

DATAPK

Information security solution for
industrial systems and critical
infrastructures



Alexey Komarov
Solutions Development Manager
Ural Security Systems Center

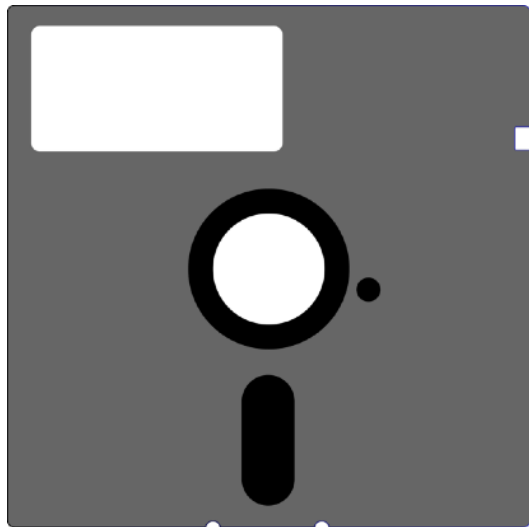
2 June 2016

Problem: new and old technologies

- 1989 - TCP/IP placed into the public domain



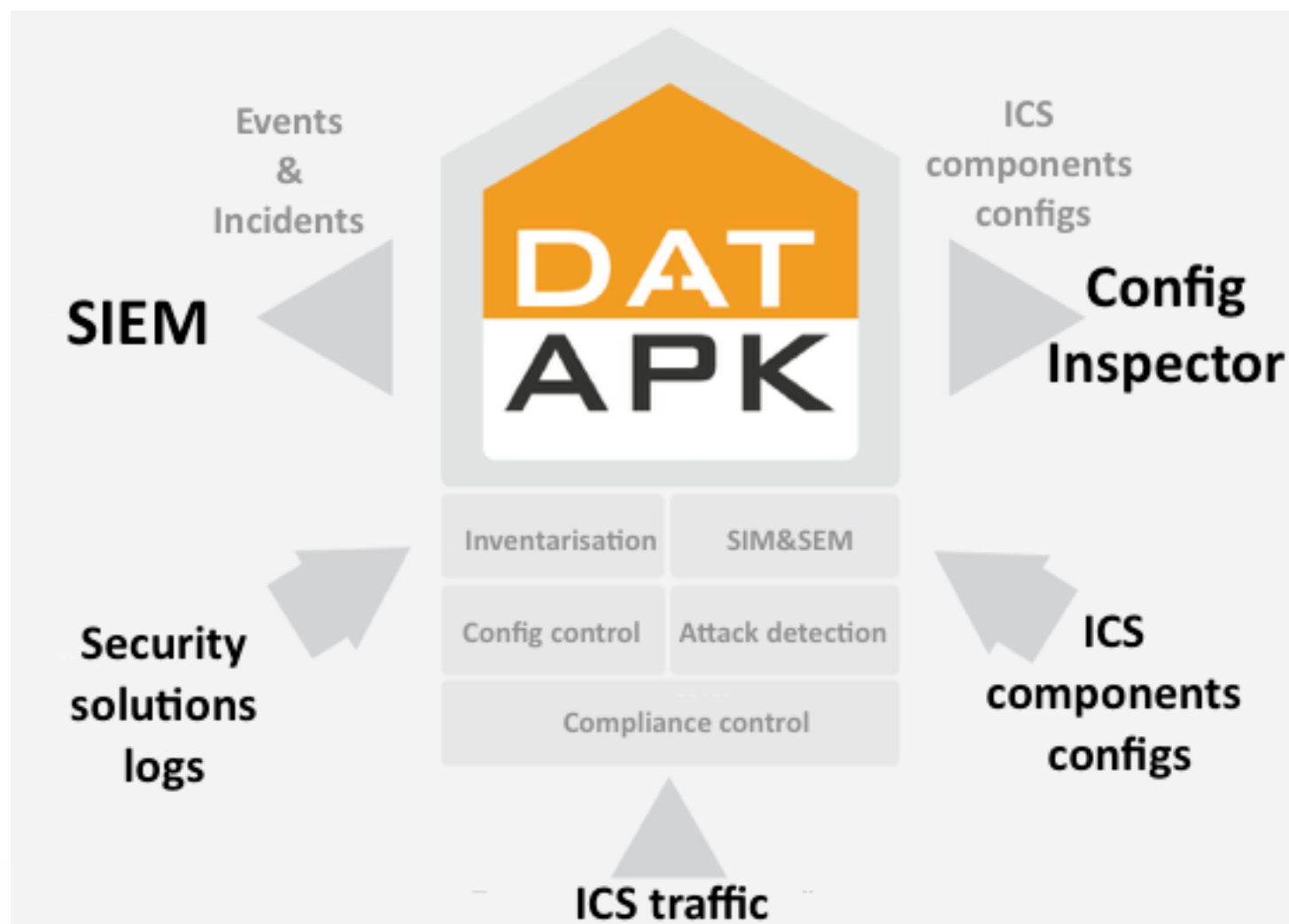
- 1958 - Sibirskaya Nuclear Power Plant (2nd in the World)
- 1958 - Lukoil
Nizhegorodnefteorgsintez
- 1968 - Gazprom mining Orenburg
- 1978 - Sayano-Shushenskaya Dam
- 1985 - Surgut-2 Power Station



Problem: IT vs ICS



Solution: DATAPK function scheme



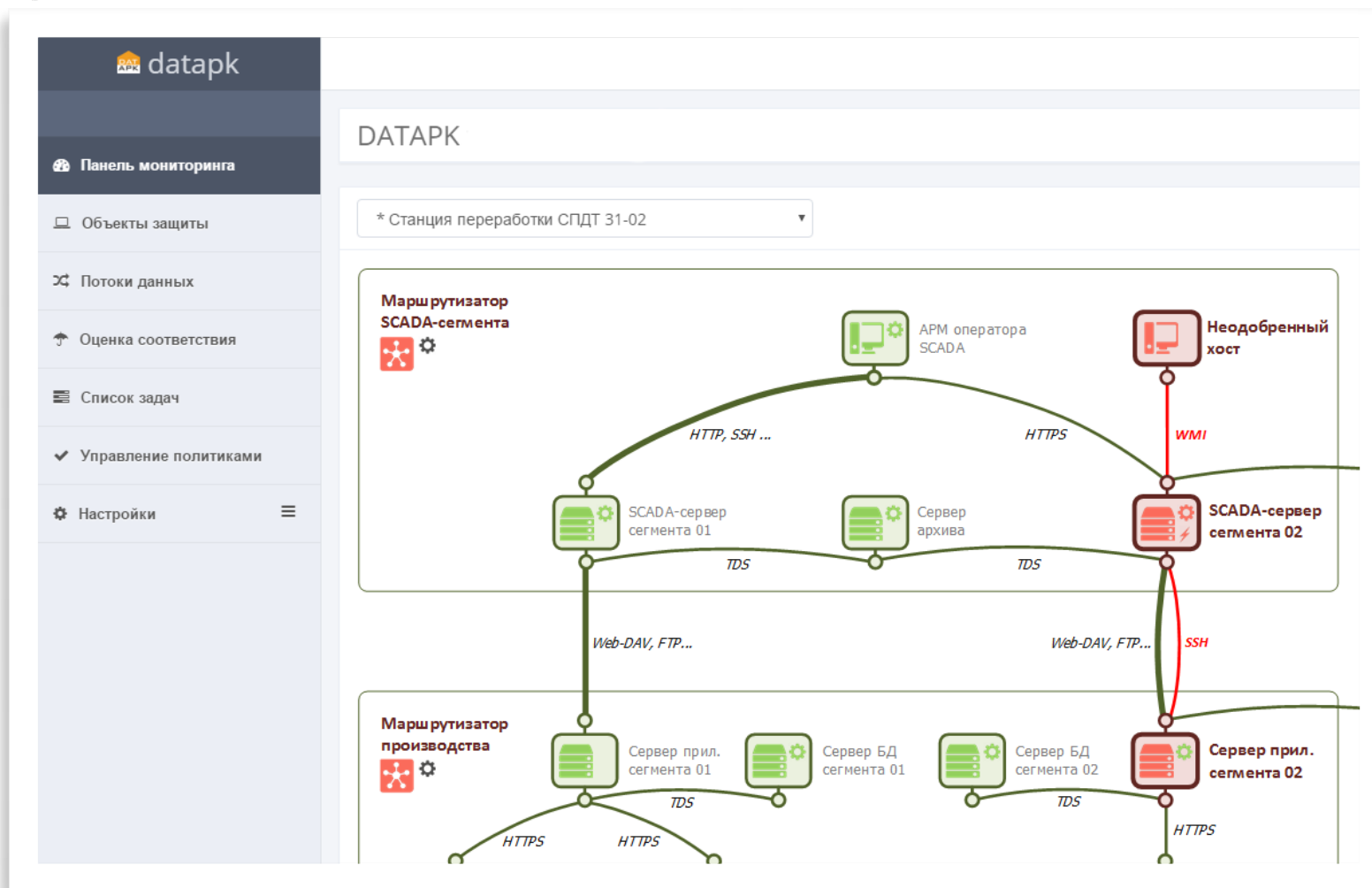


Solution: DATAPK functions

- ICS components inventory
- ICS components configuration control
- Computer attacks detection
- Centralized collection, correlation, classification and analysis of the importance of information security events
- ICS components risk assessment
- Automized compliance



Solution: DATAPK interface example 1



Solution: DATAPK interface example 2

Выявлено событие информационной безопасности!

Необходимо немедленно оповестить ответственного сотрудника по телефону:

+7(343)286-24-39

Сообщите ему нижеследующую информацию:

Код события: ИБ #15.23-1

Тип события: Нарушение целостности

Описание события: Обнаружен новый поток данных между "Сервер архивов" и "АРМ инженера АСУ ТП"

Возможное последствие: Нарушение замкнутости функционирования оборудования, ПО ИСиС или систем защиты

Дополнительная служебная информация:

Источник: 192.168.243.112

Получатель: 195.64.213.460

Протокол: ICMP

Дата и время выявления: 03 марта 2016 17:22

Крайнее время оповещения: 17:52

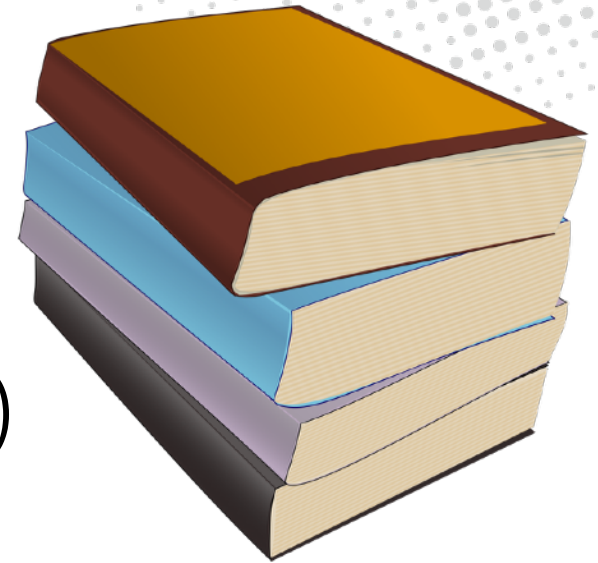
Осталось: 29 минут 43 секунды

Введите код подтверждения сотрудника:

Принять

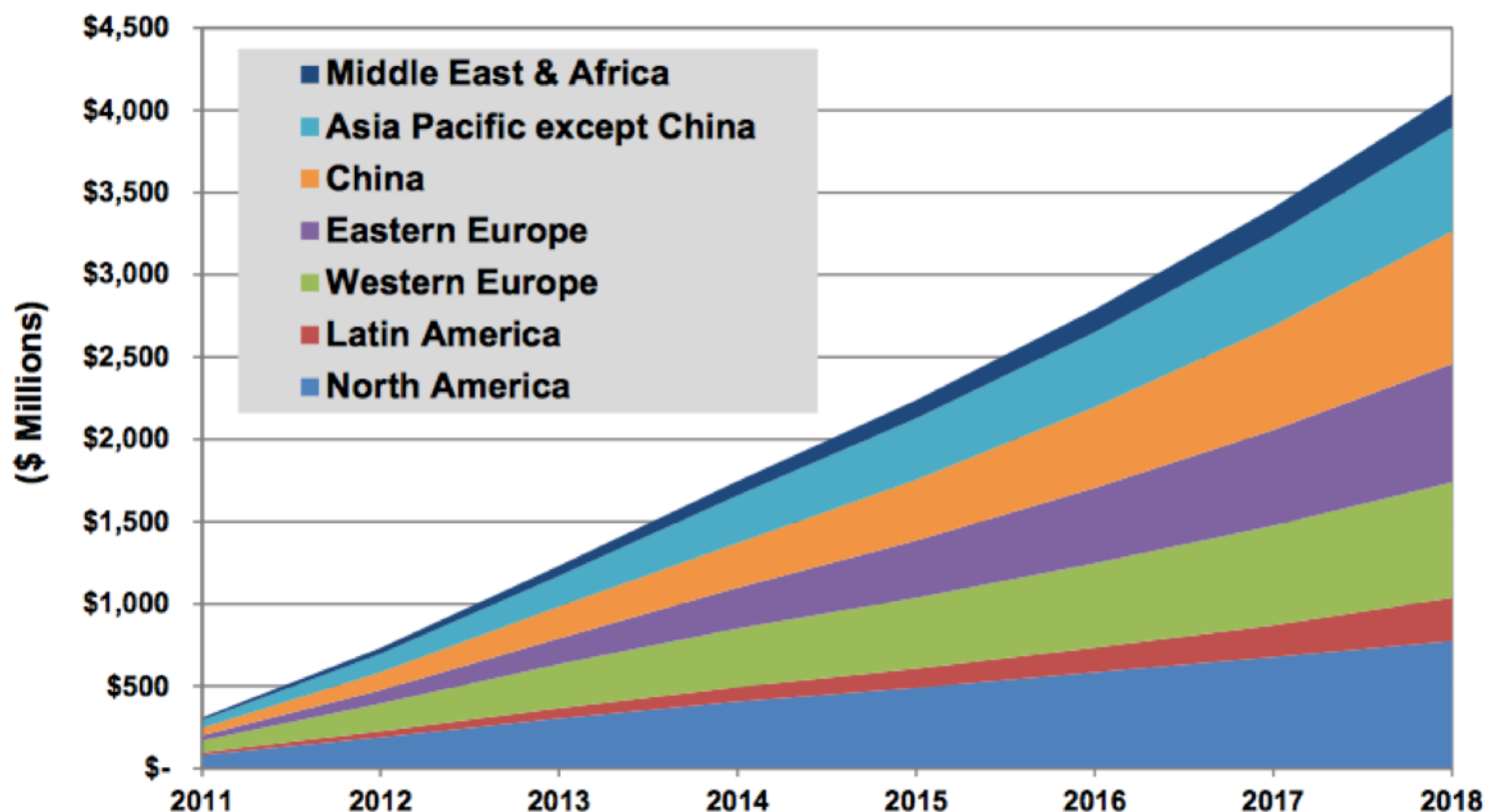
Market: sources

- Industrial Control Systems (ICS) Security Market - Global Advancements, Market Forecast & Analysis (2013 - 2018) by Markets and markets.
- ICS Cyber Security Solutions от ARC Advisory Group.
- Industrial Control Systems Security (Market Issues, Best Practices, and Global Forecasts) by Pike Research.
- <http://cis-forum.ru/assets/images/Prezi/Lukatskii.pdf> - Alexey Lukatsky, International ICS security market overview.



Market: Worldwide

Chart 2.3 Cumulative ICS Security Revenue by Region, World Markets: 2011-2018



(Source: Pike Research)

Market: enough =)

- McKinsey method: (information) security market is 5-7% of information services
- Market assessment: \$85 billions with an expected annual growth 6% by 2020 (Ministry of Industry and Trade).
- For each technology growth dynamics may be different - from 3% to 12%.
- Our market could reach \$4.5 billion.



Market: segments

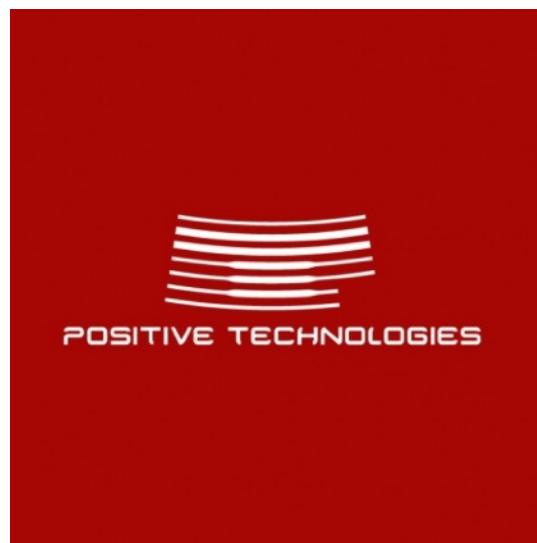
- Plants (metallurgy, chemical, petrochemical, oil and gas etc.)
- Nuclear power plants, hydropower plants, thermal power plants
- Urban transport, railway, airports, ports
- Military industrial
- Utilities



«Competitors»: who are they?

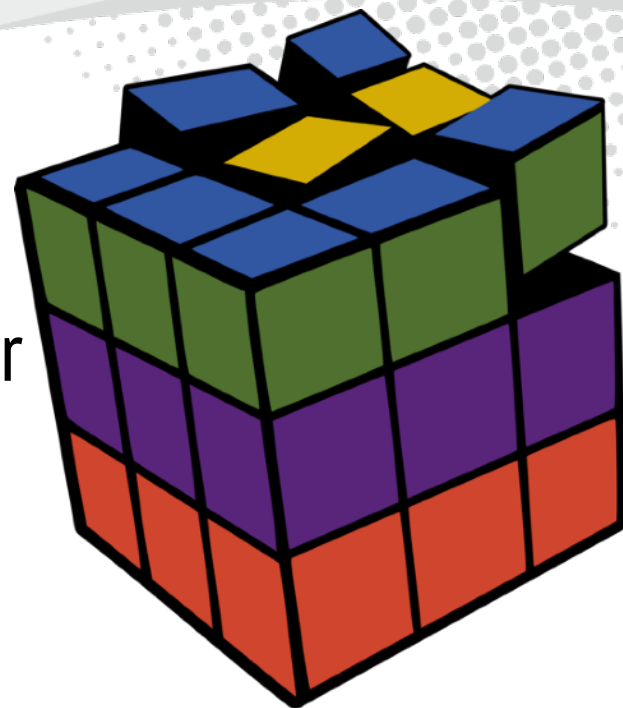


Kaspersky®
**INDUSTRIAL
CYBERSECURITY**



«Competitors»: collaboration

- DATAPK can be implemented together with them as a part of complex solution
- DATAPK can be implemented in addition to double the control
- DATAPK can collect data for them
- DATAPK can export data to them



- **АПК «ЩИТ»**
- **ASAP**
- **KICS**
- ...

«Competitors»: why DATAPK?

- **Agentless** - no change in infrastructure
- **Fast start** - no long time for implementation
- **Automized compliance** - FSTEK, NIST, NERC etc.
- **Modular and hierarchical architecture** - possible to build complex systems
- **Patented* technologies** - method for controlling data transmission network, application of soft computing for control tasks, etc.



Team

- Alexey **Komarov** - Solutions Development Manager. Information security: 10+ years. FSB Academy, secure telecommunication systems engineer, with honors.
- Nikolay **Domukhovsky** - Chief Engineer: 5+ years. Information security: 10+ years Higher education on information security.
- Anton **Afanassenko** - Head of Development, solid experience as a programmer and project management.
- 5 own and 10+ outsourced developers.
- USSC: analytics, engineers, experts.



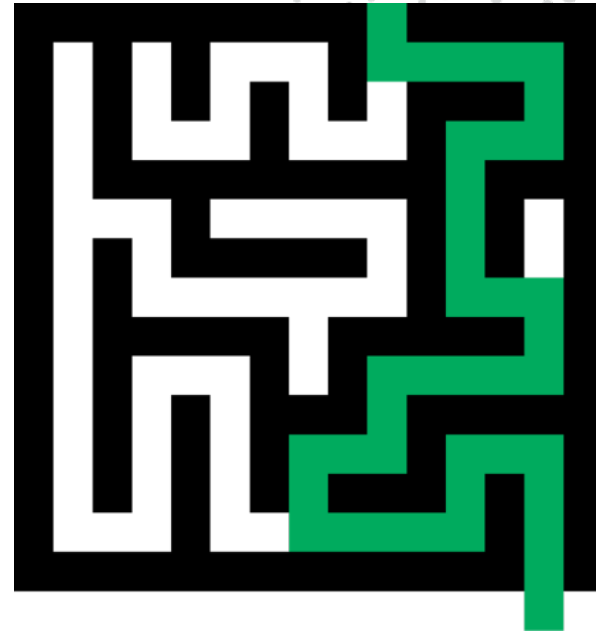


Team: experience and qualification

- Dedicated unit: 3+ years of operation
- Audits of existing ICS (40+ objects)
- Information security systems designs
- ICS security researches (ICS-CERT advisories)
- Trainings for customers
- A series of webinars Cybersecurity NON-STOP
 - <http://USSC.ru/events/webinar> (Events -> Webinar Archive)
 - 2 seasons, 8+8 series, 13+ hours, 3000+ views on YouTube

Implementation: plan

- 2016
 - First sell
 - Three pilots
 - FSTEK certification
 - Southern Federal University - labs
- 2017
 - Gazpromcert certification
 - Three active partners
 - Two collaborative product with «competitors»
 - OEM products with ICS vendors
 - Start of international expansion



- Every year
 - more ICS protocols
 - more ICS devices
 - more integrations
 - more ICS technologies partners



Thanks!

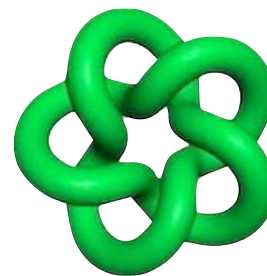


USSC

Tel.: +7 (343) 379-98-34

E-mail: info@ussc.ru

www.USSC.ru



Alexey Komarov

<http://ZLONOV.ru>

@zlonov