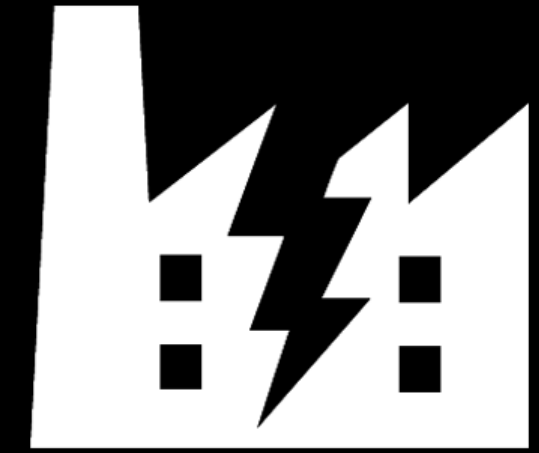
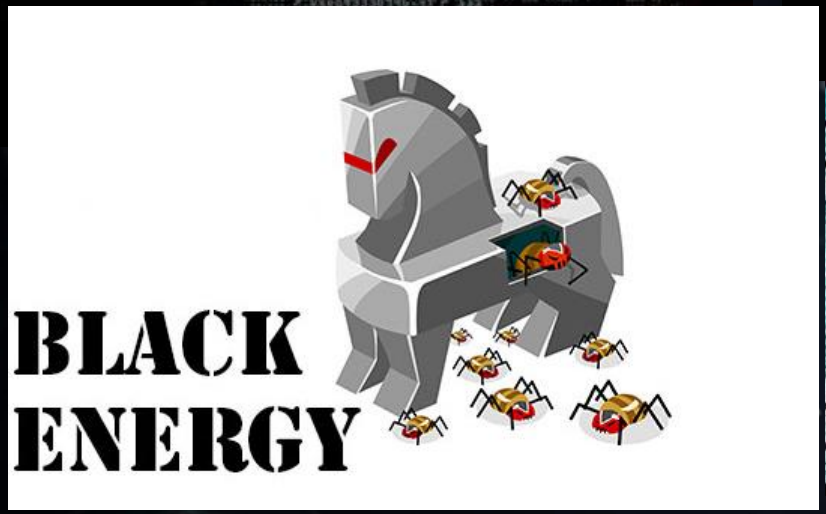
Атаки на критическую инфраструктуру и как от них защищаться.

KASPERSKY


STUXnet


INDUSTROYER

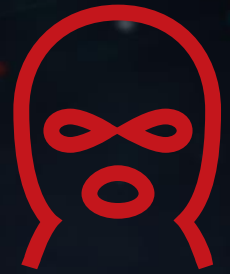

BLACK
ENERGY


LOCKERGOGA

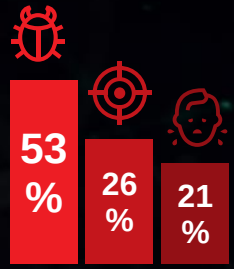
А что «в полях»?

Результаты опроса 359 специалистов,
отвечающих за ИБ АСУ по всему миру

в 54% промышленных компаний
произошло от 1 до 5 инцидентов кибербезопасности
за последние 12 месяцев



Высокая вероятность проникновения
квалифицированных и мотивированных злоумышленников
ОЧЕВИДНА



Типовое вредоносное ПО
является самой частой причиной киберинцидентов

KASPERSKY lab

44 %

USB-накопителей содержат вредоносные файлы

26%

угроз могут вызвать потерю контроля

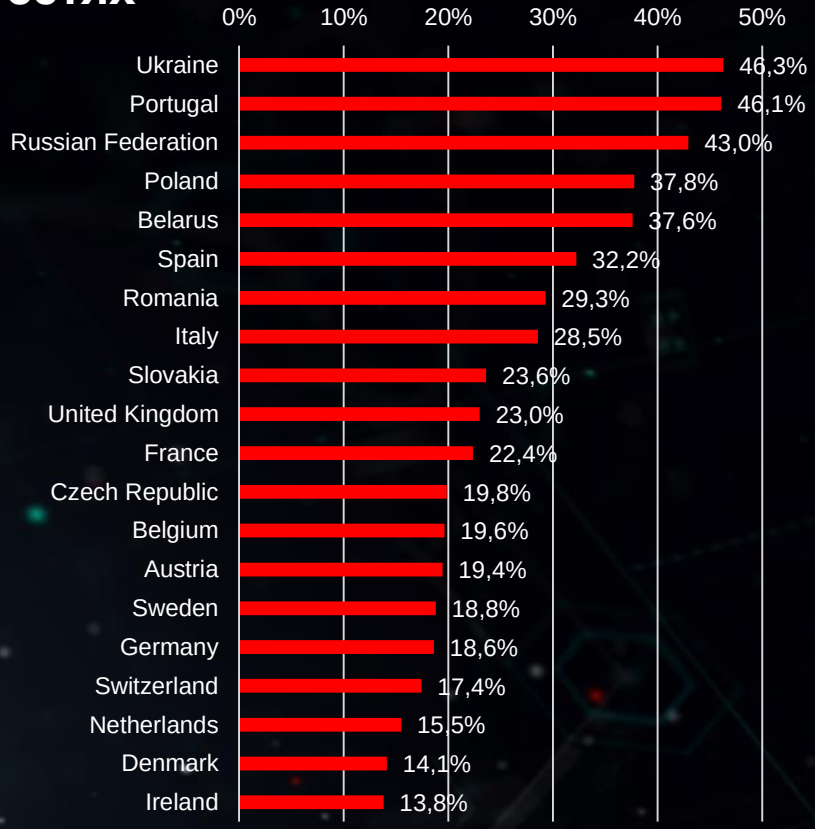
2% - Triton
2% - Stuxnet
1% - WannaCry

Данные ЛК об угрозах в промышленных сетях

KASPERSKY LAB
ICS CERT

Обозревает состояние защиты **более 100 000** промышленных узлов по всему миру

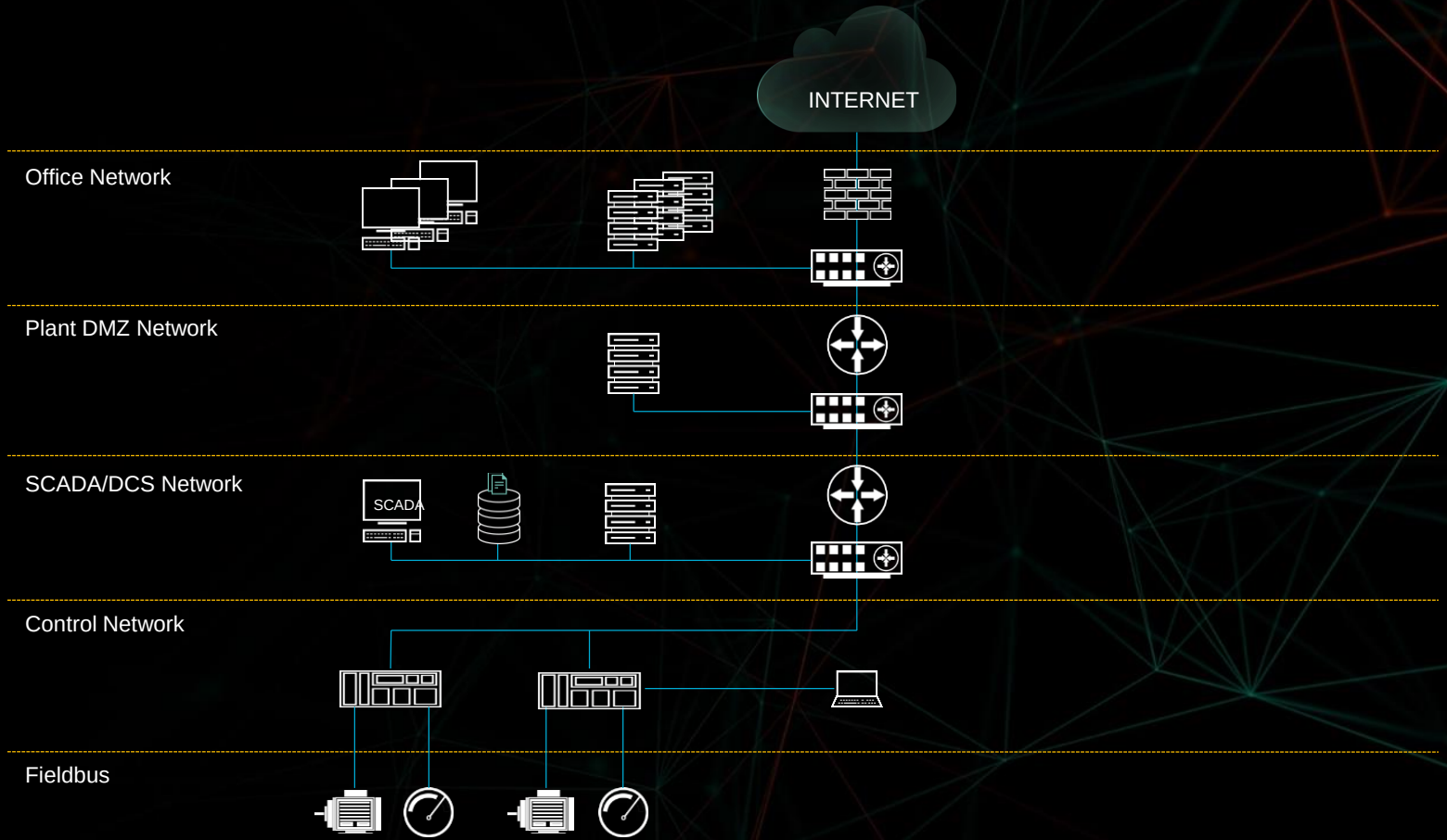
В 2018 ГОДУ
БОЛЕЕ 40%
КОМПЬЮТЕРОВ В АСУ ТП В МИРЕ ПОДВЕРГЛИСЬ АТАКЕ



Статистика Kaspersky Security Network

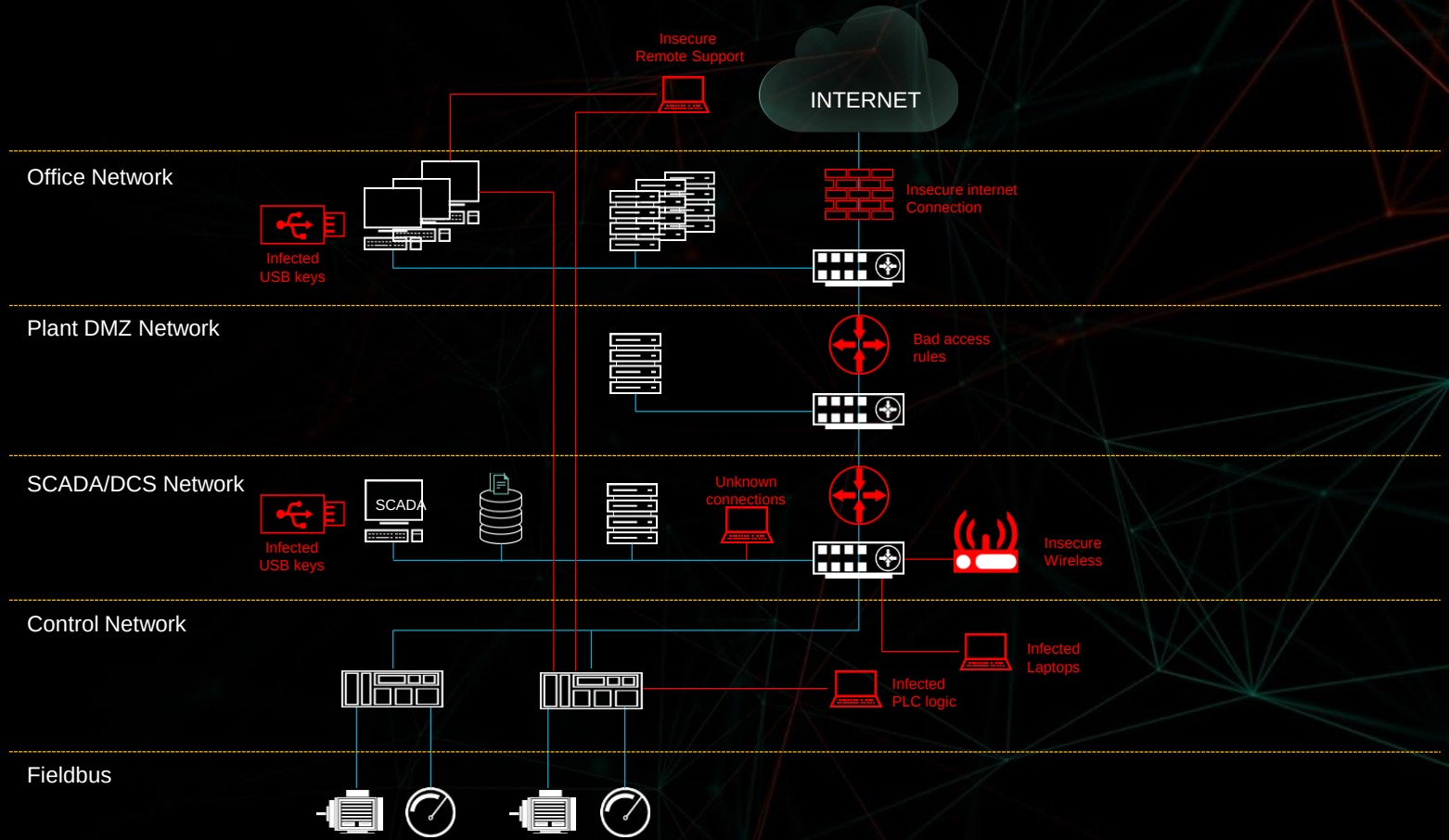
KASPERSKY lab

Типовая архитектура технологической сети



KASPERSKY lab

Векторы кибератак



KASPERSKY lab

НАШИ ИНИЦИАТИВЫ ПО ЗАЩИТЕ ПРОМЫШЛЕННЫХ ПРЕДПРИЯТИЙ

Kaspersky® Industrial CyberSecurity

KICS - набор продуктов и сервисов для защиты систем промышленной автоматизации.

Запущен в конце 2015 г.

Несколько десятков инсталляций в разных странах мира

KASPERSKY LAB
ICS CERT

KL ICS Cyber Emergency Response Team - инициатива ЛК, нацеленная на защиту промышленных предприятий

Официально запущен в конце 2016

Более **130** уязвимостей 0-го дня в ниболее популярных системах промышленной автоматизации

KSN

Отслеживаем состояние ИБ

более 100 000 промышленных узлов

KASPERSKY lab

«ЛАБОРАТОРИЯ КАСПЕРСКОГО» ОТМЕЧЕНА В ЧЕТЫРЕХ КАТЕГОРИЯХ ОТЧЕТА GARTNER ПО ПРОМЫШЛЕННОЙ БЕЗОПАСНОСТИ «COMPETITIVE LANDSCAPE: OPERATIONAL TECHNOLOGY SECURITY»

Решение «Лаборатории Касперского» для защиты промышленной инфраструктуры Kaspersky Industrial CyberSecurity было упомянуто в 4 продуктовых категориях отчета:

- ✓ Защита конечных узлов АСУ ТП
- ✓ Мониторинг промышленной сети
- ✓ Обнаружение аномалий, Реагирование на инциденты, Отчетность
- ✓ Сервисы промышленной кибербезопасности

Gartner

Competitive Landscape: Operational Technology Security, Ruggero Contu, 29 October 2018.

Kaspersky Industrial CyberSecurity

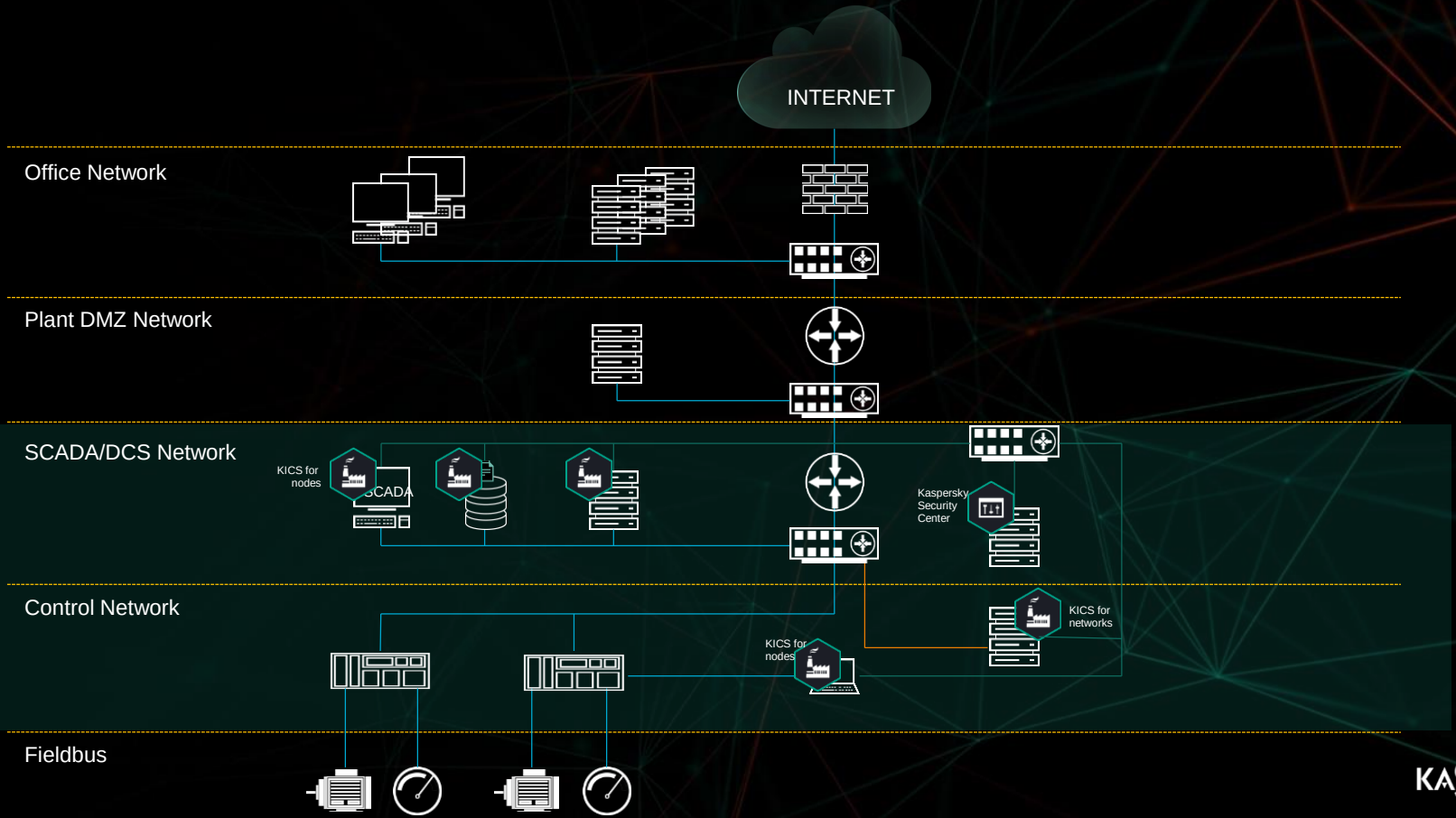
PRODUCTS

- Industrial Endpoint Protection
  - KICS for Nodes
- Industrial Anomaly and Breach Detection
  - KICS for Networks
- Centralized security management
  - Kaspersky Security Center

SERVICES

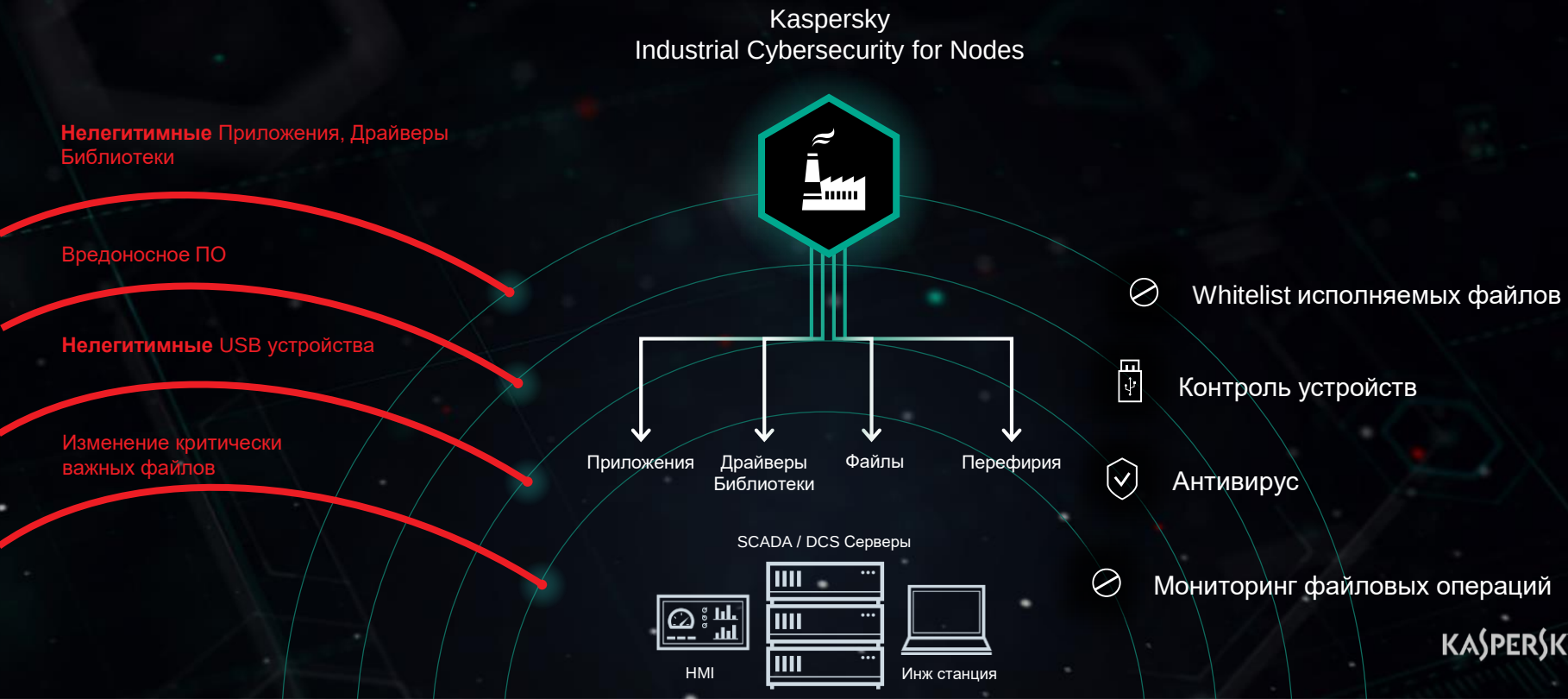
- Training and awareness
  - Kaspersky® Security Awareness
  - Kaspersky® Security Trainings
- Expert services and intelligence
  - Kaspersky® Security Assessment
  - Kaspersky® Incident Response
  - Kaspersky® Threat Intelligence

KASPERSKY INDUSTRIAL CYBER SECURITY



KASPERSKY lab

Векторы атак на промышленные ПК и серверы



«Офисные» средства защиты в технологических сетях

Корпоративные средства защиты

- Проактивные технологии
- Мониторинг работы приложений

ПРОБЛЕМЫ В ТЕХНОЛОГИЧЕСКОЙ СЕТИ:

- Высокое портребление ресурсов защищаемой системы
- Высокая вероятность ложного срабатывания

КЛАССИЧЕСКОЕ РЕШЕНИЕ:

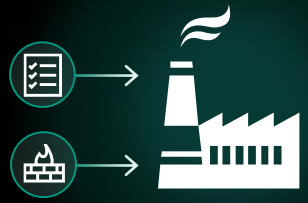
Тонкий «тюнинг» средств защиты:

- Исключение областей проверок
- Отключение защитных технологий
- Особые регламенты работы

Промышленная кибербезопасность

Статичный набор софта

Регламентированные подключения ко внешним сетям



Промышленные средства защиты

- Ограничение программной среды
- Периодические проверки

ТРЕБОВАНИЯ К СПЕЦИАЛИЗИРОВАННОМУ ПРОДУКТУ ДЛЯ ЗАЩИТЫ КОМПОНЕНТ АСУ ТП:

- Прогнозируемое портребление ресурсов защищаемой системы
- Отсутствие ложных срабатываний
- Легкая установка и настройка
- Поддержка старых ОС

KICS for Nodes – детали реализации

Ограничение программной среды

- Типовой сценарий - Запрет по умолчанию
- Локальная инвентаризация исполняемых файлов (exe, bat, dll, reg …)
- Белые списки по HASH, цифровой подписи

Защита от вредоносного ПО

- Антивирусные проверки по требованию
- Многопроцессная архитектура PHOENIX

Контроль устройств

- Белый список устройств

Ограничение сетевых подключений

- Управление Firewall Windows
- Ограничение WiFi подключений

Контроль целостности файлов

- Мониторинг файловых операций

KICS for Nodes – детали реализации

Обнаружение новых угроз

Пассивный анализ логов ОС

Поддержка старых ОС

Поддержка Windows XP SP2/ Win Server 2003 и новее

Контроль проектов ПЛК

Обнаружение изменений управляющих программ в ПЛК Siemens, Schnieder

Обновление баз сигнатур

Локальные источники обновлений

Обновление через USB

Установка/Удаление/Обновление

Установка/удаление без перезагрузки

Установка отдельных компонент

Индивидуальный набор компонент

Установка без графической консоли

KASPERSKY INDUSTRIAL CYBER SECURITY - Networks

KICS FOR NETWORKS

Контроль целостности технологической сети и IDS

- Обнаружение атак/эксплуатации уязвимостей
- Инвентаризация в технологической сети
- Обнаружение нелегитимных сетевых взаимодействий

Расследование инцидентов

- Отображение наиболее важных
- Логирование и событий и трафика

Интеграция

Kaspersky Security Center
Syslog Server
Mail Server
SIEM

Мониторинг

- Параметров технологического процесса
- Обнаружение нелитимных изменений

Обнаружение конфигураций ПЛК

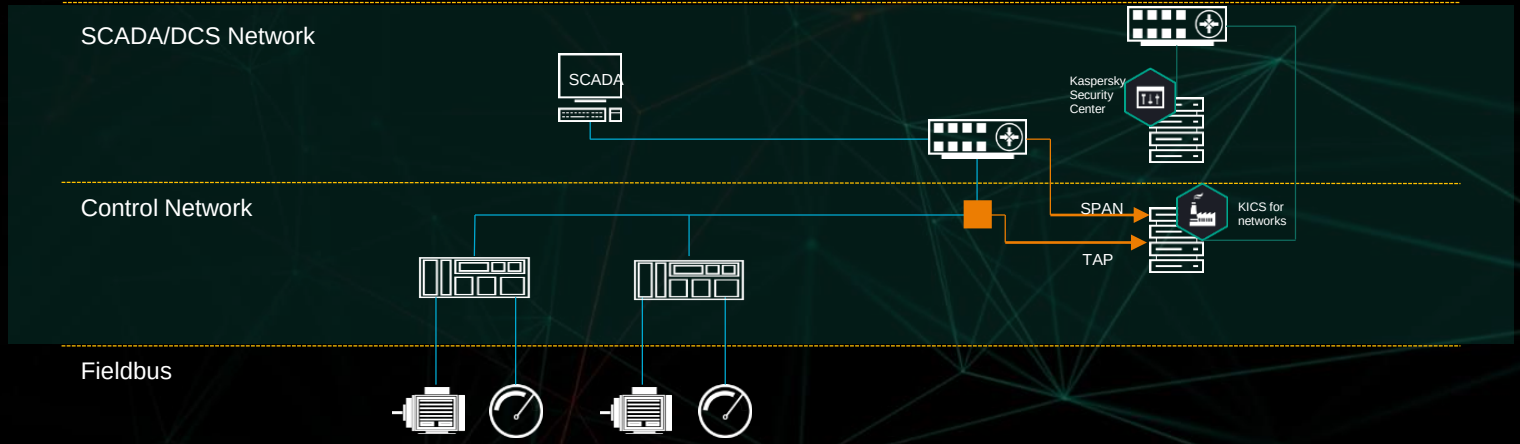
- Настраиваемая реакция на потеницально опасные команды к ПЛК
- KICS for network обнаруживает: Authentication, start/stop PLC, read/write PLC, read/write PLC configuration, etc

KASPERSKY lab

Сценарии использования KICS FOR NETWORKS

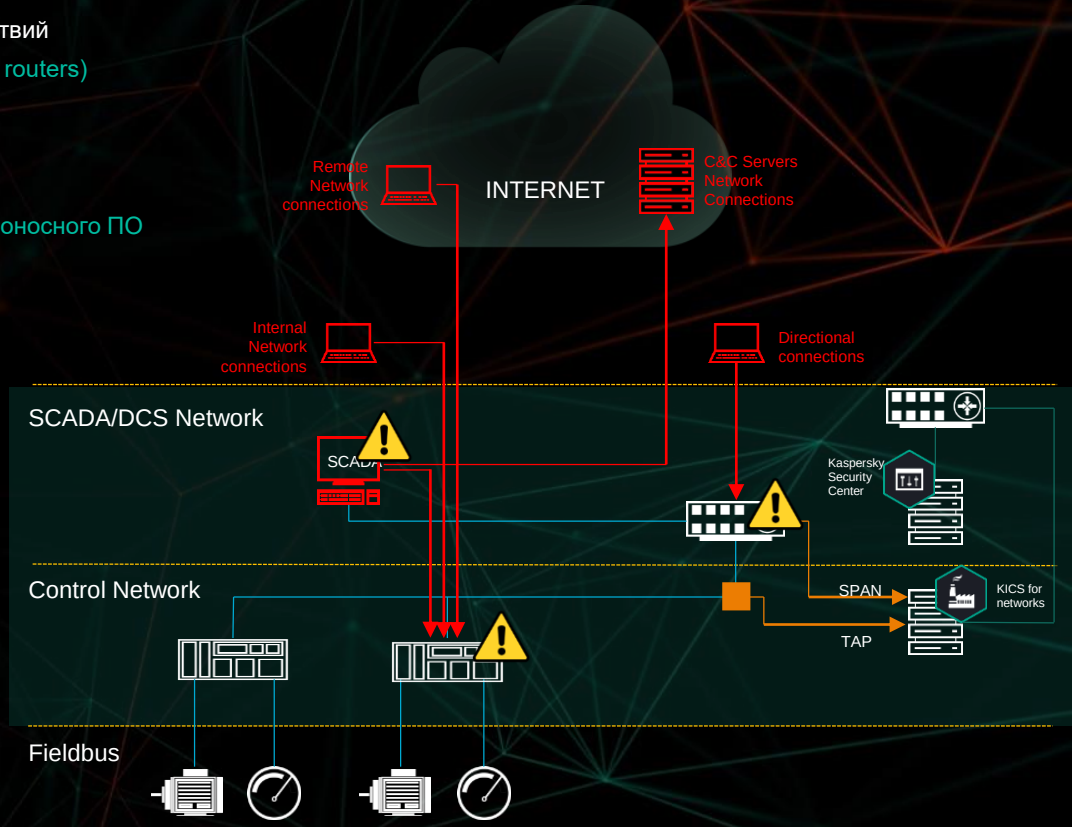
Пассивное подключение к промышленной сети:

- SPAN порт
- TAP устройство

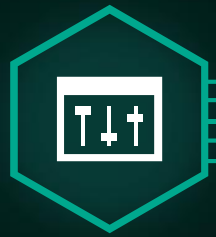


Сценарии использования KICS FOR NETWORKS

1. Инвентаризация активов в технологической сети и их взаимодействий
   1. Устройства в промышленной сети (PCs, Servers, laptops, PLCs, routers)
   2. Действительные коммуникации
2. Обнаружение нелегитимных связей и коммуникаций
   1. Новые хосты в сети
   2. Удаленный доступ, Сканирование сети, Распространение вредоносного ПО
3. Обнаружение вторжений(IDS)
   1. Эксплуатация уязвимостей
   2. Брутфорс Атаки
4. Обнаружение критических команд к ПЛК (DPI)
   1. Чтение/запись программы/проекта ПЛК
   2. Попытки аутентификации
   3. Start/stop команды
   4. Чтение/запись конфигураций
   5. И прочее…
5. Контроль параметров технологического процесса (DPI)
   1. Границы конкретных параметров (Min < X < Max)
   2. Связи между параметрами и значениями (if..and/or..if..then)
   3. Попытки фрода
   4. Ошибки конфигурации
6. Сбор и хранение информации для расследования инцидентов
   1. Хранение логов и событий безопасности



Возможности централизованного управления



Kaspersky® Security Center

SYSTEMS MANAGEMENT

Обнаружение уязвимостей и патч менеджмент
Инвентаризация ПО и оборудования
Удаленное управление

УПРАВЛЕНИЕ ПОЛИТИКАМИ

Групповые / Индивидукальные политики
Онлайн / Офлайн политики
Расписания и удаленный запуск задач

УВЕДОМЛЕНИЯ И ОТЧЕТНОСТЬ

Сбор, обработка и хранение событий
Формирование отчетов
SMS/Email уведомления

ИНТЕГРАЦИЯ С SIEM

ArcSiight, Splunk, QRADAR
И другие по SYSLOG

ИНТЕГРАЦИЯ С HMI

Отправка событий ИБ в SCADA
МЭК – 104 / OPC 2.0

Сертификация KICS

Локальные регуляторы

ФСТЭК: KICS for Networks – профиль «АВ3» уровня 3-В
KICS for Nodes – профиль «СОВ» уровня С-4

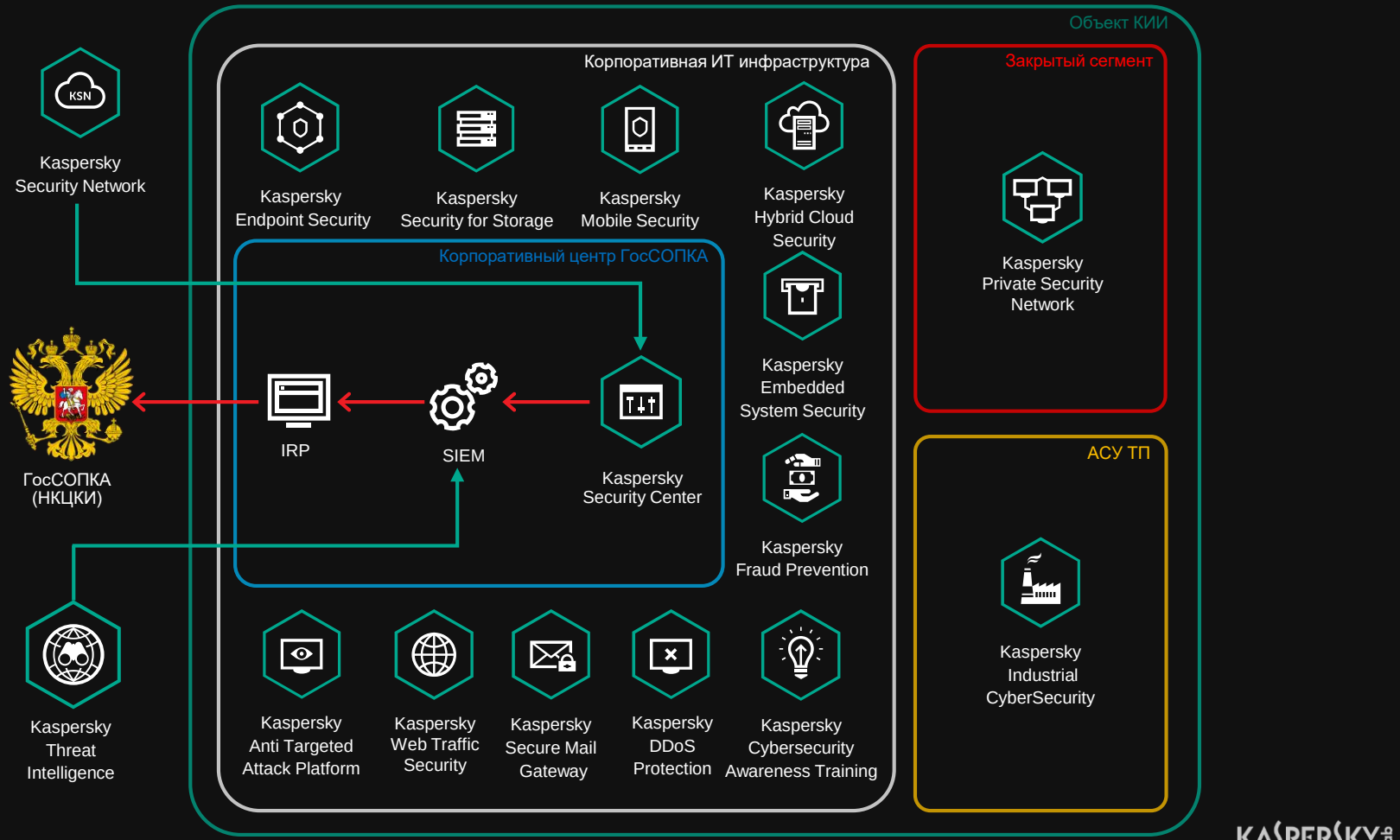
ФСБ: KICS for Networks – профиль «СОА**»** класса Г

Разработчики систем промышленной автоматизации

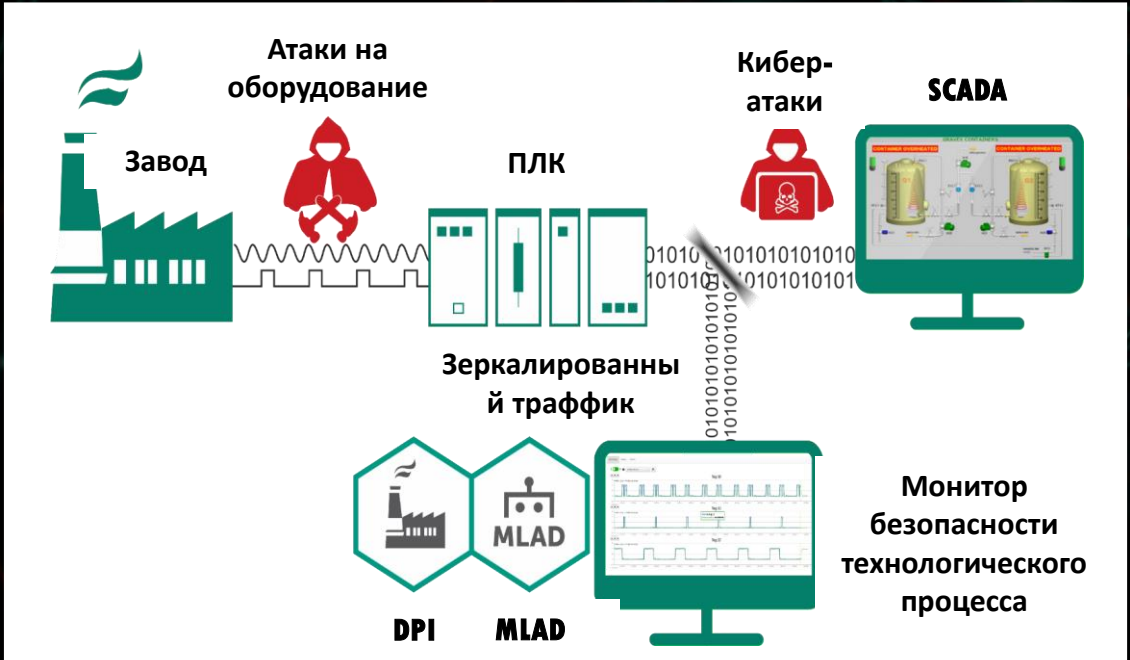
etm Professional Control
GE
EMERSON
КРУГ
YOKOGAWA
...
ICONICS Make the Invisible Visible
Schneider Electric
МОНИТОР ЭЛЕКТРИК
ЭнергопромАвтоматизация
ABB

ТРЕБОВАНИЯ ПРИКАЗА ФСТЭК 239 - KICS

- Идентификация и аутентификация
- Управление доступом
- Ограничение программной среды
- Защита машинных носителей информации
- Аудит Безопасности — Частично
- Управление обновлениями ПО
- Обеспечение доступности
- Защита технических средств
- Защита информационной системы — Частично
- Реагирование на компьютерные инциденты — Источник для SOC/SIEM
- Управление конфигурацией — Частично
- Предотвращение вторжений
- Обучение персонала
- Обеспечение целостности
- Антивирусная защита
- Планирование мероприятий по обеспечению ИБ
- Обеспечение действий в нештатных ситуациях



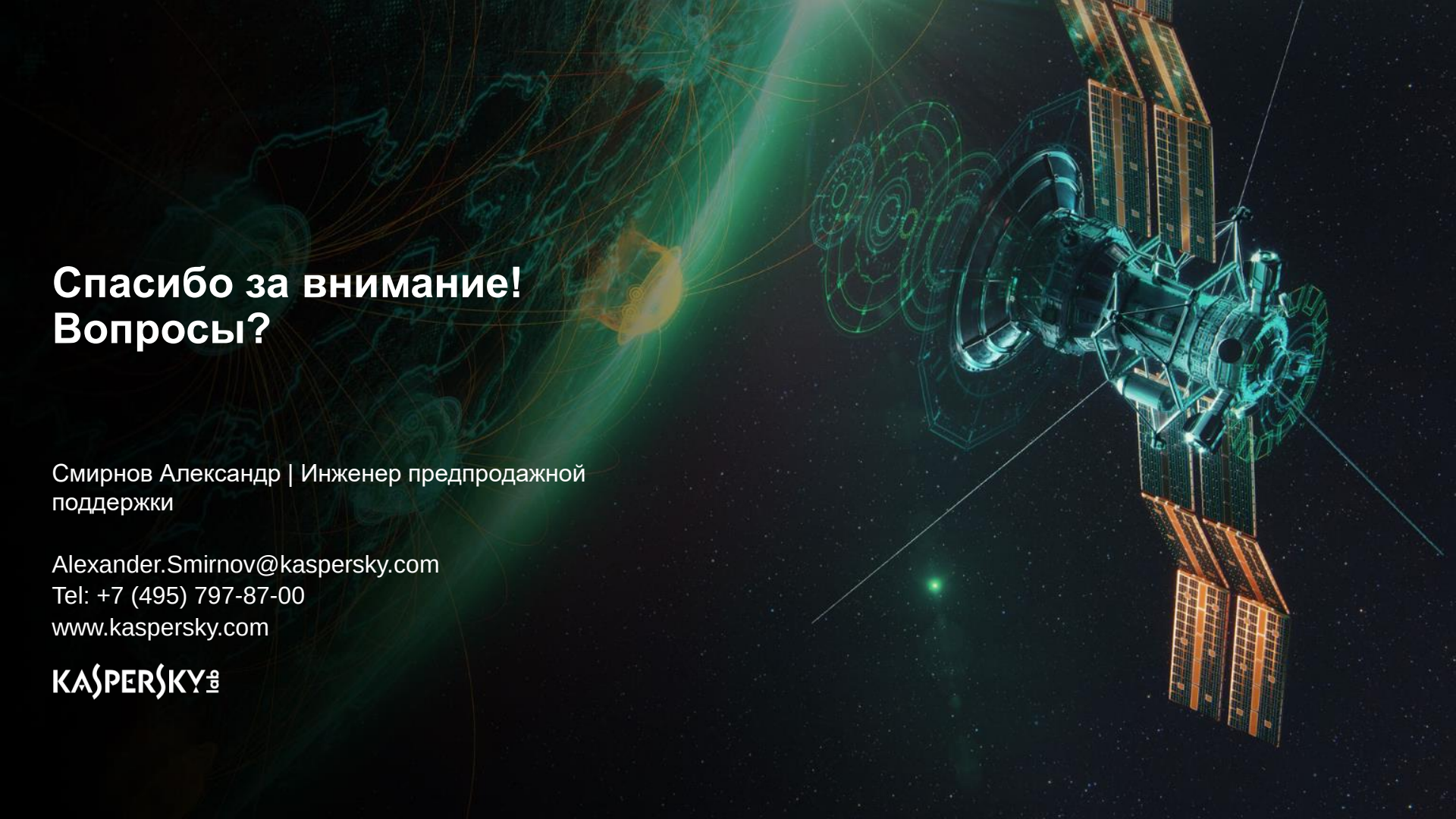
MLAD - Machine Learning for Anomaly Detection



- ✓ Непрерывно строит прогнозные значения телеметрии процессов
- ✓ Непрерывно сравнивает прогноз с реальными значениями
- ✓ Непрерывно осуществляет мониторинг ошибки прогноза
- ✓ Автоматически интерпретирует найденные аномалии
- ✓ Имеет возможность до-обучаться на новых данных

Ценность решения

- Раннее обнаружение аномалий
- Ретроспективный анализ эффективности контроля процессов
- Интерпретация аномалий
- Обнаружение редких аномалий (трудноуловимых для оператора)



Спасибо за внимание!
Вопросы?

Смирнов Александр | Инженер предпродажной поддержки

Alexander.Smirnov@kaspersky.com
Tel: +7 (495) 797-87-00
www.kaspersky.com

KASPERSKY