ИБ ПРОМЫШЛЕННОГО ИНТЕРНЕТА ВЕЩЕЙ В ЭПОХУ ИНДУСТРИАЛИЗАЦИИ 4.0:

в ожидании технологического прорыва

Василий Широков | Check Point (Russia), к.т.н.

основной м
рпреступников

2016

Вирус-вымогатель **заблокировал билетные терминалы** на станции SAN FRANCISCO'S MUNI TRANSIT

2016

DDOS атака на DNS провайдера DYN нарушила Интернет, используя **IOT** устройства как боты

2014

Отключение электроэнергии на Западной Украине в связи с фишинговой атакой **BLACKENERGY**

2015-2016

Отключение электроэнергии на Западной Украине в связи с фишинговой атакой **BLACKENERGY**

2016

Нарушение системы **водоснабжения** и **изменение** уровня **химических веществ** в очищенной водопроводной **воде**

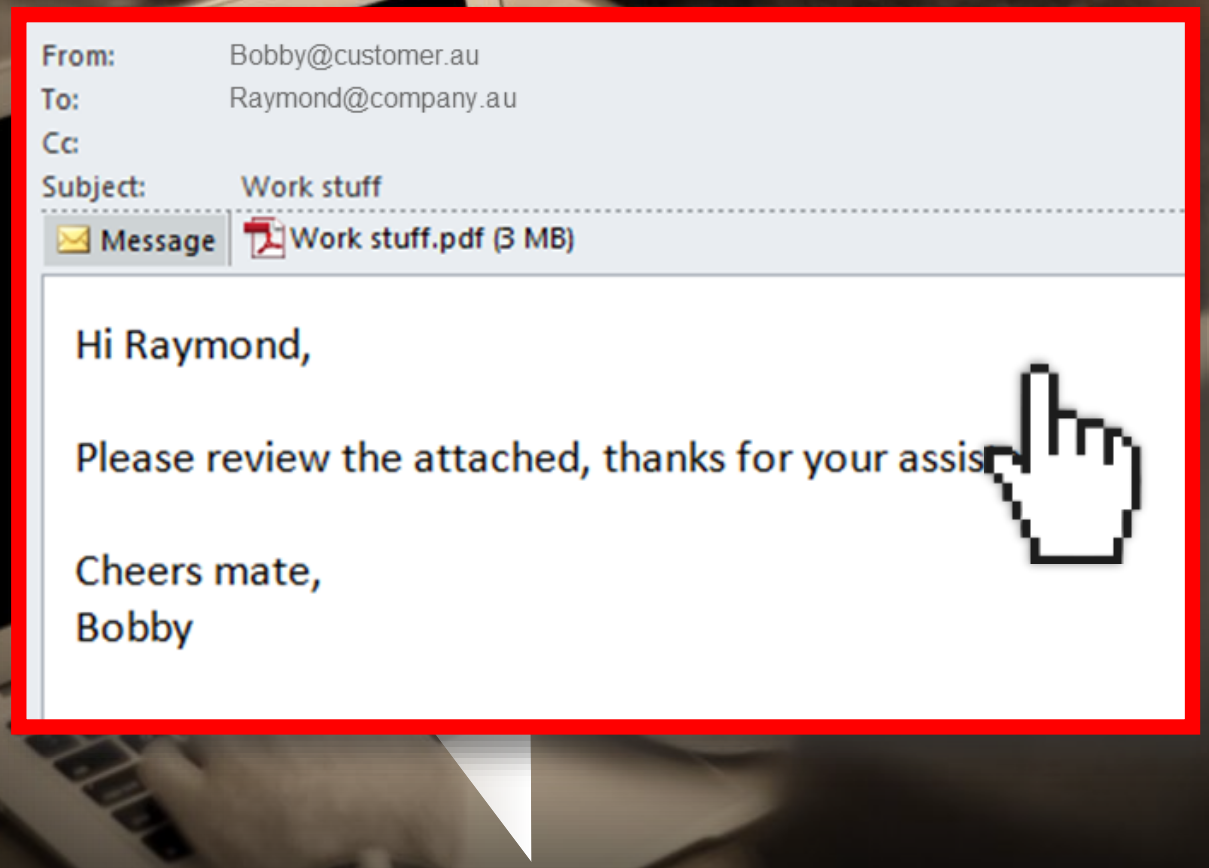
2016

Хакеры **повредили** MEDSTAR **HOSPITAL** с использованием кибератаки

[Protected] Non-confidential content

Плотина Гувера

Как будто бы невинная почта от знакомого клиента



Source: *ComputerWeekly.com*

23:00:00

Пятью минутами
позже...
Общая
неисправность
системы
23:55:3

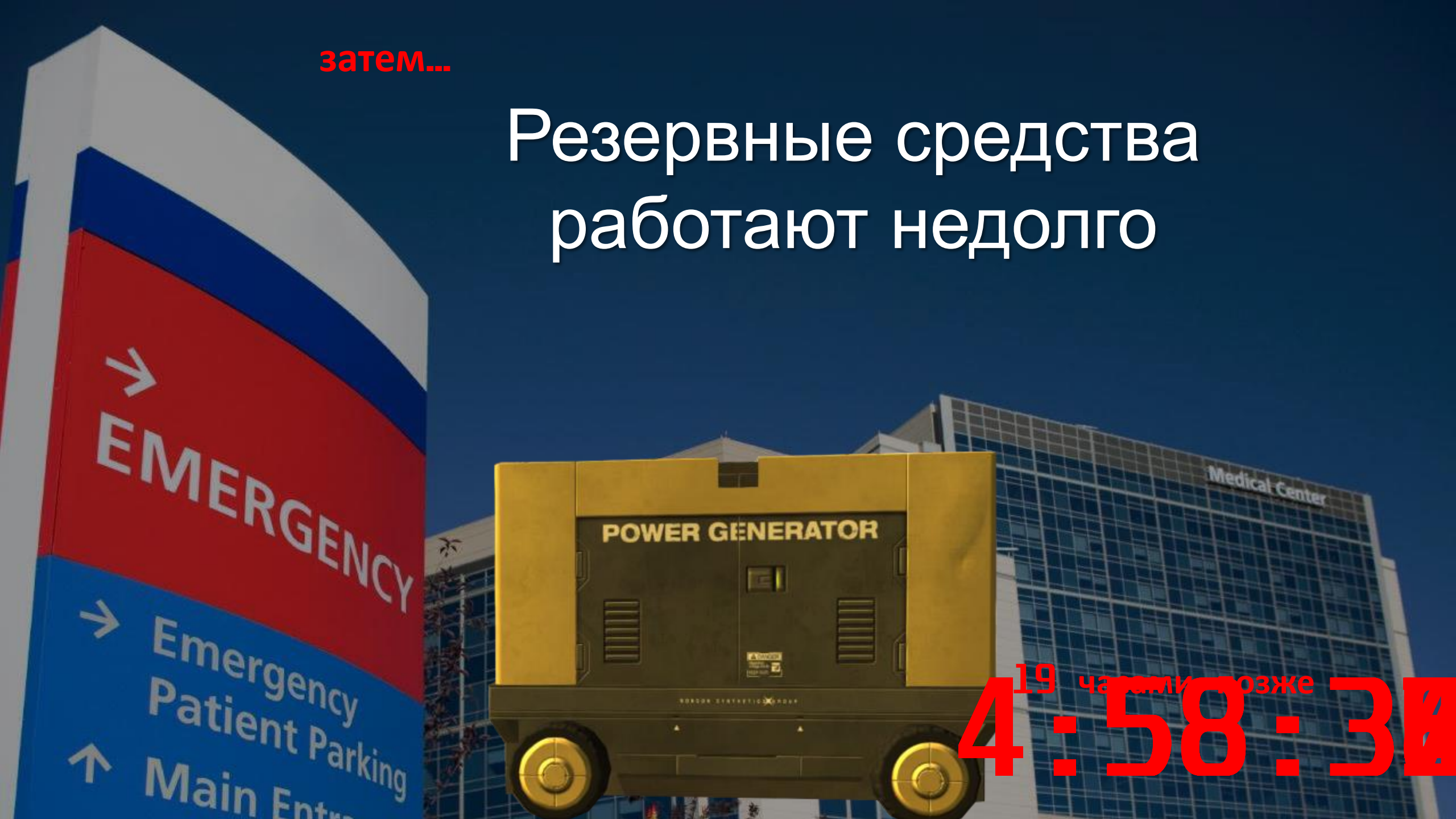
Десятью минутами позже,

Падение электроэнергии

23:45:3

затем…

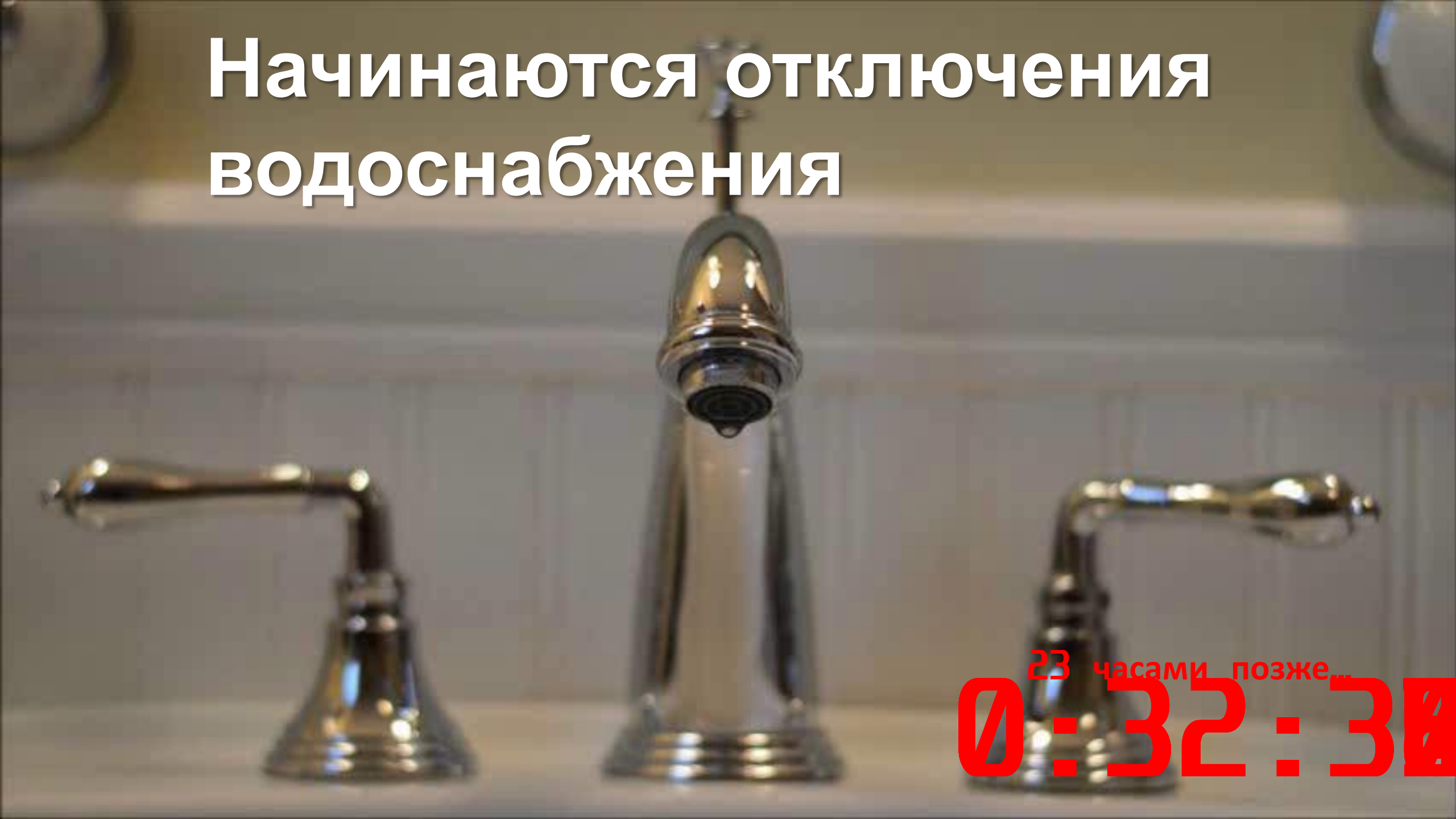
Резервные средства работают недолго



19 часами позже

4:58:3

Начинаются отключения водоснабжения



Дорожные заторы

[Protected] Non-confidential content

Разграбление магазинов
Почти 24 часами
позже...
0:04:30
Carnation
Chicolastic
Classic

ого в
разрушить систему

2016

Вирус-вымогатель **заблокировал билетные терминалы** на станции SAN FRANCISCO'S MUNI TRANSIT

2016

DDOS атака на DNS провайдера DYN нарушила Интернет, используя **IOT** устройства как боты

2014

Отключение электроэнергии на Западной Украине в связи с фишинговой атакой **BLACKENERGY**

2015-2016

Отключение электроэнергии на Западной Украине в связи с фишинговой атакой **BLACKENERGY**

2016

Нарушение системы **водоснабжения** и **изменение** уровня **химических веществ** в очищенной водопроводной **воде**

2016

Хакеры **повредили** MEDSTAR **HOSPITAL** с использованием кибератаки

[Protected] Non-confidential content

Критические инфраструктуры становятся основной мишенью киберпреступников

- Экспоненциальный рост кибератак и угроз сетевой безопасности,
- Огромные инвестиции в интеллектуальные технологии и
- Поддержка со стороны правительственных организаций для обеспечения безопасности ICS

Вот некоторые из факторов, стимулирующих рост рынка безопасности промышленных систем управления во всем мире.

MARKETSANDMARKETS

Publishing Date: June 2017
Report Code: TC 3075

[Protected] Non-confidential content

Индустриализация 4.0

Термин (Industrie 4.0) введен в Германии в 2011 году как название одного из 10 проектов государственной Hi-Tech Стратегии страны до 2020 года, описывающего концепцию умного производства (Smart Manufacturing) на базе глобальной сети IoT.

Основные области промышленных технологий, составляющие Industrie 4.0

1. Cyber Pysical Systems

2. Cloud Computing

3. Big Data

4. System Security

5. 3D Printing

6. Augmented Reality

7. Humanoid Robots

https://iot-analytics.com/industrial-technology-trends-industry-40-patents-12x/

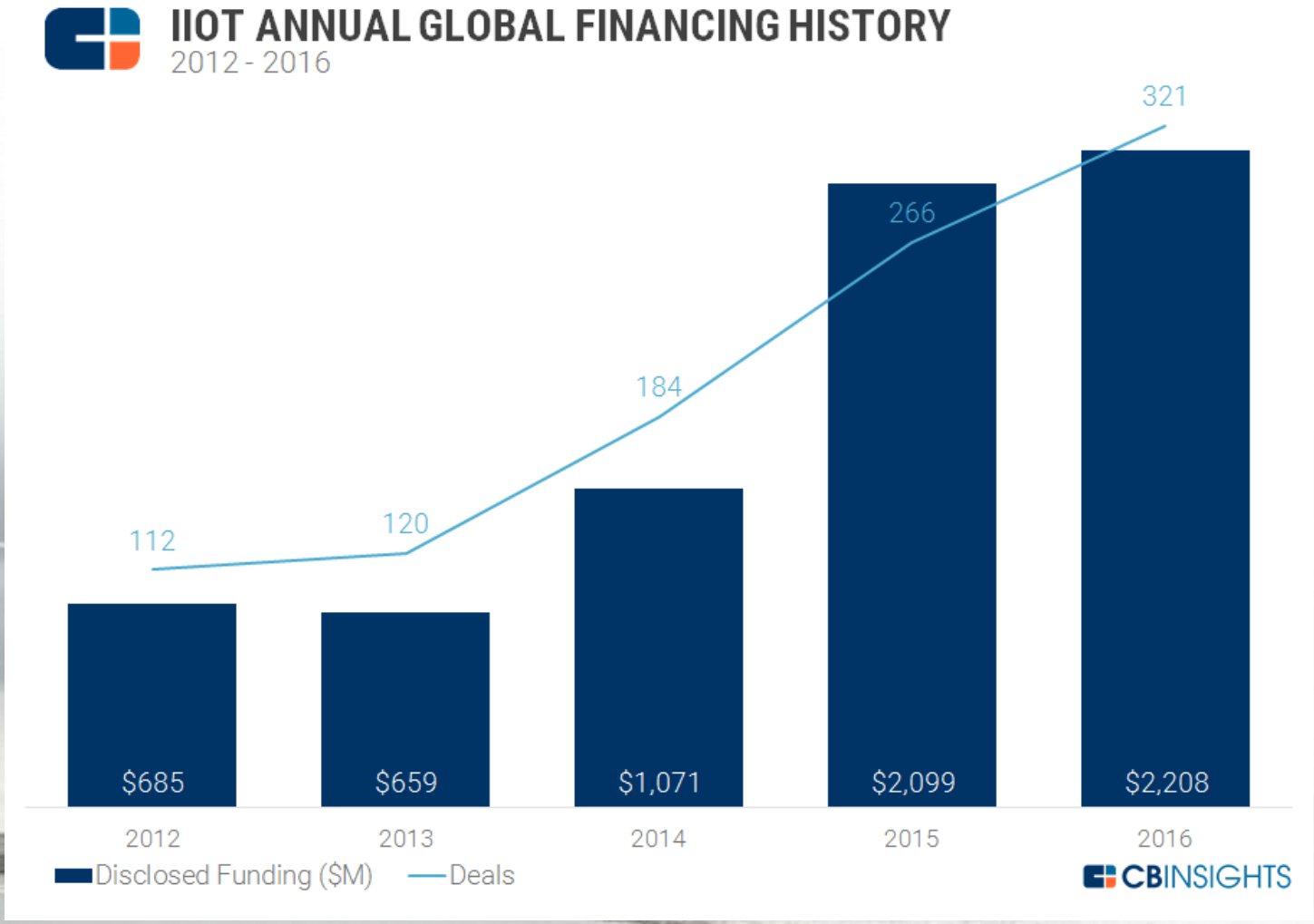
[Protected] Non-confidential content

Инвестиции в развитие IIoT

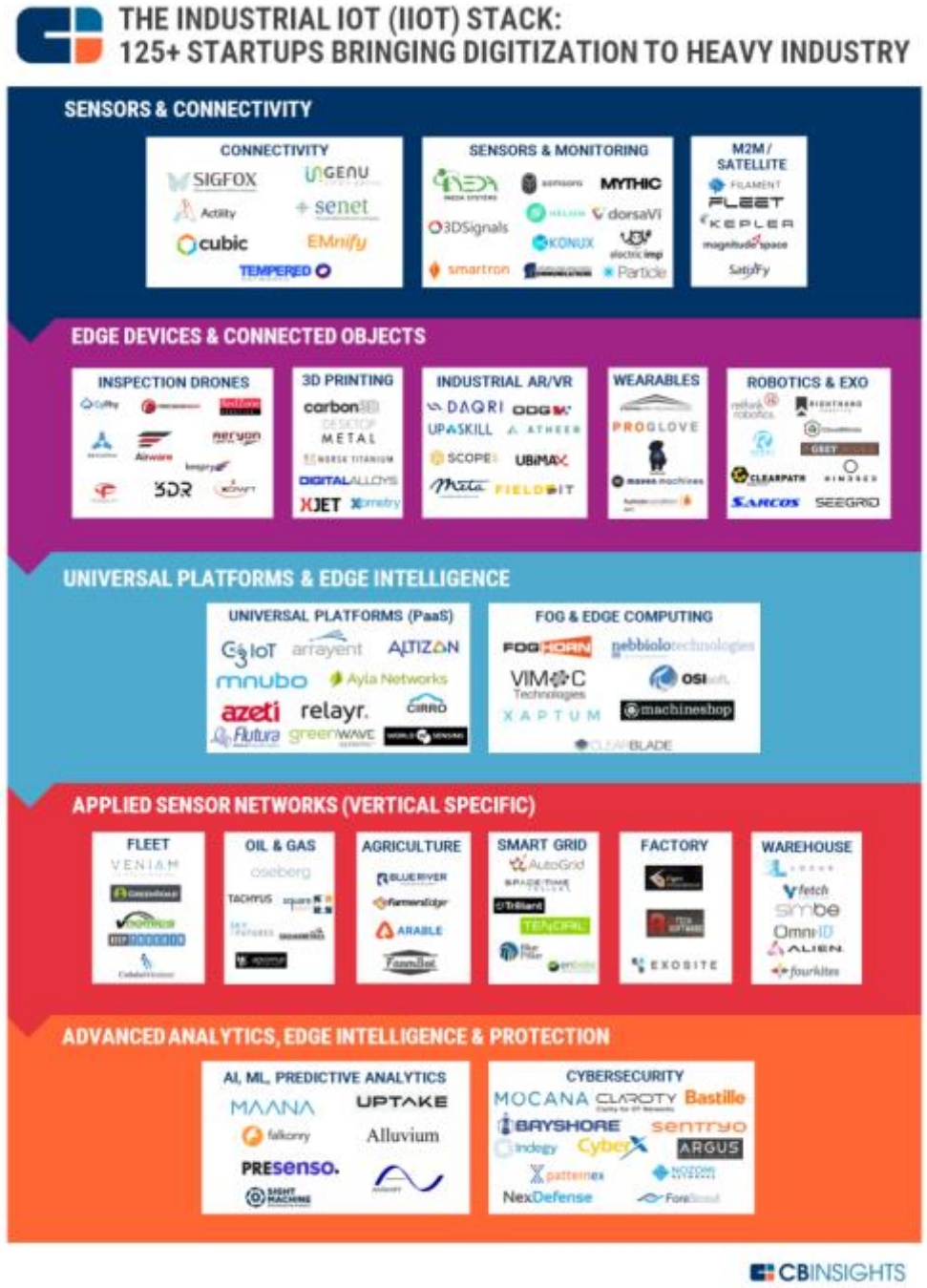
Стартапы, вносящие цифровые технологии и инфраструктуру IoT в тяжеловесные промышленные отрасли, такие как

- производство,
- логистика,
- добыча полезных ископаемых,
- нефть,
- коммунальные услуги и
- сельское хозяйство,

получают большую долю инвестиций, направленных на IIoT.



[Protected] Non-confidential content



Стартапы меняют ланшафт IIoT

До недавних пор волну IIoT возглавляла старая гвардия промышленных технологических компаний, таких как GE, IBM и Cisco, которые считают, что IIoT является основным компонентом их будущего бизнеса.

GE, в частности, впервые назвала термин «промышленный Интернет», объявив о своих инвестициях в НИОКР в размере 1,5 млрд. Долл. США еще в 2012 году.

Но все больше и больше стартапов атакуют потребности тяжелой промышленности, разрабатывая датчики, облачные платформы, сетевую инфраструктуру, а также компьютерное программное обеспечение для извлечения информации из потока данных.

CBINSIGHTS

[Protected] Non-confidential content

IIoT: датчики и подключения

CBINSIGHTS

Подключения - поставщики беспроводных сетей выступают в качестве телекоммуникационных компаний для эры IoT. Большинство компаний здесь обеспечивают LPWAN связь (маломощную широкополосную сеть), которая является популярным радиодиапазоном для устройств IoT.

LoRa Alliance - входят такие ИТ-гиганты, как IBM, Cisco, Orange, NTT, Soft Bank, Bosch, Schneider Electric, Inmarsat, Swisscom. Поддержка этих лидеров уже привела к тому, что LoRaWAN стала крупнейшей популярной LPWAN-технологией в мире.

[Protected] Non-confidential content

IIoT: датчики и подключения

CBINSIGHTS

Сенсоры и мониторинг - некоторые компании являются разрабочиками только датчиков или систем на чипах (SoC), другие разрабатывают «полный стек» (как сенсорные, так и мониторинговые платформы)

M2M / Satellite – решения для труднодоступных компонент систем IIoT. Спутники могут быть более эффективным способом передачи данных в таких системах. Аналогично в изолированных производственных средах связь между машинами и машинами (M2M) является более эффективным способом передачи информации между устройствами, например, с помощью маломощных промышленных датчиков.

[Protected] Non-confidential content

IIoT: периферийные устройства и подключенные объекты

CBINSIGHTS

Инспекционные беспилотники – анализ изображений для промышленной инспекции. На данный момент это в основном воздушные беспилотники. Категория охватывает все типы, включая подводные аппараты и аппараты для инспекции труб.

3D Printing - технология начинает выходить на промышленные масштабы изготовления деталей. Поэтому здесь инвестируют корпоративные венчурные компании GE и BMW.

Robotics & Exo - промышленные роботы автоматизации (например, складская робототехника) наряду с экзоскелетами, которые дополняют человеческие способности.

[Protected] Non-confidential content

IIoT: универсальные платформы и Edge Computing

CBINSIGHTS

Универсальные платформы - облачные вендоры здесь обычно выступают в роли общих компаний с сервисом платформа-как-услуга (PaaS), которые позволяют другим компаниям IIoT управлять и поддерживать сбор данных из своих сетей устройств. Сюда входят преиму-щественно платформы, которые используют облачную аналитику для промышленных компаний.

Fog & Edge Computing - вычисления, выполненные на «краю» или ближе к датчику, представляют собой сдвиг в тренде, происходящий в архитектуре IIoT. Применяются два подхода – вычисления, приближенные к точке сбора, и «туманные» вычисления (например, сервер в локальной сети датчиков). Оба метода позволяют критически важным устройствам безопасно работать без необходимости передачи всех данных в облако, что также может существенно сэкономить полосы пропускания.

[Protected] Non-confidential content

IIoT: аналитика и безопасность

CBINSIGHTS

Аналитика - программное обеспечение, которое позволяет компаниям получать интеллектуальную аналитику, например, по вопросам необходимости технического обслуживания устройств. Некоторые решения предлагают использование полного набора датчиков, которые обнаруживают аномалии машин.

Во избежание простоев и для сохранения безопасности на предприятии необходимо внедрение технологий, позволяющих обнаруживать и прогнозировать риски. Непрерывный проактивный мониторинг ключевых показателей дает возможность определить проблему и принять необходимые меры для ее решения. Оперативный анализ помогает пользователям быстрее находить причины неполадок.

[Protected] Non-confidential content

IIoT: кибербезопасность

CBINSIGHTS

Мониторинг в реальном времени и расследование инцидентов в системах и сетях OT. Некоторая глубокая проверка пакетов по промышленным протоколам.

Обнаружение и отслеживание устройств, непрерывная оценка уязвимости; обнаружение аномалий и моделирование атак. Использование Big Data и машинного обучения.

Пассивный мониторинг в сетях OT в сочетании с активной проверкой контроллеров. Выявление аномалий и угроз, вызванные кибератаками, вредоносным ПО или ошибками человека.

Обнаружение устройств OT, мониторинг базового функционала, обнаружение аномалий и безопасный удаленный доступ. Сегментация сети OT и возможность предотвращения угроз.

[Protected] Non-confidential content

IIoT: кибербезопасность

CBINSIGHTS

Мониторинг в реальном времени и расследование инцидентов в системах и сетях ОТ. Некоторая глубокая проверка пакетов по промышленным протоколам.

Обнаружение и отслеживание устройств, непрерывная оценка уязвимости; обнаружение аномалий и моделирование атак. Использование Big Data и машинного обучения.

Пассивный мониторинг в сетях ОТ в сочетании с активной проверкой контроллеров. Выявление аномалий и угроз, вызванные кибератаками, вредоносным ПО или ошибками человека.

Обнаружение устройств ОТ, мониторинг базового функционала, обнаружение аномалий и безопасный удаленный доступ. Сегментация сети ОТ и возможность предотвращения угроз.

[Protected] Non-confidential content

IOT AND IIOT CYBERSECURITY MARKET MAP

CRITICAL INFRASTRUCTURE

CyberX, Bastille, sparkcognition, PFP, TEMPERED, PingThings, Indegy, NEXDEFENSE, SECURE RF, BAYSHORE, SCADAfence, IONIC SECURITY, NOZOMI, EagleEye, THETARAY, mPrest, SENRIO, sentryo, CAMGIAN

MOBILE PHONES

okta, Skycure, wickr, appthority, Lookout, AppDome, silent circle, TRUSTLOOK, avast!, OPENPEAK, ZIMPERIUM, SEQUITUR LABS

CONNECTED DEVICES

Auth0, STEEL MOUNTAIN, netskope, ihiji, mojo Networks, IMUBIT, PWNIE EXPRESS, SECURITHINGS, DEVICE AUTHORITY, ICON LABS, SECURITY INNOVATION, MedCrypt, BATBLUE, BEAR Systems, MOCANA, ZITOVAULT, Rubicon, RazorSecure, ZingBox, DELTA ID

ENTERPRISE ENDPOINTS

LogRhythm, Centrify, Avecto, CYLANCE, CounterTack, INTERSET, CROWDSTRIKE, TANIUM, red canary, DUO SECURITY, SentinelOne, MORPHISEC, ForeScout, CODE42, nexthink, CARBON BLACK, Bromium, LIGHTCYBER, Workspot, bitglass, DIGITAL GUARDIAN

CONNECTED CARS

Trillium, CLOUD MADE, ARGUS, baimos, Karamba Security, VisualThreat

CBINSIGHTS

На этой карте представлены пять «монстров» кибербезопасности стоимостью $ 1B +, включая: Okta, Lookout, Avast Software, Tanium и Cylance.

И ни один из них не находится в разделе Critical Infrastructure

Это схема не является исчерпывающей в части присутствующих в ней компаний.

IIoT: кибербезопасность

Gartner

Market Guide for Operational Technology Security

Published: 17 August 2017 **ID:** G00310067

Analyst(s): Earl Perkins, Ruggero Contu, Saniye Burcu Alaybeyi

Operational technology security products and services protect existing and evolving OT for industrial and commercial critical infrastructure ecosystems. Security and risk management leaders should gauge the market state and direction, and understand the types of OT security providers in the market.

Key Findings

- Market offerings continue to deliver in key areas of anomaly and vulnerability detection, incident response, endpoint (including device) protection and access management, with many including asset discovery and tracking functions.
- While today's solutions are more mature than previous versions, acceptance by clients remain moderate due to uneven levels of client maturity and the pace of information technology/ operational technology (IT/OT) integration.
- In the professional services marketplace, IT security teams and managed security service providers are expanding skills and presence to compete with established specialist operational technology (OT) security services providers.
- The market for OT security functions with cloud-based delivery (and cloud versions of enterprise-based platforms) is nascent, but interest is continuing to grow.

Cisco

GE Digital

Siemens Building Technologies

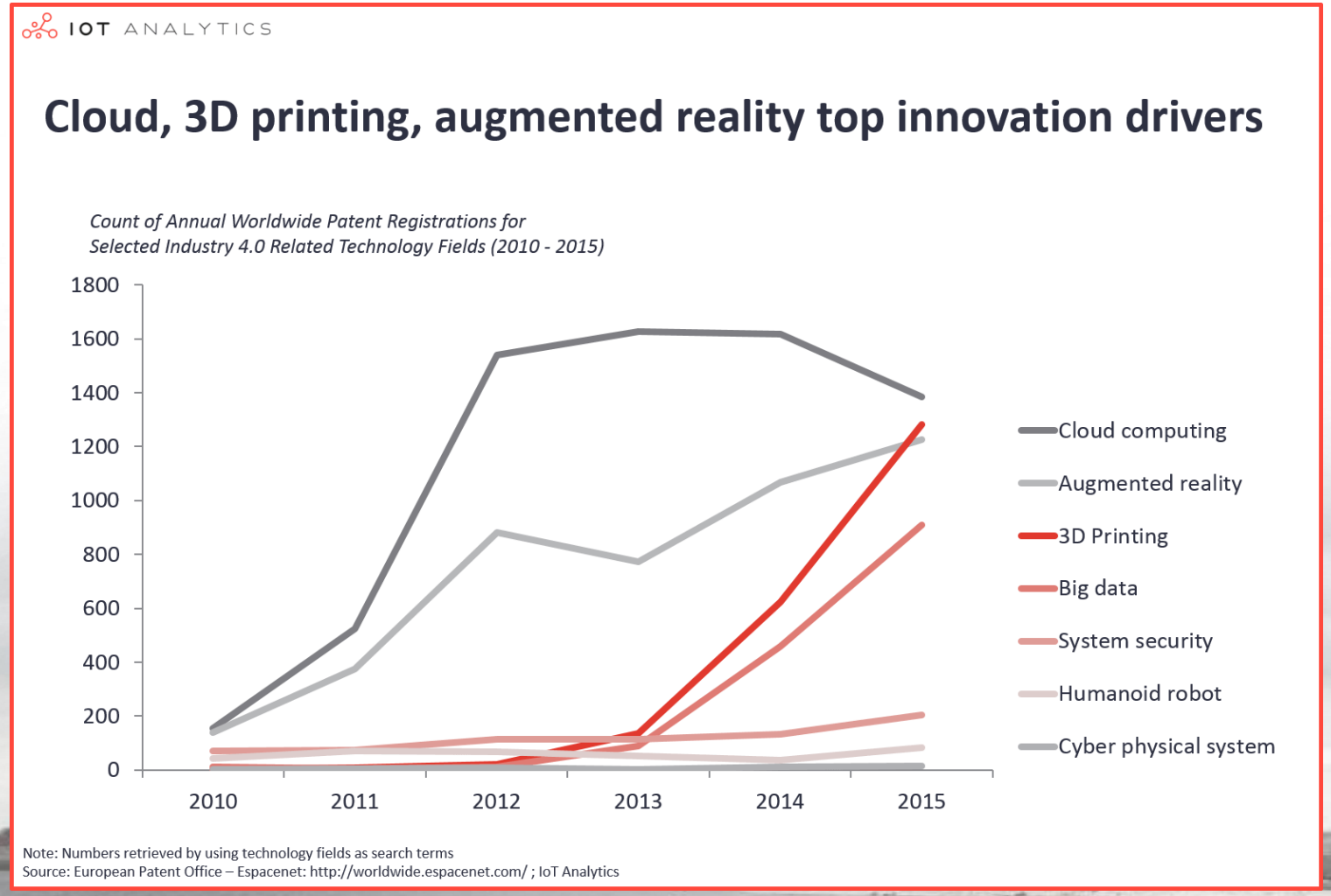
Rockwell Automation

Kaspersky Lab ....

Kaspersky Lab предлагает решение KICS - обнаружение аномалий в сетях OT и реагирование на них, контроль целостности сети OT и расследование инцидентов. ... А также Machine Learning for Anomaly Detection

[Protected] Non-confidential content

Индустриализация 4.0. Инновации



Каналы данных и связи, а также все другие промышленные системы, машины и компоненты должны быть надлежащим образом защищены от кибератак. Однако уровень патентных инноваций все еще низок

https://iot-analytics.com/industrial-technology-trends-industry-40-patents-12x/

[Protected] Non-confidential content

IIoT: глобальные тренды 2017

2017 будет переломным годом для IIoT. Наблюдается значительный рост инвестиций в отрасль промышленными организациями. В ходе опроса 69% организаций-респондентов планируют увеличить свои ежегодные инвестиции в IIoT в ближайшие год.

Безопасность и конфиденциальность

Количество устройств, подключенных к Интернету для обмена информацией, будет расти, и все больше компаний займутся внедрением интегрированных решений. Это растущее количество подключенных устройств также увеличит новые проблемы безопасности. Организации очень хорошо осведомлены о проблемах безопасности, которые могут возникнуть с IoT, и будут инвестировать в решения, которые могут предложить надежные меры безопасности для устройств, а также облачных данных.

APOGAEIS
BEYOND INNOVATION

[Protected] Non-confidential content

IIoT: глобальные тренды 2017

Accenture оценивает, что Industrial Internet of Things (IIoT) способен добавить $14.2 триллионов в глобальную экономику к 2030 году.

accenture
High performance. Delivered.

APOGAEIS: Internet of Things (IoT) будет включать в себя 26 миллиардов единиц, установленных к 2020 году. К этому времени поставщики продуктов и услуг IoT будут генерировать дополнительный доход, превышающий 300 миллиардов долларов, в основном в сфере услуг.

APOGAEIS
BEYOND INNOVATION

IDC: ожидает, что к 2018 году распространение связанных сетей информации, инструментов и решений в облачных экосистемах будет стимулировать производителей к перестройке их архитектур безопасности

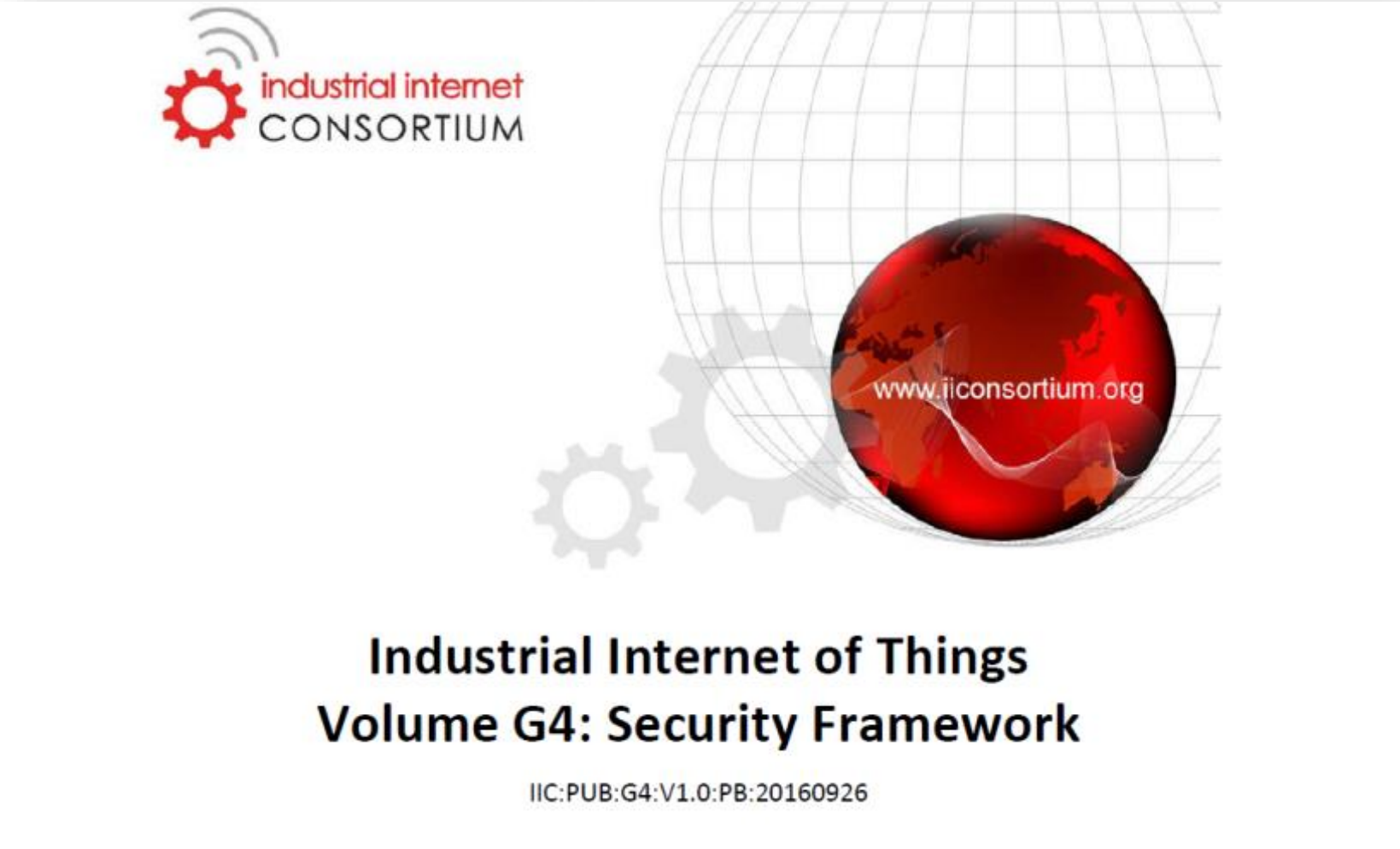
IDC
Analyze the Future

The Industrial control systems security market size is expected to grow from USD 10.24 Billion in 2017 to USD 13.88 Billion by 2022, at a Compound Annual Growth Rate (CAGR) of 6.3%.

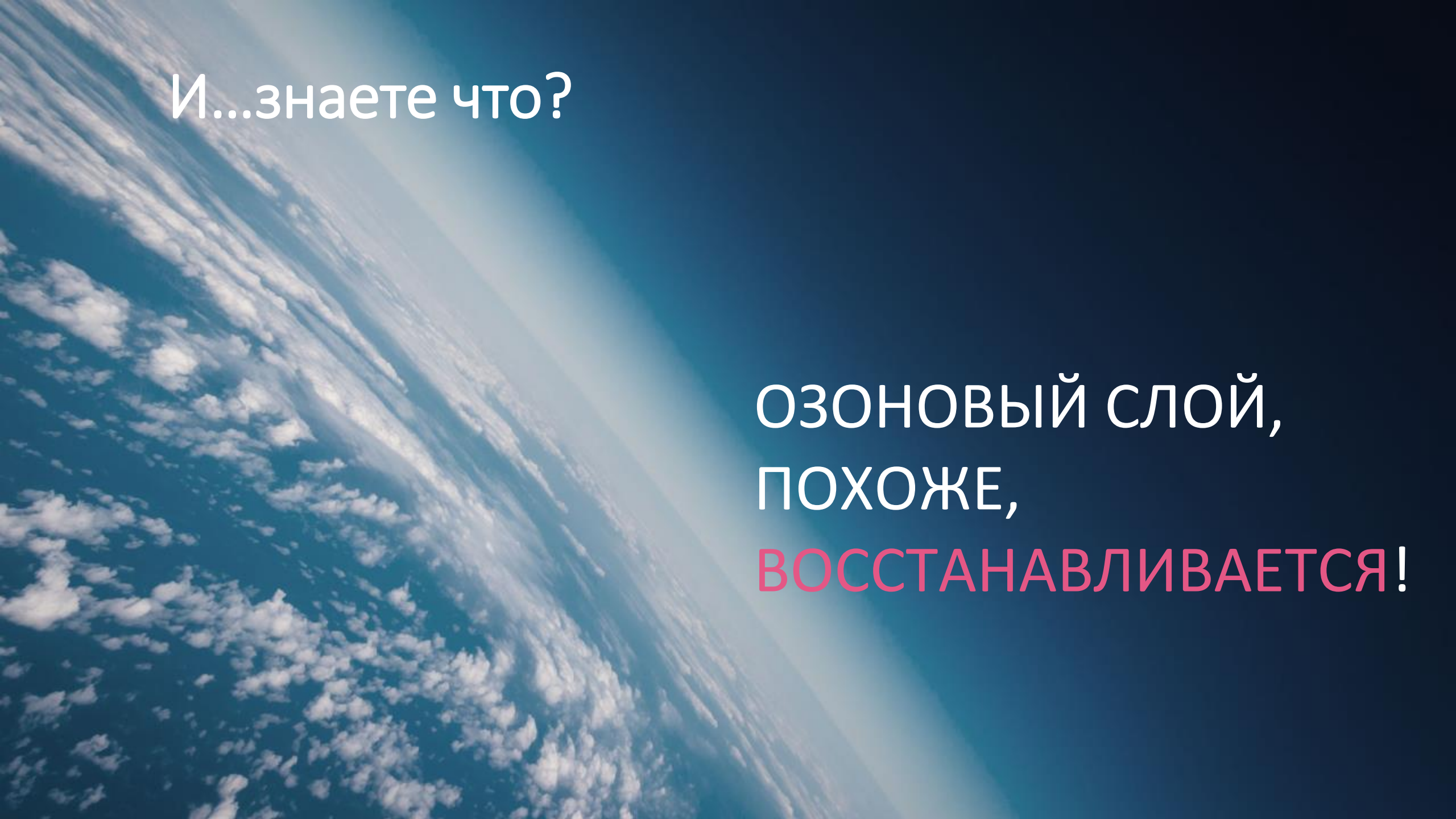
MARKETSANDMARKETS

[Protected] Non-confidential content

IIoT: глобальные тренды 2017



[Protected] Non-confidential content



И…знаете что?

ОЗОНОВЫЙ СЛОЙ,
ПОХОЖЕ,
ВОССТАНАВЛИВАЕТСЯ!