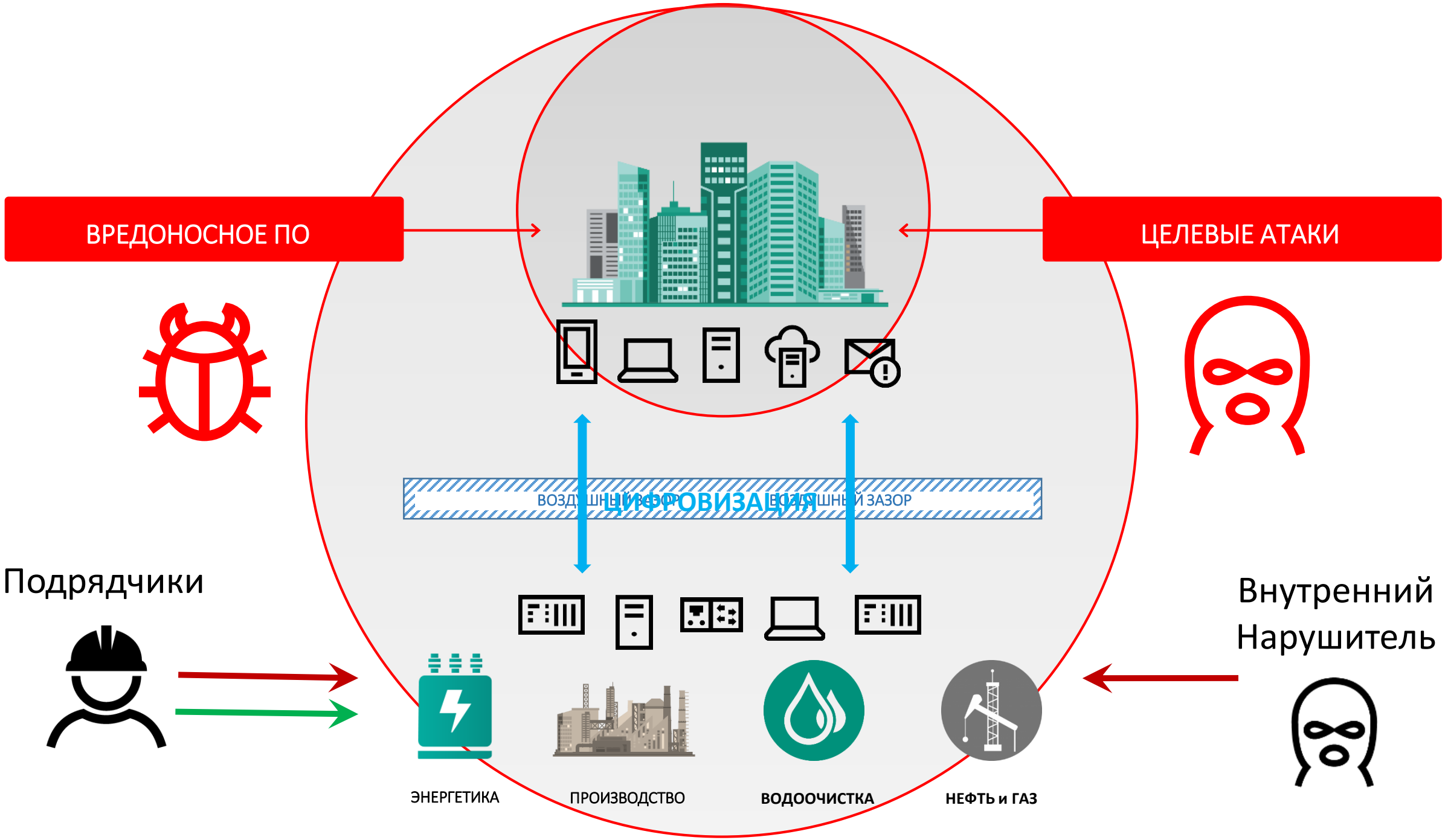
kaspersky

Применение комплексного решения **Kaspersky Industrial CyberSecurity** на объектах КИИ


ВРЕДОНОСНОЕ ПО
ЦЕЛЕВЫЕ АТАКИ
ВОЗДУШНЫЙ ЗАЗОР
ЦИФРОВИЗАЦИЯ
ВОЗДУШНЫЙ ЗАЗОР
Подрядчики
Внутренний Нарушитель
ЭНЕРГЕТИКА
ПРОИЗВОДСТВО
ВОДООЧИСТКА
НЕФТЬ и ГАЗ

Kaspersky ICS CERT

Authorized to Use CERT℠
CERT is a mark owned by
Carnegie Mellon University

Глобальный проект «Лаборатории Касперского», нацеленный на координацию действий производителей систем автоматизации, владельцев и операторов промышленных объектов, исследователей информационной безопасности при решении задач защиты промышленных предприятий и объектов критически важных инфраструктур.

Металлургический концерн BlueScope

Киберинцидент был обнаружен в одной из компаний в США, атака незначительно затронула предприятия в Азии и новой Зеландии. Сильнее всего от атаки пострадали производственные и торговые операции в Австралии: некоторые процессы были приостановлены, а другие, включая отправку стали, осуществлялись преимущественно без использования средств автоматизации.

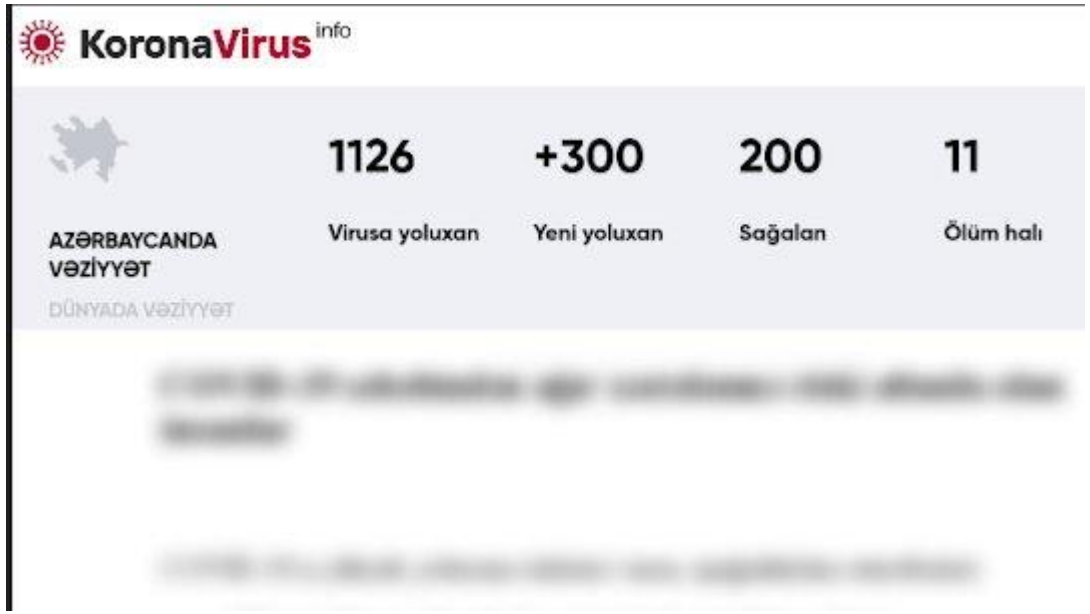
Energias de Portugal (EDP)

13 апреля EDP подверглась атаке вымогателя. В результате атаки с шифровальщика **Ragnar Locker** системы компании были зашифрованы.

Помимо этого, киберпреступники утверждают, что они украли 10 Тб конфиденциальных файлов компании и теперь угрожают опубликовать их, если не будет уплачен выкуп в размере **10,9 млн долларов.**

Вредоносные кампании в Азербайджане

В апреле 2020 года стало известно о целевых атаках с использованием нового троянца удаленного доступа **PoetRAT**. Атаки были направлены на гос сектор, транспортные и промышленные компании Азербайджана, главным образом энергетические, особенный интерес злоумышленники проявляли к SCADA-системам, связанным с ветряными турбинами. В качестве приманки использовались документы якобы правительства Азербайджана, посвященные COVID-19.



Одинцовский Водоканал

Атака программы-шифровальщика.

Зловред зашифровал все данные как на самом заражённом устройстве, так и в сетевых папках.

В результате этой атаки под угрозой оказалась сохранность технической документации и данных абонентов организации, а также процедура выставления счетов.

Kaspersky Industrial CyberSecurity

СЕРВИСЫ

Обучение и программы повышения осведомленности

- Kaspersky® Security Awareness
- Kaspersky® Security Trainings

Экспертные сервисы и данные об угрозах

- Kaspersky® Security Assessment
- Kaspersky® Incident Response
- Kaspersky® Threat Intelligence

РЕШЕНИЯ

Защита промышленных компьютеров

- KICS for Nodes

Обнаружение аномалий и угроз в промышленной сети

- KICS for Networks

Централизованное управление безопасностью

- Kaspersky Security Center

Защита предприятия

Industrial Endpoint Protection

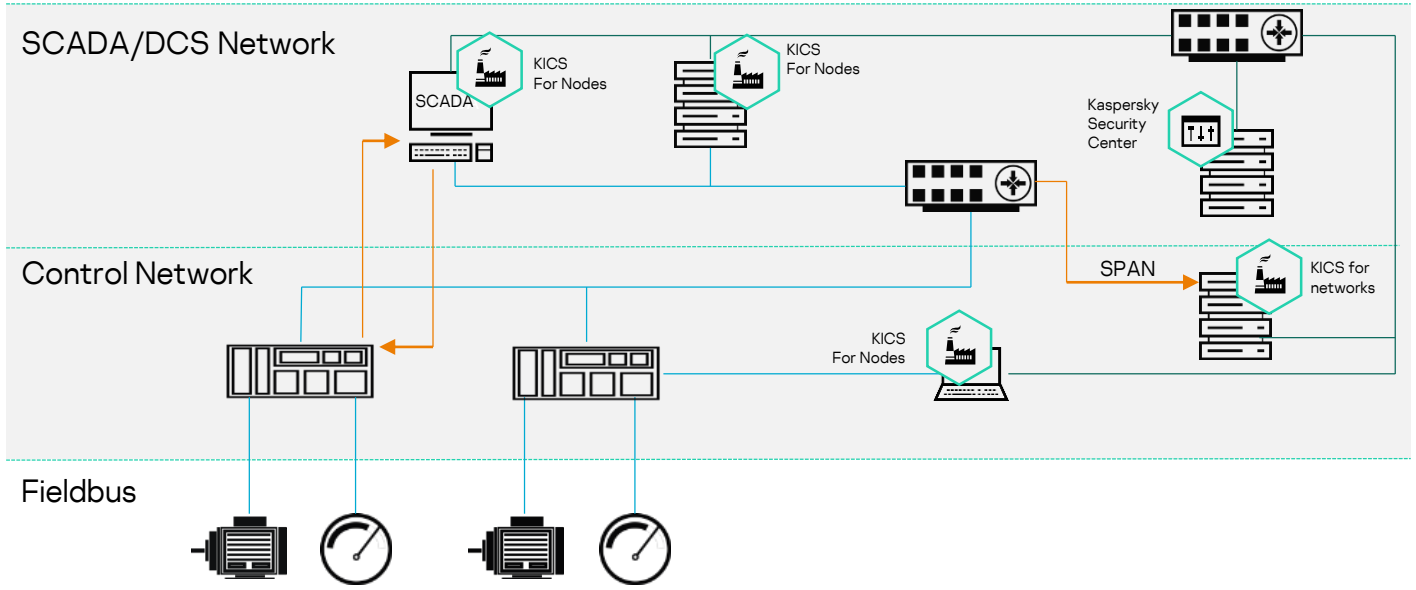
KICS for Nodes

- Контроль запуска приложений (Whitelisting)
- Промышленный антивирус
- Контроль подключаемых устройств
- Мониторинг файловых операций
- Анализ логов ОС
- Защита от шифрования

Industrial Anomaly and Breach Detection

KICS for Networks

- Контроль целостности сети
- Промышленный DPI
- Промышленный IDS
- Пассивная инвентаризация устройств
- Карта сети
- Корреляция событий



kaspersky

KICS for Nodes

Корпоративные подходы к кибербезопасности не применимы для промышленных инфраструктур

НЕДОСТАТКИ «КОРПОРАТИВНЫХ» РЕШЕНИЙ:

Высокое потребление ресурсов защищаемой системы может привести к ее отказу

Проактивные технологии защиты повышают вероятность ложного срабатывания

ТРАДИЦИОННОЕ РЕШЕНИЕ ПРОБЛЕМЫ

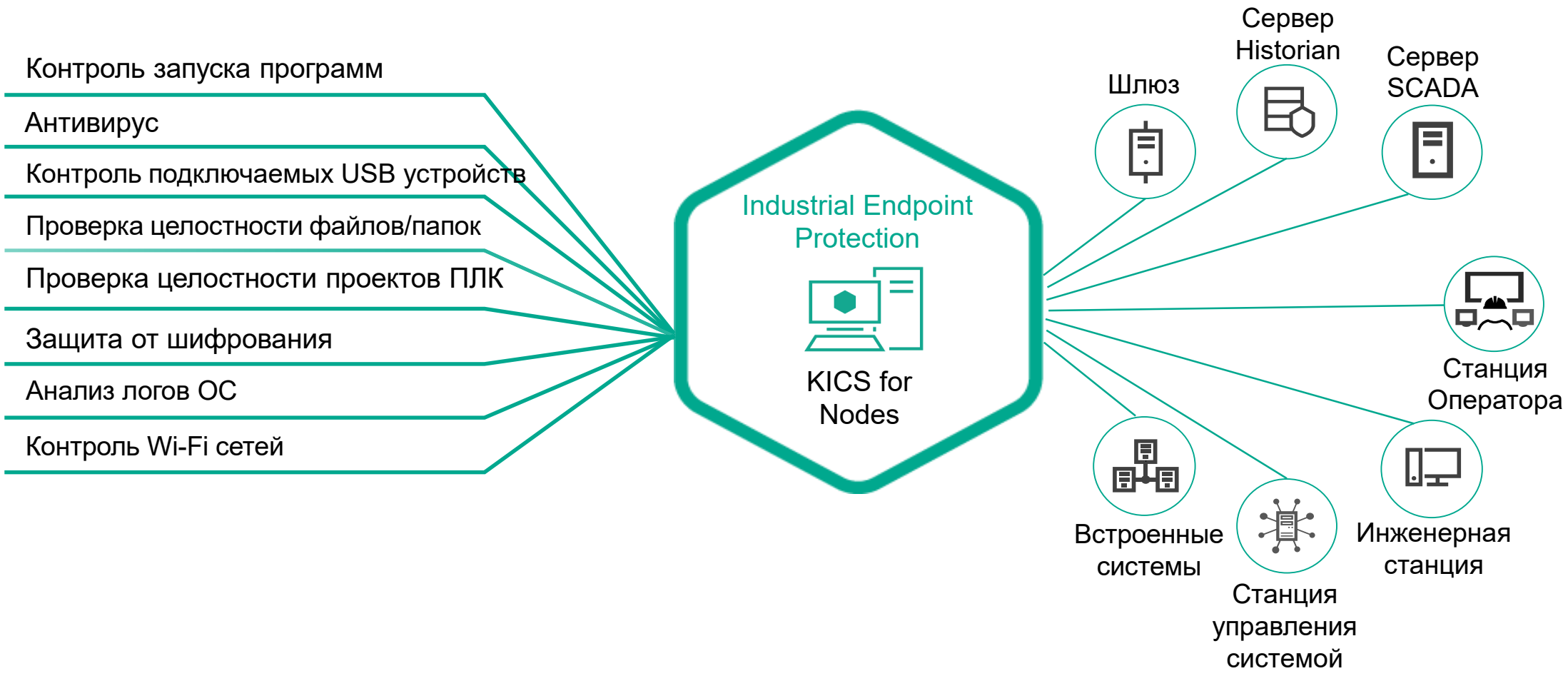
Настроить средства защиты для предотвращения негативного воздействия на защищаемую промышленную систему:

- Ручная установка
- Создание списка исключений
- Отключение защитных компонент антивирусного ПО

СЛИШКОМ СЛОЖНО УПРАВЛЯТЬ

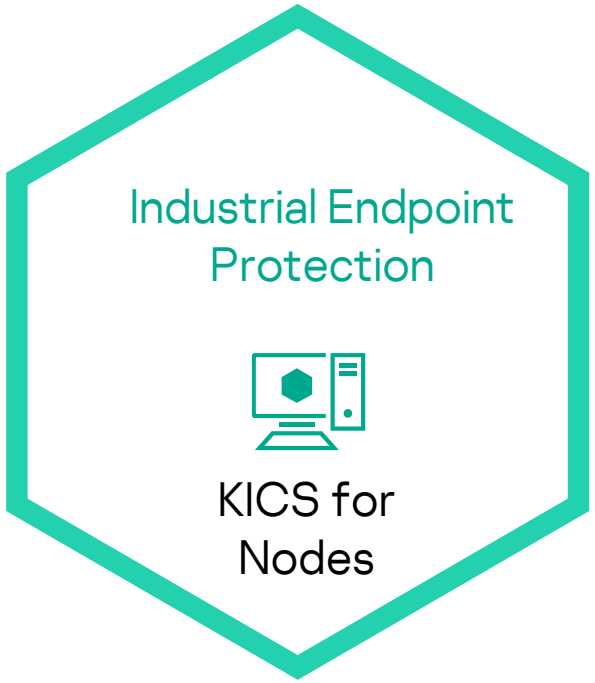
ОСТАВЛЯЕТ БРЕШИ В СИСТЕМЕ БЕЗОПАСНОСТИ

Kaspersky Industrial Cybersecurity **for Nodes**



KICS for Nodes: промышленная специфика

Почему нужно использовать **KICS** вместо корпоративного антивируса для защиты АСУ ТП?



- Уменьшено потребление ресурсов
  - 512 MB Оперативной памяти для Windows XP SP2 / XP Embedded
- Установка/Обновление/Удаление без перезагрузки
- Возможность работы в полностью неблокирующем режиме
- Возможность обнаружения угроз нулевого дня (в том числе в неблокирующем режиме)
  - Контроль запуска приложений, Анализ логов, Мониторинг файловых операций

- Позволяет не допустить ложных срабатываний и перерасхода системных ресурсов
- Значительно снижает затраты на обслуживание в сравнении с корпоративными решениями

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

ПНХЗ

Нефть под защитой: «Лаборатория Касперского» реализовала проект промышленной безопасности на Павлодарском нефтехимическом заводе

КазМунайТениз

«Лаборатория Касперского обучает сотрудников «КазМунайТениз» основам промышленной кибербезопасности

ezenta

Тестирование на проникновение в АСУ ТП: «Лаборатория Касперского» способствует бизнес-росту компании Ezenta

TATNEFT

Промышленная кибербезопасность — залог успешного бизнеса

TANECO

Танеко защищает свои

TANECO

Пилотирование системы

- Акт проверки совместимости с программным комплексом Redkit SCADA от ООО «Прософт
- Акт проверки совместимости с программным комплексом «Энергосфера» от ООО «Просо
- Акт проверки совместимости с устройством противоаварийной автоматики энергоузла от ООО «Прософт-Сис
- Акт проверки совместимости с программным комплексом СК-11 от ЗАО «Монитор Электрик»
- Заключение о совместимости с программным комплексом учета движения, инвентаризации и расчета материа «ИнфТех»
- Акт проверки совместимости с ПТК КРУГ-2000 версии не ниже 4.2 от ООО НПФ «КРУГ»
- Акт проверки совместимости с «ОИК-Диспетчер НТ» от ООО «НТК Интерфейс»
- Акт проверки совместимости со SCADA NPT Expert от ООО «ЭнергопромАвтоматизация»
- Заключение о совместимости с EKRASCADA от ООО НПП «ЭКРА»
- Заключение о совместимости с EKRASMS от ООО НПП «ЭКРА»
- Заключение о совместимости с EKRASMS-SP от ООО НПП «ЭКРА»
- Заявление о совместимости с EcoStruxure Foxboro DCS (Foxboro Evo) от Schneider Electric
- Заявление о совместимости с HOLLiAS MACS от Hangzhou HollySys Automation Co., Ltd.
- Заявление о совместимости с PCS 7 V8.2 SP1 от ООО «Сименс»
- Заявление о совместимости с PcVue от ARC Informatique
- Заявление о совместимости с VideoXpert Enterprise и VideoXpert Professional от Pelco by Schneider Electric
- Заявление о совместимости с Wonderware System Platform от Aveva
- Заявление о совместимости с продуктами Schneider Electric
- Заявление о совместимости с продуктами ООО «Иокогава Электрик СНГ»

kaspersky

KICS for Networks

KICS for Networks

ЧТО БОЛЬШЕ ВСЕГО ИНТЕРЕСУЕТ В ПРОМЫШЛЕННОЙ СЕТИ?

КИБЕРБЕЗОПАСНОСТЬ:

- Обнаружение проникновений в промышленную сеть (сетевые сканирования, вредоносное ПО и т.д.)
- Обнаружение целевых атак направленных на контроллеры и системы противоаварийной защиты

НЕ КИБЕРБЕЗОПАСНОСТЬ:

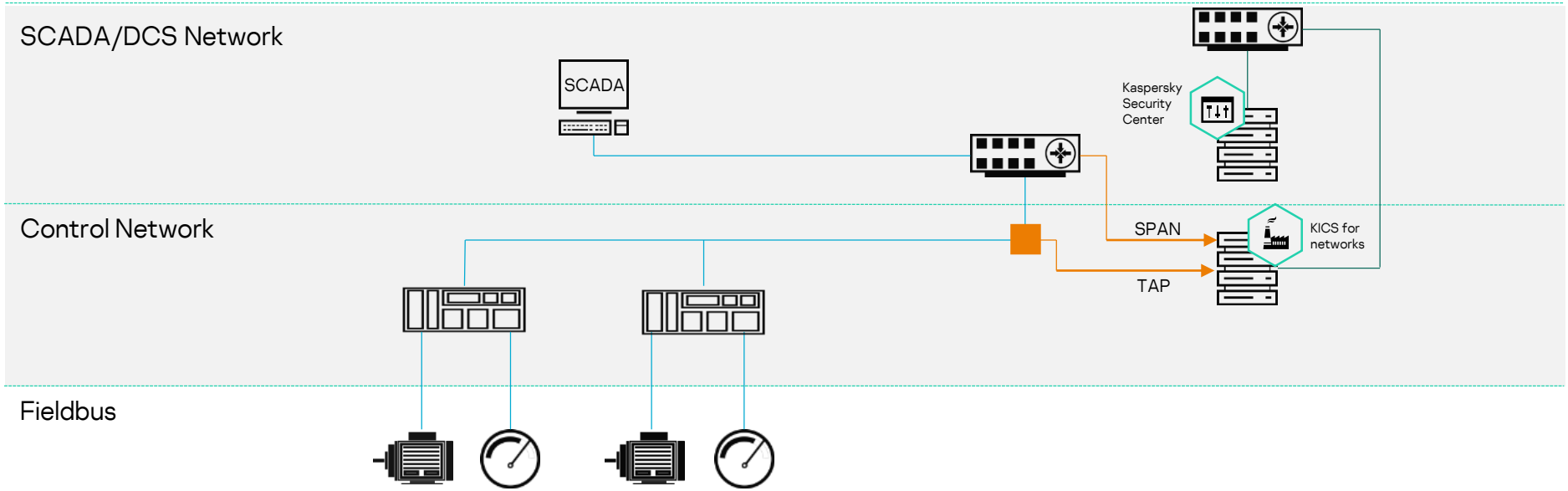
- Управление активами в мультивендорной инфраструктуре развернутой и поддерживаемой различными организациями на протяжении многих лет
- Поддержка целостности промышленной сети и предотвращение неразрешенных Интернет-соединений и несогласованных изменений конфигурации сети
- Мониторинг и регистрация действий сторонних организаций действующих локально или удаленно в рамках сервисного контракта

KICS for Networks

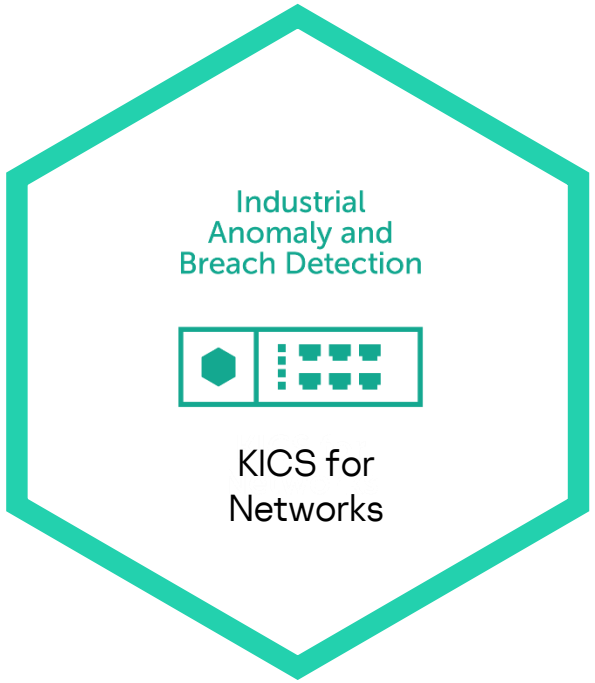
ПО или **VIRTUAL APPLIANCE**

ПАССИВНЫЙ МОНИТОРИНГ СЕТИ В РЕЖИМЕ РЕАЛЬНОГО ВРЕМЕНИ:

- Анализ **зеркалированной копии** трафика (SPAN)
- Возможность подключения через TAP-устройство



KICS for Networks: особенности и сценарии применения



ОБНАРУЖЕНИЕ УСТРОЙСТВ и КОНТРОЛЬ ЦЕЛОСТНОСТИ СЕТИ

- Пассивное обнаружение устройств и взаимодействий между ними
- Визуализация с помощью карты сети
- Белый список сетевых взаимодействий

УПРАВЛЕНИЕ ИНЦИДЕНТАМИ

- Отображение наиболее важных событий
- Корреляции событий
- Управление историей событий

ИНТЕГРАЦИЯ ПРОМЫШЛЕННОЙ и КОРПОРАТИВНОЙ БЕЗОПАСНОСТИ

- Kaspersky Security Center
- Syslog Server
- SIEM

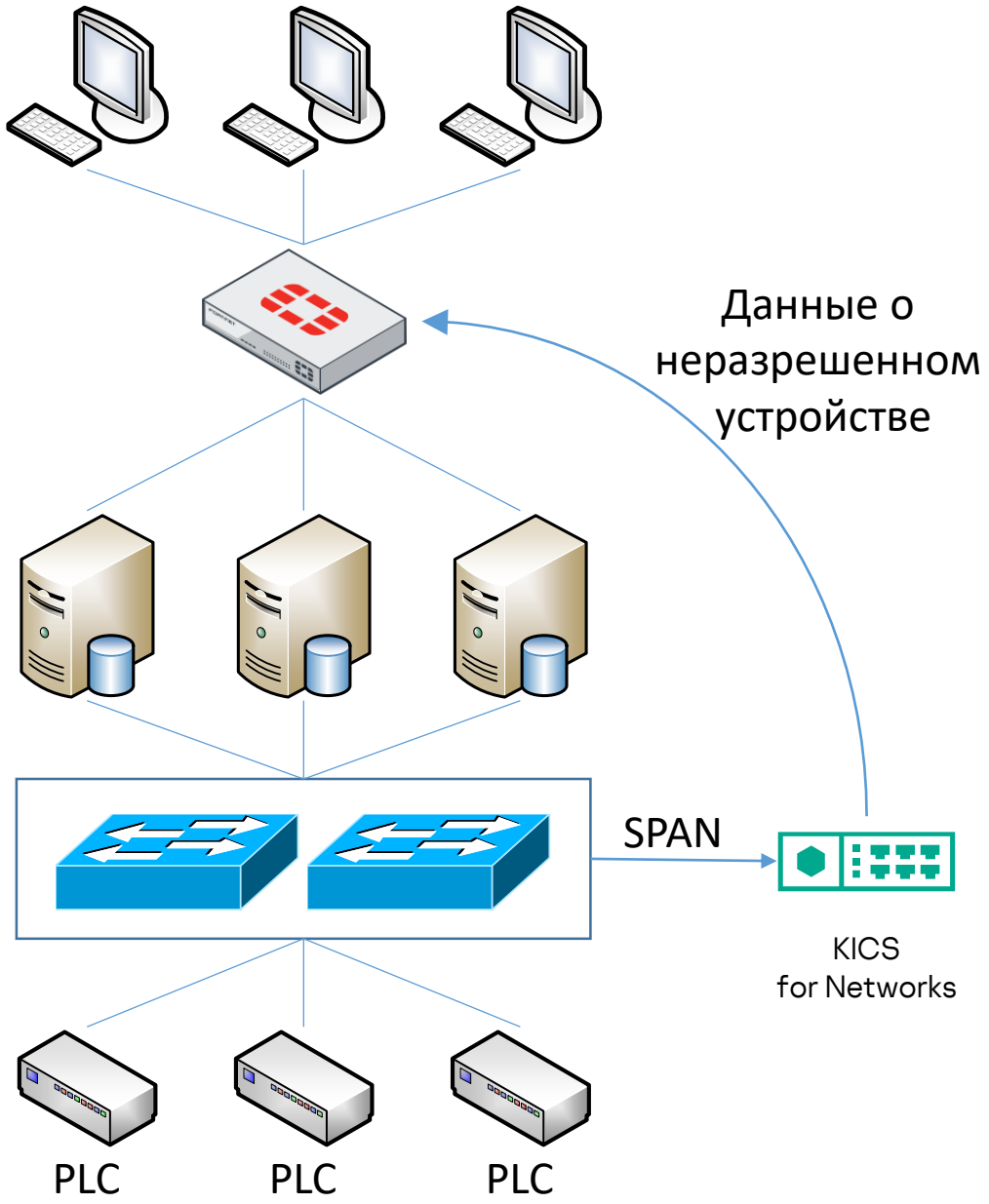
МОНИТОРИНГ ТЕХНОЛОГИЧЕСКОГО ПРОЦЕССА

- Анализ параметров технологического процесса
- Обнаружение попыток злонамеренного вмешательства в технологический процесс

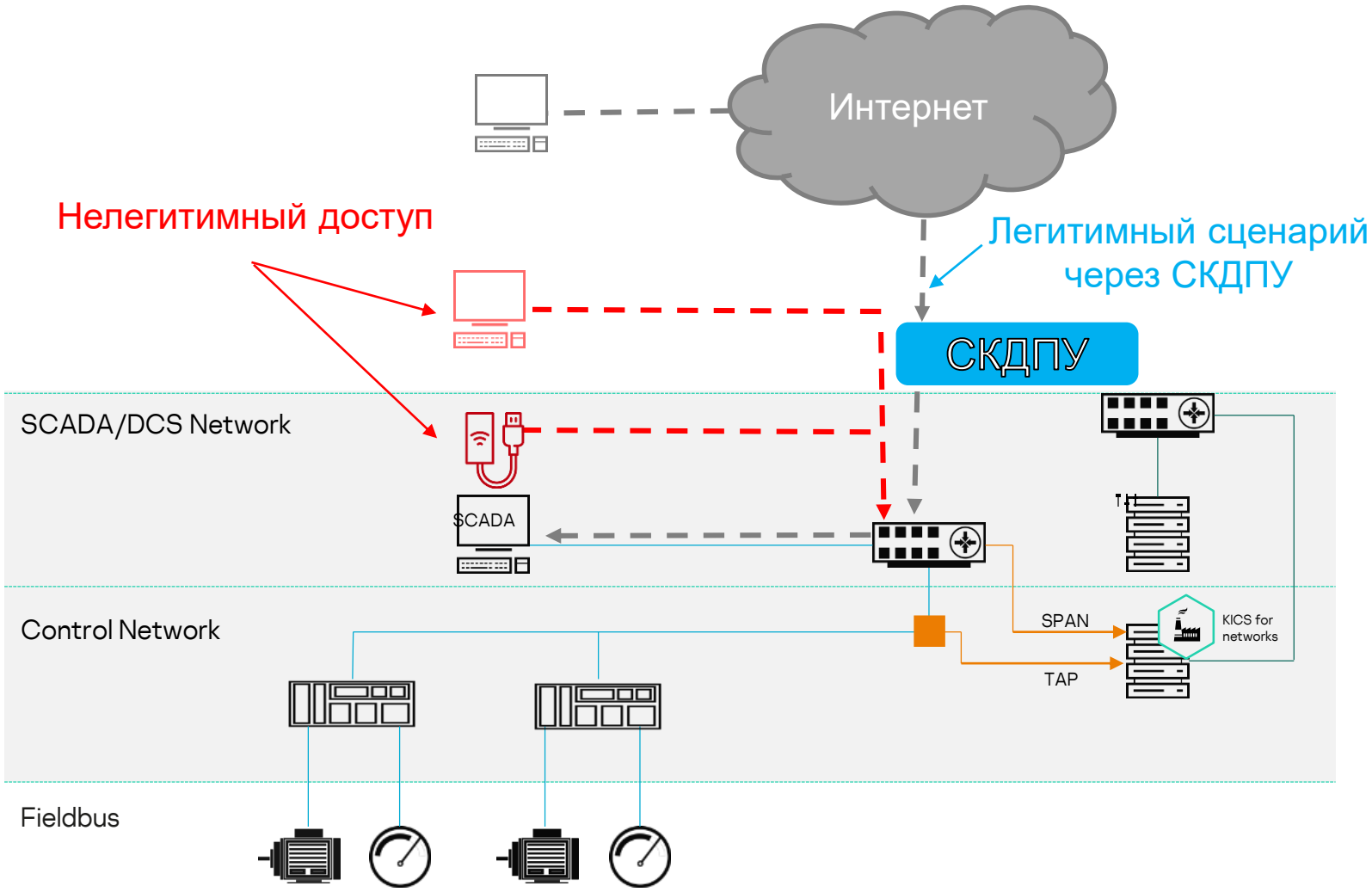
МОНИТОРИНГ КОМАНД К ПЛК

- Обнаружение появления потенциально опасных команд к ПЛК
- Регистрация событий: Authentication on ПЛК, Start/Stop PLC, Read/Write PLC, Read/Write PLC configuration, и др.

Расширенная функциональность API



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

Дорожная карта

Kaspersky Industrial Cybersecurity **for Nodes 3.0**

Kaspersky Industrial CyberSecurity **for Networks 3.0**

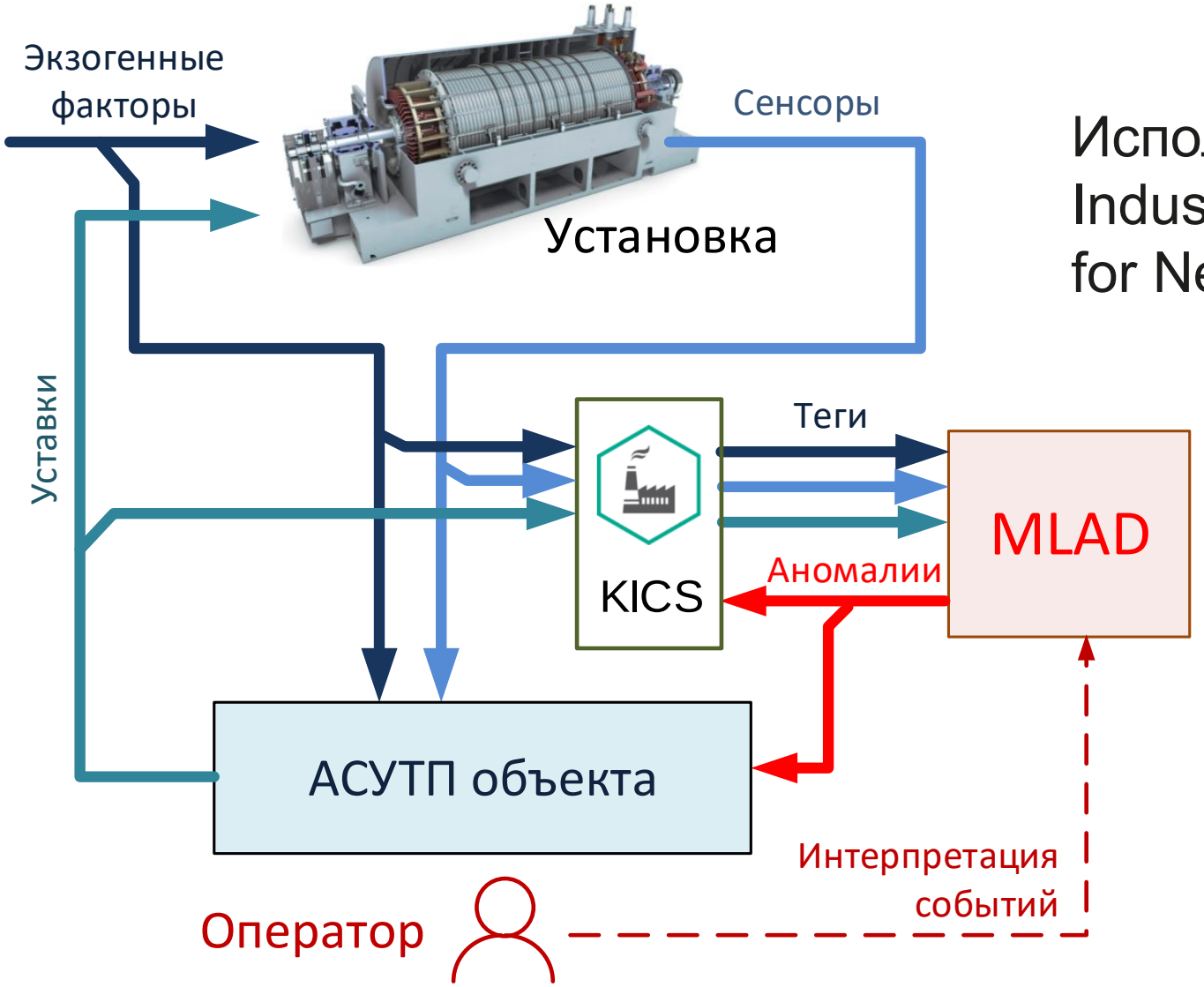
Интеграция KICS Nodes и Networks:

- 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

kaspersky

Kaspersky MLAD

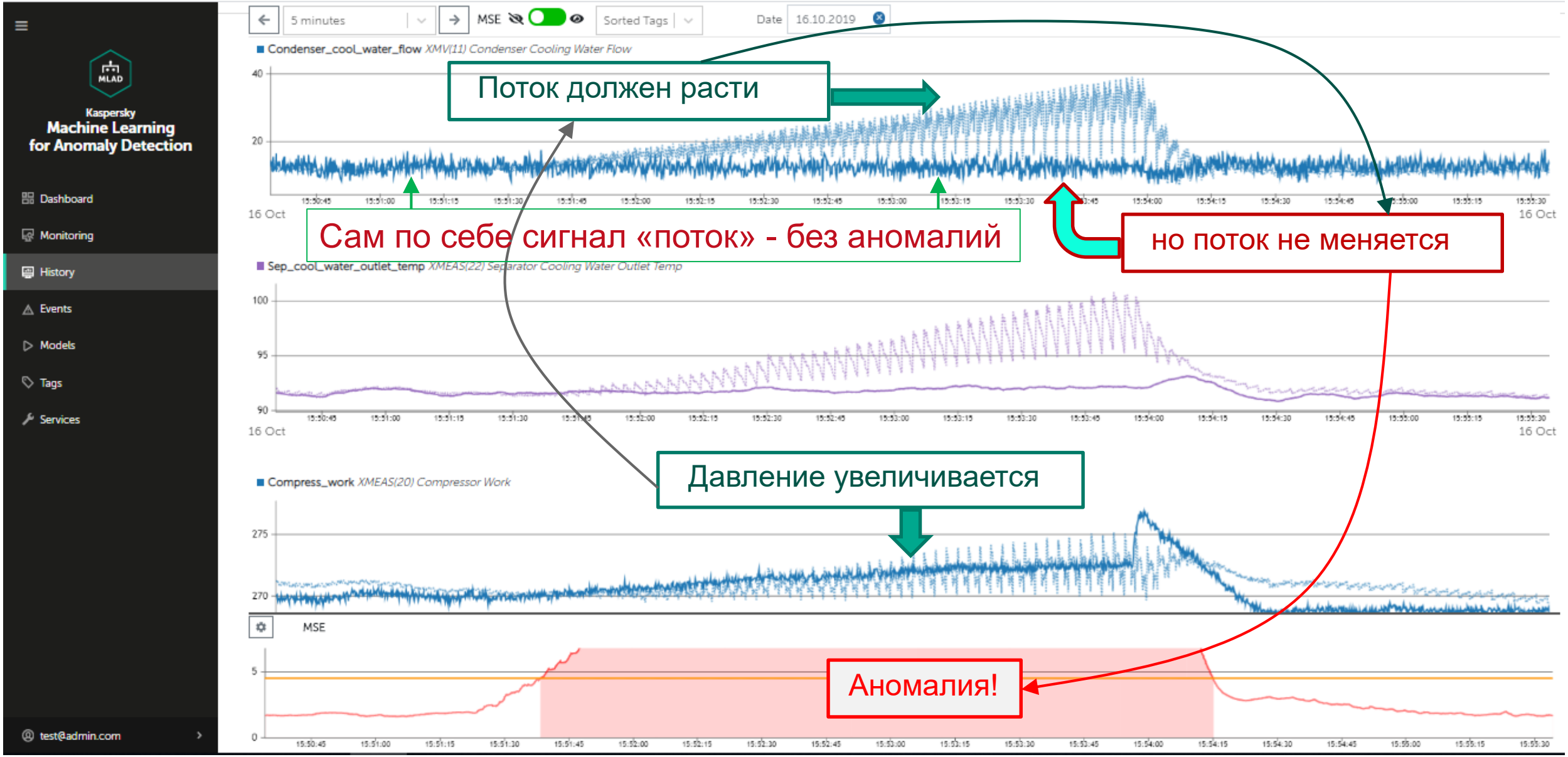
Интеграция MLAD на объекте



Используя Kaspersky Industrial CyberSecurity for Networks

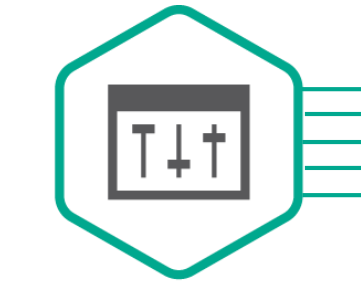
Kaspersky Machine Learning for Anomaly Detection

Kaspersky MLAD



Kaspersky Security Center

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 ПОЛИТИКАМИ

- Централизованное управление политикой безопасности
- Удаленное планирование и выполнение задач

ИНТЕГРАЦИЯ С HMI

ИНТЕГРАЦИЯ ПАНЕЛИ MES

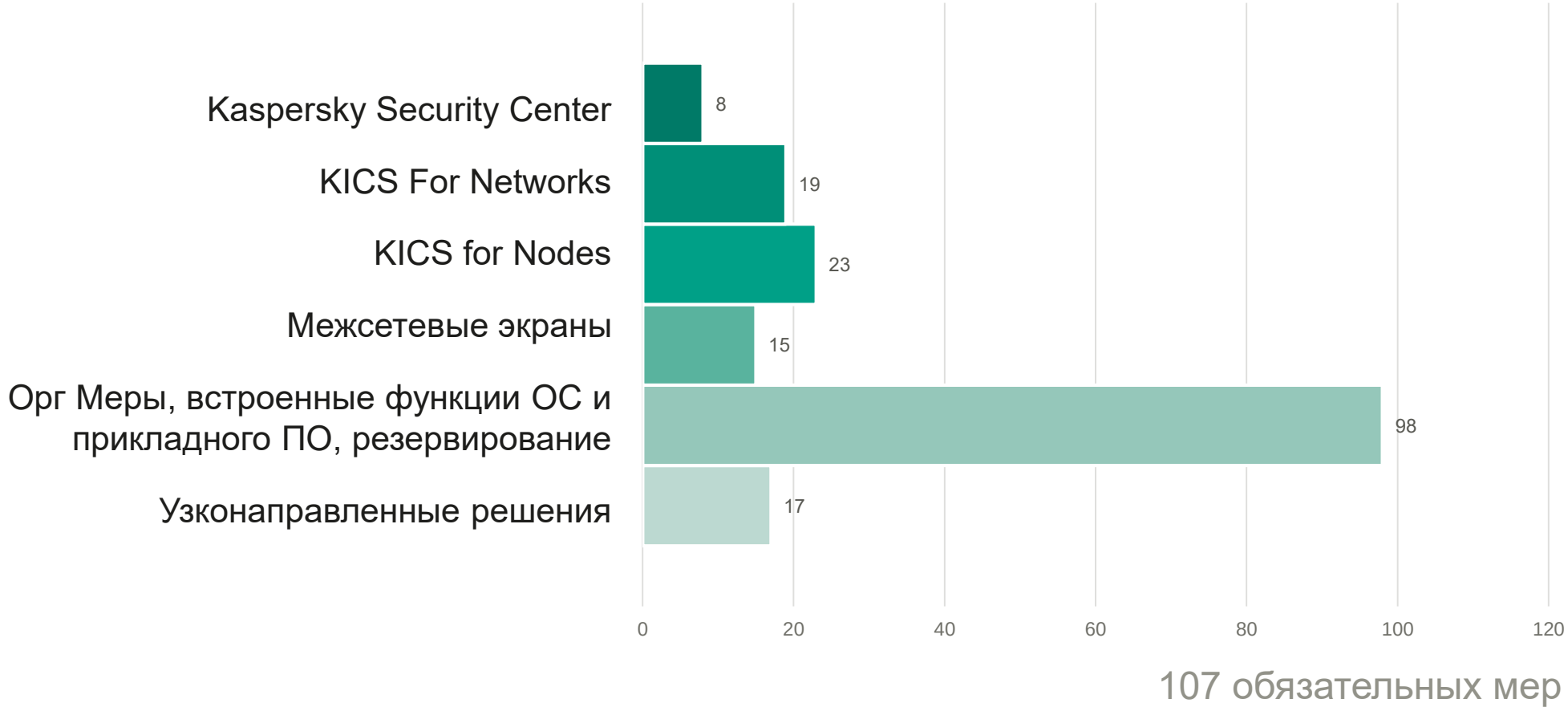
- Состояние безопасности доставляется на совместимый с IEC 104 / OPC 2.0 хост

ОТЧЕТНОСТЬ И УВЕДОМЛЕНИЯ

- Регистрация событий
- Отчетность
- Уведомления по SMS/Email

Роль KICS в реализации требований приказа ФСТЭК 239

Минимальные меры ИБ
(согласно 239 приказу ФСТЭК, 3 категория)



107 обязательных мер

KICS 2015-2020

Истории успеха

ТАНЕКО

«Этот проект наглядно продемонстрировал возможность использования подобных решений на промышленных объектах. ТАНЕКО планирует и далее расширять своё сотрудничество с «Лабораторией Касперского» в области защиты индустриальных сетей.» - Марат Гильмутдинов, Начальник отдела АСУ ТП, ТАНЕКО

Производитель нефти

Основанная в 2005 году, входит в состав группы «Татнефть», которая оценивается в 15 миллиардов долларов

Использует промышленные системы управления, чтобы обеспечить технологическое преимущество над конкурентами и минимизировать производственные затраты

Растущий уровень автоматизации производства и использование технологий, изначально разработанных для корпоративных сетей, в своей промышленной инфраструктуре подвергли компанию риску кибератак.

Защищена непрерывность производственного процесса

Обнаружены аномалии и несанкционированные попытки перенастроить контроллеры

Отслеживаются технологические процессы и автоматически обнаруживаются отклонения процесса от нормального поведения с технологией MLAD

Системы обнаружения аномалий, анализа отклонений и автоматического раннего предупреждения

НЛМК

«Внедрение современных интеллектуальных систем автоматического управления на производстве увеличивает риски потенциальных кибератак, которые могут повлиять на технологический процесс. Для их предотвращения на НЛМК мы внедряем комплексную эшелонированную защиту на уровне инфраструктуры систем автоматизации.» - Сергей Слаута, директор дирекции по автоматизации технологических процессов НЛМК

Производитель стали

Крупнейший металлургический завод в России

Основано в 1931

Работает в России, Европе и США.

Защищено

Промышленные системы управления в цехе динамной стали защищены от кибератак

Модернизирована инфраструктура автоматизации благодаря объединению вычислительных ресурсов АСУ ТП в нескольких территориально распределенных центрах обработки данных.

Внедрена не только возможность киберзащиты конечных узлов АСУ ТП, но и обнаружения нештатных ситуаций и вторжений в промышленные сети при помощи технологий пассивного мониторинга.

МосГаз

«Уверены, что этот совместный проект послужит основой для тесного многолетнего сотрудничества. Модернизация системы кибербезопасности АСУ ТП АО «МОСГАЗ» будет продолжаться» – Александр Кузин, заместитель начальника управления информатизации АО «МОСГАЗ»

Транспортировка природного газа по газораспределительным сетям Москвы

Основано в 1865

Ежегодная отгрузка 23 миллиардов кубометров природного газа

7500 километров газораспределительных сетей

Защищены промышленные узлы и сети

Более 500 газораспределительных станций с KICS for Network

- Всего ~600 ПЛК Siemens
- До 20 клапанов в каждом ПЛК

Группа из 7 централизованных SCADA-серверов с KICS for Nodes

Познякевич Александр
Менеджер по развитию бизнеса KICS

Alexander.Poznyakevich@kaspersky.com
Tel: +7 (903) 527 65 88
www.kaspersky.com

kaspersky

Расширенная поддержка протоколов

- ABB SPA-Bus
- Allen-Bradley EtherNet/IP
- BECKHOFF ADS/AMS
- CODESYS V3 Gateway
- DCE/RPC
- DMS для устройств ABB AC 700F
- DNP3;
- Emerson ControlWave Designer
- Emerson DeltaV
- FTP
- General Electric SRTP
- IEC 60870: IEC 60870-5-101, IEC 60870-5-104
- IEC 61850: GOOSE, MMS (включая MMS Reports), Sampled Values
- Mitsubishi MELSEC System Q
- Modbus TCP
- OMRON FINS
- OPC UA Binary
- Siemens Industrial Ethernet
- Siemens S7comm™, S7comm-plus
- Yokogawa Vnet/IP
- Релематика BDUBus
- Модификация протокола MMS для устройств ABB AC 800M
- Модификация протокола Modbus TCP для устройств ЭКРА серии 200
- Протокол взаимодействия устройств Moxa серии NPort IA 5000
- Протокол начальной настройки устройств Прософт-Системы
- Протокол устройств с системным ПО Siemens DIGSI 4

Поддержка устройств: ПЛК

- ABB™ AC 700F, 800M
- Allen-Bradley® серий ControlLogix®, CompactLogix™BECKHOFF® серий CX
- Emerson DeltaV серий MD, MD Plus, MQ
- Emerson серии ControlWave
- General Electric RX3i
- Mitsubishi System Q E71
- OMRON серии CJ2M
- Schneider Electric серии Modicon: M580, M340, Momentum
- Siemens™ SIMATIC™ серий S7-200, S7-300, S7-400, S7-1200, S7-1500
- Yokogawa ProSafe-RS
- Yokogawa серий AFV10, AFV30, AFV40
- ПЛК с системой исполнения для CODESYS V3
- Прософт-Системы Regul R500

Поддержка устройств: IED

- ABB серии Relion™: REF615, RED670, REL670, RET670;
- General Electric серии MULTILIN: B30, C60;
- Schneider Electric Sepam серии 80 NPP;
- Siemens серии SIPROTEC™ 4: 6MD66, 7SA52, 7SJ64, 7SS52, 7UM62, 7UT63;
- Релематика ТОР 300;
- ЭКРА серий 200, БЭ2502, БЭ2704;
- устройства, поддерживающие протокол DNP3;
- устройства, поддерживающие протоколы стандарта IEC 60870: IEC 60870-5-101,
- IEC 60870-5-104;
- устройства, поддерживающие протоколы стандарта IEC 61850: IEC 61850-8-1 (GOOSE, MMS),
- IEC 61850-9-2 (Sampled Values);
- устройства, поддерживающие протокол Modbus TCP