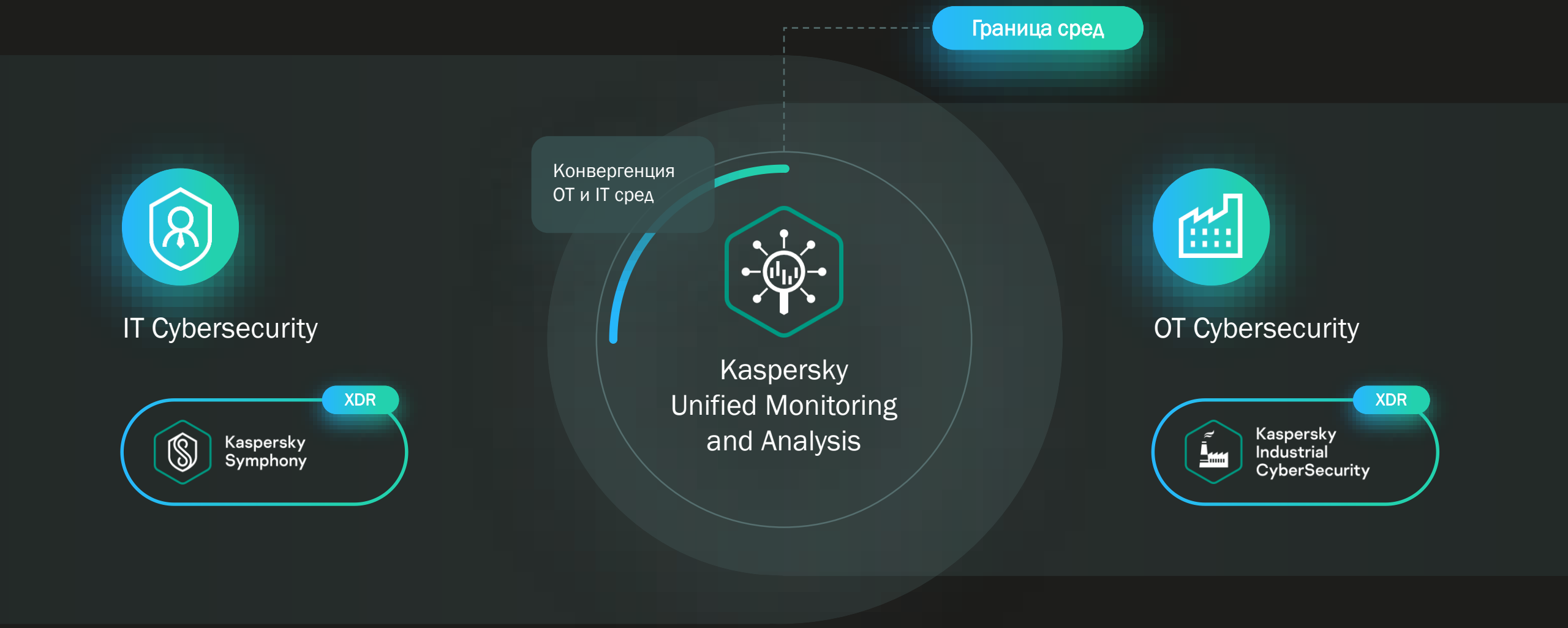
XDR

Использование в рамках OT XDR концепции

Цельное предложение для защиты OT и IT сред

Цельное предложение для защиты OT и IT сред

Цельное предложение для защиты OT и IT сред



Управление уязвимостями

Реализован собственный OVAL интерпретатор

Реализован механизм активного опроса узлов

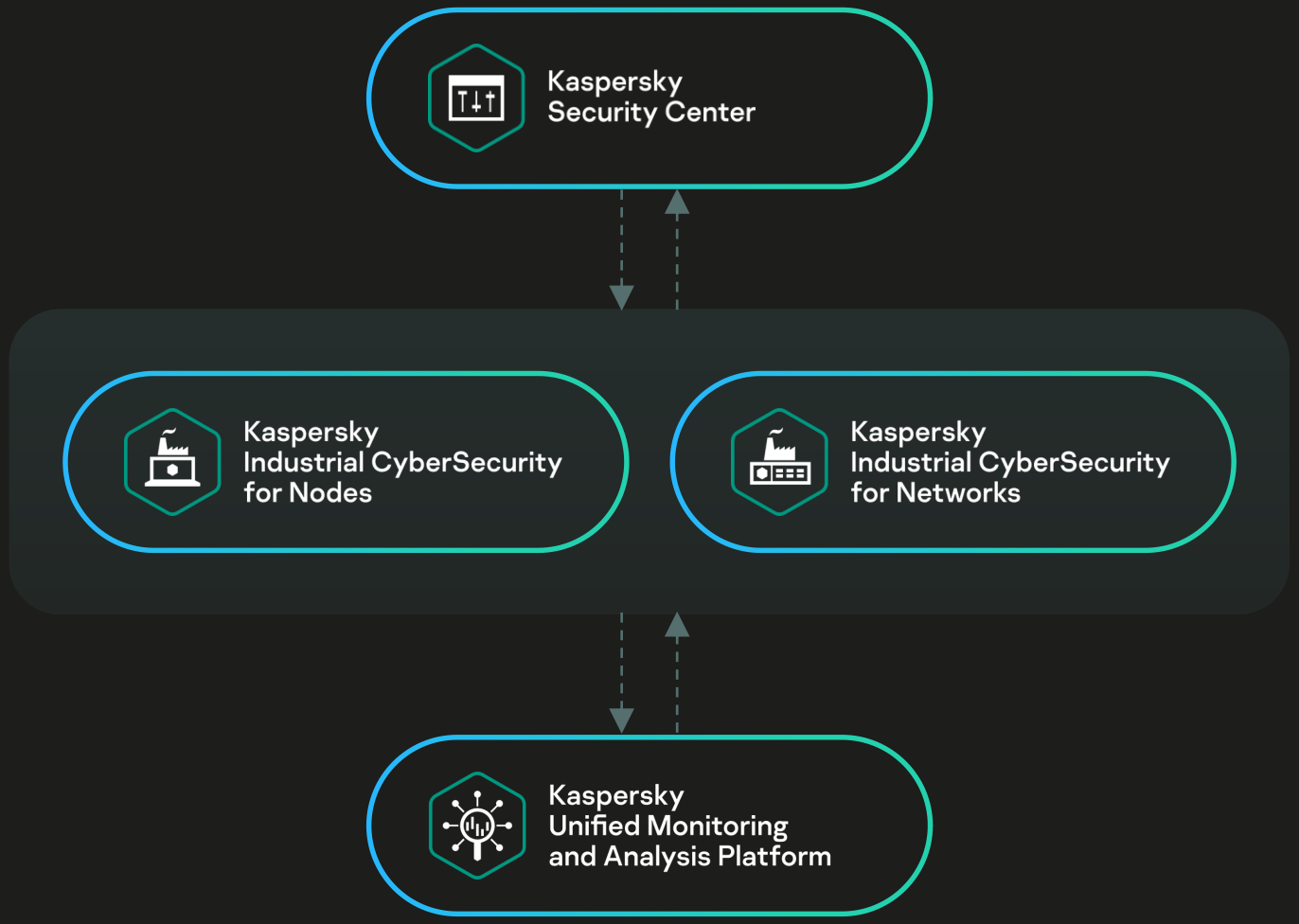
Кроме проверки уязвимостей прошивки PLC как одного из атрибутов узла — появляется возможность контроля уязвимостей ICS приложений

Подключены Банк данных угроз безопасности информации:

- ФСТЭК РФ
- База ICS CERT

Для многих уязвимостей OVAL база ICS CERT обогащена сценариями реагирования без установки обновления уязвимого ПО

Кросс-продуктовые сценарии реагирования



Инвентаризация

Обогащение представления, полученного при помощи сетевого сканирования, за счет данных с приложения на конечной точке

Корреляция событий

Учет в правилах корреляции KUMA SIEM параметров сетевых устройств и результатов формализованной оценки рисков (risk score)

Реагирование с использованием сетевого оборудования

Предопределенные сценарии реакции с использованием API сетевого оборудования через custom connector к API (на сегодня только «де-авторизация» узла)

Анализ событий

Объединение телеметрии с конечных точек (атрибуты учетных записей, соединений, использование неавторизованных флэшек) с данными о сетевом окружении для проверки по ICS MITRE базе и построения единой карты процессов атаки

Использование виртуализации сетевой функции (SD-WAN)

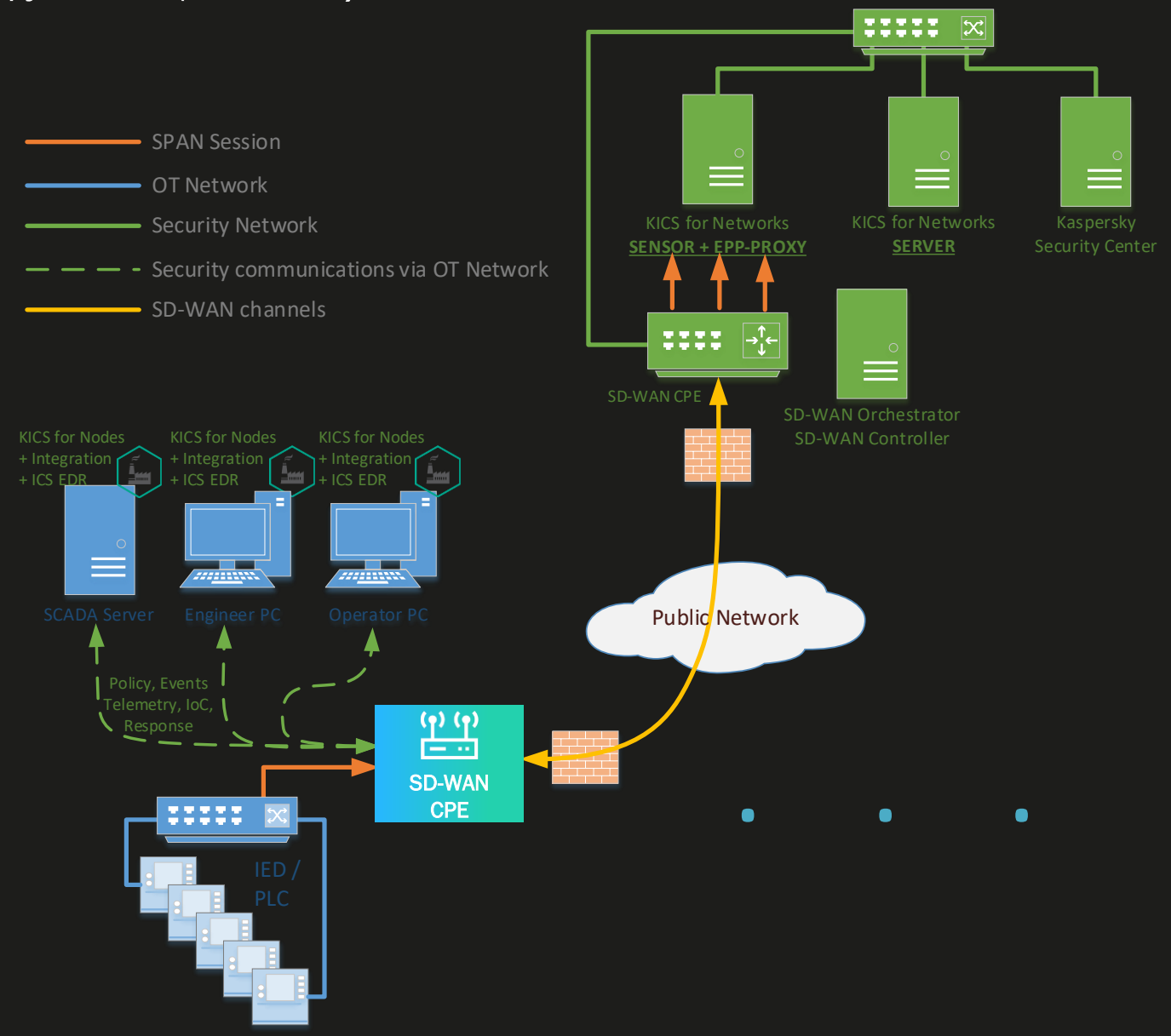
Единая точка входа для KICS4Networks

Разделение потоков данных от разных площадок

Упрощение подключения новых площадок

Кроме зеркала трафика возможно удаленное взаимодействие с ИБ решениями на конечных точках

Подключение географически распределённых объектов в единую инфраструктуру мониторинга сети



Единая концепция промышленной кибербезопасности

Kaspersky
OT CyberSecurity

Технологии

Полный арсенал защитных решений, протестированных вендорами АСУ ТП

Знания

Достоверная аналитика угроз в АСУ ТП и специальные тренинги

Экспертиза

Набор экспертных сервисов для комплексной промышленной кибербезопасности

Состав Kaspersky OT CyberSecurity

Технологии

Промышленный XDR и SIEM

Kaspersky Unified Monitoring and Analysis Platform

XDR

Kaspersky Industrial CyberSecurity for Networks

Kaspersky Industrial CyberSecurity for Nodes
+ встроенный EDR

Специализированные решения

Kaspersky SD-WAN

Kaspersky Antidrone

Kaspersky Machine Learning for Anomaly Detection

Решения на базе KOS

Kaspersky IoT Infrastructure Security

Kaspersky Secure Remote Workspace

Знания

Аналитика об угрозах

Kaspersky ICS Threat Intelligence

Kaspersky Ask the Analyst

Kaspersky Digital Footprint Intelligence

Повышение осведомленности

Kaspersky Security Awareness

Тренинги для специалистов

Kaspersky ICS CERT Training

Экспертиза

Анализ защищенности

Kaspersky ICS Security Assessment

Управляемая защита

Kaspersky Managed Detection and Response

Скорая помощь

Kaspersky Industrial Emergency Kit

Kaspersky Incident Response

Почему Kaspersky?

Глобальное присутствие, опыт и знания мирового уровня

ICS CERT

Собственное международное подразделение ICS CERT

Высокий статус в индустрии безопасности IT/OT-систем

Доказанная эффективность технологий и соответствие стандартам

Более 80 сертификатов о совместимости с решениями вендоров АСУ ТП

Спасибо!

kaspersky