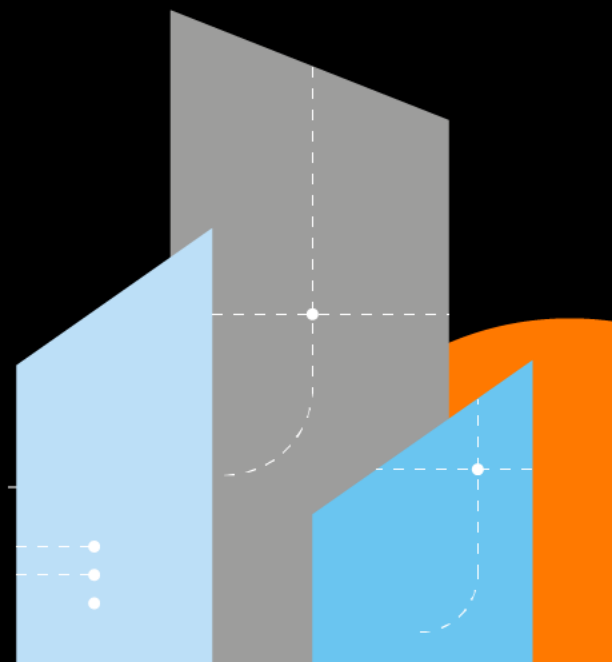
Как построить современную службу ИБ с помощью CyberSOC



Приятно познакомиться!

Мы являемся ведущим европейским поставщиком услуг по обеспечению безопасности, оказывающим поддержку бизнесу по всему миру.

€768 миллионов оборот в 2020.

Более **2500** высококвалифицированных экспертов по кибербезопасности

4,000 клиентов по всему миру, лучшие в своем классе по всем вертикалям.

Очень сильный игрок в области Global Managed Security Services

GlobalData.

50 млрд логов регистрируются нашими CyberSOCs.

Сильнейший MSSPs

FORRESTER®

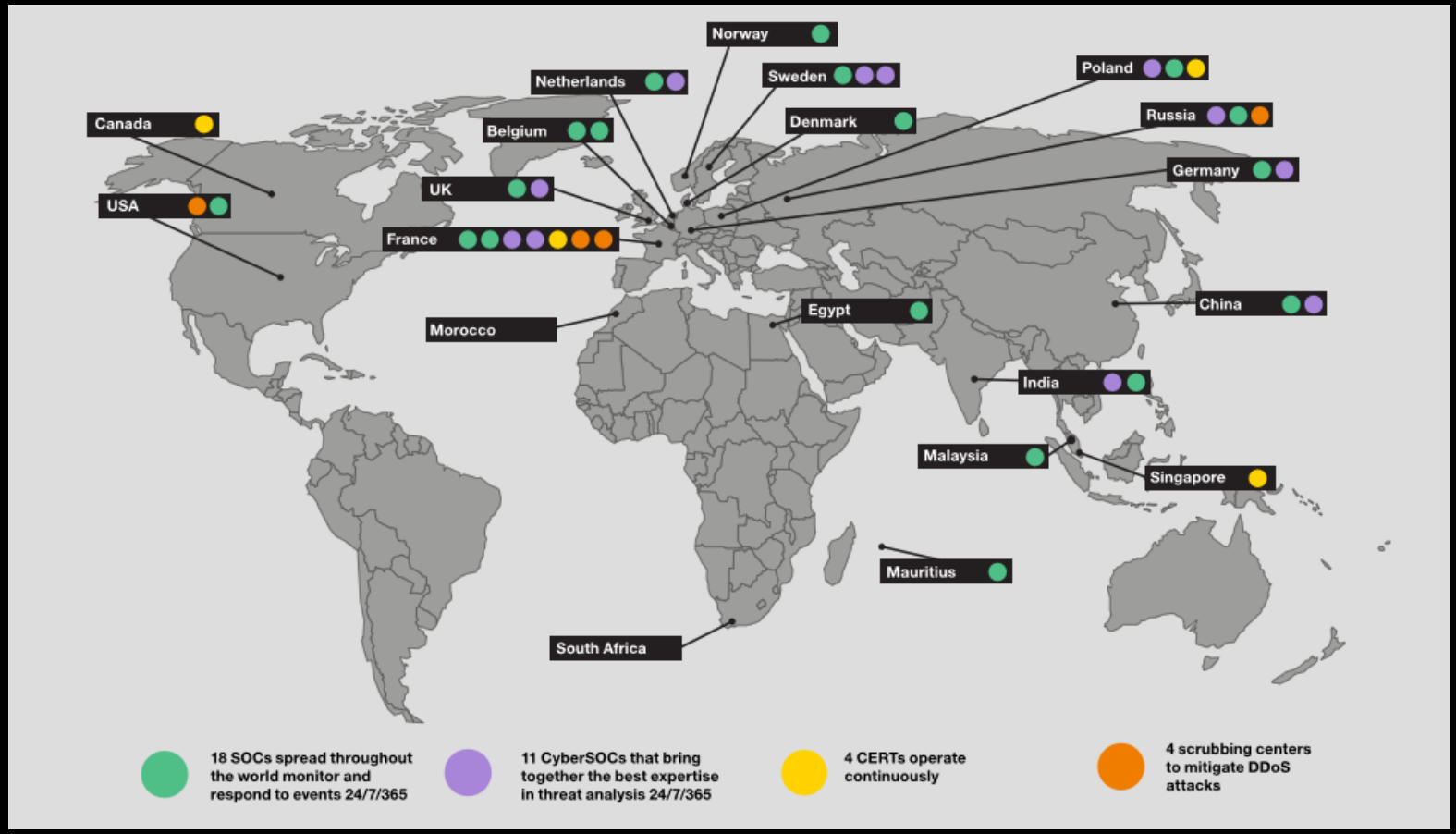
24/7/365 непрерывный мониторинг систем безопасности по всему миру.

Знаковый поставщик списка в области Managed Detection and Response & Managed Security Services

Gartner

Приятно познакомиться!

- Коммерческий SOC CyberSOC
- Внутренний SOC
- Центр очистки от DDoS-атак



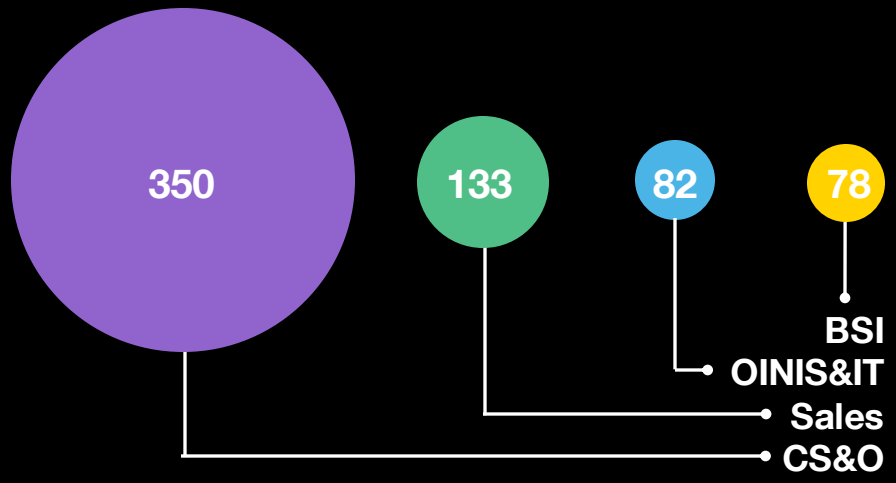
Orange в России

B2B-подразделение группы Orange: провайдер цифровых сервисов с экспертизой в области телекоммуникаций

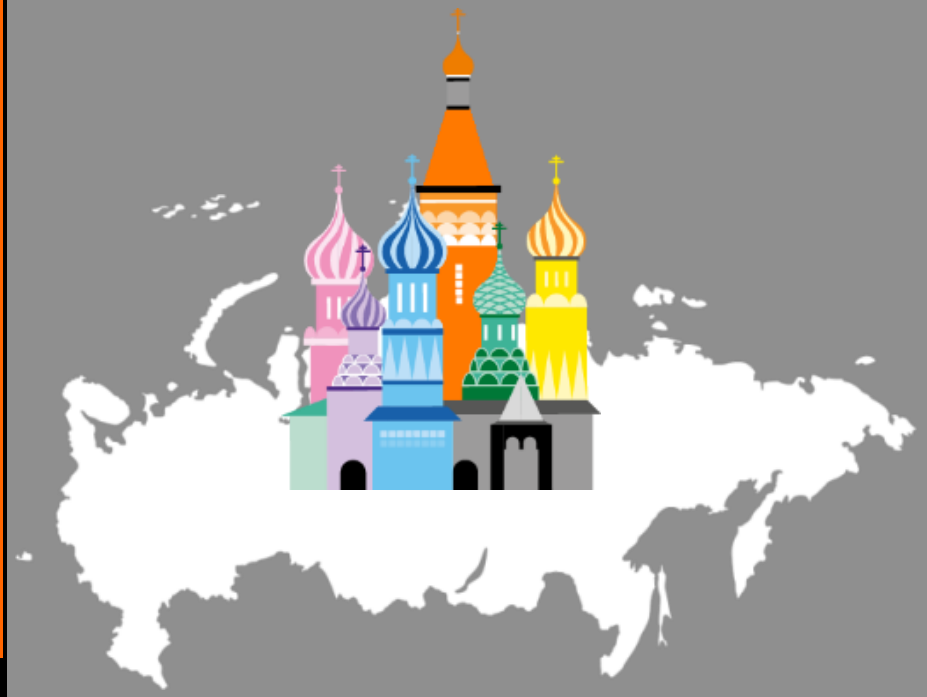
Единственный международный оператор связи с собственной инфраструктурой

Сильные местные компетенции: центр инноваций и центр мониторинга киберугроз (SOC)

Создаем инновации для крупного бизнеса: 8 из 10 крупнейших российских компаний Forbes-2000 Top-10 – наши клиенты*



800+ сотрудников

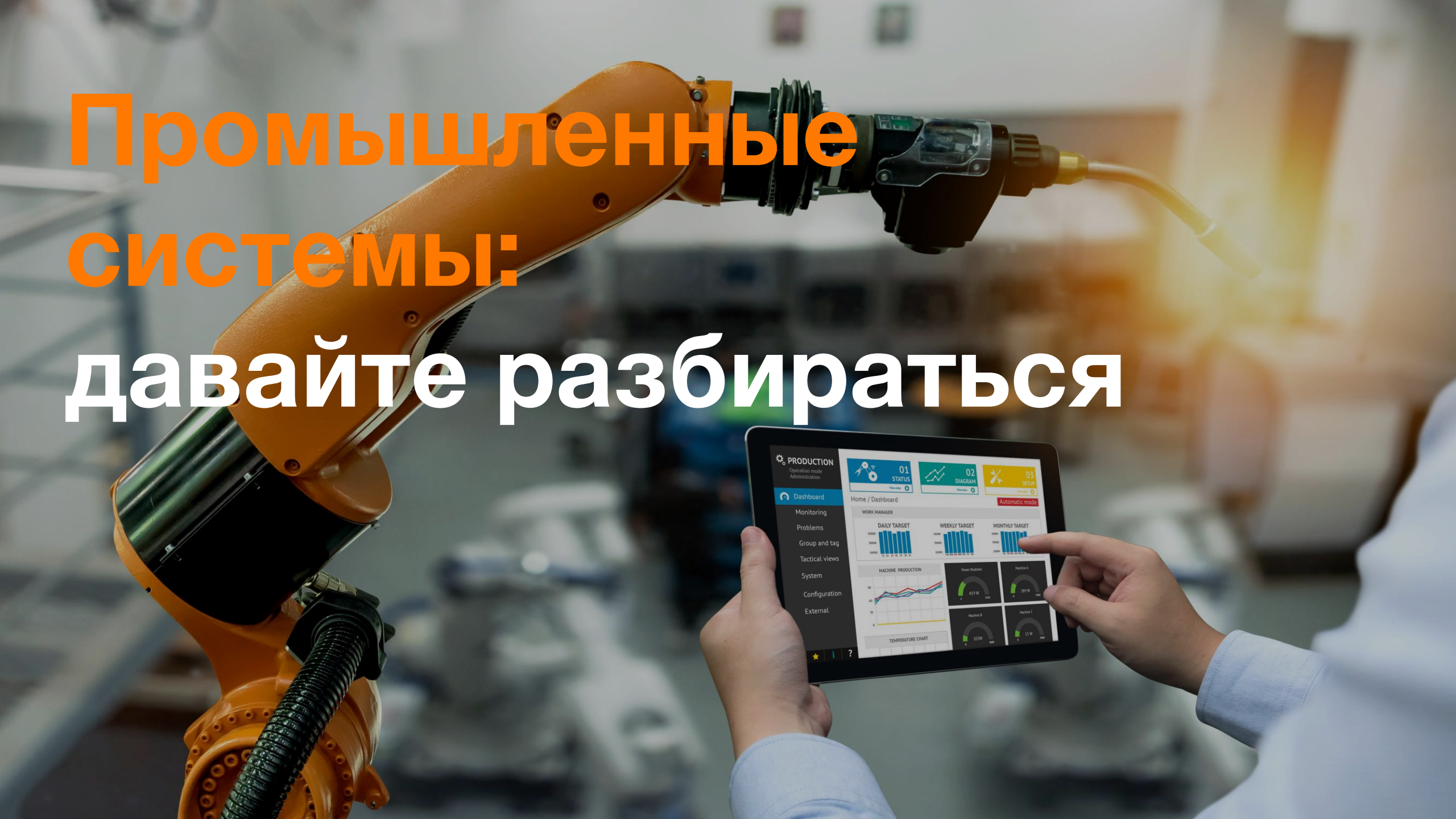


В России с 1958 года (SITA)

- **31 отделение**
- **13 офисов продаж**
- **1500 корпоративных клиентов**

*according to Top-2000 Forbes 2018 rating

Промышленные системы: давайте разбираться



Промышленные системы повсюду

Военная промышленность

Автомобильная промышленность

Силикатная промышленность

Космическая индустрия

Химическая промышленность

Очистка воды и управление отходами

Пищевая промышленность

Умные города и здания

Энергетика и сети

Целлюлозно-бумажная промышленность

Здравоохранение

Нефтегазовая промышленность

Металлургическая и горнодобывающая промышленность

Транспорт и логистика

Что такое промышленные системы?

Любые аппаратные или программные устройства, используемые для управления физическими или механическими процессами.

Например: регулирование температуры, давления, движение, изменение расхода и скорости.

Кибератаки на промышленные системы

1903 Взлом Marconi Radio

2008 Система трамвайной сети в Лодзь

Атака на трубопровод в Турции

2009 Система управления светофорами в LA

2010 Stuxnet

2016 Triton

2017 Альянс Renault-Nissan

Производитель продуктов питания Mondelez

2018 Black Energy

2019 Нефтегазовая и металлургическая компания Hydro

Компания Honda

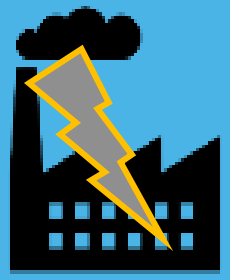
2020 Производитель вакцин Fareva

Уроны от кибератак

Репутация бренда

- потеря доли рынка
- снижение доверия клиентов
- более низкая производительность…

Остановка производства

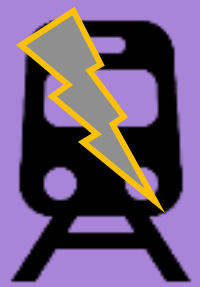


- остановка линии производства
- переаккумуляция складов
- незапланированные затраты

Финансовые потери

Остановка деятельности

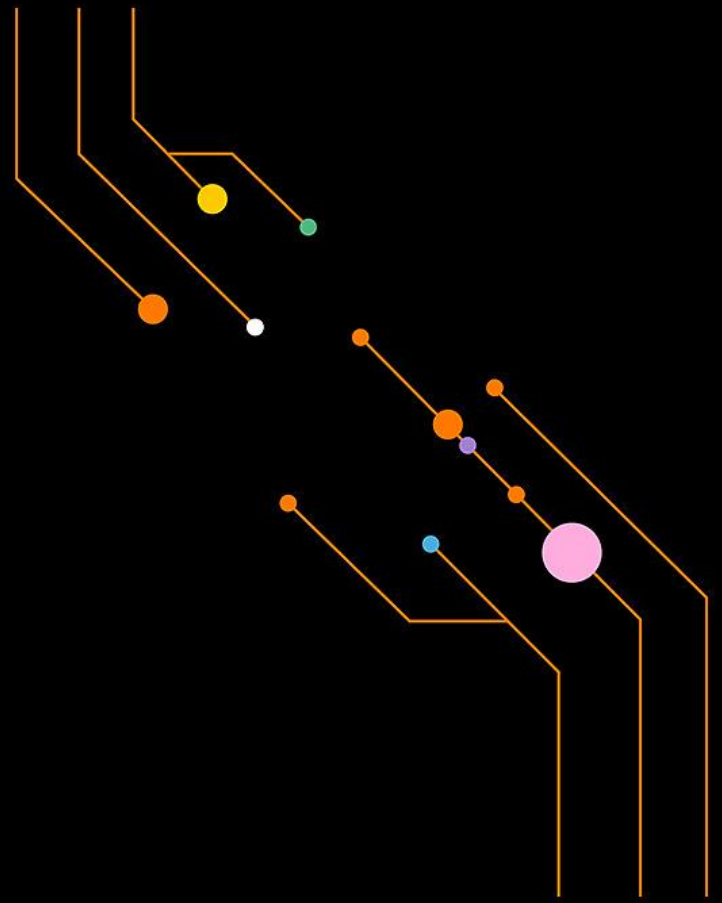
- движение транспорта
- работа климатических установок
- системы сортировки багажа
- системы сканирования на пунктах досмотра
- электропитание



Физические повреждения

- пострадавшие люди…в том числе летальные случаи

Что мы можем сказать о промышленных системах



- Устаревшие технологии
- Проприетарные системы
- Длительный срок службы (иногда больше 20 лет)
- Отсутствие безопасности by design
- Сложная модернизация (часто невозможная)

поэтому легко взламываемые

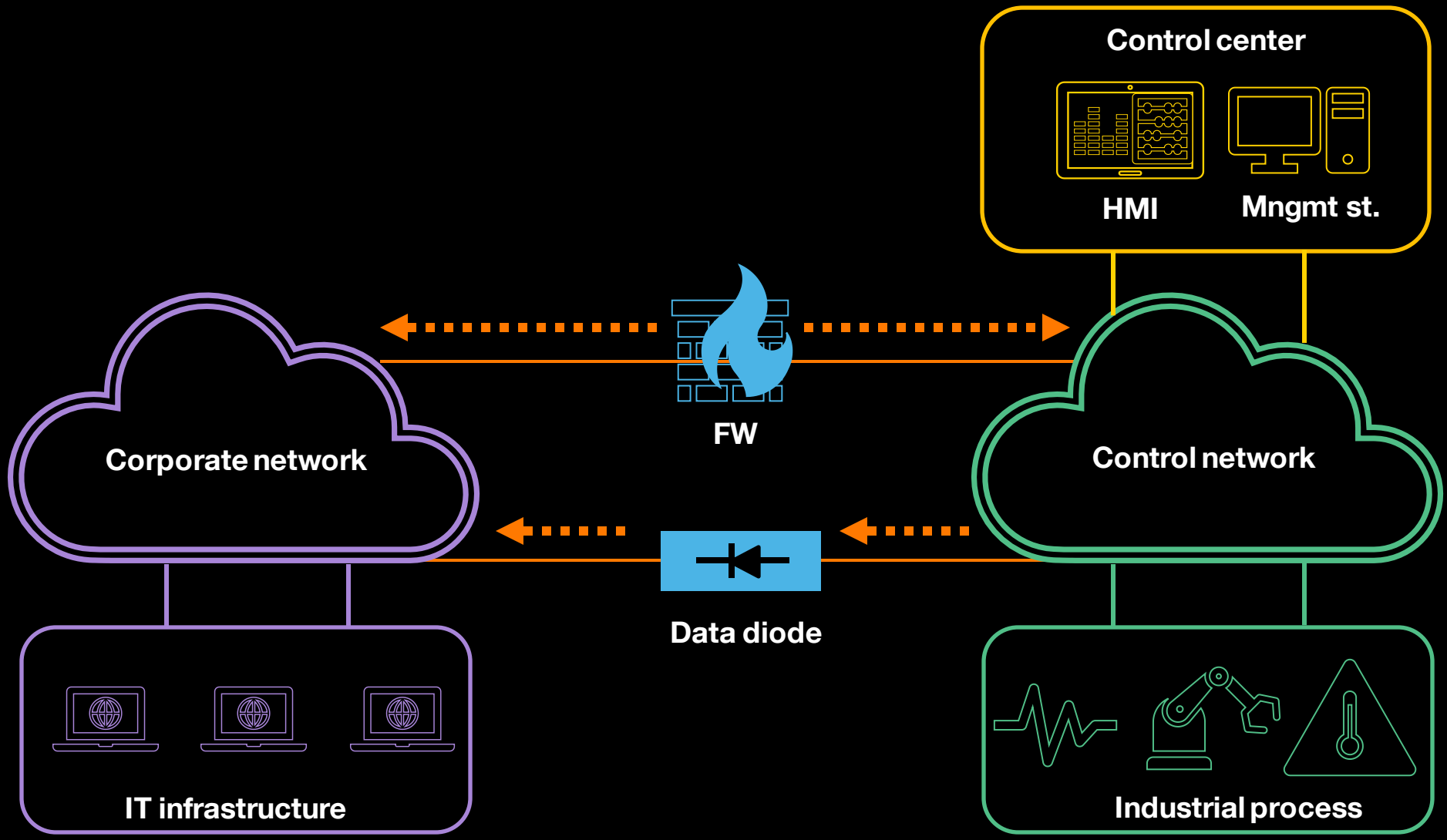
Зоны для защиты

40%
промышленных систем имеют прямое подключение к Интернету

53%
промышленных систем имеют устаревшие операционные системы

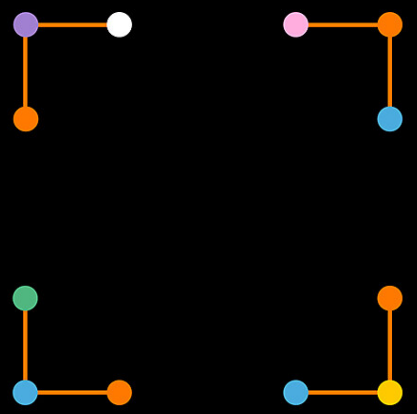
57%
промышленных систем не имеют защиты своих терминалов

Типовая архитектура промышленных систем



Типичные проблемы кибербезопасности с промышленными системами и SCADA

- Управляются инженерами, не ИТ специалистами
- Устаревшие системы работают вместе с современными, из-за чего сложно обеспечивать унифицированную защиту
- Критически важные системы имеют собственные протоколы, которые не имеют security by design
- Уязвимы к сетевым атакам



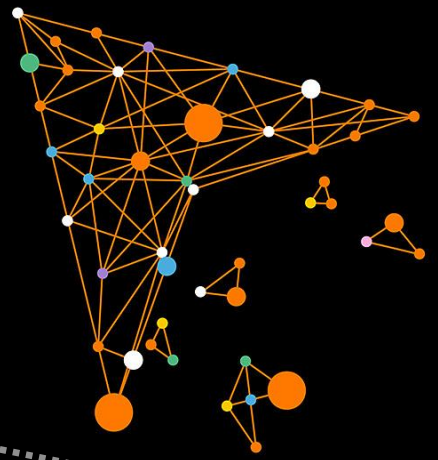
Цифровизация промышленных систем

Все более взаимосвязанная отрасль, основанная на стандартах ИТ

Ускорение процесса слияния традиционных информационных технологий (ИТ) с промышленными технологиями (ПТ)

Эта новая цифровая зависимость оказывает значительное влияние на обе среды в отношении их потенциальной подверженности киберрискам

Кибербезопасность индустриальных систем: ключевые характеристики



RAMS

Reliability

способность системы функционировать в течение определенного периода времени.

Availability

способность системы находиться в рабочем состоянии в данный момент времени

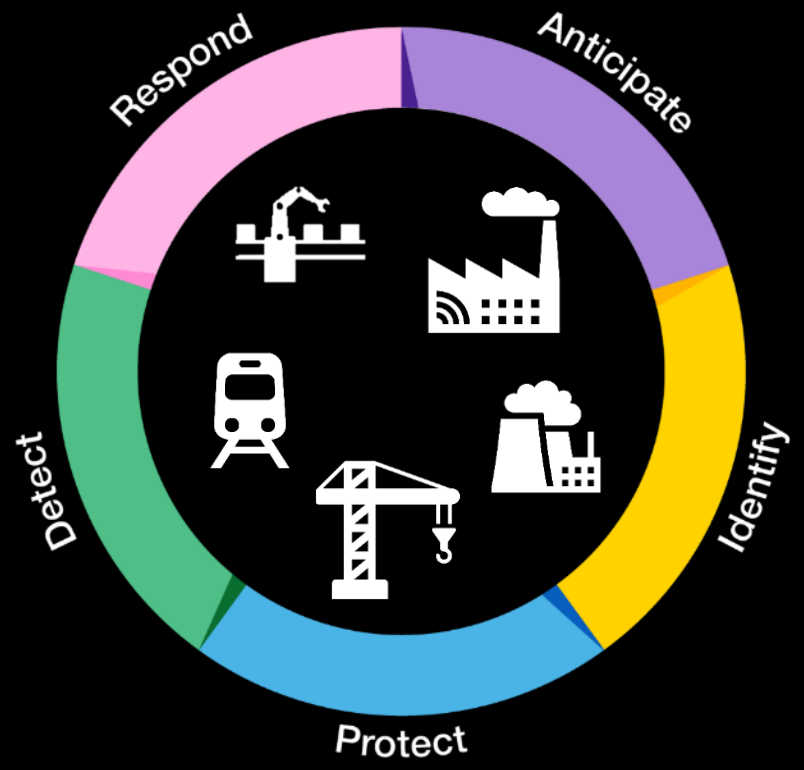
Maintainability

способность системы поддерживаться или восстанавливаться в рабочем состоянии.

Safety

способность не приводить к недопустимым авариям

Обеспечение кибербезопасности в промышленной экосистеме



Шаг 1

Анализируйте, повышайте осведомленность, обучайте, проводите инвентаризацию, повышайте видимость, объединяйте команды ИТ/ТП

Шаг 2

Сегментируйте ИТ/ТП, защищайте конечные точки, защищайте Сети ОТ

Шаг 3

Следите за аномальной активностью и будьте готовы действовать

Шаг 4

Реагируйте на инциденты и анализируйте их для выработки шагов по исправлению

Шаг 5

Проводите периодические аудиты, открывайте для себя новые методы атак, проводите киберучения, работайте с уязвимостями

Сервисы по защите промышленных систем

Identify

- Industrial system Identification
- Security Governance
- Classification
- Risk analysis
- Asset Inventory
- Maturity assessment
- Training
- Legal compliance

Protect

- Awareness / Training
- IT / OT Segmentation
- Component hardening
- Endpoint protection
- Identity Access Management
- Malware cleaner
- Lockbox
- Back up / restore
- OT Segmentation
- Remote access

Detect

- Sensors Deployment
- Anomaly Detection
- Cyber SOC
- Training

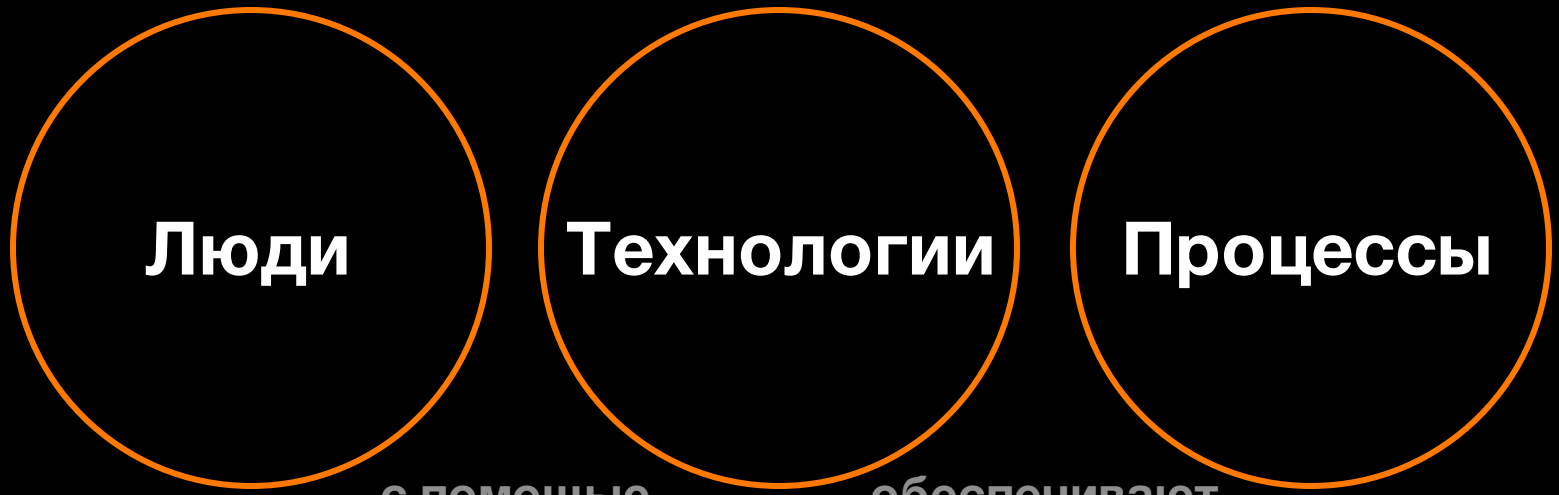
React

- Incident Response
- Disaster's recovery
- Cyber resilience
- Training
- Forensics

Anticipate

- Threat Intelligence
- Vulnerability Intelligence
- Technical Watch
- Pentest / Ethical hacking
- Training

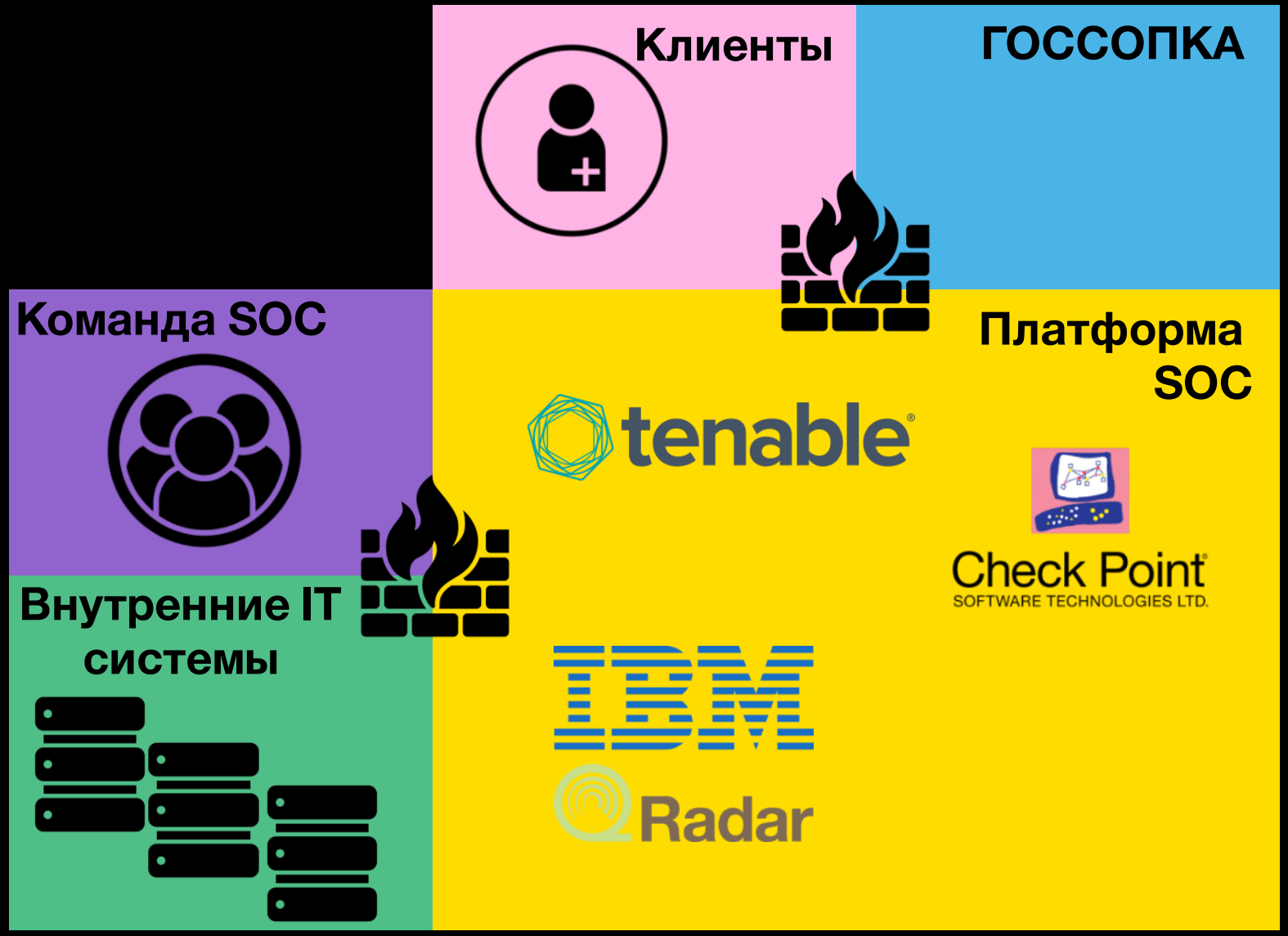
Что же такое SOC?



Кто чем занимается?

L1 Аналитики		Работа с инцидентами в IRP Составление отчетов Взаимодействие с клиентами по инцидентам
L2 Аналитики		Работа с инцидентами в IRP Проведение углубленного анализа инцидентов
L3 Аналитики	Pentesters Solution experts Technical architects Security experts	Разработка use cases, настройка включений Аудиты/тесты на защищенность Имплементация новых функций
Группа реагирования	Security team IT team	Оперативное реагирование Устранение инцидентов Координация действий при инциденте

Инфраструктура SOC



- Выделенные сетевой сегмент
- Выделенный сетевой периметр под каждого клиента
- SIEM IBM Qradar в multitenant режиме
- Check Point Sandblast
- Сканнер уязвимостей Tenable

Инфраструктура SOC

Сравнение SOC

Параметр	Свой SOC	SOC as a Service
Контроль	Полный	Частичный
Понимание информационных потоков	Высокое	Низкое или отсутствует
Гибкость в настройке	Высокая	Средняя
Скорость развертывания	От полугода (обычно 2-3 года)	2-4 месяца
Режим работы (обычно)	5 x 8	24 x 7
Возможности по реагированию	Высокие	Средние / Высокие (MDR)
Скорость масштабирования	Средняя	Высокая
Уровень компетенций	Средний	Высокий
Форма наибольших затрат	CAPEX	OPEX
Предсказуемость затрат	Непредсказуемые	Предсказуемые
Гарантии (финансовые и т.п.)	Отсутствуют	Возможны
Зависимость от каналов связи	Средняя	Высокая
Хранение данных о безопасности	Локально	За пределами организации / гибридно
Права на технологии и процессы	Принадлежат заказчику	Принадлежат провайдеру
Уровень независимой экспертизы / взгляд со стороны	Низкий	Высокий
Выделенный персонал заказчика	Да	Тоже да, но меньше

Сравнение SOC

Параметр	Свой SOC	SOC as a Service
Контроль	Полный	Частичный
Скорость развертывания	От полугода (обычно 2-3 года)	2-4 месяца
Режим работы (обычно)	5 x 8	24 x 7
Скорость масштабирования	Средняя	Высокая
Уровень компетенций	Средний	Высокий
Форма наибольших затрат	CAPEX	OPEX
Предсказуемость затрат	Непредсказуемые	Предсказуемые
Уровень независимой экспертизы / взгляд со стороны	Низкий	Высокий
Выделенный персонал заказчика	Да	Тоже да, но меньше

Типовые ошибки при пилотировании


Слишком сложный сценарий для пилота


Неготовность пилотировать сразу нескольких провайдеров


Задержки по времени из-за взаимодействия с ИТ- и ИБ-командами


Инфраструктура заказчика оказывается не готова к внедрению SOC


Нет команды реагирования

На что обращать внимание при выборе провайдера услуг SOC

- Собственная инфраструктура
- Возможности
- Готовность в данной отрасли
- «Круглосуточность» и способы взаимодействия

Спасибо!

Типовой ввод в эксплуатацию

Prepare

- Консультация заказчика
- Организация единой схемы сбора событий ИБ
- Определение перечня источников событий
- Согласование способа передачи событий ИБ
- Подготовка инфраструктуры
- Подготовка инструкций для конфигурации источников событий

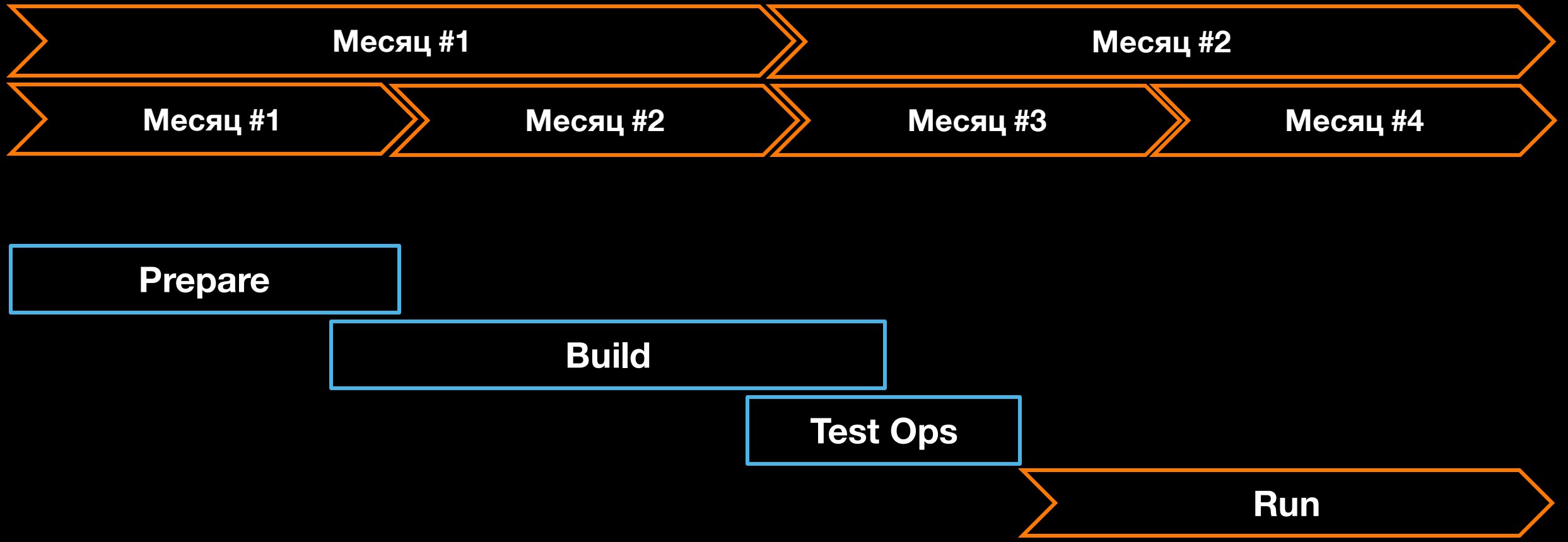
Build

- Настройка схемы сбора логов
- Подключение всех источников событий
- Модернизация схемы сбора событий ИБ
- Включение каталога use-case в соответствие с заданием

Run

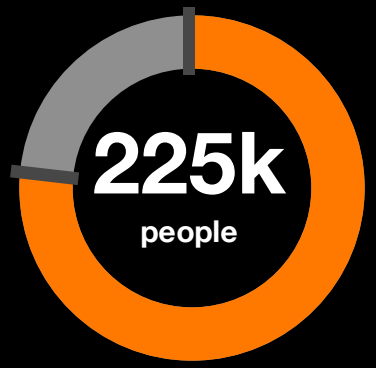
- Работа с use-cases переданными в эксплуатацию
- Уведомление об инцидентах

Столько может длиться пилот



Black Energy - 2018

The attack scenario: a massive phishing campaign with an infected Excel document was launched to introduce the Black Energy malware



Without electricity

Power shutdown time

Power shutdown

Work station sabotage

POWER

Featured Categories

Connected Plant

BlackEnergy, Grid-Disrupting Malware, Has a Successor, Researchers Warn

Oct 18, 2018
by Sonal Patel

BlackEnergy, the malware used in a cyberattack that prompted a large-scale blackout in Ukraine in December 2015, has a successor—GreyEnergy. A group is using the malware to target industrial networks outside Ukraine, researchers from Slovakian cybersecurity firm ESET warn.

ALSO IN THIS ISSUE
October 18, 2018

Distributed Power | Oct 18, 2018
Distributed Energy Is Disrupting the Power Industry: Is the Sky Falling?
by Aaron Larson

News | Oct 18, 2018

Marconi Radio Hack Of - 1903

The attack scenario: wireless communication hack, based on morse code

Need to secure communications

ORIGIN OF WIRELESS SECURITY: THE MARCONI RADIO HACK OF 1903

by: Richard Baguley

33 Comments

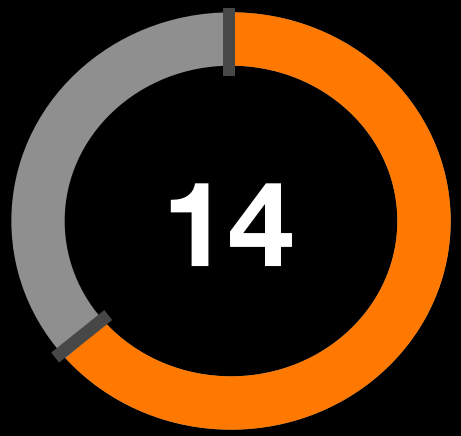
March 2, 2017

The place is the historic lecture theater of the Royal Institution in London. The date is the 4th of June 1903, and the inventor, Guglielmo Marconi, is about to demonstrate his new wireless system, which he claims can securely send messages over a long distance, without interference by tuning the signal.

The inventor himself was over 300 miles away in Cornwall, preparing to send the messages to his colleague Professor Fleming in the theater. Towards the end of Professor Flemings lecture, the receiver sparks into life, and the morse code printer started printing out one word repeatedly: "Rats". It then spelled out an insulting limerick: "There was a young man from Italy, who diddled the public quite prettily". Marconi's supposedly secure system had been hacked.

Tramway de Lodz – Poland 2008

The attack scenario: during a tram depot visit, a teenager collects information needed to build a remote-control system to drive railway switches



Hacker's age

Derailment and tram collision

Injured passengers

The Telegraph

Home News World Sport Finance Comment Culture Travel

USA Asia China Europe Middle East Australasia Africa Nelson

HOME » NEWS » WORLD NEWS

Schoolboy hacks into city's tram system

The boy, described as a 'genius' and some of the equipment he used

By Graeme Baker

12:01AM GMT 11 Jan 2008

A teenage boy who hacked into a Polish tram system used it like "a giant train set", causing chaos and derailing four vehicles.

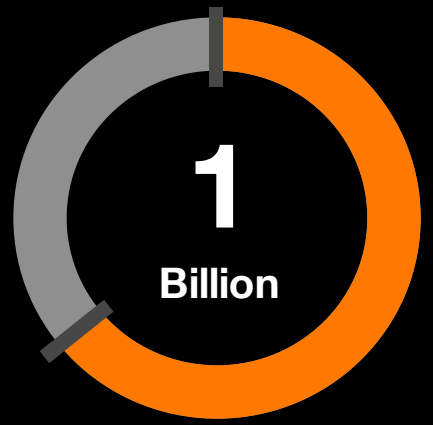
The 14-year-old, described by his teachers as a model pupil and an electronics "genius", adapted a television remote control so it could change track points in the city of Lodz.

Pipeline destruction in Turkey - 2008

The attack scenario: video surveillance and intrusion system de-activation for physical access to the industrial system, modifications of the industrial process leading to the destruction of the pipeline

Downtime

Modifications of the industrial process



Losses

Pipeline destruction

Most Violent Cyber Attack Noted To Date: 2008 Pipeline Explosion Caused By Remote Hacking

Bob Gourley December 13, 2014

Share this:

LinkedIn Facebook Twitter Reddit Email

Reporting by Jordan Robertson and Michael Riley in Bloomberg is shedding new light on a destructive attack against an oil pipeline that caused a massive explosion in Refahiye Turkey in August 2008. The cyber attack component of the event was not realized till years after it occurred, which is part of the reason the main stream media did not widely report on this cyber act of war.

Robertson and Riley's reports indicate that the pipeline was fitted with sensors and cameras to monitor all 1099 miles of the pipeline from the Caspian Sea to the Mediterranean, but the blast did not trigger a single distress signal. They also did not trigger the massive explosion and continuing combustion in eastern Turkey.

Traffic lights - 2009

The attack scenario: Two unionized traffic engineers in the City of Los Angeles scheduled a work stoppage and blocked access to the computer that controlled 3,200 traffic signals

Road sign off

Traffic jams

Hackers could engineer traffic jams, by using their cars to lie to smart traffic lights

By Dr Alfred Chen and Z. Morley Mao

Uhoh. Image: Getty.

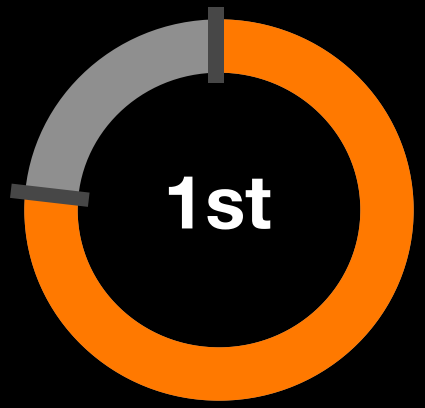
The day when cars can talk to each other – and to traffic lights, stop signs, guardrails and even pavement markings – is rapidly approaching. Driven by the promise of reducing traffic congestion and avoiding crashes, these systems are already rolling out on roads around the U.S.

For instance, the Intelligent Traffic Signal System, developed with support from the U.S. Department of Transportation, has been tested on public roads in Arizona and California and is being installed more widely in New York City and Tampa, Florida. It allows vehicles to share their real-time location and speed with traffic lights, which can be used to effectively optimise the traffic timing in coordination with the real-time traffic demand to dramatically reduce vehicle waiting time in an intersection.

Our work, from the RobustNet Research Group and the Michigan Traffic Laboratory at the University of Michigan, focuses on making sure these next-generation transportation systems are secure and protected from attacks. So far we've found they are in fact relatively easy to trick. Just one car that's transmitting fake data can cause enormous traffic jams, and several attack cars could work together to shut down whole areas. What's particularly concerning is that our research has found the weakness is not in the underlying communication technology, but in the algorithms actually used to manage the traffic flow.

Stuxnet - 2010

The attack scenario: 1st malware that changed the behavior of an industrial installation. It specifically targeted the Iranian uranium enrichment control system



Use of a cyber weapon

False display on SCADA Modified PLC program

Damaged or even destroyed uranium spinner

Stuxnet worm hits Iran nuclear plant staff computers

26 September 2010

A complex computer worm has infected the personal computers of staff at Iran's first nuclear power station, the official IRNA news agency reported.

However, the operating system at the Bushehr plant - due to go online in a few weeks - has not been harmed, project manager Mahmoud Jafari said.

The Stuxnet worm is capable of seizing control of industrial plants.

Some Western experts say its complexity suggests it could only have been created by a "nation state".

It is the first sign that Stuxnet, which targets systems made by the German

Triton - 2016

The attack scenario: intrusion into the IT network then bounces to the industrial network to corrupt the program of a safety PLC

2014 -2017: a planned, calculated and sophisticated attack

Attack on a Safety Instrumented System, the ultimate programmed safety

Production shutdown

Triton: hackers take out safety systems in 'watershed' attack on energy plant

Sophisticated malware halts operations at power station in unprecedented attack which experts believe was state-sponsored

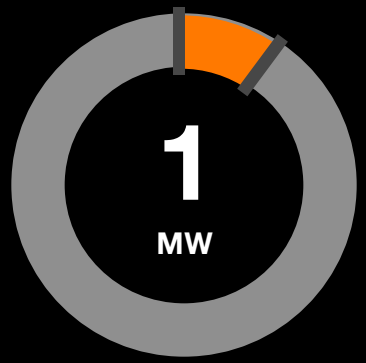
▲ Targeted ... a power plant in Saudi Arabia. Photograph: Lena Kara/Rex Features

In what experts are calling a watershed moment, hackers have infiltrated the critical safety systems for industrial control units used in nuclear, oil and gas plants, halting operations at at least one facility.

The attackers, who are believed to be state-sponsored, targeted the Triconex industrial safety technology made by Schneider Electric SE, according to security firm FireEye and Schneider, who disclosed the incident on Thursday.

Tidal turbine Sabella - 2016

The attack scenario: the computer that allowed the satellite connection was hacked

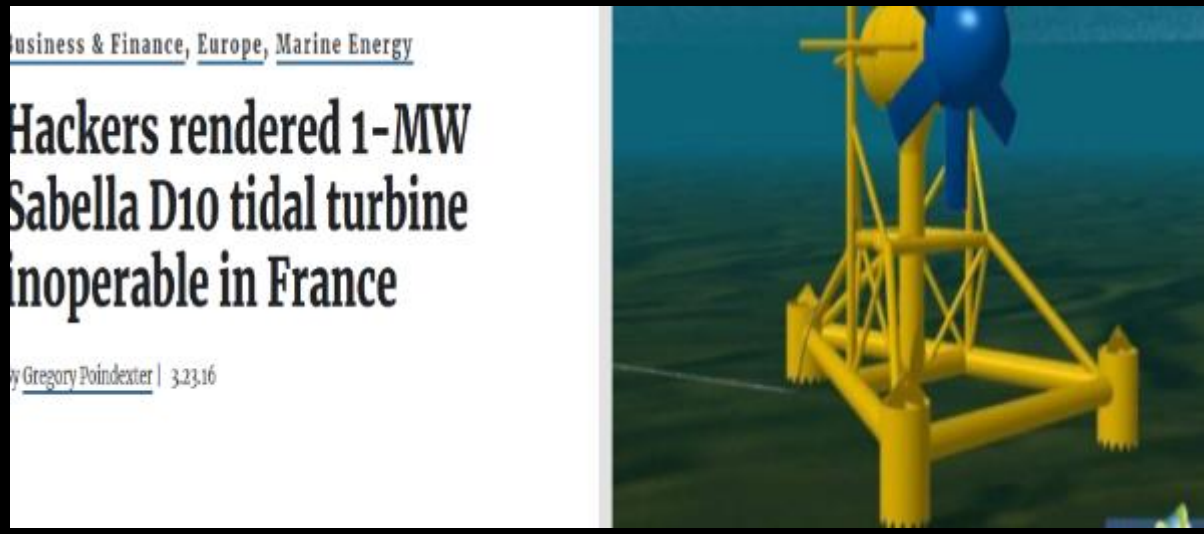


Of production blocked

Shutdown time

Server encryption

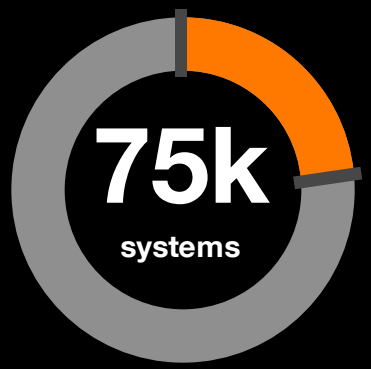
Ransomware



Renault-Nissan - 2017

The attack scenario: production problems resulting from WannaCry ransomware worm attack that spread to more than 150 countries

Asked per file



Affected

Production shutdown

Work station sabotage

Renault-Nissan is resuming production after a global cyberattack caused stoppages at 5 plants

REUTERS

Laurence Frost and Naomi Tajitsu , Reuters May 15, 2017, 7:25 PM

Renault-Nissan said on Monday that output had returned to normal at nearly all its plants, after a global cyber attack caused widespread disruption including stoppages at several of the auto alliance's sites.

A security guard walks past 'Micra' cars lined at the newly-inaugurated Renault-Nissan Alliance auto plant in the southern Indian city of Chennai. Reuters/Babu Babu

Renault and its Japanese partner are the only major car manufacturers so far to have reported production problems resulting from Friday's WannaCry ransomware worm attack that spread to more than 150 countries.

Mondelez - 2017

The attack scenario: malware affected a significant portion of the company's global Windows-based applications and its sales, distribution and financial networks across the company

Losses

inoperable

Production shutdown

Work station sabotage

Technology / Smart Industry / Cybersecurity

Malware May Have Cost Mondelez $100 Million

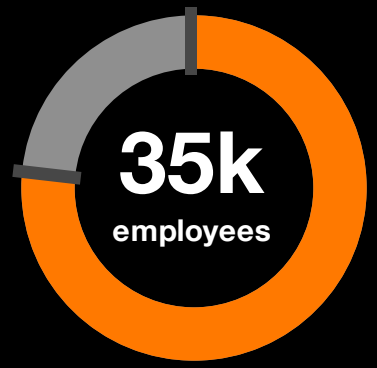
A June 27 ransomware attack crippled the top food company, especially its overseas business units.

Nov 06, 2017

A June 27 global malware incident may have impacted Mondelez International's business to the tune of $100 million.

Hydro - 2019

The attack scenario: one employee unknowingly opened an infected email from a trusted customer. That allowed hackers to invade the IT infrastructure and covertly plant their virus.



Affected

Losses

Ransomware

Work station sabotage

Cyber-attack on Hydro

Hydro became victim of an extensive cyber-attack in the early hours of Tuesday, March 19, 2019, impacting operations in several of the company's business areas.

Cyber-attack on Hydro in brief

On March 19, 2019, Hydro was hit by an extensive cyber-attack. The attack affected our entire global organization, with the business area Extruded Solutions having suffered the most significant operational challenges and financial losses. Hydro's other business areas – Bauxite & Alumina, Primary Metal, Rolled Products and Energy – was able to produce close to normal despite the attack, although based on work-intensive workarounds and manual procedures.

News about the cyber attack

Zweites Quartal 2019:
Ergebnisrückgang aufgrund niedrigerer erzielter Preise
Juli 23, 2019

Erstes Quartal 2019:
Ergebnisrückgang aufgrund von

Honda - 2020

The attack scenario: an internal server in Japan was attacked and malware spread through Honda's computer network, leading to difficulties in accessing servers, email and other systems

Shutdown time

Closed

Production shutdown

Work station sabotage

Honda Pauses Production and Closes Offices due to Ransomware Attack

June 12, 2020

KEYWORDS cyber security /

Honda's global operations have been hit with a ransomware attack. The company said earlier that the attack had affected operations at several facilities, as well as both customer service and financial services operations.

Fareva - 2020

The attack scenario: Fareva data center near its Cosmeva cosmetics factory, was targeted by a virus. Ten minutes later, the IT staff on duty shut down the so-called ERP central system.

Shutdown time

Blocks

Production shutdown

Ransomware

Health

French anti-Covid vaccine manufacturer stricken by cyberattack

December 19, 2020 · 3 min read · admin

Posted on Dec 19 2020 at 9:20

Nasty advertisement for a pharmaceutical manufacturer that will participate in the production of an anti-Covid vaccine. French manufacturer Fareva suffered a cyberattack overnight from Tuesday to Wednesday, which blocks around fifteen factories in France, except two. "We no longer have access to our computer systems, this stops all the manufacturing processes", testifies a union representative of the Amboise plant (Indre-et-Loire).