KASPERSKY INDUSTRIAL CYBERSECURITY. ОБЗОР РЕШЕНИЯ

KASPERSKY lab

ЛАНДШАФТ УГРОЗ АСУ ТП

НЕДАВНИЕ (ИЗВЕСТНЫЕ) ИНЦИДЕНТЫ

Hackers shut down power grid in Ukraine

It's thought to be the first cyber attack to cause a blackout.

Malware is no longer reserved for the millions of consumer PCs all over the world -- it's now used in corporate espionage, as tool to disrupt the infrastructure of entire countries. It's been revealed that just on December 23rd, attackers were successfully able to infect computers belonging to the Ukrainian national grid, which resulted in hundreds of homes in the Ivano-Frankivsk region going dark. It's thought to be the first cyber attack to result in a power outage.

DEC 2015

JAN 2016

Wed Apr 27, 2016 9:02am EDT
Related: TECH, GERMANY

German nuclear plant infected with computer viruses, operator says

FRANKFURT | BY CHRISTOPH STEITZ AND ERIC AUCHARD

FEB 2016

IRONGATE ICS MALWARE STEALS FROM STUXNET PLAYBOOK

by Tom Spring — June 2, 2016 , 8:45 am

New malware that targets industrial control systems called Irongate was found by researchers who say the discovery should serve as another wakeup call to the security industry to shore up its detection capabilities around ICS and SCADA threats. Irongate, which shares some of the same attributes as the lethal Stuxnet malware, was found by researchers at FireEye Labs Advanced Reverse Engineering which published its findings today.

APRIL 2016

MAY 2016

S. Korea accuses North of hacking railway systems and officials' phones

Published time: 8 Mar, 2016 07:31
Edited time: 8 Mar, 2016 08:17

Get short URL

533

South Korea's National Intelligence Service has accused Pyongyang of attempting to hack into railway control systems and wiretap officials' smartphones as tensions continue to mount on the peninsula.

The National Intelligence Service (NIS) said in a press release on Tuesday that North Korean hackers penetrated the smartphones of dozens of senior South Korean officials, stealing text and voice messages, Yonhap news agency reported.

MAR 2016

The Register®
Biting the hand that feeds IT

DATA CENTRE SOFTWARE NETWORKS SECURITY INFRASTRUCTURE DEVOPS BUSINESS HARDWA

Security

Michigan electricity utility downed by ransomware attack

Don't click on the links, don't click on the links, don't …

3 May 2016 at 01:40, Richard Chirgwin — 64 — 530

A water and electricity authority in the US State of Michigan has needed a week to recover from a ransomware attack that fortunately only hit its enterprise systems.

PLC-Blaster: A Worm Living Solely in the PLC

Ralf Spenneberg, Maik Brüggemann, Hendrik Schwartke

[1]OpenSource Security Ralf Spenneberg

info@os-s.de

Abstract. *Industrial processes are controlled by programmable logic controllers (PLC). Many PLCs sold today are equipped with Ethernet ports and can communicate using IP. Based on the Siemens SIMATIC S7-1200 we will demonstrate a worm. This worm does not require any additional PCs to proliferate. The worm lives and runs only on the PLC. The worm scans the network for new targets (PLCs), attacks these targets and replicates itself onto the found targets. The*

KASPERSKY lab

BLACKENERGY – УКРАИНА, ДЕКАБРЬ 2015

- Дек 2015 – атаки на энергосеть «Прикарпатьеоблэнерго»
- 100 предприятий получили письма с целевым фишингом.
- После кражи учетных записей с доступом в АСУ ТП, подстанции были выключены дистанционно (SSH бэкдор) в ручном режиме. Параллельно происходила DDoS атака на ситуационный call-центр, а вредоносный модуль KillDisk отключал ряд технологических процессов и повреждал данные на серверах АСУ ТП.
- В Ивано-Франковской области более 1000 подстанций были остановлены на несколько часов.

ВЗЛОМ АСУ ТП – СЦЕНАРИЙ КРАЖИ

Наполнение бензовозов «лишним» топливом. Основано на реальных событиях

Система автоматизации взломана. Как это использовать?

Пустой бензовоз приезжает на нефтебазу

Заливка топлива… с «небольшой» поправкой

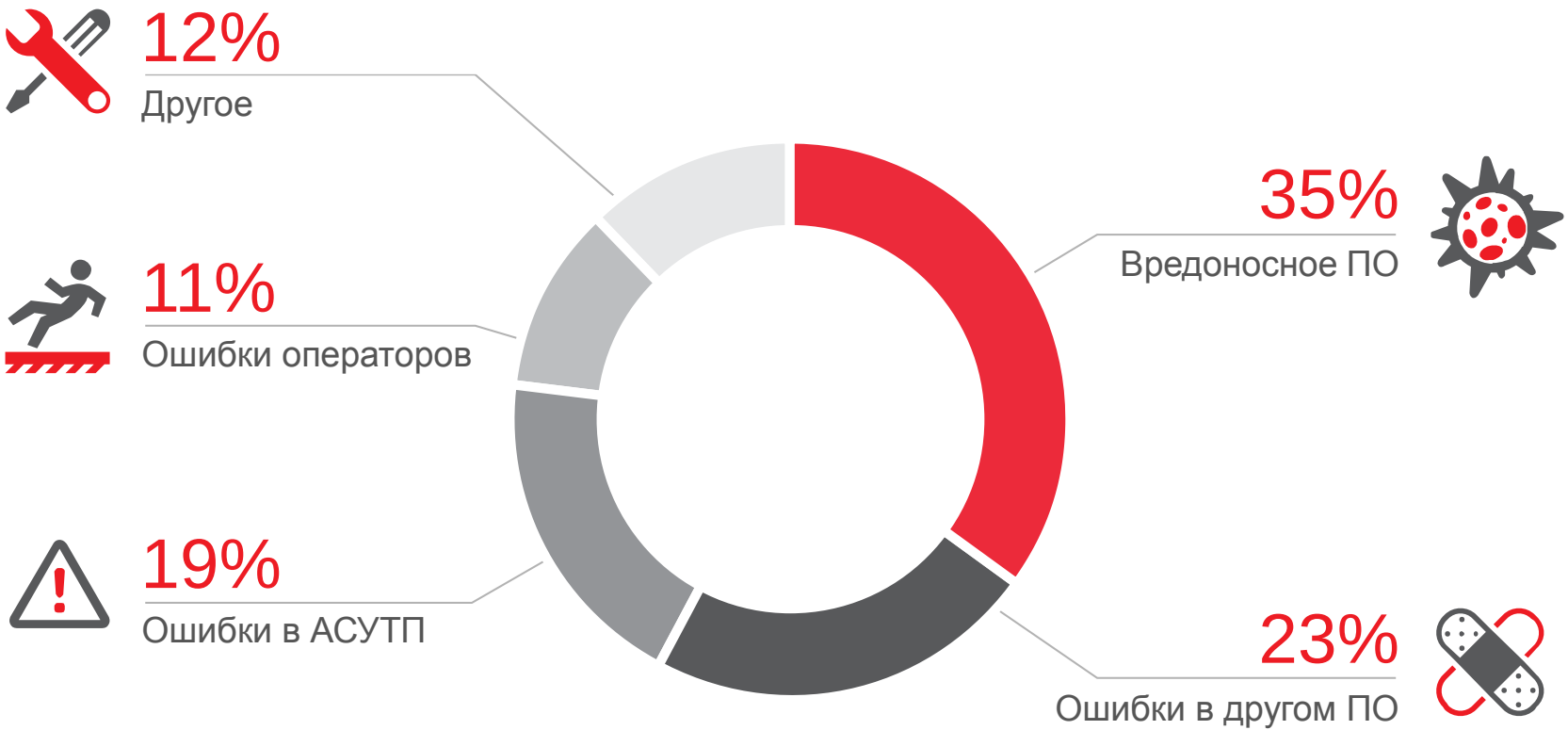
Бензовоз покидает нефтебазу

«Лишнее» топливо сливается

2% топлива с каждого бензовоза

KASPERSKY lab

ПРИЧИНЫ ИНЦИДЕНТОВ



Источник: RISI Annual Summary 2013

KASPERSKY lab

В ЧЕМ СЛОЖНОСТЬ ЗАЩИТЫ

Слабая осведомленность, отсутствие точных данных и обилие недостоверной информации

Невозможно применить традиционные «офисные» подходы к обеспечению безопасности

Большинство атак нацелены на устаревшие, незащищенные и с трудом поддающиеся обновлениям объекты

Отсутствие навыков борьбы с киберугрозами и практического опыта обеспечения кибербезопасности в промышленности

Нет понимания того, насколько важна защищенность от кибератак для промышленных предприятий

KASPERSKY lab

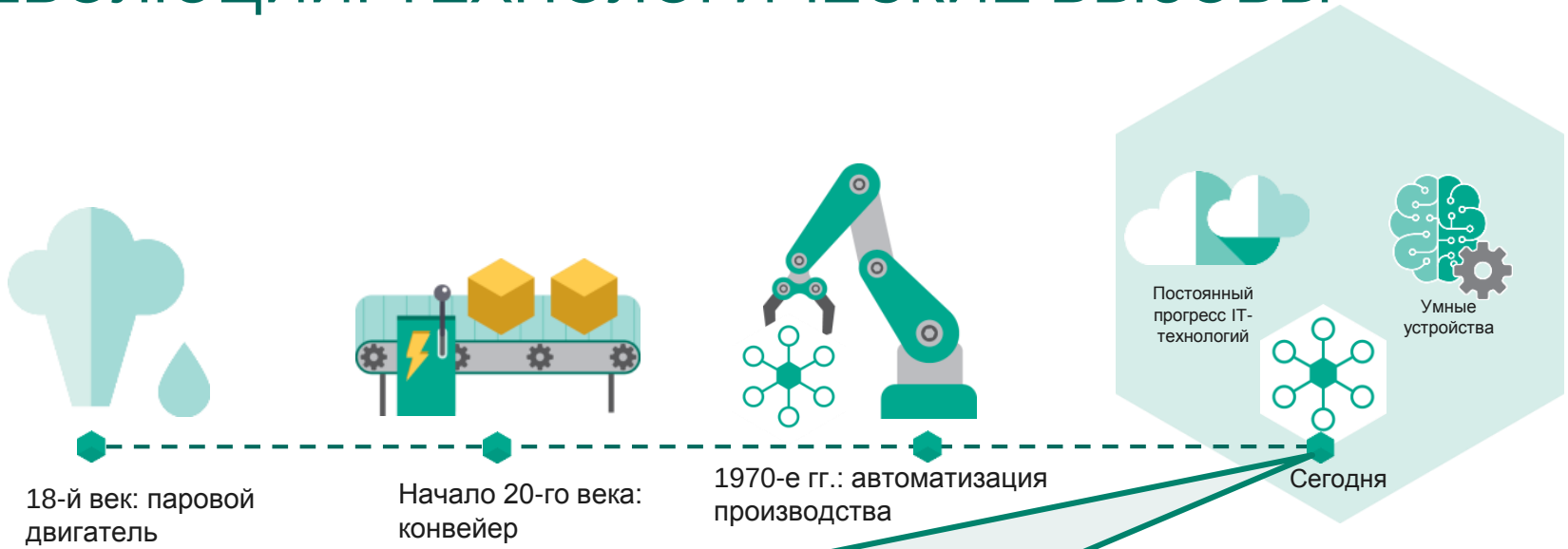
О ПРОМЫШЛЕННОЙ СПЕЦИФИКЕ

ДРУГИЕ ПРИОРИТЕТЫ БЕЗОПАСНОСТИ

1. ДОСТУПНОСТЬ
2. ЦЕЛОСТНОСТЬ
3. КОНФИДЕНЦИАЛЬНОСТЬ

1. КОНФИДЕНЦИАЛЬНОСТЬ
2. ЦЕЛОСТНОСТЬ
3. ДОСТУПНОСТЬ

НА ПОРОГЕ ЧЕТВЕРТОЙ ПРОМЫШЛЕННОЙ РЕВОЛЮЦИИ: ТЕХНОЛОГИЧЕСКИЕ ВЫЗОВЫ



Потоковые вычисления

Интернет вещей в промышленности

Аддитивное производство

Межмашинное взаимодействие

КОМПЛЕКСНЫЙ ПОДХОД К ОБЕСПЕЧЕНИЮ КИБЕРБЕЗОПАСНОСТИ ПРОМЫШЛЕННЫХ СИСТЕМ

Уровень 4
Планирование бизнеса и логистика

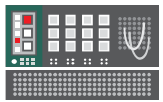
Управление всей цепочкой снабжения: финансы,производство, использование материалов, доставка и транспортные операции.

Уровень 3
Управление производственными операциями

Управление и учет производственных операций. Ведение записей и оптимизация производственного процесса.

Уровень 2, 1
Групповое управление, непрерывное управление, дискретное управление

Мониторинг, диспетчерский контроль и автоматизированное управление производственным процессом



Измерение и задание параметров производственного процесса

Уровень 0
Физический

Физические устройства

Kaspersky Security для бизнеса и профессиональные сервисы

Kaspersky Industrial CyberSecurity

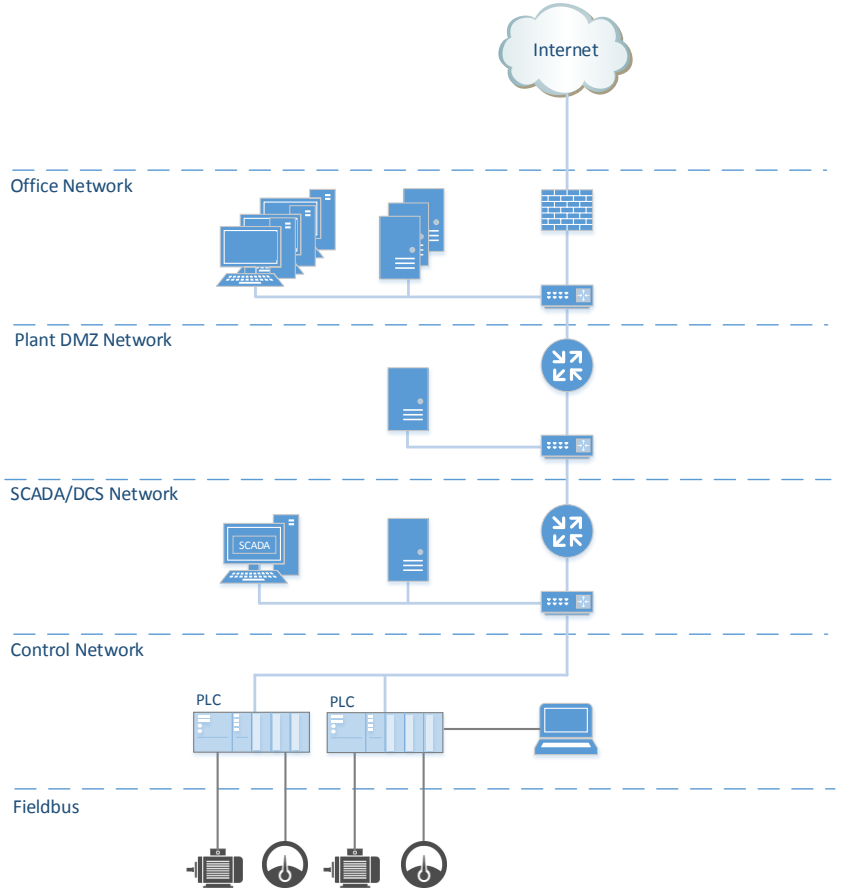
Физическая безопасность

KASPERSKY INDUSTRIAL CYBERSECURITY: СТРУКТУРА РЕШЕНИЯ

KASPERSKY lab

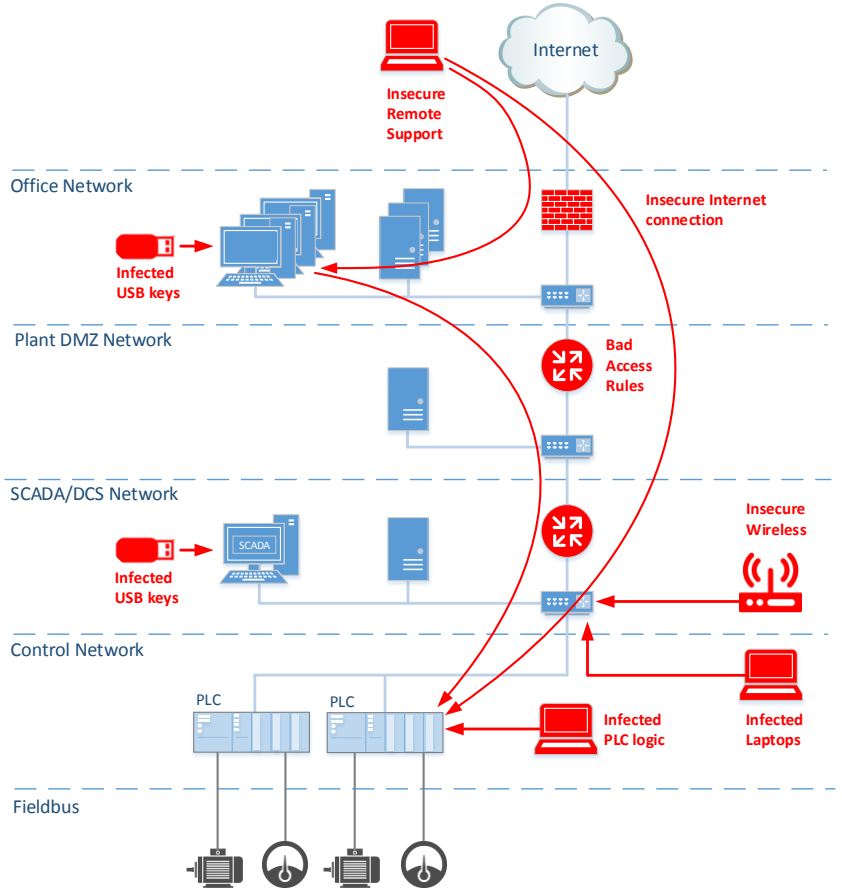
ОБЗОР РЕШЕНИЯ

ТИПОВАЯ АРХИТЕКТУРА



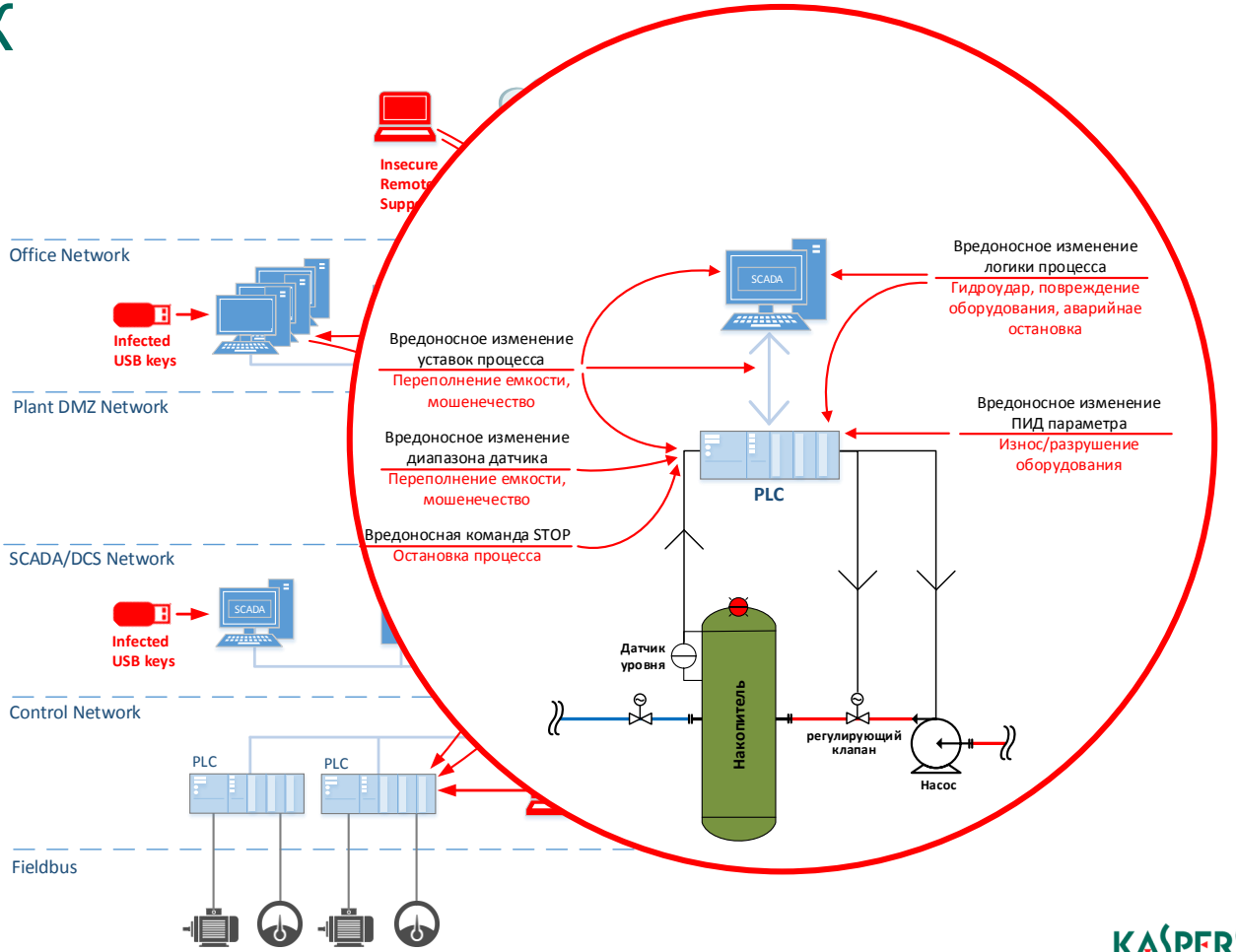
KASPERSKY lab

ВЕКТОРА АТАК

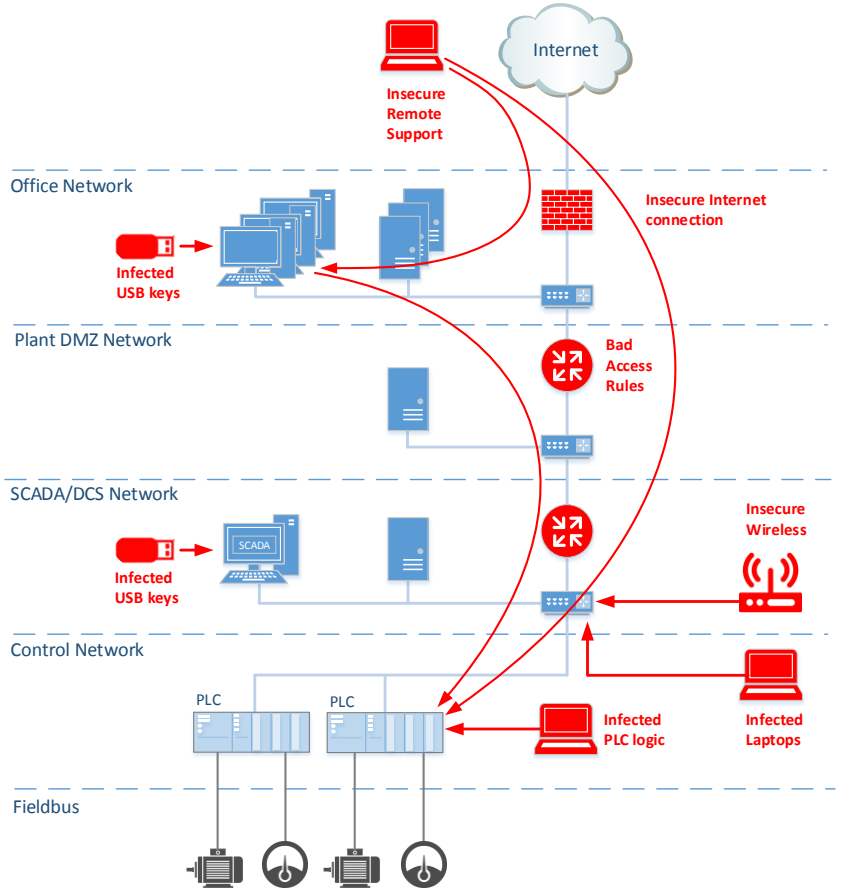


KASPERSKY lab

ВЕКТОРА АТАК

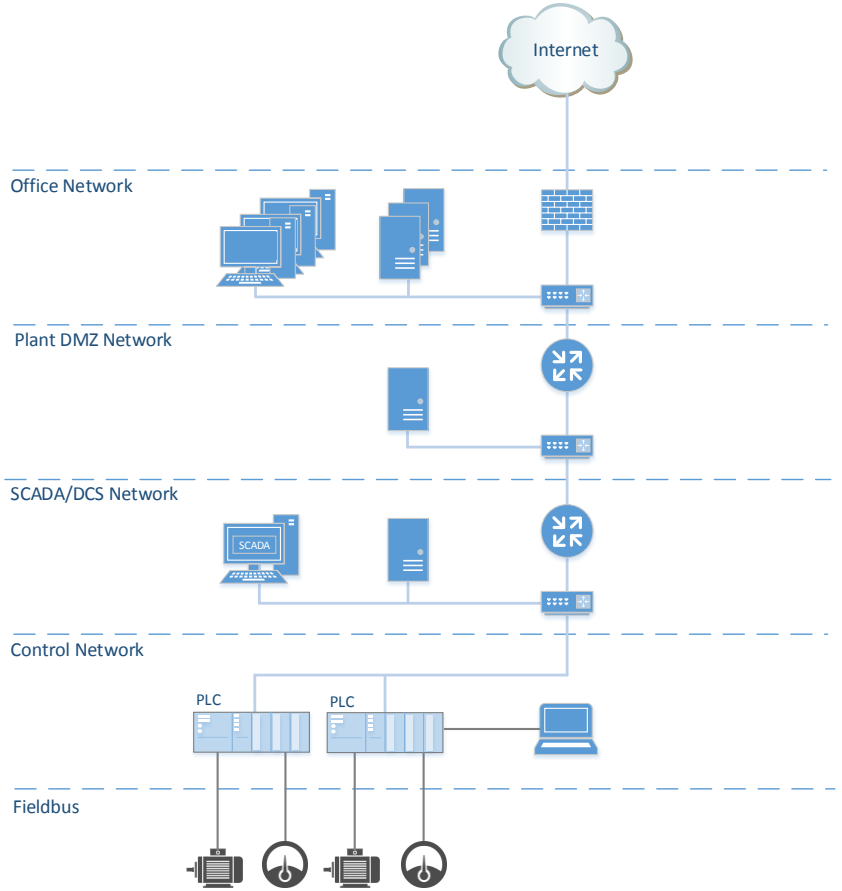


ВЕКТОРА АТАК

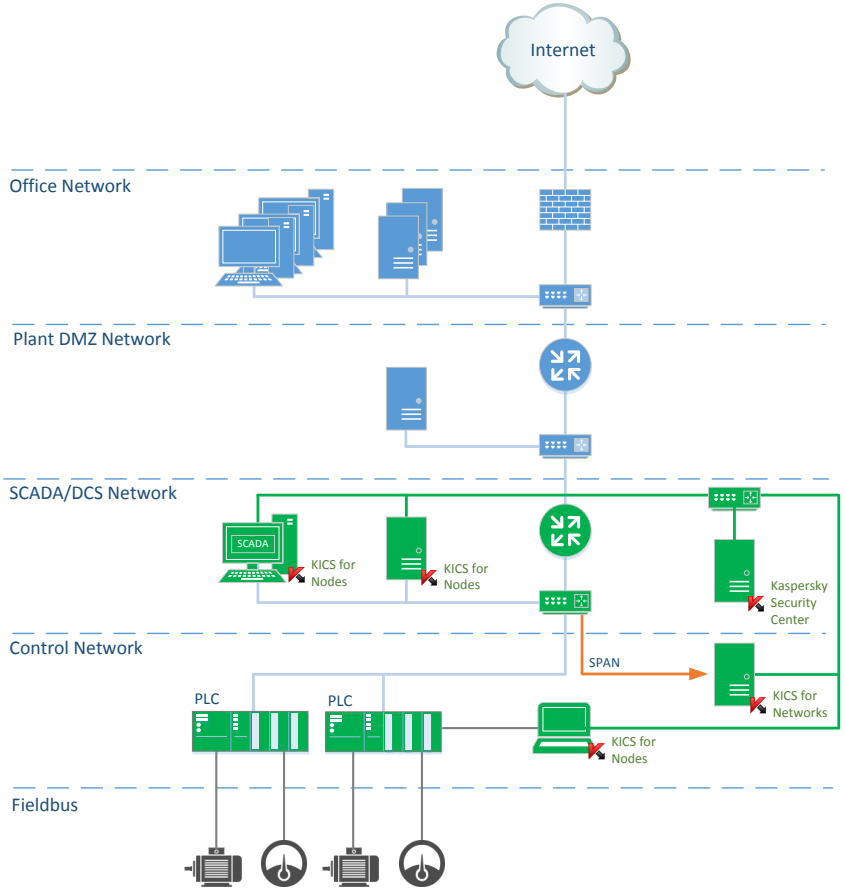


KASPERSKY lab

KASPERSKY INDUSTRIAL CYBERSECURITY

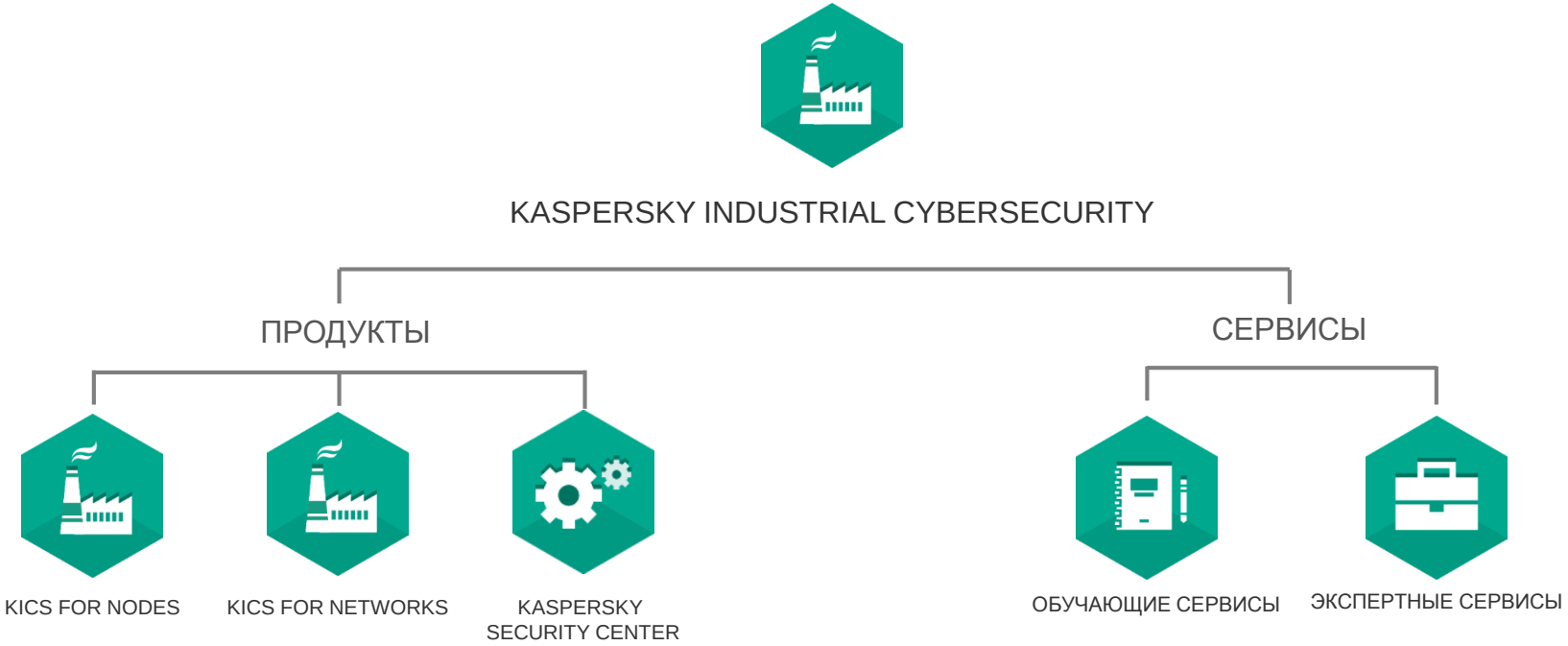


KASPERSKY INDUSTRIAL CYBERSECURITY



КИБЕРБЕЗОПАСНОСТЬ — ПОСТОЯННЫЙ ПРОЦЕСС

KASPERSKY INDUSTRIAL CYBERSECURITY: СТРУКТУРА РЕШЕНИЯ



KASPERSKY INDUSTRIAL CYBERSECURITY (KICS) СЕРВИСЫ

Обучающие сервисы

- Тренинги для специалистов по безопасности
- Программа повышения осведомленности
- Деловая игра KIPS

Экспертные сервисы

- Анализ защищенности / Cyber Security Assessment
- Проектирование и внедрение решения
- Поддержка и сопровождение решения
- Реагирование и расследование инцидентов

KASPERSKY INDUSTRIAL CYBERSECURITY (KICS) ТЕХНОЛОГИИ

Kaspersky Industrial CyberSecurity for Nodes (KICS for Nodes)

Защита рабочих станций, серверов и ПЛК в промышленной сети от угроз

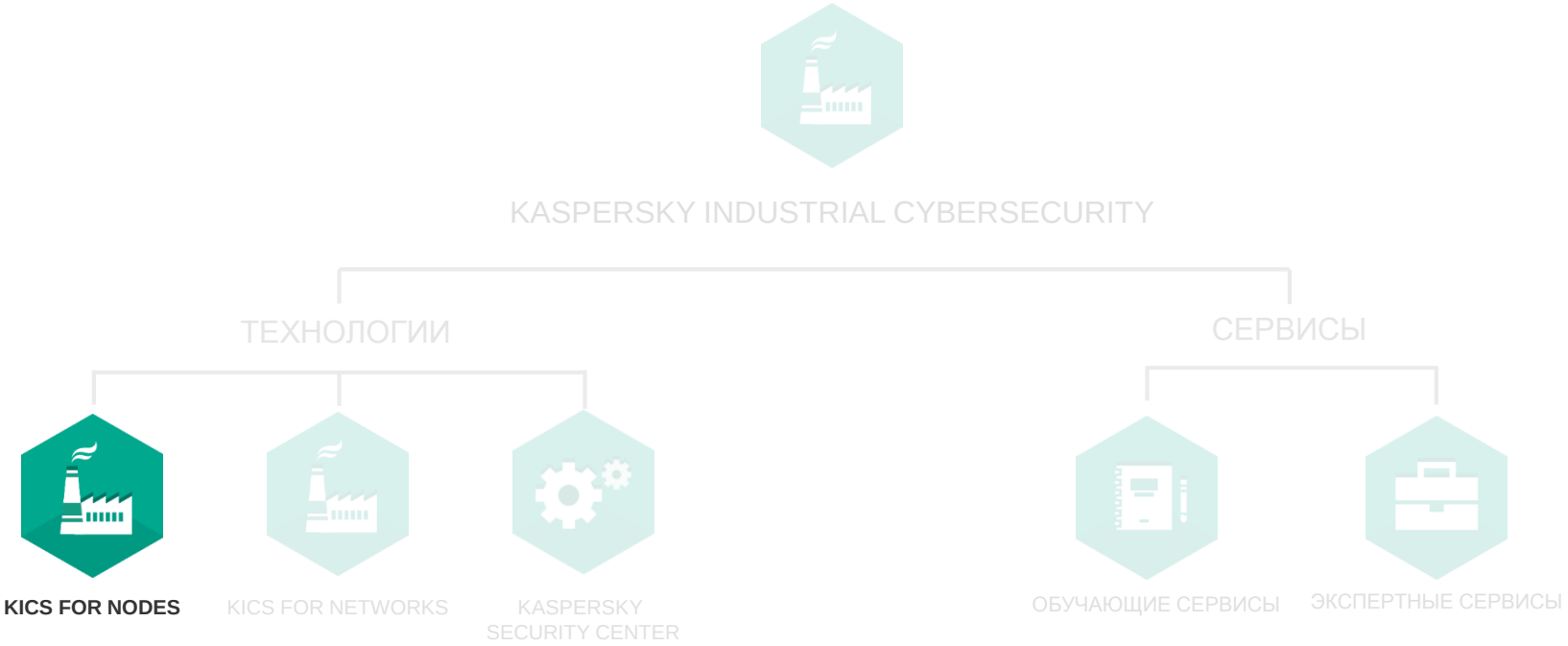
Kaspersky Industrial CyberSecurity for Networks (KICS for Networks)

Пассивный мониторинг сетевого трафика промышленной сети и обнаружение угроз

Kaspersky Security Center (KSC)

Централизованный мониторинг и управление компонентами KICS

KASPERSKY INDUSTRIAL CYBERSECURITY:



KICS FOR NODES
ФУНКЦИОНАЛ

Application control

Предотвращение и мониторинг запуска неразрешенных приложений (вирусы, плееры, игры и т.д.)

Device Control

Предотвращение подключения неразрешенных устройств (USB носители, беспроводные адаптеры, 3G модемы)

Antimalware

Блокирование ВПО (эвристические и сигнатурные методы)

Vulnerability monitor

Обнаружение уязвимых приложений на АРМ и серверах

Host-based firewall

Фильтрация сетевого трафика на уровне АРМ и серверов

PLC Integrity checker

Контроль целостности программ PLC

KICS FOR NODS
ПОДДЕРЖИВАЕМЫЕ ОС

Windows XP Professional SP3 и выше:

Windows 7 Professional / Enterprise / Ultimate SP1 и выше

Windows 7 Professional / Enterprise / Ultimate x64 Edition SP1 и выше

Windows Server® 2003 R2 Standard / Enterprise SP2 и выше

Windows Server 2003 R2 Standard / Enterprise x64 Edition SP2 и выше

Windows Server 2003 Standard / Enterprise SP2 и выше

Windows Server 2003 Standard / Enterprise x64 Edition SP2 и выше

Windows Server 2008 R2 Standard / Enterprise x64 Edition

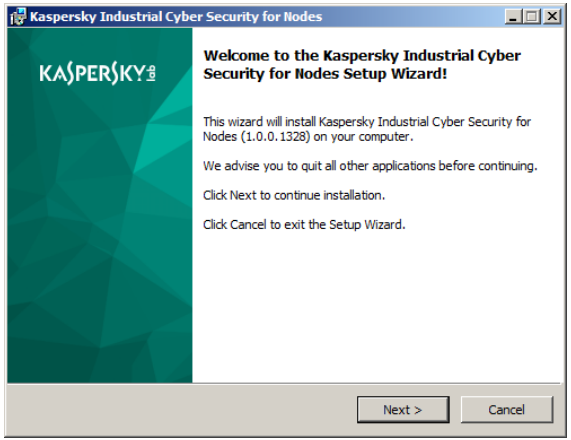
Windows Server 2008 R2 Standard / Enterprise x64 Edition SP1 и выше

--

Windows XP Professional SP2

Windows 10

Windows Embedded

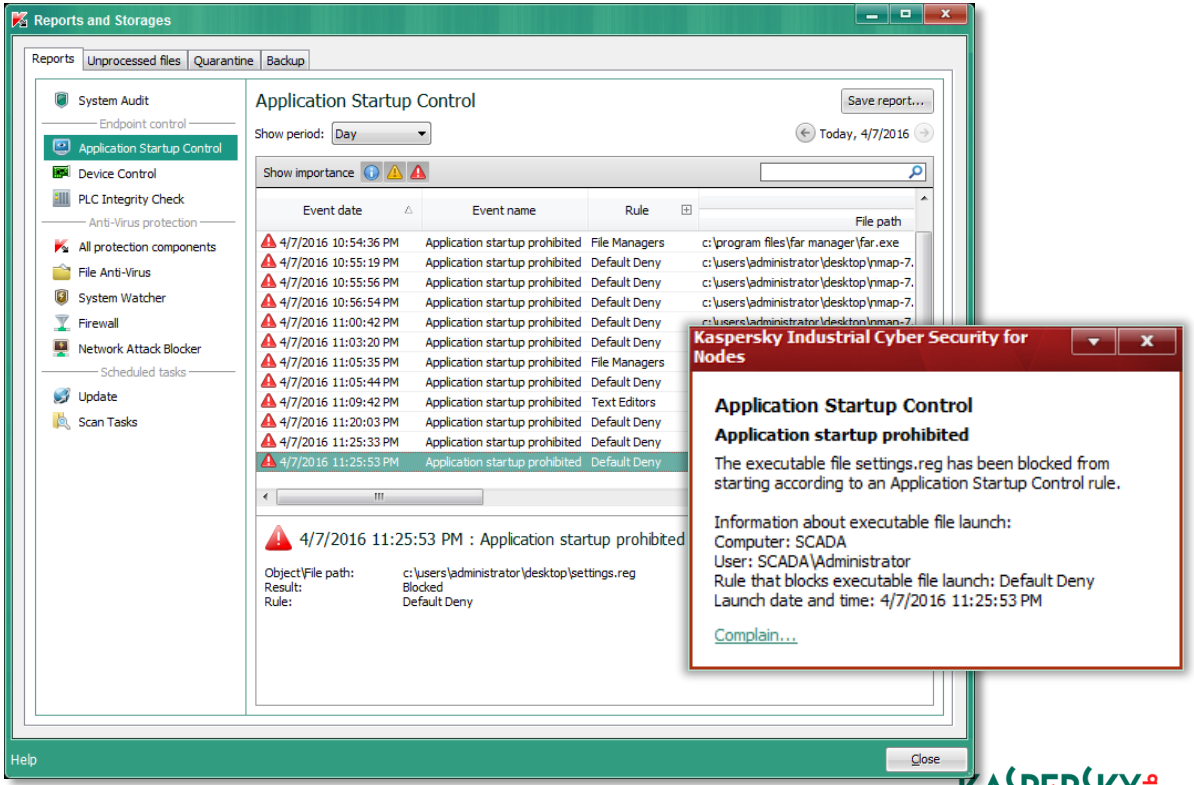


KICS FOR NODES VS KES

- Оптимизированный набор компонентов
- Самостоятельная реализация Контроль запуска программ
- Добавлена Проверка целостности проектов PLC
- Самоограничение потребления ресурсов
- Возможность обновления с внешнего носителя
- Возможность работы без перезагрузки до полугода
- Отключение монитора antimalware / только плановые проверки
- Сертификация с разработчиками компонент АСУ ТП

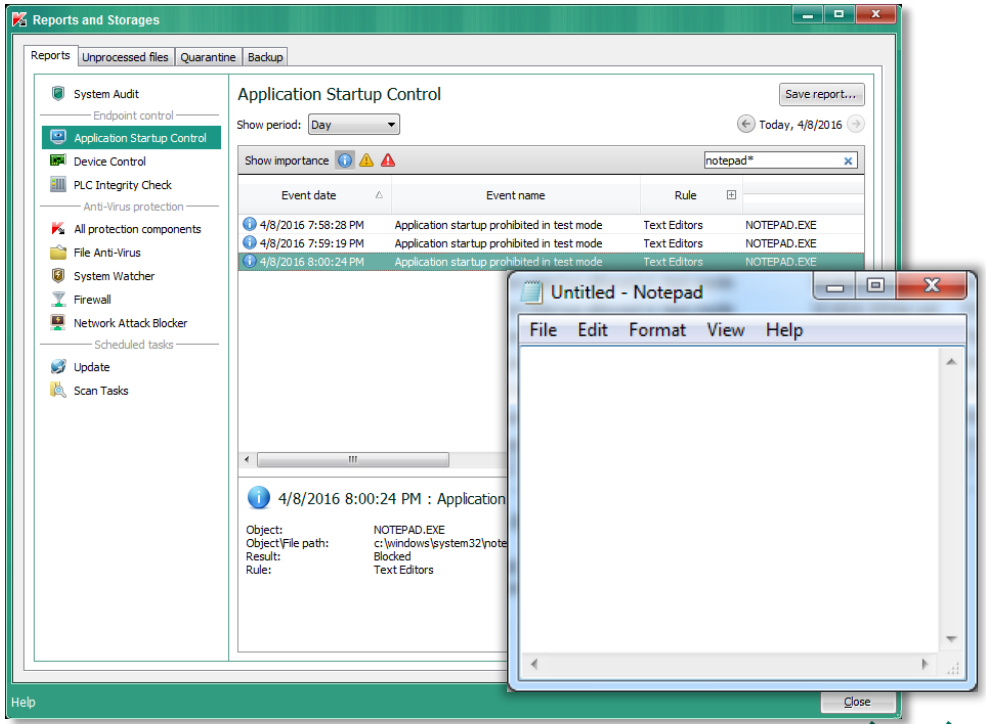
KICS FOR NODES
APPLICATION CONTROL

- Portable executables
  .exe, .scr, .sys
- rundll32.exe
  .dll
- cmd.exe
  .bat
  .cmd
  .com
- msiexec.exe
  .msi
- mmc.exe
  .msc
- wscript.exe / cscript.exe
  .js
  .vbs
  .wsf
- regedit.exe
  .reg



KICS FOR NODES
APPLICATION CONTROL / ТЕСТОВЫЙ РЕЖИМ

Тестовый режим работы может применяться как для тестирования правил запуска приложений, так и для пассивного мониторинга узлов информационной системы



KICS FOR NODES
PLC INTEGRITY CHECKER

— Компонент предназначен для периодической проверки целостности проектов ПЛК

— Принцип работы

Администратор назначает для каждого ПЛК эталонный проект

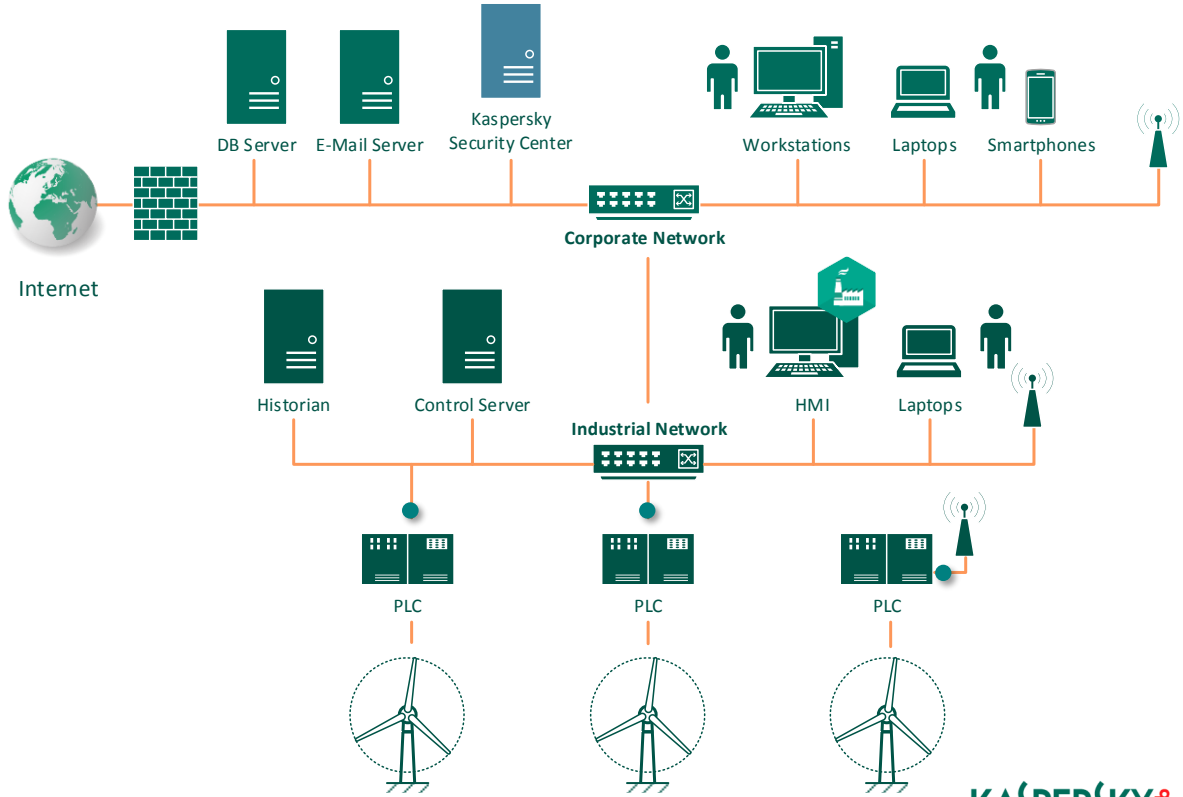
KICS for Nodes периодически опрашивает ПЛК и сравнивает текущий проект с эталонным

В случае расхождения контрольной суммы генерируется событие нарушения целостности проекта

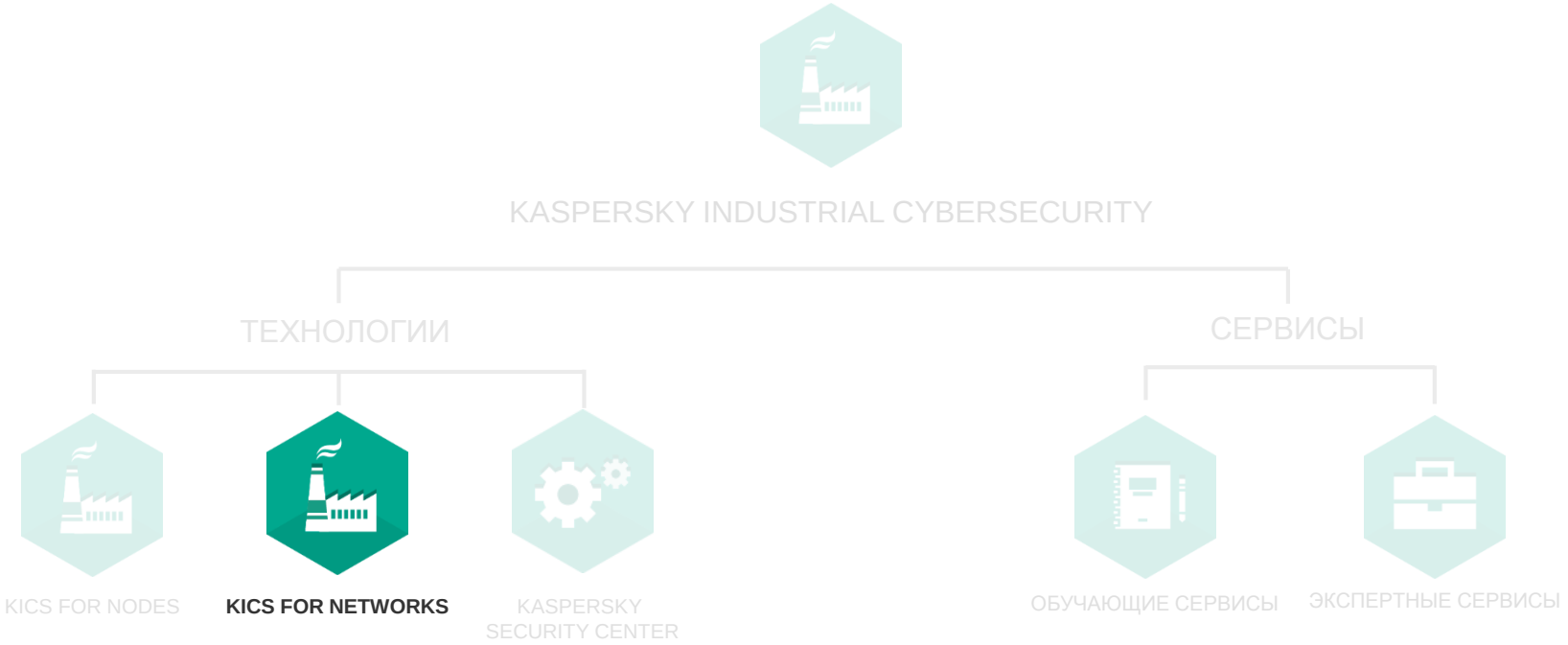
— KICS for Nodes защищает следующие модели ПЛК:

Siemens Simatic серии S7-300

Siemes Simatic серии S7-400



KASPERSKY INDUSTRIAL CYBERSECURITY:



KICS FOR NETWORKS
ФУНКЦИОНАЛ

Пассивное обнаружение в трафике промышленной сети …

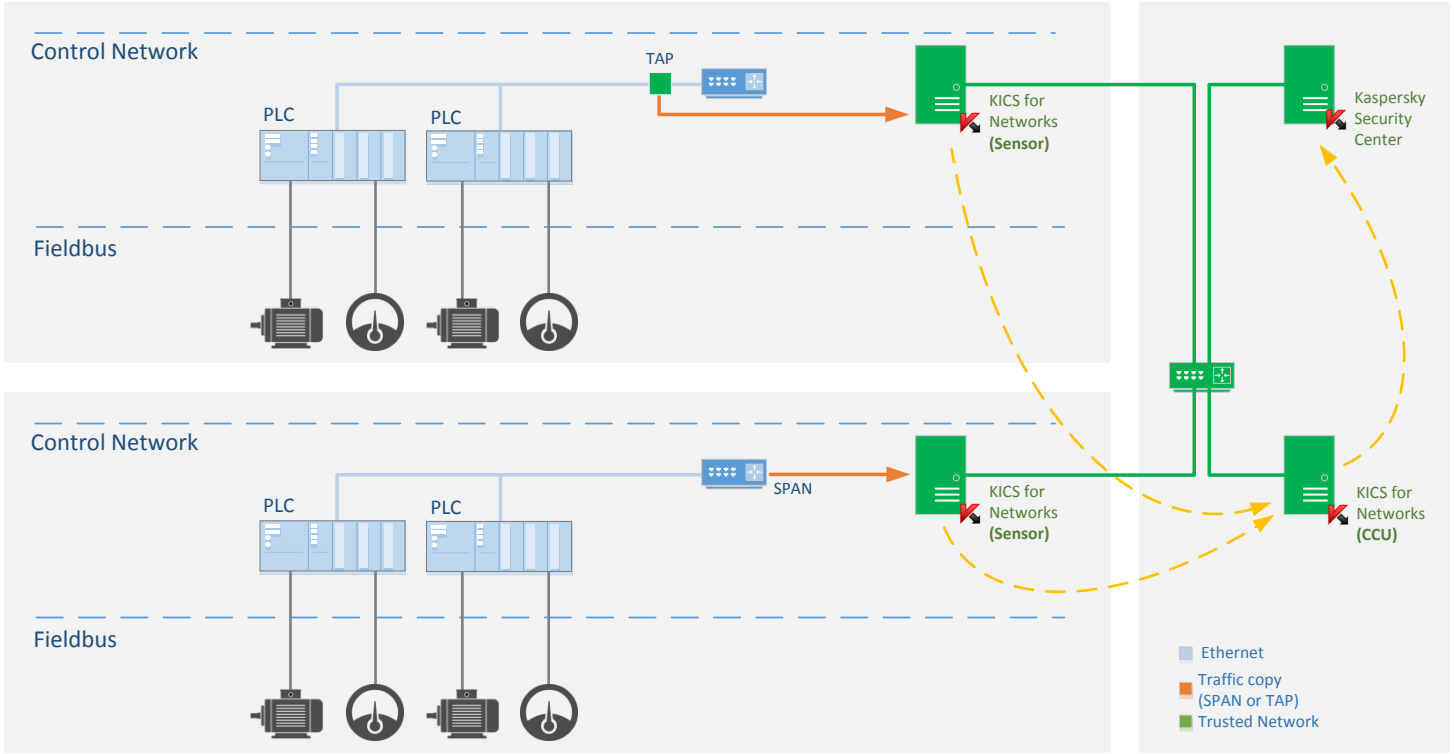
NETWORK INTEGRITY CONTROL

- … несанкционированных сетевых устройств
- … аномальных сетевых потоков между устройствами

PROCESS INTEGRITY CONTROL

- … критических команд, посылаемых на PLC
- … изменений значений параметров техпроцесса

KICS FOR NETWORKS
АРХИТЕКТУРА



KICS FOR NETWORKS
PROCESS INTEGRITY CONTROL (ПОДХОД)

- Изучение технологического процесса с технологами и программистами АСУ ТП объекта
- Моделирование сценариев возможных промышленных аварий
- Подключение KICS for Networks к точкам сбора сетевого трафика
- Импорт тегов из систем для формирование правил отклонения параметров от нормы
- Формирование, применение и тестирование правил
- Эксплуатация системы, мониторинг, обнаружение отклонений от правил
- Проведение расследование инцидента
- Внесение изменений по результатам инцидента

KICS FOR NETWORKS
ПОДДЕРЖИВАЕМЫЕ ПЛК

Vendor*	Model*
Siemens	Siemens Simatic S7-300 Siemens Simatic S7-400
Schneider Electric	Modicom Momentum Modicom M340
Allen-Bradley / Rockwell Automation	ControlLogix 5571 with Communication Modules 1756-EN2TRB.
Mitsubishi	MELSEC-Q
Any	Any models with IEC 61850 support
Any	Any models with IEC 60870-5-104 support

*Новое оборудование добавляется по плану,
а так же по запросу в течении 3 – 6 месяцев

KICS FOR NETWORKS
ПОДДЕРЖИВАЕМЫЕ КОМАНДЫ ПЛК

- Команды аутентификации на оборудовании
- Команды запуска / остановки PLC;
- Команды установки / разрыва соединения
- Команды очистки памяти PLC.
- Команды чтения / записи программы в PLC;
- Команды чтения / записи конфигурации в терминал
- Команды чтения / записи параметров в терминал
- …

KICS FOR NETWORKS
ПОДДЕРЖИВАЕМЫЕ SCADA

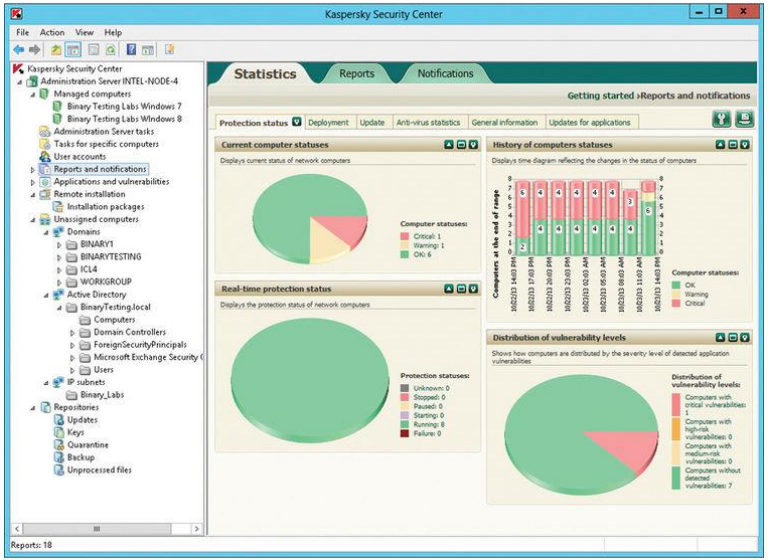
Vendor	Software/Version
Siemens	SIMATIC Win CC 7.X
Schneider Electric	Citect SCADA 7.X
General Electric	Proficy iFix 5.X
General Electric	Unity Pro XL 4.0
ARC Informatique	PcVue 10.x и 11.x

*Для автоматизации процесса импорта тегов, а так же в ручном режиме

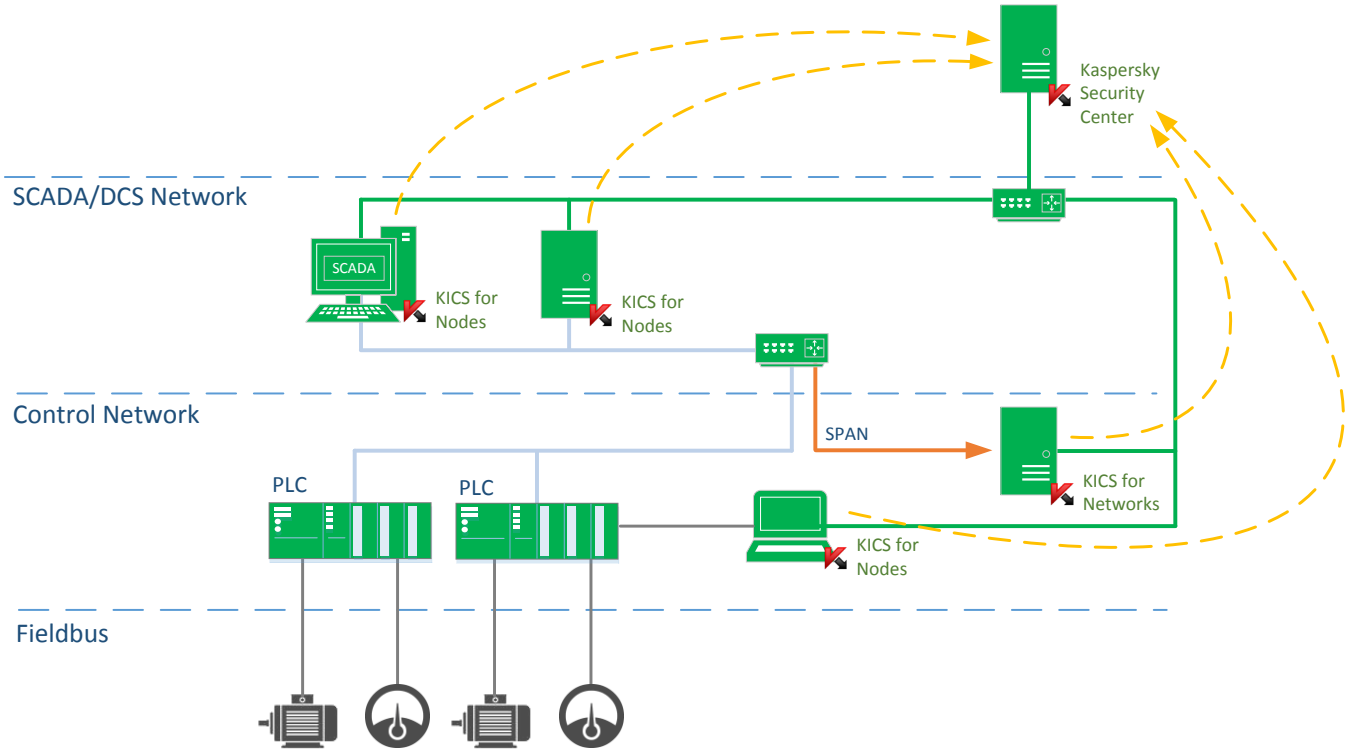
KASPERSKY INDUSTRIAL CYBERSECURITY:

KASPERSKY SECURITY CENTER ФУНКЦИОНАЛ

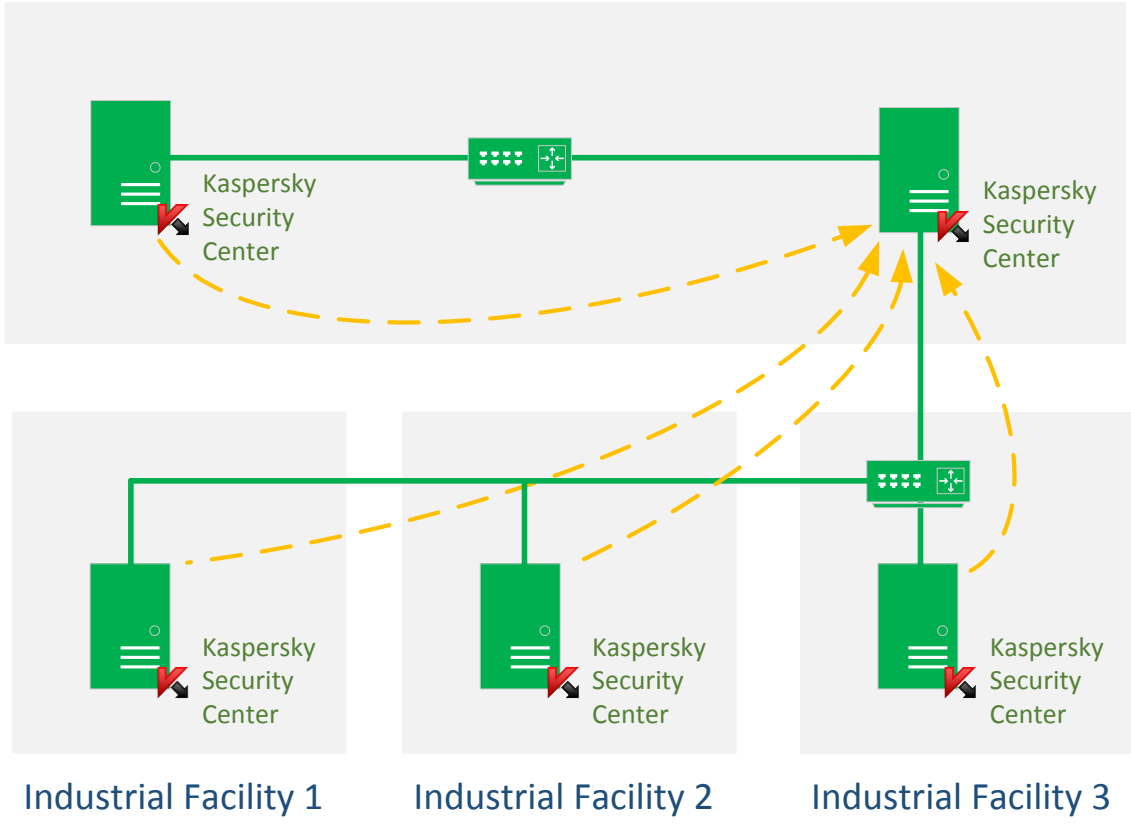
- Централизованное управление и мониторинг, на уровне устройств и групп
- Централизованное обновление сигнатурных баз
- Централизованное установка агентов
- Ролевое управление
- Интеграция SIEM, HMI, ERP, BI



KASPERSKY SECURITY CENTER
ЦЕНТРАЛИЗАЦИЯ



KASPERSKY SECURITY CENTER ИЕРАРХИЯ



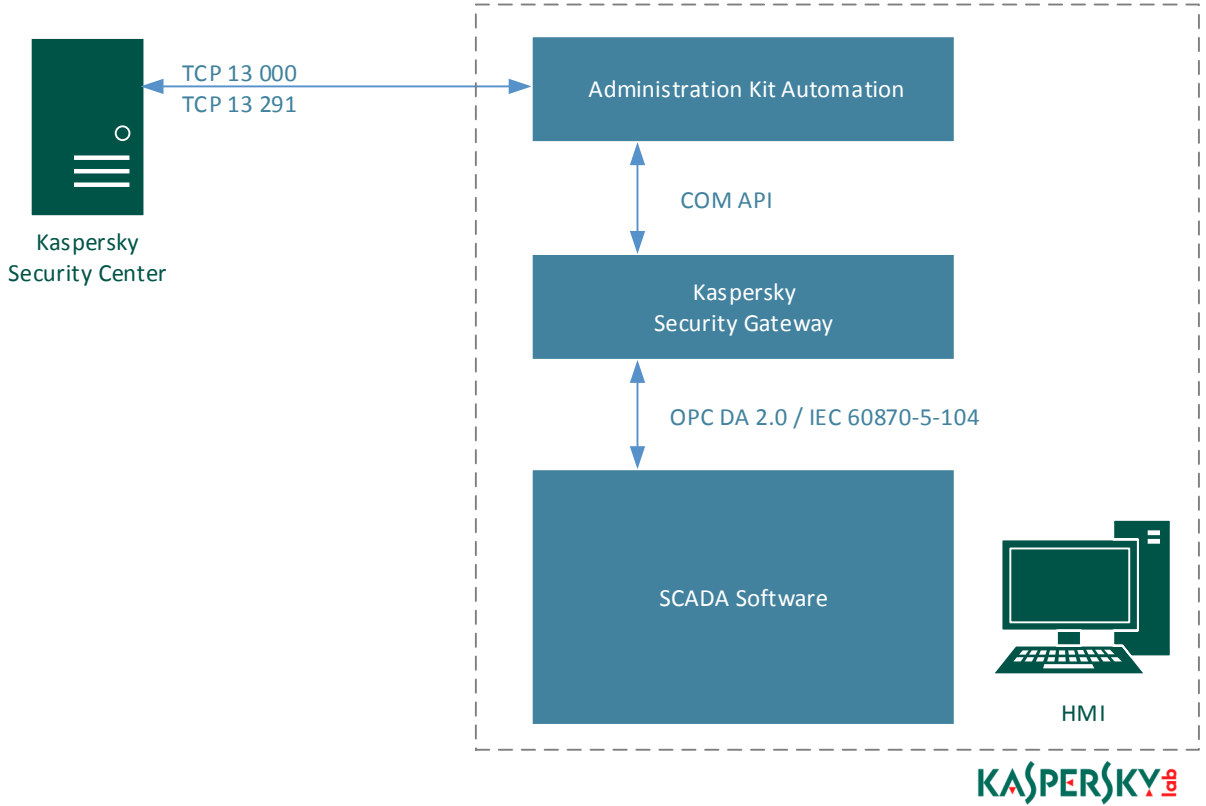
ИНТЕГРАЦИЯ KSC С HMI

- Kaspersky Security Gateway поддерживает два протокола обмена данными со SCADA

  IEC 60870-5-104

  OPC 2.0 DA

- Связь с сервером администрирования осуществляется через механизм автоматизации KLAKAUT



KASPERSKY lab

РЕАЛИЗОВАННЫЕ ПРОЕКТЫ

ЗАЩИТА ТРАНСПОРТНОГО ТЕРМИНАЛА VARS

ЗАДАЧА:

Терминал является местом хранения и перевалки токсических материалов: поэтому противодействие вирусным атакам жизненно важно для ведения бизнеса.

ОСОБЕННОСТИ:

- Защита в изолированной среде
- Контроль на основе белых списков

«Решение Kaspersky Industrial CyberSecurity полностью удовлетворяло нашим требованиям, а также обеспечило такие функции, как контроль устройств и возможность централизованного управления и мониторинга состояния защищенных узлов».
Роман Янукович, технический директор, VARS

ТАНЕКО ЗАЩИЩАЕТ ПРОИЗВОДСТВЕННЫЕ МОЩНОСТИ

TANECO

ЗАДАЧА:

Поддержание непрерывности технологических процессов как основной приоритет компании

ОСОБЕННОСТИ

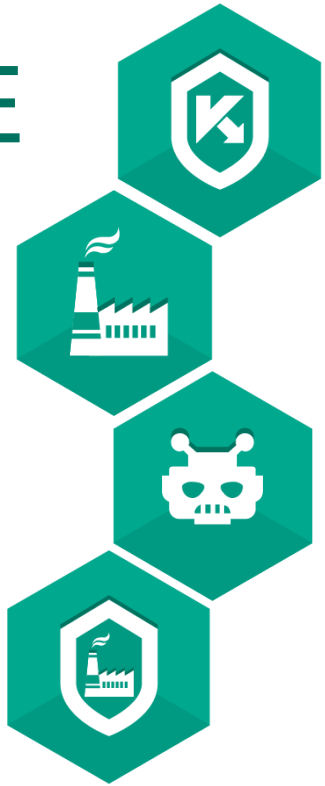
- Оперативная поддержка на всех этапах
- Обнаружение несанкционированных подключений

«Уже в первые месяцы работы решение по защите индустриальных объектов «Лаборатории Касперского» обнаружило несанкционированное подключение стороннего ноутбука к одному из контроллеров, а также попытку изменить параметры работы датчика».
Марат Гильметдинов, начальник отдела АСУ ТП, ТАНЕКО

KASPERSKY lab

СПАСИБО ЗА ВНИМАНИЕ

KASPERSKY.RU/ICS



KASPERSKY lab