kaspersky

Kaspersky Industrial Cybersecurity Conference 2021

Вениамин Левцов

Директор глобального центра экспертизы по корпоративным решениям, «Лаборатория Касперского», Россия

#KasperskyICS

Чат конференции: https://kas.pr/kicscon

Kaspersky Industrial Cybersecurity Conference 2021

Стратегия трансформации решений Лаборатории Касперского для промышленных сред

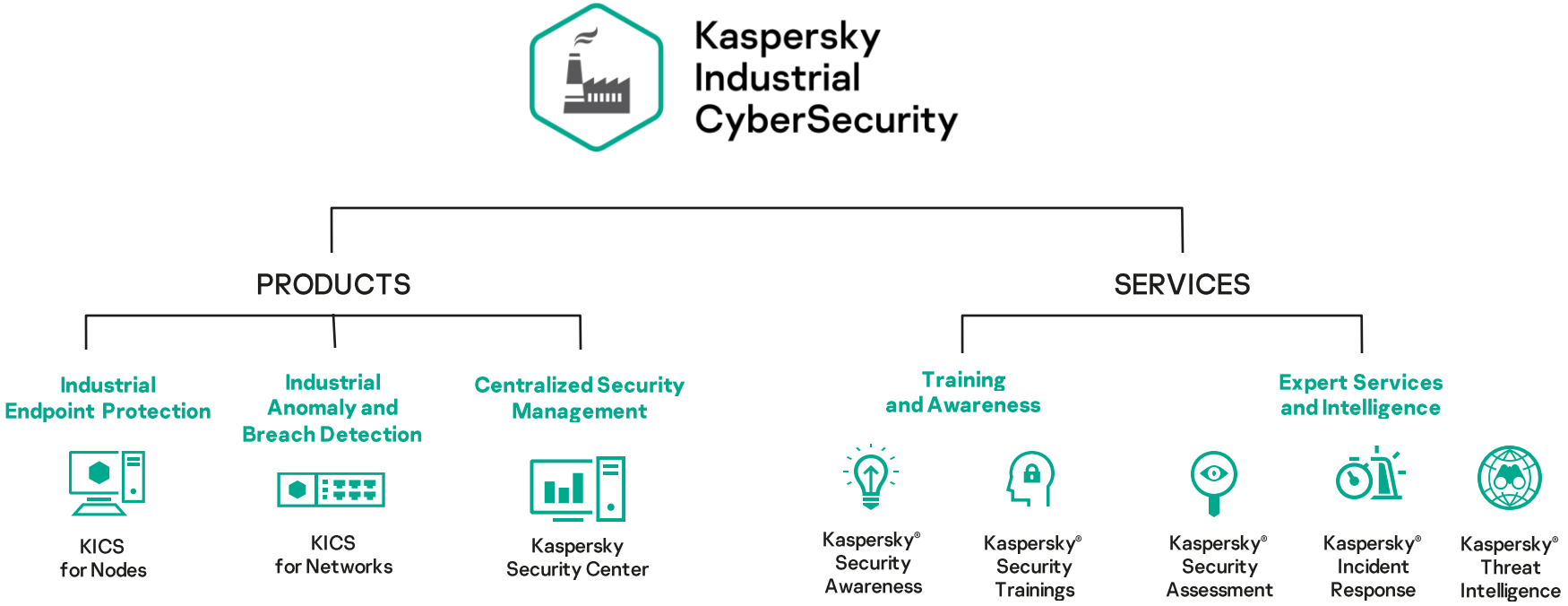
Вениамин Левцов
Директор Центра экспертизы по корпоративным решениям

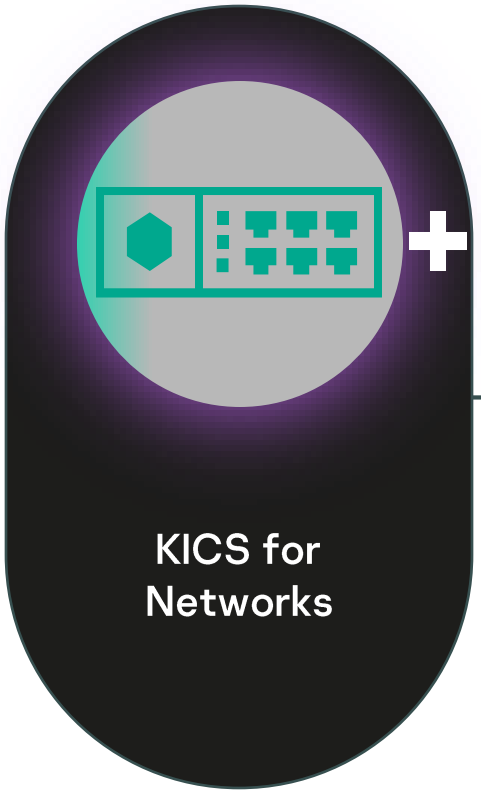
kaspersky

Некоторые глобальные тенденции, значимые для ИБ промышленных сред

- Растущая связанность ИТ и промышленных сетей
- Тенденция снижения изолированности промышленных сред
- Усложнение ситуации с уязвимостями решений для промышленных сред
- Усложнение требований соответствия нормативным актам и необходимость автоматизации в этой области

Предложение Лаборатории Касперского для защиты промышленных сред



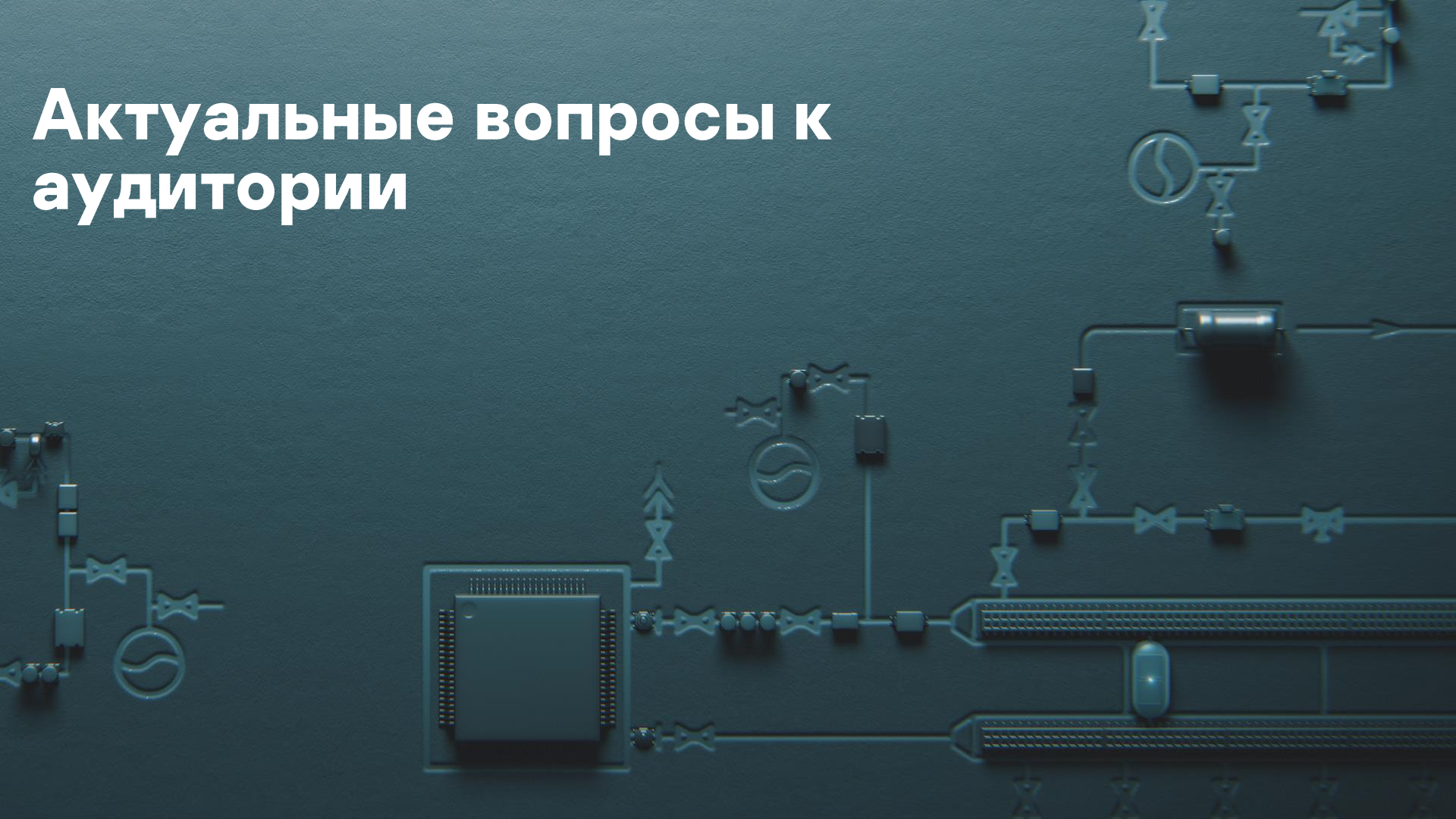


- Самодостаточный продукт для анализа промышленного трафика -> элемент комплексного решения
- Задачи инвентаризации объектов среды
- Отслеживание соответствия требованиям (control compliance)
- Развитие DPI возможностей, подключение новых протоколов как баз

Технологическое развитие решения для защиты конечных точек

- Развитие функционала расширенного обнаружения, расследования и реагирования на угрозы (EDR, SIEM)
- Доверенная «флэшка» (перенос данных, аудита изолированных, устаревших узлов)
- Более тесная интеграция с другими решениями (инвентаризация, контроль уязвимостей, compliance)
- Защита узлов на Linux

Актуальные вопросы к аудитории



Изолированность промышленных сред	• Считаете ли вы обязательным строгую изоляцию промышленных подсетей? • Чем приходится жертвовать? • Какие есть перспективы сервиса удаленного обнаружения угроз (MDR для промышленных сред)?
Расширенные средства обнаружения угроз	• Видите ли перспективы в использовании «песочниц»? • Сценарии MITRE ATT&CK, специфичные для промышленных сред, готовы использовать? • Есть ли потребность в сборе «сырой» телеметрии? • OT-SOC как часть единого SOC – это актуально?

Security Operations Center для промышленных сред

Целевая архитектура SOC на базе решений Лаборатории Касперского

KUMA как платформа для IT/OT SOC

- Высокая производительность, простая горизонтальная масштабируемость, низкие системные требования
- Модульность, микросервисность – гибкость использования в т.ч. для нужд IT/OT SOC
- Интегральная связанность с другими продуктами в том числе KICS
- Лицензирование, упрощающее покрытие площадок
- Реализация элементов концепции XDR
- Встроенный движок Threat Intelligence (ISC Feed)

Данные об угрозах

- Развитие активности ISC CERT, https://ics-cert.kaspersky.ru/
- Фокус на рост полноты потоков данных об уязвимостях
- Банк данных угроз безопасности информации ФСТЭК РФ, https://bdu.fstec.ru/vul
- National Vulnerability Database, https://nvd.nist.gov/vuln
- Базы приземляются в KICS for Network
- Развитие продуктов с учетом автоматизации реакции на уязвимости

Стратегия трансформации: от приложений – к доменам ИБ

Стратегическая трансформация от отдельных решений – к предложению для доменов ИБ

Инвентаризация объектов сети

- Обогащение данными с локальных агентов
- Активный опрос узлов сети
- Улучшения для сканирования уязвимостей

Оркестрирование системы ИБ

- Развитие практики проектирования, внедрения и поддержки OT-SOC на KUMA
- Управление всеми решениями KICS из Open Single Management Console в концепции XDR
- Инструменты определения кросс-сетевых сценариев атак (IT <-> OT)

Потоки данных об угрозах

- ISC threat feeds – обогащение из разных источников, предопределенные правила
- CVEs feeds – максимальное обогащение

Техническая защита объектов сети

- Глубокая интеграция собственных решений KICS
- Интеграция с активным сетевым оборудованием для обогащения детекта и реагирования
- Предложение для сетей с доступом из Интернета (MDR) и изолированных узлов
- Поддержка различных сценариев расширенного детекта и реагирования (EDR)

Control Compliance

- Интегрированное использование решений KICS с предустановленной базой правил соответсивмя, интерпретатором и хранилищем телеметрии

Сервисы оценки состояния, обнаружения угроз

- Оценка защищенности конечных точек
- Анализ сетевых потоков с KICS for Network Portable
- Проведение штабных учений

Стратегия без тактики — это самый медленный путь к победе.
Тактика без стратегии — это просто суета перед поражением.

Сунь Цзы,
древнекитайский стратег и мыслитель

Спасибо за ваше внимание

Вениамин Левцов,
Директор глобального Центра экспертизы по корпоративным решениям

veniamin.levtsov@kaspersky.com

kaspersky