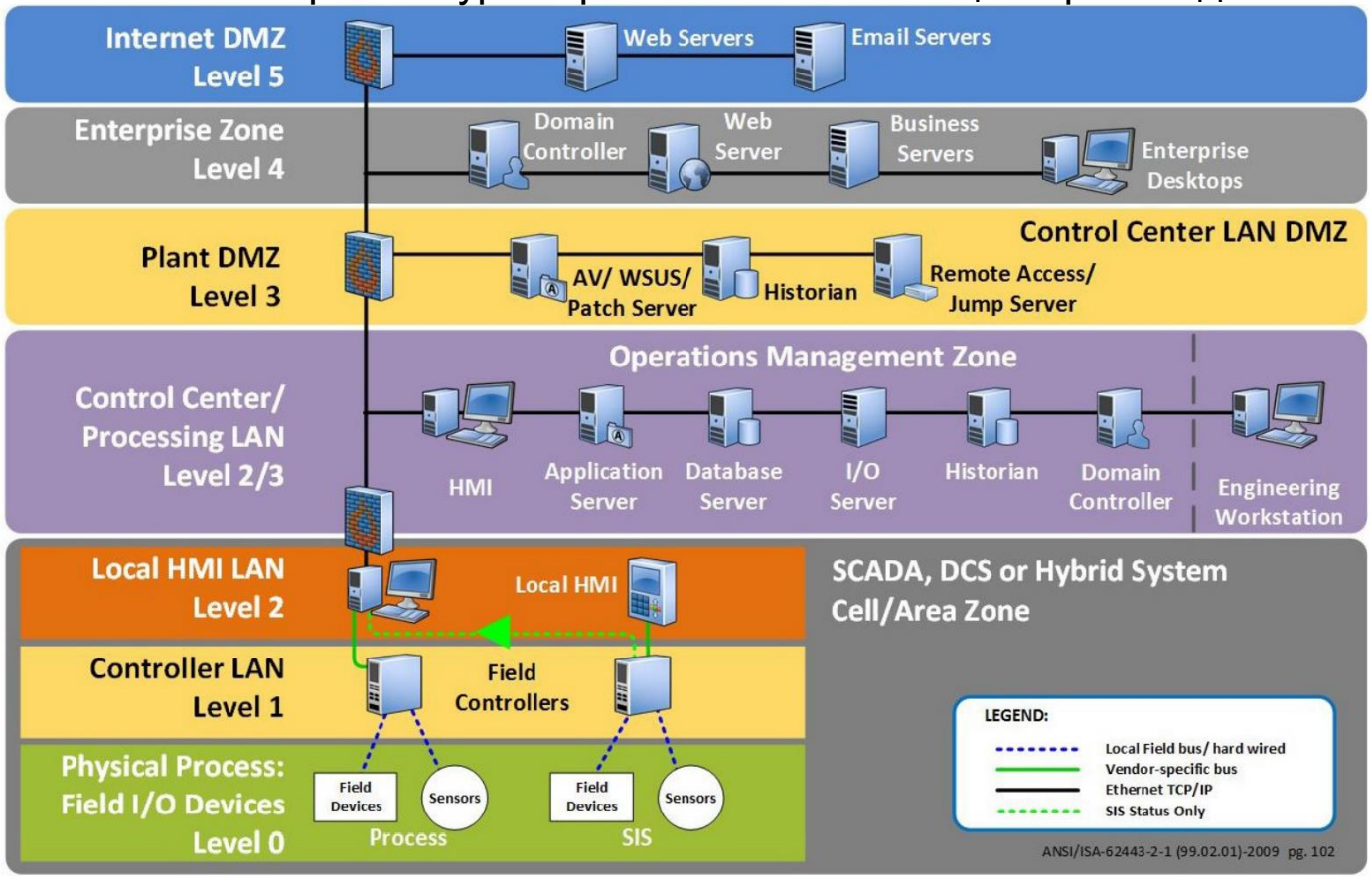
Kaspersky
Industrial
CyberSecurity

Kaspersky Industrial CyberSecurity в проектах СОБИ КВО – от дифференцированного подхода к интегрированной экосистеме

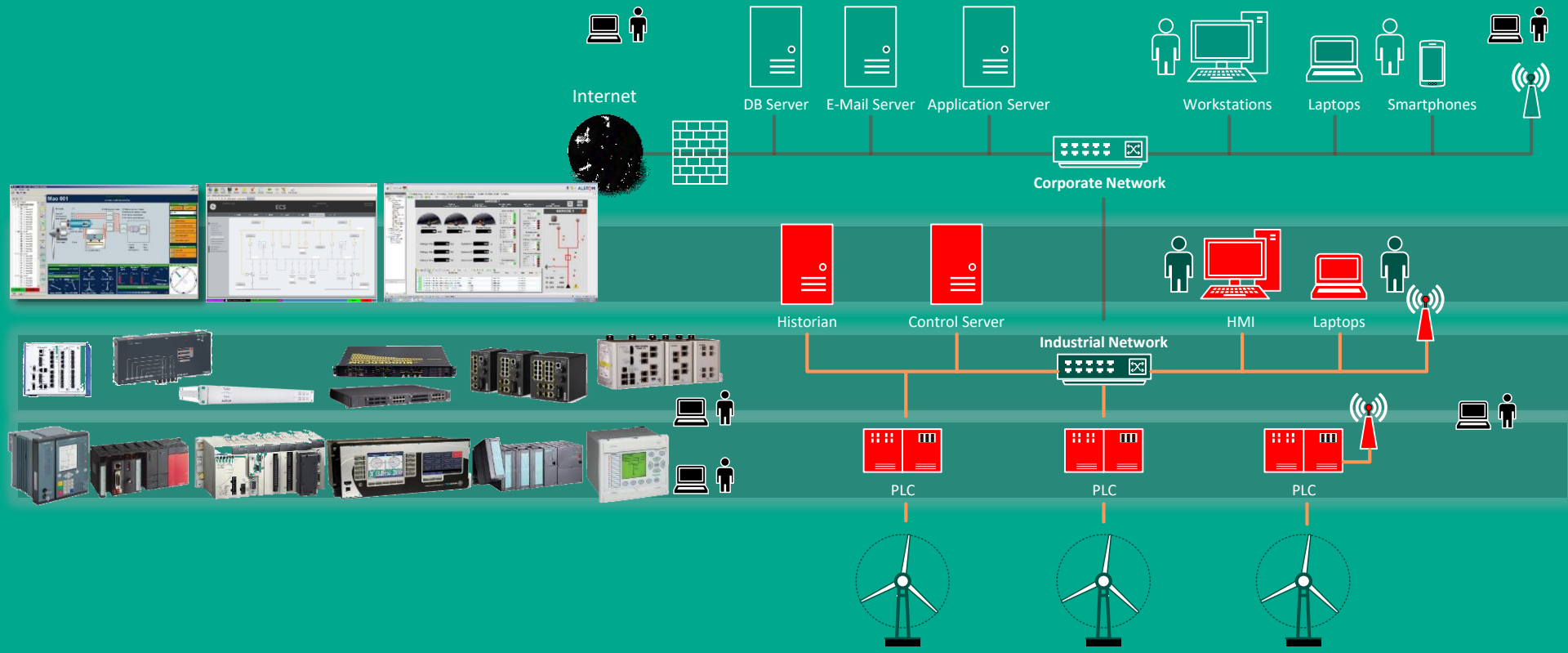
Азат Шайхутдинов
Менеджер проектов Kaspersky Industrial CyberSecurity

Усложнение архитектуры в рамках автоматизации производства

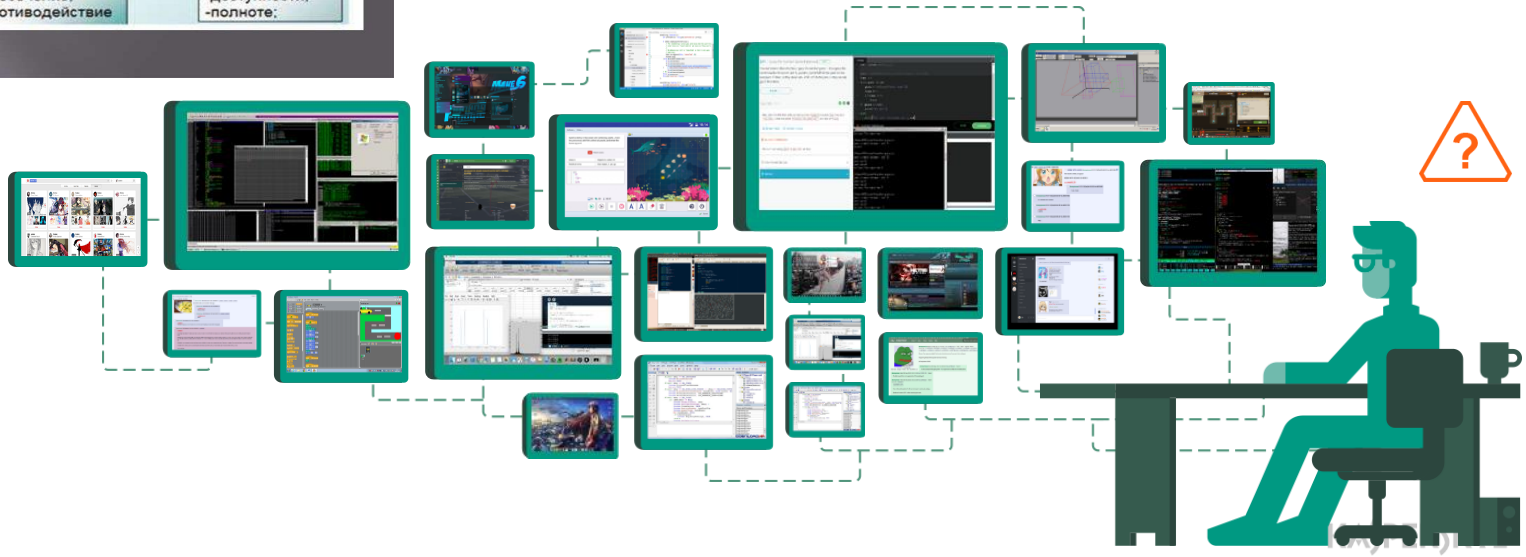


Kaspersky

Векторы атак и уровни уязвимостей



Как выстроить прозрачную и эффективную экосистему для управления СОБИ КВО?



Kaspersky

Kaspersky Industrial CyberSecurity – наш подход к защите АСУТП

CERT LEVEL

Исследование уязвимостей IoT и OT систем

Kaspersky®
Professional Trainings

TI Feeds, Аналитические отчёты

Kaspersky®
Threat Intelligence

Консалтинговые услуги

Kaspersky®
ICS CERT

SOC LEVEL

Тренинги по анализу и разбору событий в OT

Kaspersky®
Professional Trainings

OT Threat Data feeds

Kaspersky®
Threat Intelligence

SIEM Integration

Managed Protection Service

Kaspersky®
Managed Protection

Incident Response

Kaspersky®
Incident Response

PLANT LEVEL

Повышение осведомлённости по защите OT систем

Kaspersky®
Security Awareness

Специализированные решения

KICS
for Nodes

KICS
for Networks

Machine Learning
for Anomaly
Detection

Pen Test and Assessment

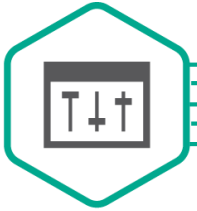
Kaspersky®
Security Assessment

Kaspersky

https://ics.kaspersky.ru/resources/

KASPERSKY lab

Kaspersky Security Center



Kaspersky Security Center

УПРАВЛЕНИЕ СИСТЕМОЙ

- Централизованная система сбора данных
- Централизованное развертывание ПО
- Обнаружение уязвимостей и управление обновлениями
- Расширенные возможности управления клиентами

ИНТЕГРАЦИЯ С SIEM

- ArcSight, Splunk, QRadar
- Syslog сервер

УПРАВЛЕНИЕ ПОЛИТИКОЙ

- Централизованное управление политикой безопасности
- Удаленное планирование и выполнение задач

ИНТЕГРАЦИЯ С ЧМИ

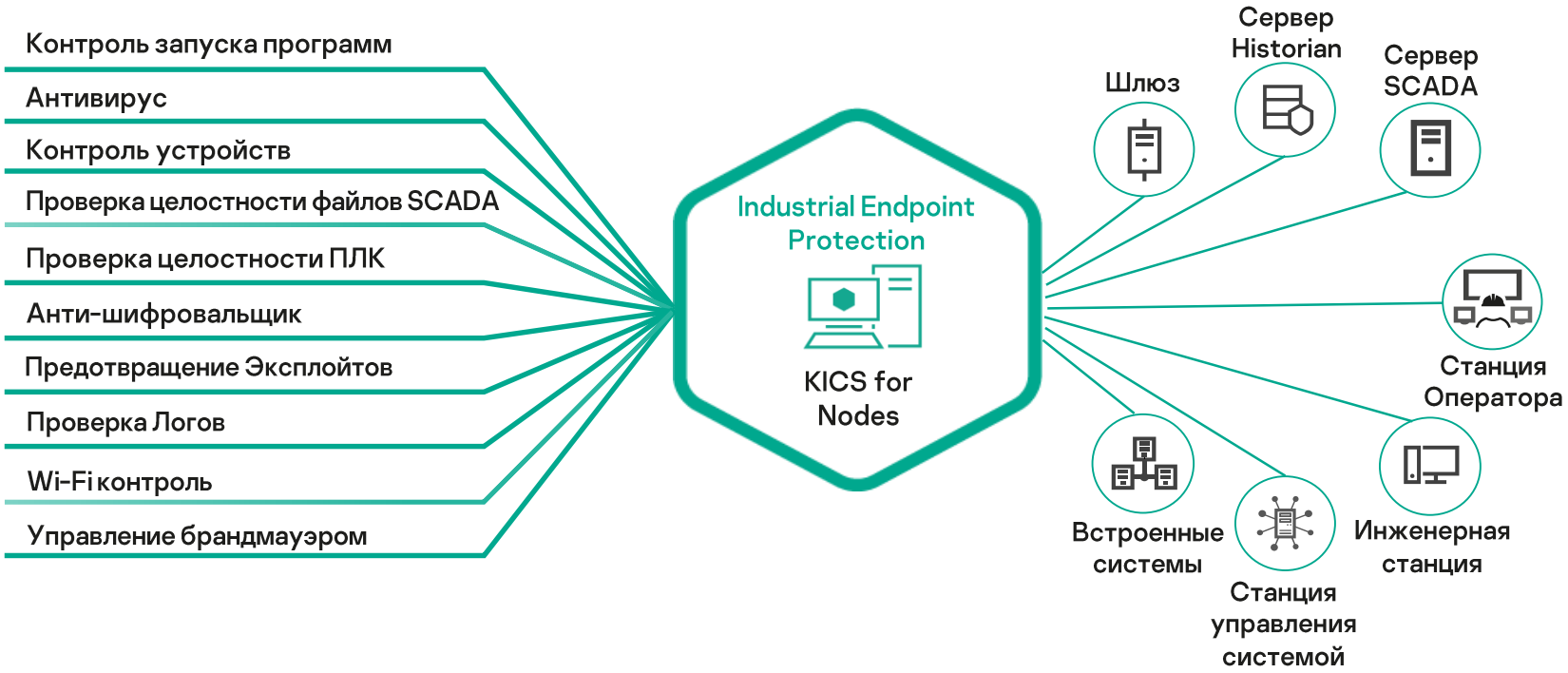
ИНТЕГРАЦИЯ ПАНЕЛИ MES

- Состояние безопасностидоставляется на совместимый с IEC 104 / OPC 2.0 хост

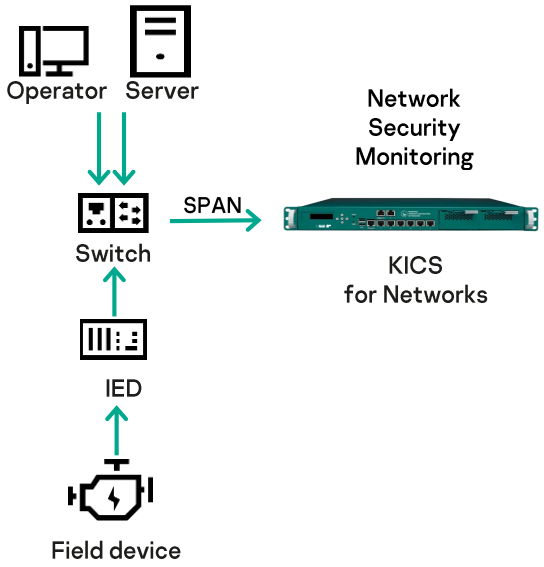
ОТЧЕТНОСТЬ И УВЕДОМЛЕНИЯ

- Регистрация событий
- Отчетность
- Уведомления по SMS/Email

Kaspersky Industrial Cybersecurity **for Nodes**



Приложение для защиты конечных узлов, разработанное специально для промышленности: минимальное воздействие на защищаемое устройство и высочайшая совместимость



Программное обеспечение или виртуальное устройство

пассивно подключено к промышленной сети и использует следующие технологии:

Обнаружение узлов– пассивное определение и инвентаризация элементов технологического процесса

Глубокая Проверка Пакетов– Телеметрический анализ технических процессов фактически в реальном времени

Контроль целостности сети– обнаруживает неавторизованные сетевые узлы и потоки

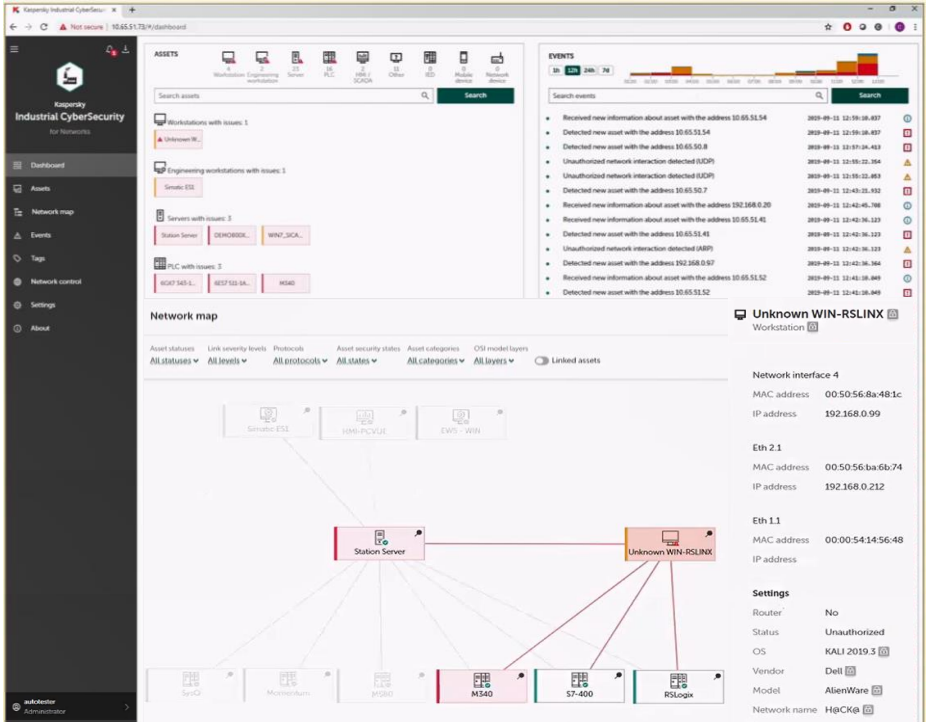
Система обнаружения вторжений– сигналы тревоги при признаках вторжения в сеть

Контроль команд– проверяет команды над промышленными протоколами

Внешние Системы– технологии внешнего обнаружения, интегрированные в API

Machine Learning for Anomaly Detection (MLAD) – обнаруживает кибер или физические нарушения с помощью телеметрии в реальном времени, а также собирает исторические данные (Рекуррентная нейронная сеть)

Kaspersky Industrial CyberSecurity **for Networks**



Обнаружение вторжения в ТП

Способность обнаруживать APT-атаки на самом низком уровне (Промышленные протоколы DPI и специальные подписи)

Инвентаризация узлов

Пассивное обнаружение компонентов ТП и их связей

Защита конечных узлов ТП

Защита от вредоносных программ, Белый список программ и устройств, а также другие компоненты

Дорожная карта

Дек. 2020

Kaspersky Industrial Cybersecurity **for Nodes 3.0**

Kaspersky Industrial CyberSecurity **for Networks 3.0**

Интеграция KICS Nodes и Networks:

- Расширенная информация об активах, отправляемая в KICS for Networks
- Статус активов, доступных в KICS for Networks
- Корреляция событий от KICS for Nodes в KICS for Networks
- Оценка уязвимостей

Дополнительные возможности использования

Реагирование

Передача событий на внешние устройства:

- Возможность реагирования на уровне межсетевого экрана
- Возможность реагирования на уровне рабочей станции / сервера

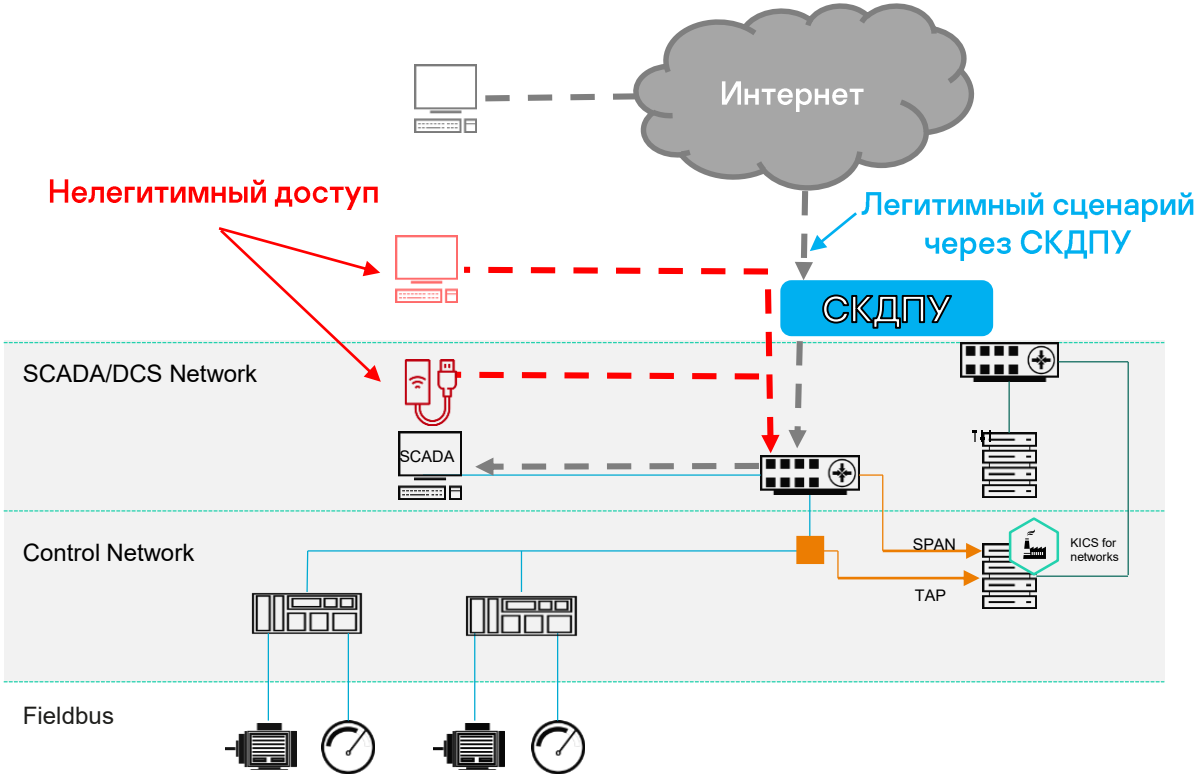
Аудит

Аудит устройств в сети

Аудит коммуникаций

Аудит вредоносного программного обеспечения

Сценарии интеграции с СКДПУ



Контроль подключений:

Анализ действий пользователя
(в части промышленных протоколов и команд)

История действий в АСУ ТП
(для разбора инцидентов)

Дополнительная защита подключений
(анализ команд доверенного пользователя через промышленный IDS)

Выявление «не согласованных» подключений

Продукт MLAD

- Backend:
  - Получение и хранение потоков или истории тегов от внешней системы
  - *Обучение модели (off-premise)*
  - Обнаружение аномалий
  - Отправка информации об обнаруженных аномалиях во внешнюю систему
- Frontend:
  - Просмотр графиков тегов и аномалий
  - Журнал событий (аномалий)
  - Исторический поиск

https://mlad.kaspersky.com/

ubuntu docker python TensorFlow kafka influxdb

Kaspersky Machine Learning for Anomaly Detection

Интеграция MLAD на объекте

используя Kaspersky Industrial CyberSecurity for Networks

Kaspersky Machine Learning for Anomaly Detection

Kaspersky MLAD

Market recognition

Kaspersky is a representative vendor for OT security

KICS was recognized by the leading analysts from:

- Gartner
- Forrester
- ARC Advisory
- Bloomberg NEF

https://kas.pr/kics-gartner

Kaspersky Industrial CyberSecurity **Целостный подход**

Trainings and Awareness

Профессиональное образование по реагированию на инциденты и расследованию

Базовые тренинги для специалистов

Assessment and other security services

Тестирование на проникновение
Оценка кибербезопасности
Построение модели зрелости кибербезопасности
APT Отчеты
Консультации SOC и CERT

Threat Intelligence

База данных исследований уязвимостей и вредоносных программ

Incident Response

Расследование компьютерных инцидентов (удаленное и локальное)
Подготовка руководства и моделирование

Сертификация с поставщиками АСУ ТП

SIEMENS

ICONICS

Make the Invisible Visible™

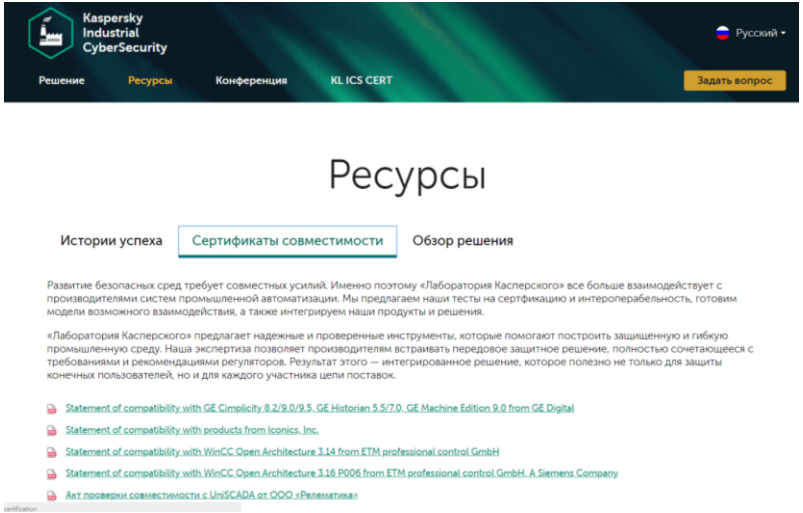
ABB

etm

Professional Control

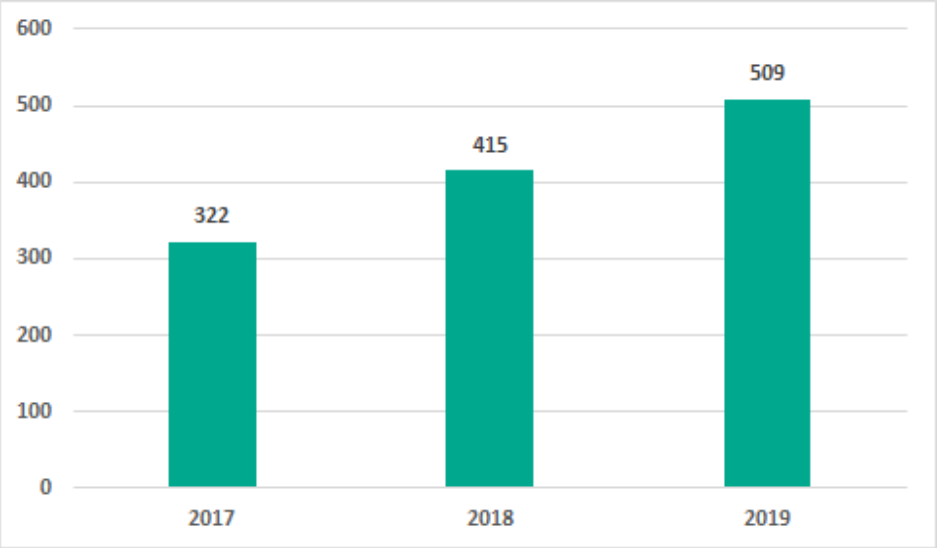
Schneider Electric

EMERSON

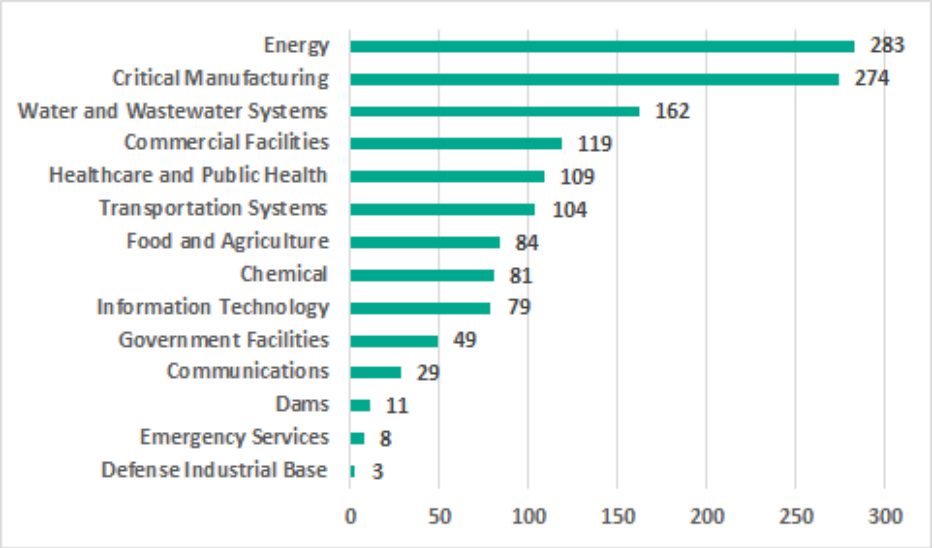


https://ics.kaspersky.ru/resources/#certification

Уязвимости в АСУ ТП обнаруженные в 2019



Количество уязвимостей в разных компонентах АСУ ТП, опубликованных на US ICS-CERT



Количество уязвимых продуктов, используемых в различных отраслях (US ICS-CERT 2019)

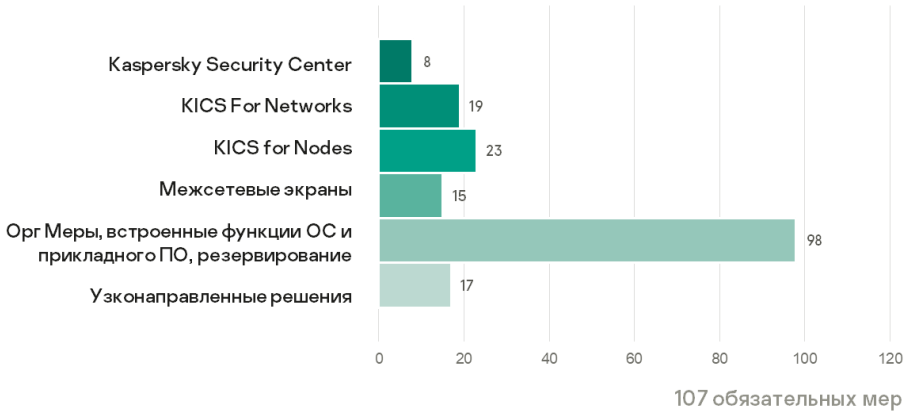
Оценка степени риска	от 9 до 10 (критическая)	от 7 до 8,9 (высокая)	от 4 до 6,9 (средняя)	от 0 до 3,9 (низкая)
Количество уязвимостей	97	249	143	18

Kaspersky Lab ICS CERT выявил **103 уязвимости** промышленных и IIoT/IoT систем в 2019.
33 из обнаруженных нами уязвимостей до сих пор не исправлены производителями соответствующих продуктов, хотя они получили для этого всю необходимую информацию.

Минимальные меры ИБ

Согласно 239 приказу ФСТЭК

3 категория

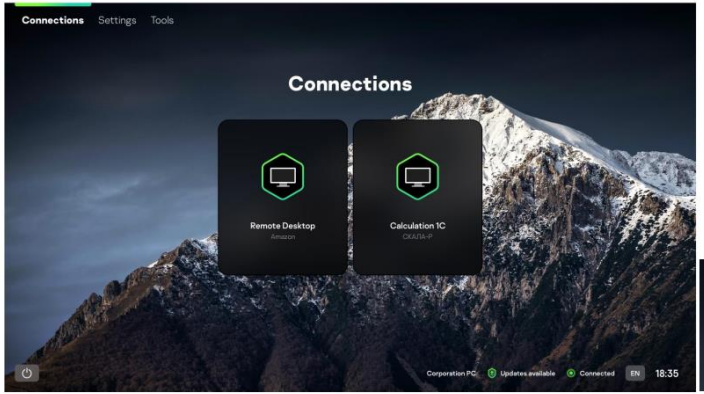


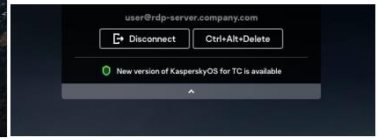
	Требование	Категория значимости		
		3	2	1
ИАФ.2	Идентификация и аутентификация устройств	+	+	+
АУД.1	Инвентаризация информационных ресурсов	+	+	+
АУД.4	Регистрация событий безопасности	+	+	+
АУД.7	Мониторинг безопасности	+	+	+
ЗИС.3	Эшелонированная защита информационной (автоматизированной) системы	+	+	+
ИНЦ.1	Выявление компьютерных инцидентов	+	+	+
ИНЦ.2	Информирование о компьютерных инцидентах	+	+	+
ИНЦ.3	Анализ компьютерных инцидентов	+	+	+

KasperskyOS

Иммунный подход к защите информационных систем

https://os.kaspersky.ru/





Интеграция с технологическими партнерами

Depo Sky 270

Тонкий клиент производства компании Depo Computers — первый среди поддерживаемых операционной системой KasperskyOS https://www.depo.ru/catalog/kompyutery/tonkie-klienty-depo-sky/depo-sky-270/

RDP и Скала-Р

На старте мы поддерживаем работу не только со «стандартным» RDP, но и отечественной системой виртуализации Скала-Р BPM производства компании IBS, нашего технологического партнера. Важно, что система Скала-Р уже интегрирована с продуктом KSV. Список поддерживаемых подключений будет расти от версии к версии.

РУТОКЕН

SafeNet

JaCarta

Поддержка двухфакторной аутентификации — одно из основных требований бизнеса к тонкому клиенту. В версии продукта 1.0 мы реализуем работу с наиболее распространенными носителями ключевой информации

kaspersky

Kaspersky IoT Secure Gateway

V2.0 – Май 2020

Основные функции

- Получает, проверяет и распределяет сообщения датчиков, полученные по протоколу MQTT.

Аппаратная платформа

- Advantech UTX-3117FS-S6A1N (2020)

Транспорт и анализ данных

- Поддержка протокола MQTT (Broker)
- Интеграция с облачными платформами IBM Bluemix, Yandex IoT Core

Сетевые функции

- Отчетность (push, syslog)
- Веб-интерфейс управления
- IP-Routing (NAT, DHCP)

KasperskyOS

- Обеспечивает безопасность устройства на уровне ядра ОС
- Безопасное обновление прошивки

Функции безопасности

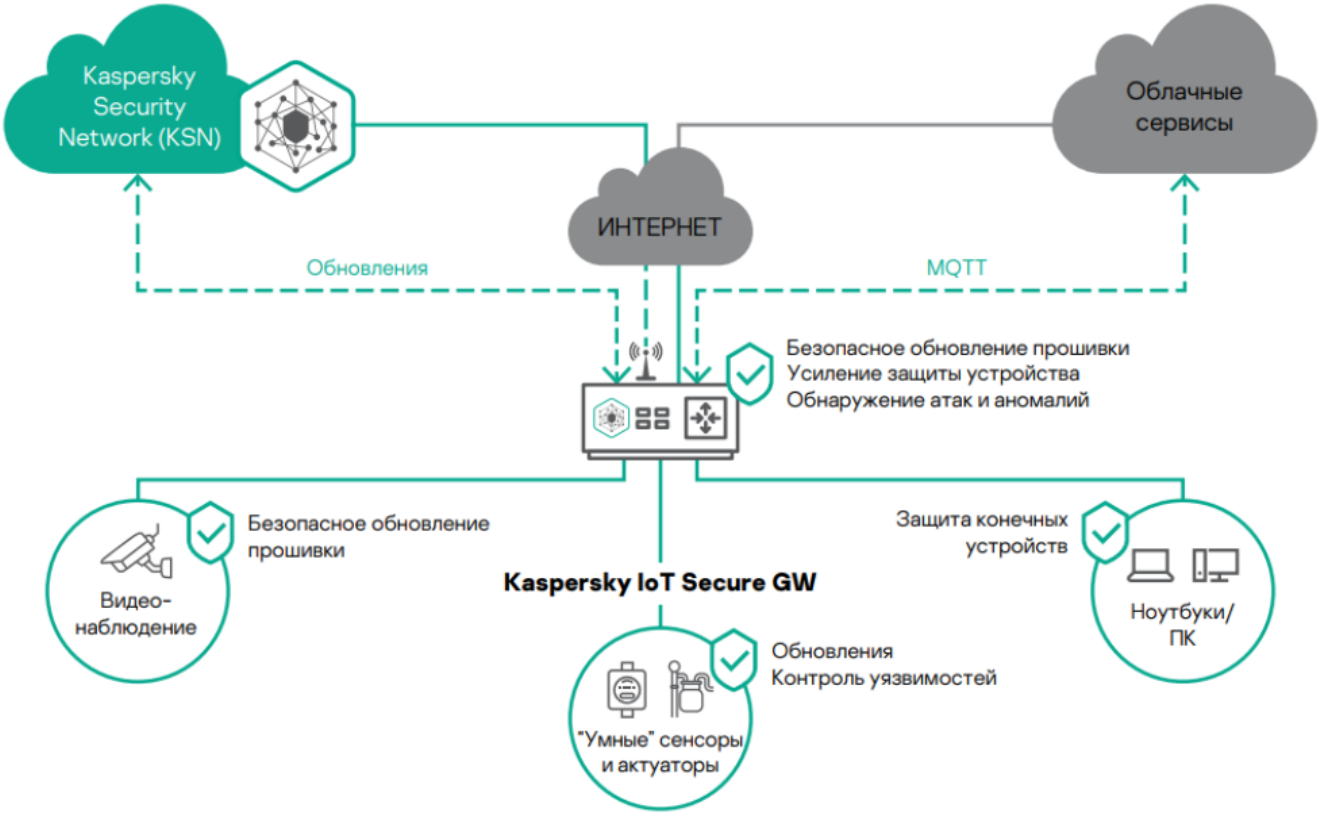
- Обнаружение и классификация устройств
- Регистрация события безопасности системы и сети.
- Защита от сетевых атак (IDS/IPS)
- Firewall

Централизованное управление через KSC

Kaspersky
IoT Security

kaspersky

Промышленное производство



Kaspersky IoT Security

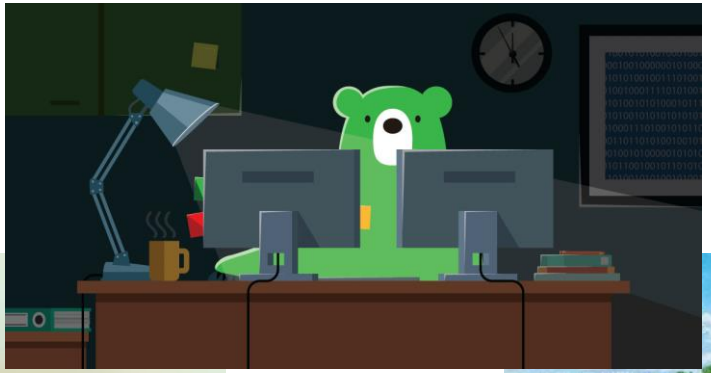
АДАПТИВНЫЕ ПРОМЫШЛЕННЫЕ ТЕХНОЛОГИИ

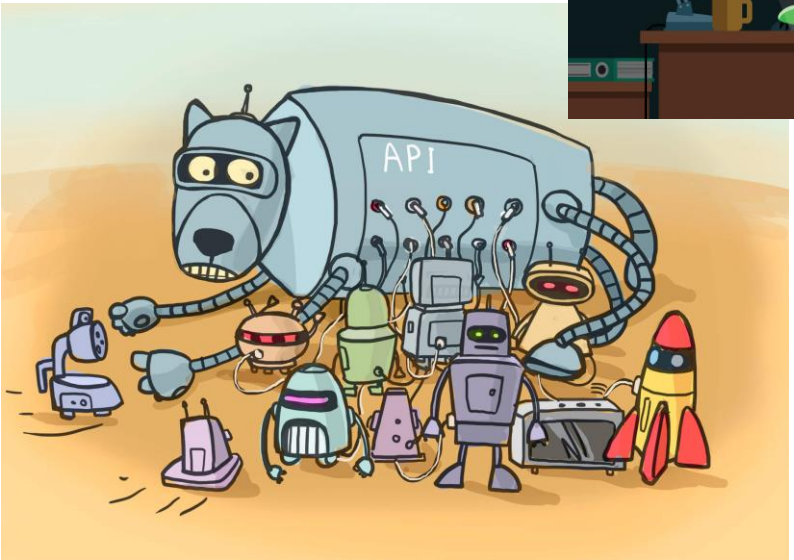
Сценарии применения:

- Мониторинг работы промышленного оборудования (например, станки ЧПУ)
- Если требуется разработка вертикального решения – кооперация с командой АПРОТЕХ

kaspersky

Причем тут «Экосистема» и медведь KUMA? ☺



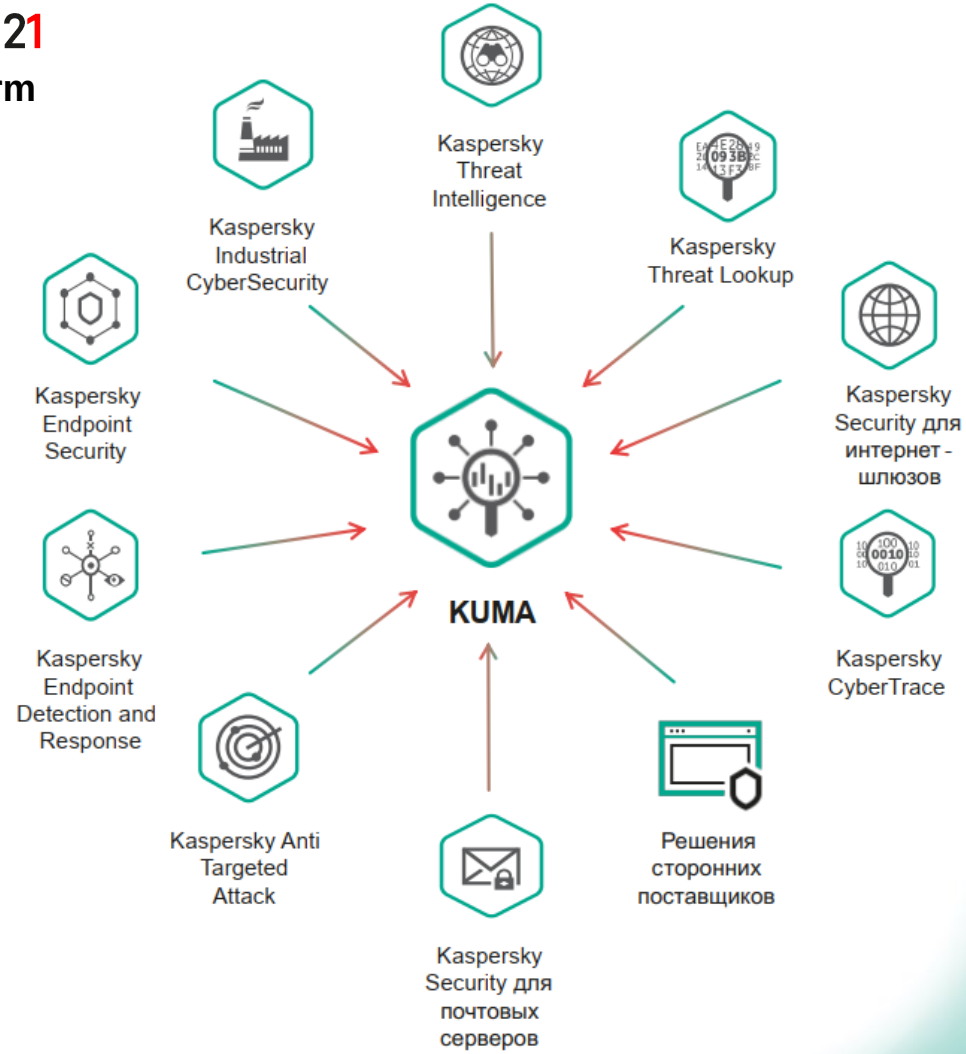


Или как перейти от «костылей» в интеграции к гармонии в экосистеме ИБ?

Что за KUMA? SIEM by Kaspersky Lab 2021

Kaspersky Unified Monitoring and Analysis Platform

- Комплексная экосистема безопасности, объединяющая как решения «Лаборатории Касперского», так и сторонних производителей с API для SOAR & etc
- Потоковая корреляция в реальном времени / >300K EPS
- Модульная архитектура
- Автоматизированное реагирование на инциденты при интеграции с Kaspersky EndPoint Detection & Response
- Автоматический сбор информации с конечных точек в связке с Kaspersky EndPoint Security
- Интеграция с Kaspersky Threat Intelligence
- Доступ к экспертизе «Лаборатории Касперского»



kaspersky

Kaspersky Industrial CyberSecurity

Активируем будущее вместе

Азат Шайхутдинов

Менеджер проектов KICS

Azat.Shaykhutdinov@Kaspersky.com

+7 917 920 00 78

ics.kaspersky.com

Kaspersky Industrial Cybersecurity Conference 2020

https://ics.kaspersky.ru/conference/