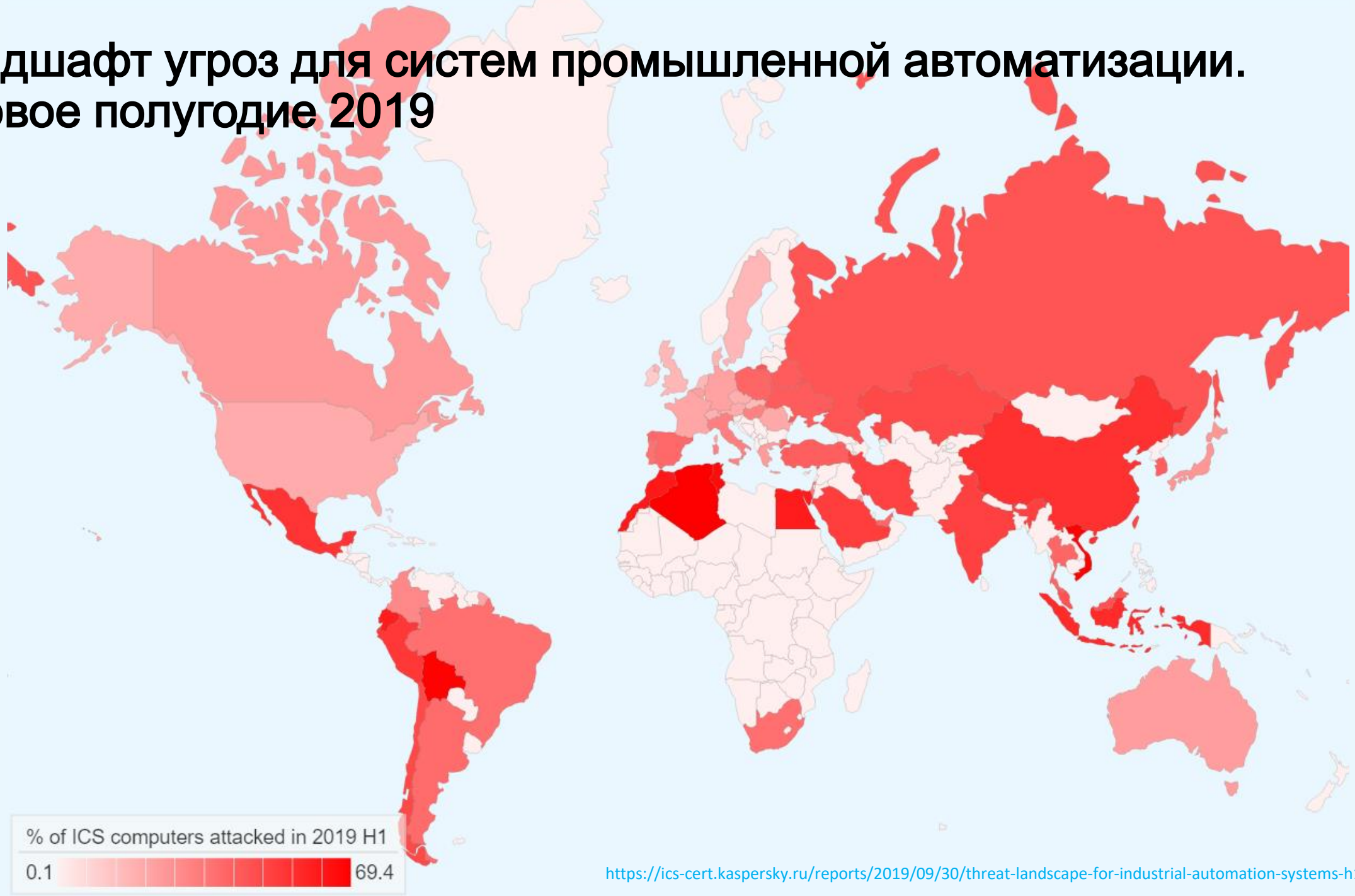
kaspersky

Kaspersky
Industrial
CyberSecurity

Kaspersky Industrial CyberSecurity

Петухов Алексей
Руководитель направления защиты промышленных систем

Ландшафт угроз для систем промышленной автоматизации. Первое полугодие 2019



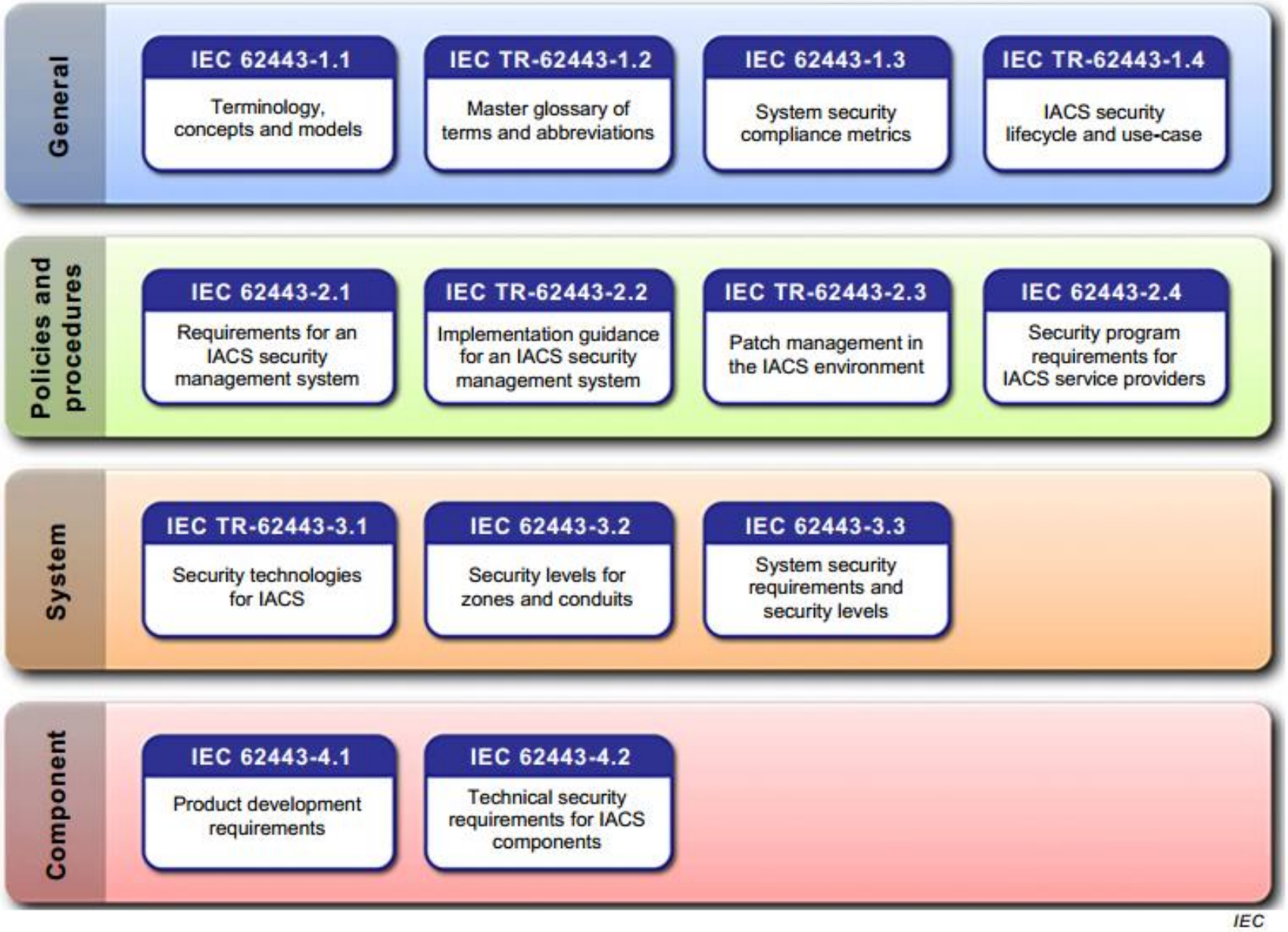
https://ics-cert.kaspersky.ru/reports/2019/09/30/threat-landscape-for-industrial-automation-systems-h1-2019/


S. GÄRTNER
the production people, and from technical customer service.
Hydro
HYDRO

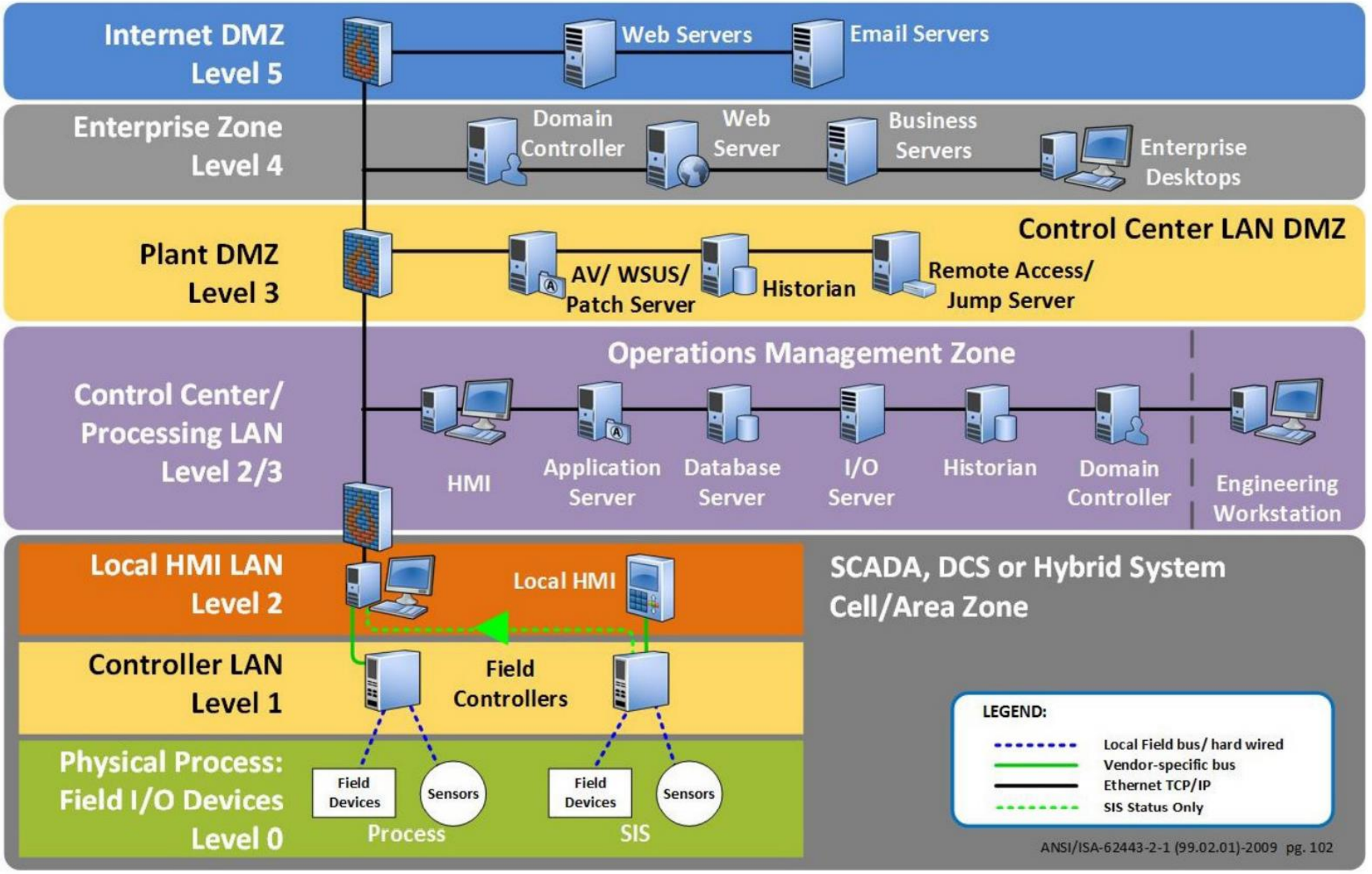
Зачастую риски приемлемы для предприятия

но не допустимы для Государства

Kaspersky


General
IEC 62443-1.1
Terminology, concepts and models
IEC TR-62443-1.2
Master glossary of terms and abbreviations
IEC 62443-1.3
System security compliance metrics
IEC TR-62443-1.4
IACS security lifecycle and use-case
Policies and procedures
IEC 62443-2.1
Requirements for an IACS security management system
IEC TR-62443-2.2
Implementation guidance for an IACS security management system
IEC TR-62443-2.3
Patch management in the IACS environment
IEC 62443-2.4
Security program requirements for IACS service providers
System
IEC TR-62443-3.1
Security technologies for IACS
IEC 62443-3.2
Security levels for zones and conduits
IEC 62443-3.3
System security requirements and security levels
Component
IEC 62443-4.1
Product development requirements
IEC 62443-4.2
Technical security requirements for IACS components
IEC

Kaspersky

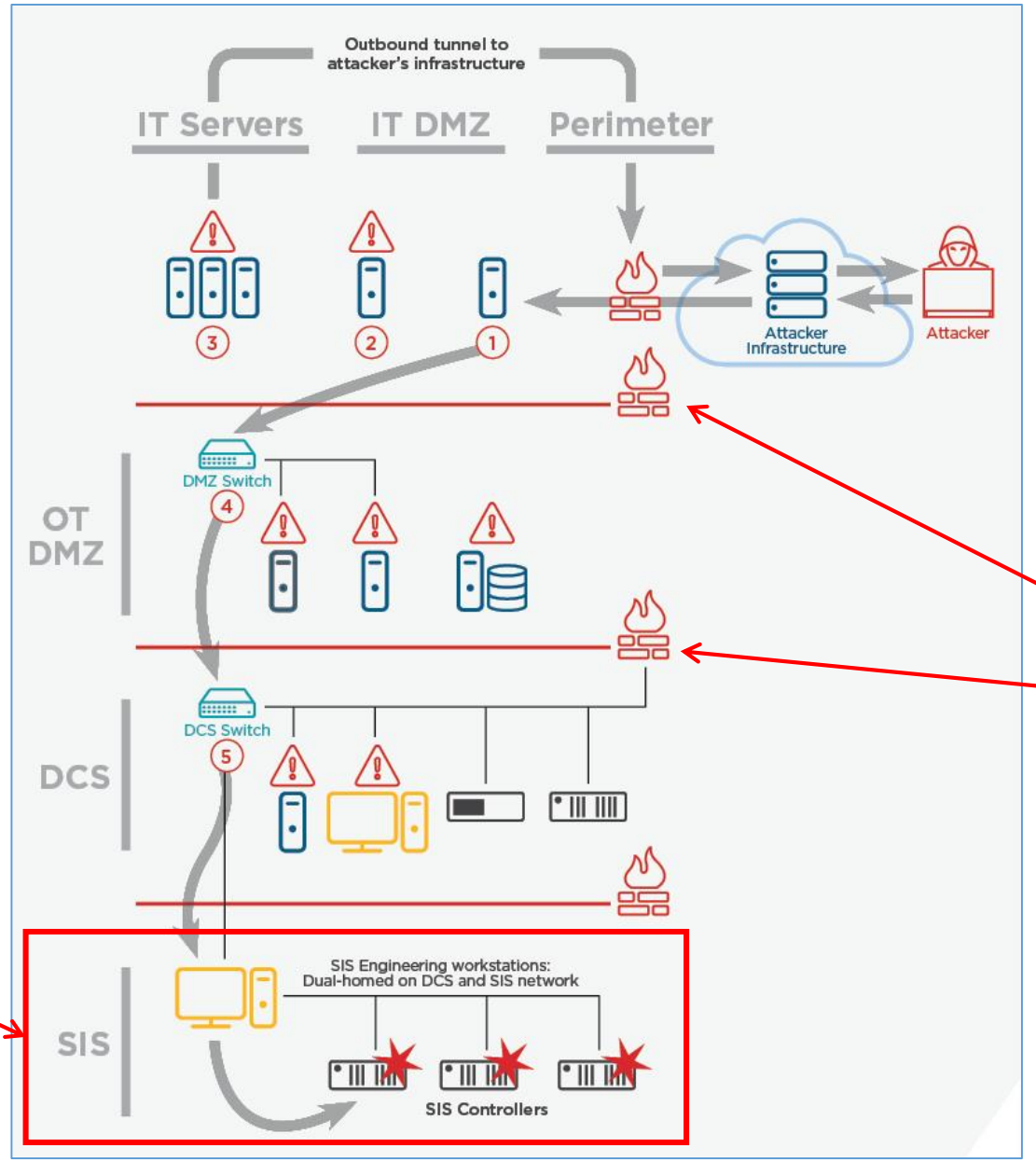

Internet DMZ
Level 5
Web Servers
Email Servers
Enterprise Zone
Level 4
Domain Controller
Web Server
Business Servers
Enterprise Desktops
Plant DMZ
Level 3
Control Center LAN DMZ
AV/ WSUS/ Patch Server
Historian
Remote Access/ Jump Server
Control Center/ Processing LAN
Level 2/3
Operations Management Zone
HMI
Application Server
Database Server
I/O Server
Historian
Domain Controller
Engineering Workstation
Local HMI LAN
Level 2
Local HMI
SCADA, DCS or Hybrid System
Cell/Area Zone
Controller LAN
Level 1
Field Controllers
Physical Process:
Field I/O Devices
Level 0
Field Devices
Sensors
Process
Field Devices
Sensors
SIS
LEGEND:
Local Field bus/ hard wired
Vendor-specific bus
Ethernet TCP/IP
SIS Status Only
ANSI/ISA-62443-2-1 (99.02.01)-2009 pg. 102

Kaspersky

Petro Rabigh

июнь 2017 года

TRITON / Путь атаки



Исследовано ранее

Не хватило!

Kaspersky

Kaspersky Industrial CyberSecurity

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

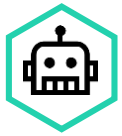
Повышение осведомлённости по защите OT систем

Kaspersky®
Security Awareness

Специализированные решения

KICS
for Nodes

KICS
for Networks



Machine Learning
for Anomaly
Detection

Pen Test and Assessment

Kaspersky®
Security Assessment

Kaspersky

Kaspersky Industrial CyberSecurity

Industrial Endpoint Protection

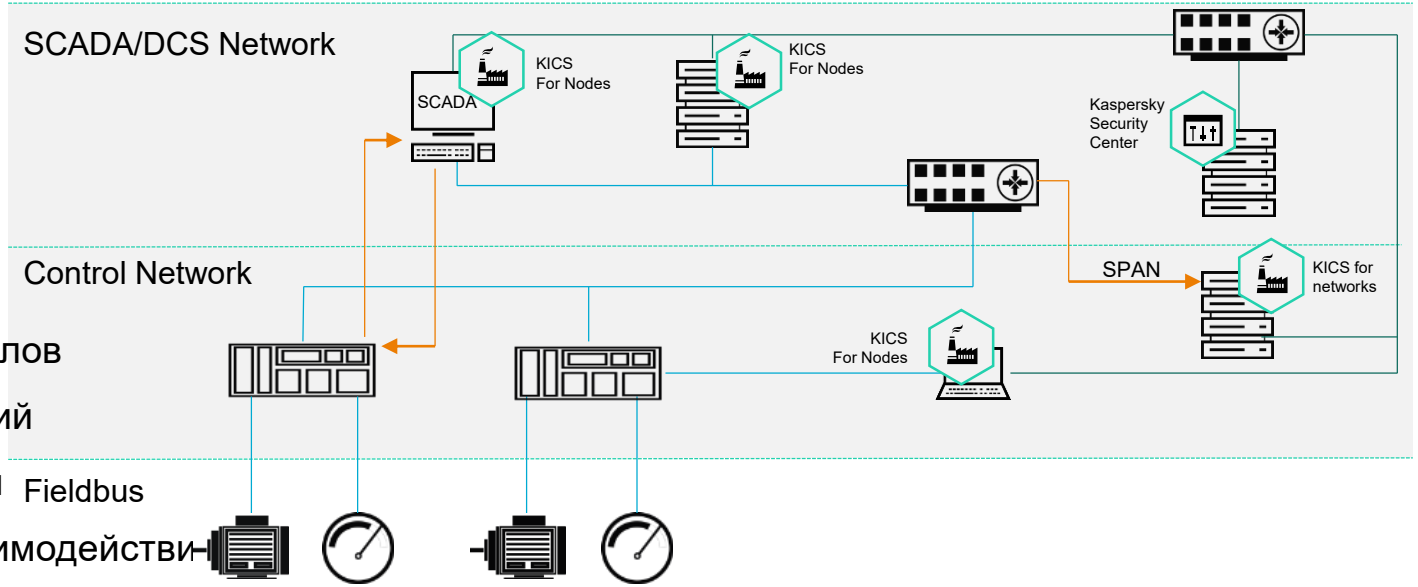
KICS for Nodes

- Белый список приложений
- Антивирус
- Антишифровальщик
- Контроль устройств
- Контроль целостности файлов
- Анализ логов

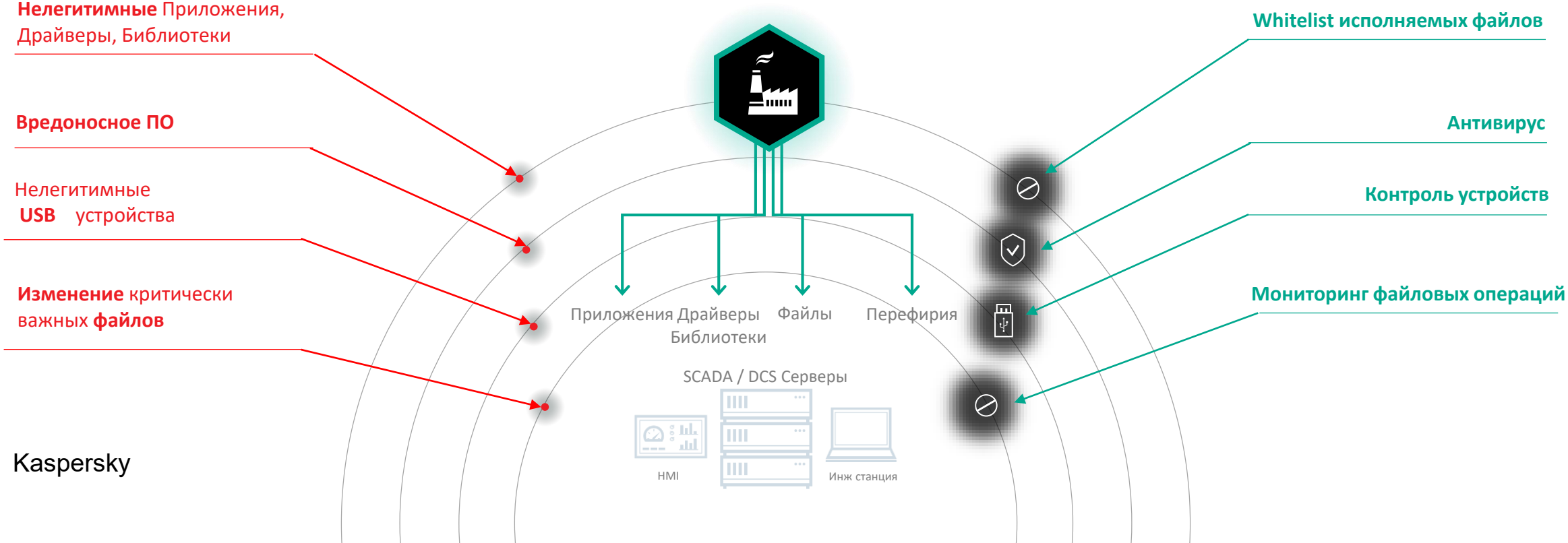
Industrial Anomaly and Breach Detection

KICS for Networks

- Контроль целостности сети
- Разбор промышленных протоколов
- Система обнаружения вторжений
- Пассивный анализ уязвимостей
- Визуализация карты сети и взаимодействи
- Корреляция событий



KICS for Nodes



Kaspersky

Сертификация с поставщиками АСУ ТП

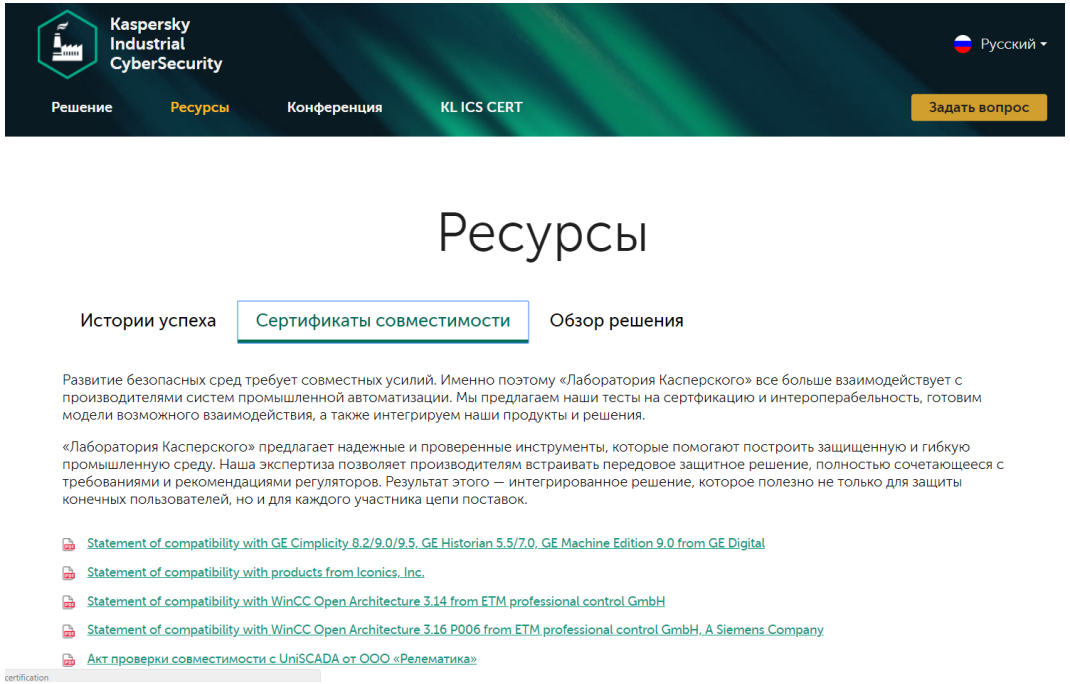
SIEMENS

YOKOGAWA

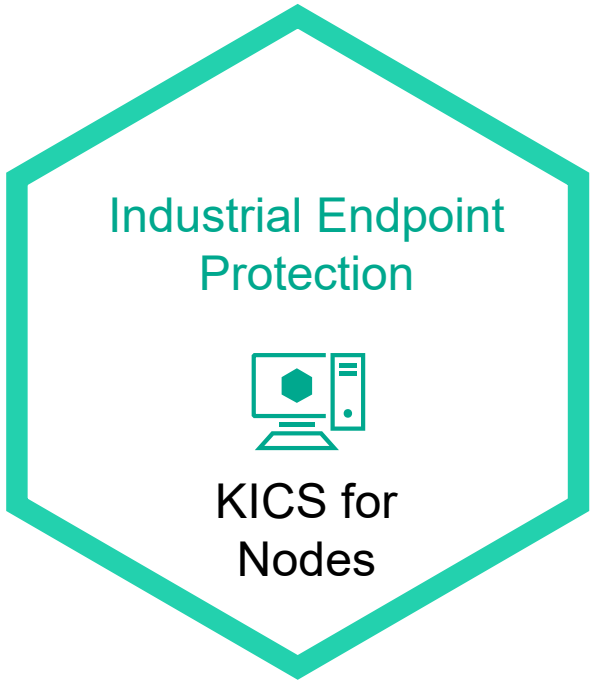
ABB

Schneider Electric

EMERSON



KICS for Nodes



ПРЕДОТВРАЩЕНИЕ ЗАПУСКА НЕЖЕЛАТЕЛЬНОГО ПО
КОНТРОЛЬ ЗАПУСКА ПРИЛОЖЕНИЙ

- Контроль за тем, какое приложение может быть запущено на каждом конкретном узле
- Работа от «белого списка».
  Возможность протестировать «белый список» перед применением
- Защита от целевых атак
- Защита от нежелательной активности пользователя

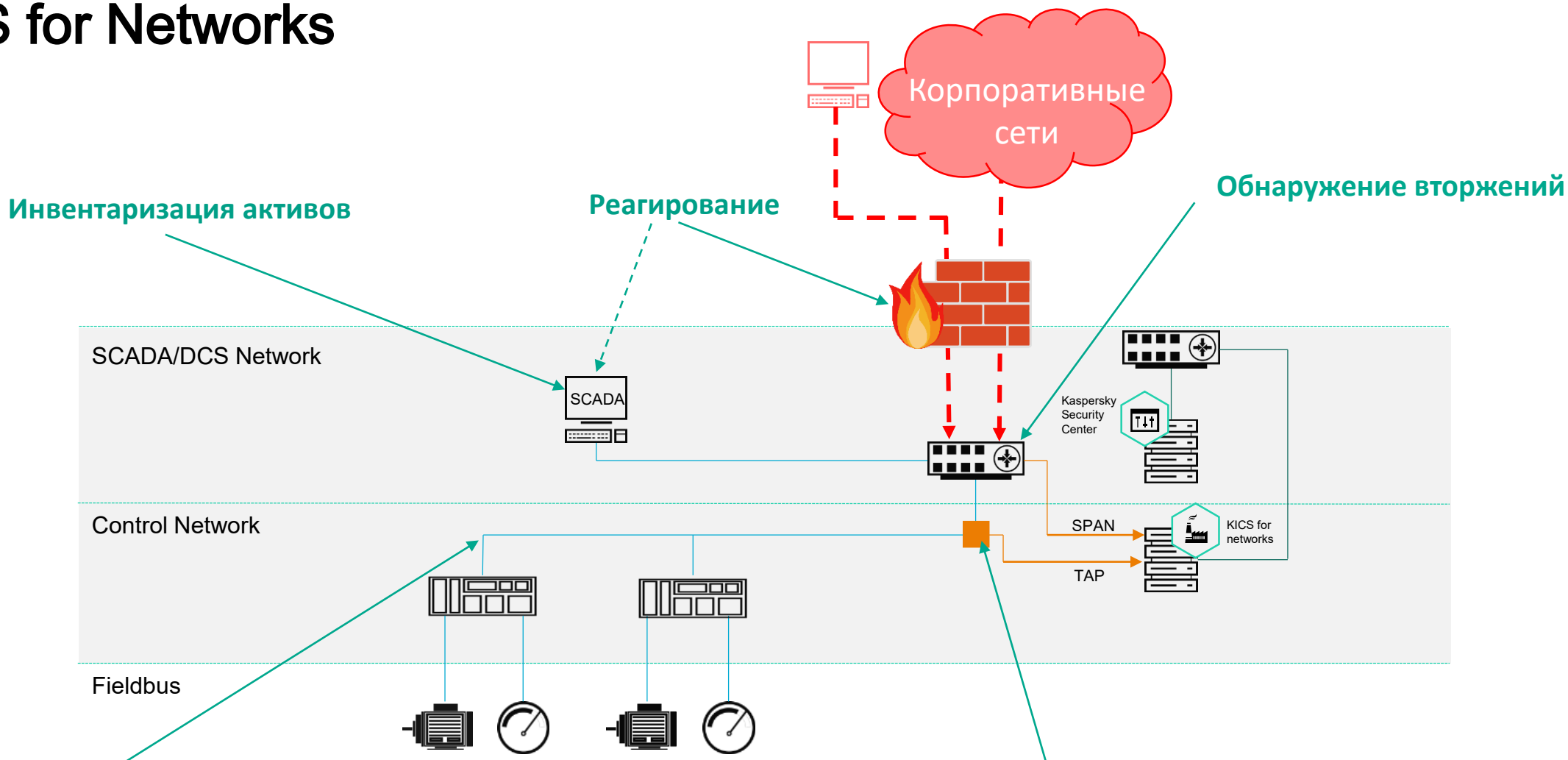
ОБНАРУЖЕНИЕ ВРЕДОНОСНОГО ПО БЕЗ НЕГАТИВНОГО ВЛИЯНИЯ НА
РАБОТУ АСУ ТП

- Мульти-процессная архитектура с возможностью ограничить количество потребляемых ресурсов
- Неинвазивная архитектура
- Защита от шифровальщиков
- Анализ логов операционной системы

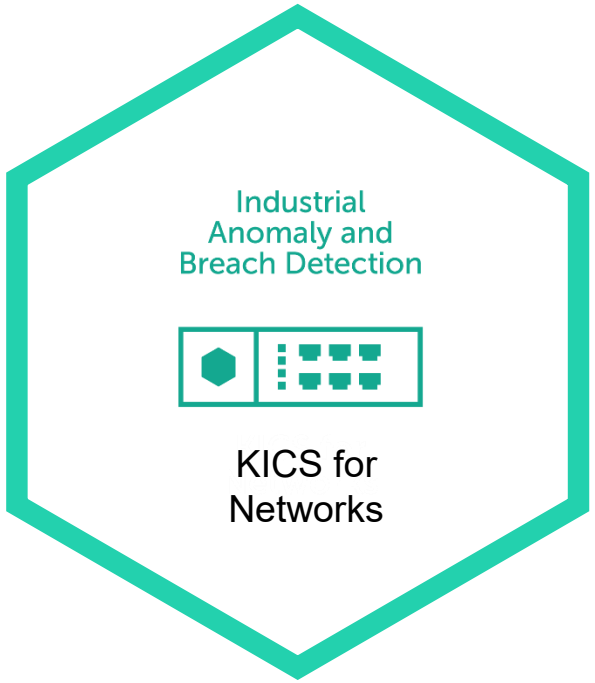
КОНТРОЛЬ ИНФОРМАЦИОННОГО ОКРУЖЕНИЯ

- Контроль подключаемых устройств
- Контроль подключения к Wi-Fi сетям
- Мониторинг файловых операций

KICS for Networks



KICS for Networks



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

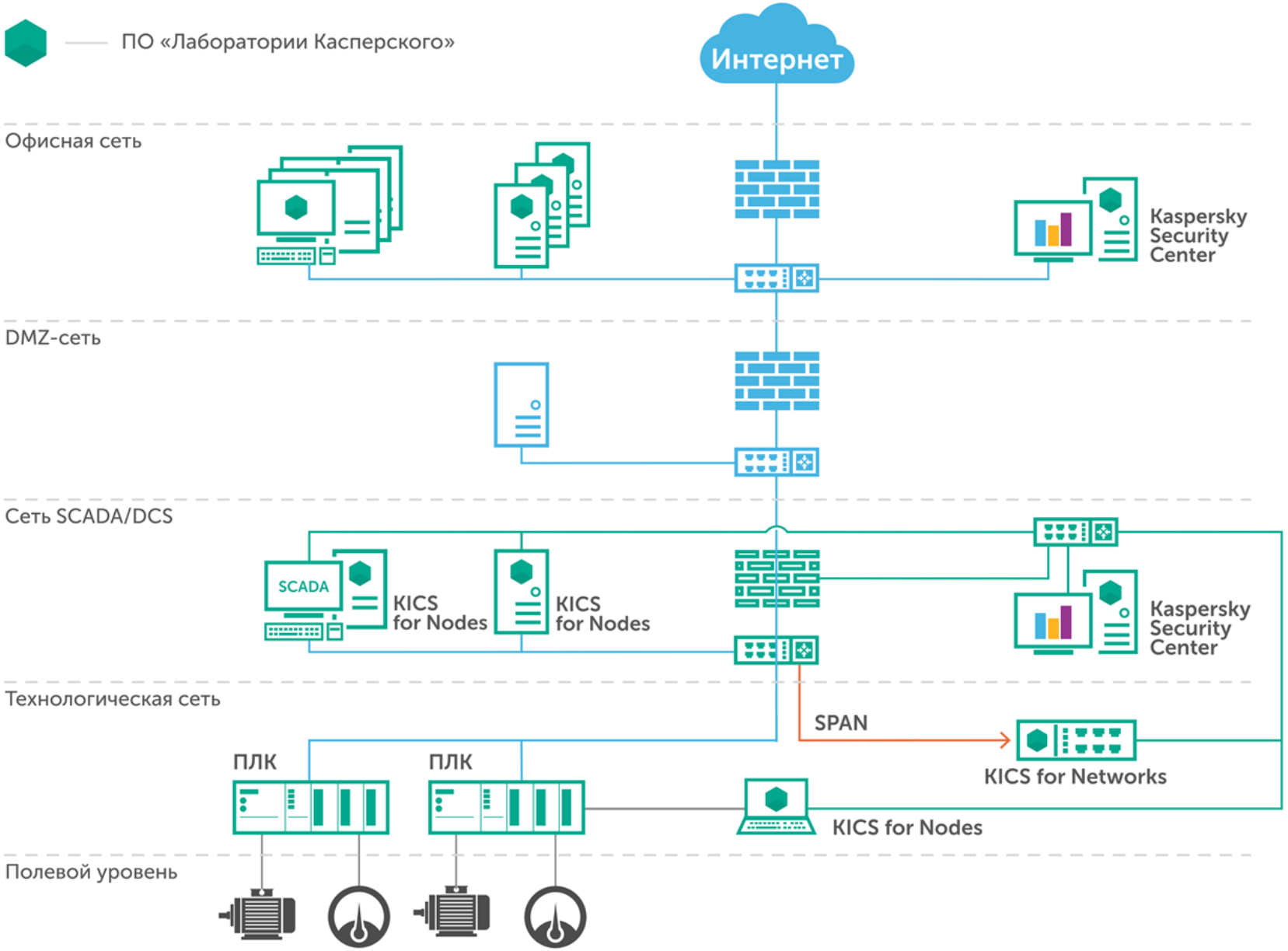
- Kaspersky Security Center
- Syslog Server
- SIEM

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.


ПО «Лаборатории Касперского»
Интернет
Офисная сеть
Kaspersky Security Center
DMZ-сеть
Сеть SCADA/DCS
SCADA
KICS for Nodes
KICS for Nodes
Kaspersky Security Center
Технологическая сеть
SPAN
KICS for Networks
ПЛК
ПЛК
KICS for Nodes
Полевой уровень

Роль KICS в реализации требований приказа ФСТЭК 239

Сертификаты

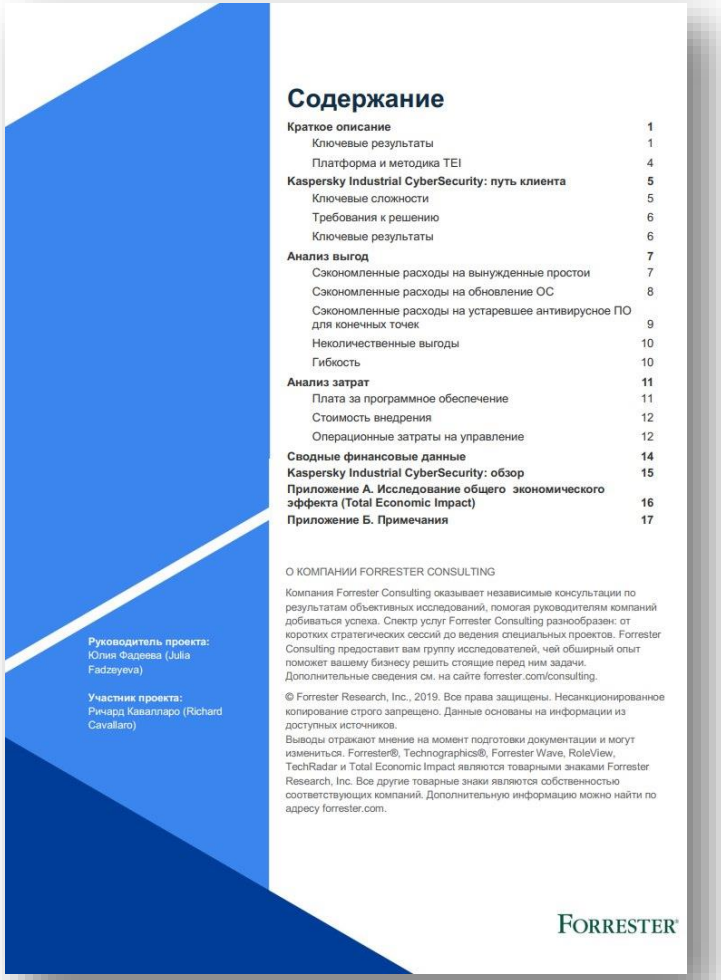
ФСТЭК: Nodes - «АВЗ» уровня 3-В

Networks – «СОВ» С-4

ФСБ: СОА класса Г

Опыт внедрения

Последовательный подход Forrester для оценки эффекта от Kaspersky Industrial CyberSecurity



Содержание

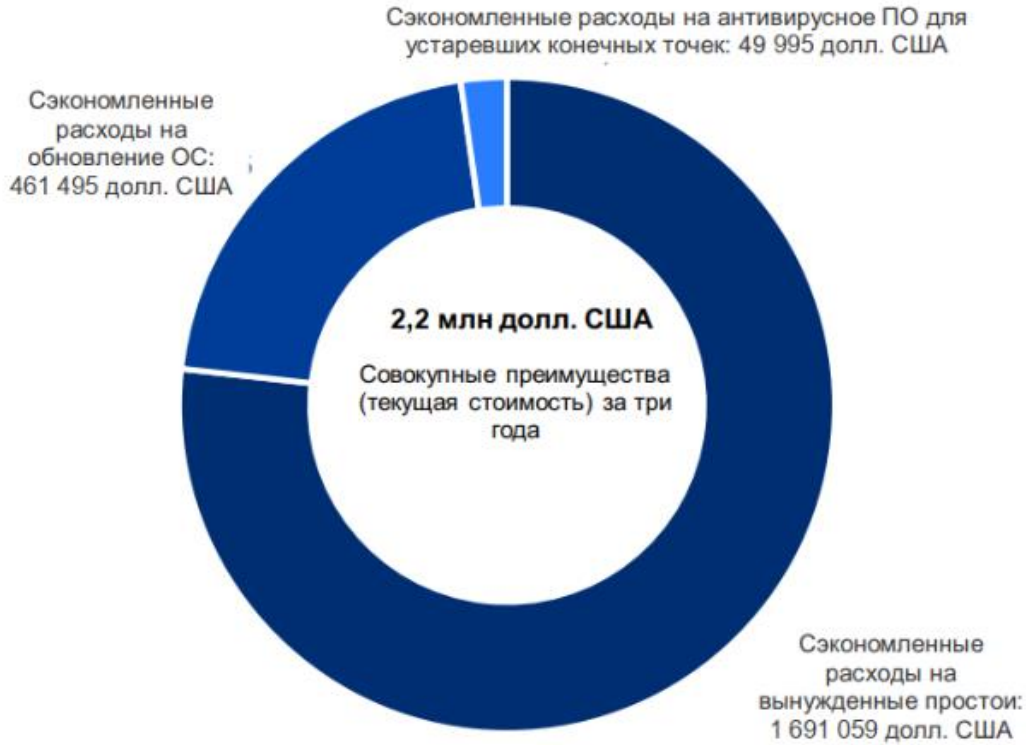
Руководитель проекта:
Юлия Фадеева (Julia Fadzeyeva)

Участник проекта:
Ричард Кавалларо (Richard Cavallaro)

О КОМПАНИИ FORRESTER CONSULTING

Компания Forrester Consulting оказывает независимые консультации по результатам объективных исследований, помогая руководителям компаний добиваться успеха. Спектр услуг Forrester Consulting разнообразен: от коротких стратегических сессий до ведения специальных проектов. Forrester Consulting предоставит вам группу исследователей, чей обширный опыт поможет вашему бизнесу решить стоящие перед ним задачи. Дополнительные сведения см. на сайте forrester.com/consulting.

FORRESTER



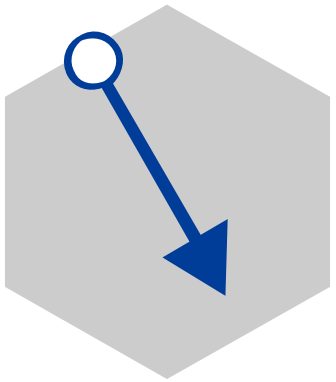
Kaspersky

https://ics.kaspersky.ru/media/Forrester-TEI_Kaspersky-ICS-RU.pdf

Ключевые моменты

УСТРАНЕНА СТОИМОСТЬ ВЫНУЖДЕННЫХ ПРОСТОЕВ

Снизили количество и длительность вынужденных простоев из-за блокирования и замедления работы



УСТРАНЕНЫ РАСХОДЫ НА ОБНОВЛЕНИЕ ОС

Устранили необходимость затратного обновления ОС для совместимости с традиционным антивирусом

УСТРАНЕНЫ РАСХОДЫ НА ТРАДИЦИОННЫЙ АНИВИРУС

Отпала необходимость покупки лицензий офисного антивируса

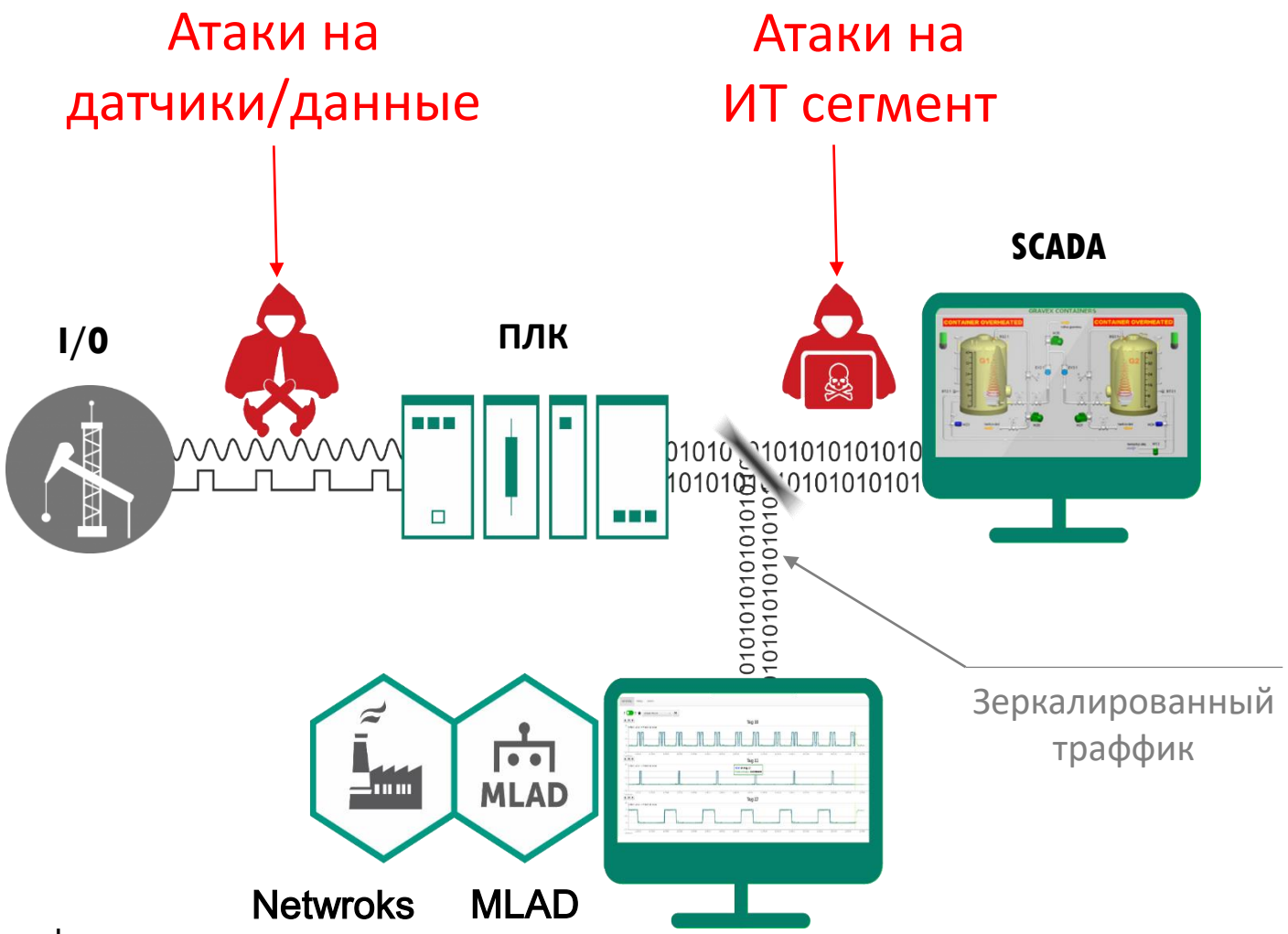
kaspersky

Kaspersky Industrial CyberSecurity

Machine Learning for Anomaly Detection

MLAD

MLAD - Machine Learning for Anomaly Detection



Выявляет воздействие на процесс

Определяет источник(и)

Подсказывает как было решено

Ценности MLAD

Сценарий использования	Возможный ущерб	Ценность
Раннее обнаружение • среагировать быстрее	• Неэффективность • Потери от простоя	⇧ % от процесса
Автоматическое обнаружение • известных сбойных ситуаций	Потери от влияния человеческого фактора	⇧ % от процесса ⇩ чел. фактора
Ретроспективный анализ • эффективности контроля процессов	Длительное неэффективное функционирование	существенный ⇧ % от процесса
Интерпретация аномалий • эффективности контроля процессов	Потери времени и ресурсов на ручной поиск причин	⇧ % от процесса ⇩ чел. фактора
Обнаружение редких аномалий • трудно уловимых для оператора • ведущих к серьезным последствиям	Потенциально огромный: простои, поломки обор., финансовые потери ∞	Существенное ⇩ рисков

kaspersky

Kaspersky
Industrial
CyberSecurity

ICS FEEDS

Репрезентативная выборка

Источники данных

- Более 200 тысяч компьютеров по всему миру;
- Более 150 стран;
- Классификация для 15 различных индустрий (в т.ч. различные виды производств);
- Порядка 20 тысяч модификайци вредоносного ПО детектируется в технологических сетях (в течении 6 месяцев).

Структура и состав данных

Агрегированные даные за 3 месяца;

Порядка 300 тысяч записей;

Ключевые данные:

- MD5 / SHA1 / SHA256

Дополнительные данные:

- IP / URL
- Распределение по странам

Поддерживаемые форматы:

- JSON / CSV

Возможные канал поставки:

- SFTP / HTTPS


```
{
    "MD5" : "84A5746202DECEE74D907A37015A01D4",
    "SHA1" : "872B8D1F2269E645237BB8303EA96012482F9FC2",
    "SHA256" : "97549D52F601A27B336660E8D4983BA10504E371162C64B36077A7670CA0D032",
    "file_size" : 136505,
    "first_seen" : "2017-02-06T13:53:07.000Z",
    "last_seen" : "2018-02-05T19:23:52.000Z",
    "popularity" : 5,
    "threat" : "Trojan.Win32.AutoIt.cfo",
    "geo" : "dz, in, bd, cn, id, sd, za, ci, cd, cm",
    "file_names" : "googleupdate.a3x, google~1.a3x, googleupdate.a3x.vir, googleupdate (2).a3x, cav2b65.tmp, cav2f8d.tmp,
    googleupdate_???_2017-6-16-12-23-45.a3x, cav395e.tmp, cav2ec2.tmp, cav4a7d.tmp"
},
{
    "MD5" : "B18903F14C92F3B9D3D08CA13A39EFDD",
    "SHA1" : "D146AF98EB5CE7A3ECBFF8163EEF002458A1F442",
    "SHA256" : "AA00AAD043D88370E5225A1DABAE3EA49CC703A9575EDD41F24263B013C2F949",
    "file_size" : 1064448,
    "first_seen" : "2017-07-14T08:19:42.000Z",
    "last_seen" : "2018-02-07T07:59:41.000Z",
    "popularity" : 5,
    "threat" : "HackTool.Win32.KMSAuto.i",
    "geo" : "cn, br, tw, ru, mx, de, my, us, lb, es",
    "file_names" : "office 2010 ????????.exe, mini-kms_activator_v1.1_office.2010.v1.eng.exe, microsoft office professional plus 2010 x64 silent
    install.rar, microsoft.office.2010.14.0.4763.1000.x32.rus.iso, office 2010 ????????.exe, a0180675.exe, activator.exe,
    mini-kms_activator_v1.1_office.2010.v1.eng.exe, office_2010_br_brazil_pt_portugues_32_64.nrg, mini-kms activator v1.1 final.exe"
},
{
    "MD5" : "EE570E841175090073F9A5408FFDD549",
    "SHA1" : "F0AFA4ECB2F3638F2FFB32DA5F3D8CC4156A63F3",
    "SHA256" : "5E923C942C85C3F186201DFF44E8FA3019727AA878C4B89070621404B695D43C",
    "file_size" : 225618,
    "first_seen" : "2018-01-12T04:48:01.000Z",
    "last_seen" : "2018-01-30T18:21:06.000Z",
    "popularity" : 5,
    "threat" : "Trojan.Script.Generic",
    "geo" : "br, dz, fr, mx, es, co, tr, vn, us, at",
    "file_names" : "cr2[1].js, packed, crlt[1].js, f_00393b, f_003034, f_0033c2, f_0034b7, f_003342, f_003809, f_00136b",
    "urls" : [
        {
            "url" : "https://zxcl-ustokyyneikyfasnm.stackpathdns.com/assets/javascript/cr2.js"
        },
        {
            "url" : "https://zxcl-ustokyyneikyfasnm.stackpathdns.com/assets/javascript/cr.js"
        }
    ],
    "IP" : "151.139.240.18"
},
```

kaspersky

Kaspersky
Industrial
CyberSecurity

Отчёты по угрозам

Kaspersky | ICS CERT

Contents

kaspersky

Kaspersky
Industrial
CyberSecurity

Сервисы

Kaspersky®
Security
Assessment

- Тест на проникновение
- Набор приоритезированых рекомендаций по устранению проблем и целевая архитектура сети
- Опытная в АСУТП команда

Kaspersky®
Incident
Response

- Команда экстренного реагирования для локализации инцидента и выяснения его причин
- Доступна по запросу или по подписке

kaspersky

Kaspersky
Industrial
CyberSecurity

Тренинги

Kaspersky®
Security
Awareness

- **Industrial CyberSecurity in Practice awareness training**

  1 или 2 ДНЯ, от 10 участников

Kaspersky®
Security
Trainings

- **ICS Penetration Testing for Professionals**

  5 дней, до 10 участников в группе

- **ICS Digital Forensics for Professionals**

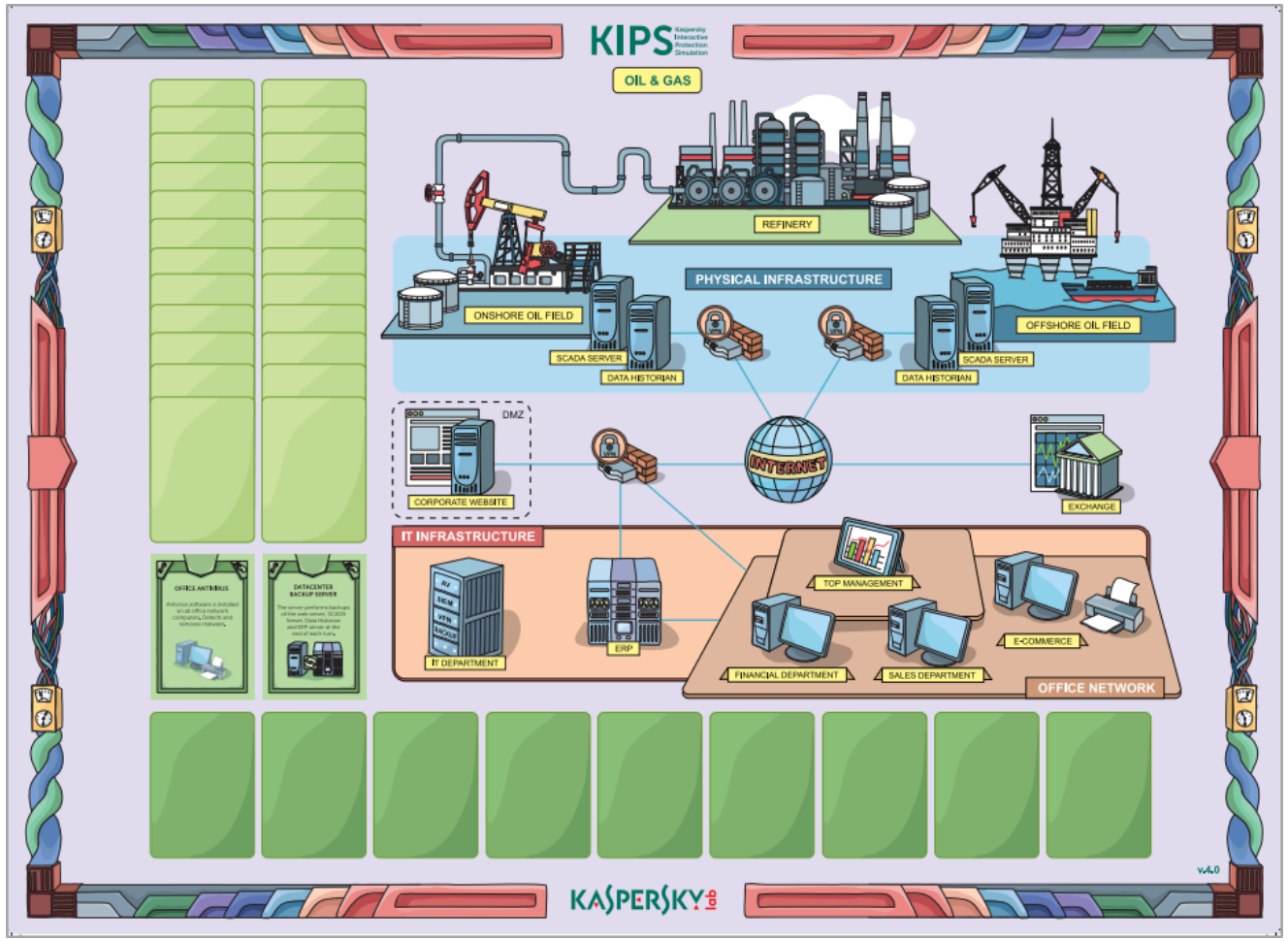
  4 дней, до 10 участников в группе

- **ICS Vulnerability Research for Professionals**

  8 дней, до 10 участников в группе

Kaspersky Interactive Protection Simulation (KIPS)

Kaspersky®
Cybersecurity
Awareness Training



kaspersky

Kaspersky Operation System

KasperskyOS – не общее, а целевое назначение; направления применения

ПРИМЕНЕНИЕ:

Корпоративные информационные системы

Компьютерные системы специального назначения

Мобильный устройства

Интернет вещей

Промышленные системы

Телекоммуникационное оборудование

Транспортные системы

Объекты критически важной инфраструктуры

OEM

KOS, KSS, KHS

Networking

Коммутаторы, маршрутизаторы, Wi-Fi, МЭ

IoT

Умные города, IoT и SCADA, PLC, IIoT

Transportation

Автомобили, автобусы, поезда

Desktop & Mobile

Встроенные системы, пользовательские устройства

kaspersky

Благодарю!

Петухов Алексей
Руководитель направления защиты промышленных систем
Alexey.Petukhov@Kaspersky.com
+7 963 686 07 83

Ics.kaspersky.com