softline SOFL

A few stories from Russia

Short sketches about cybersecurity

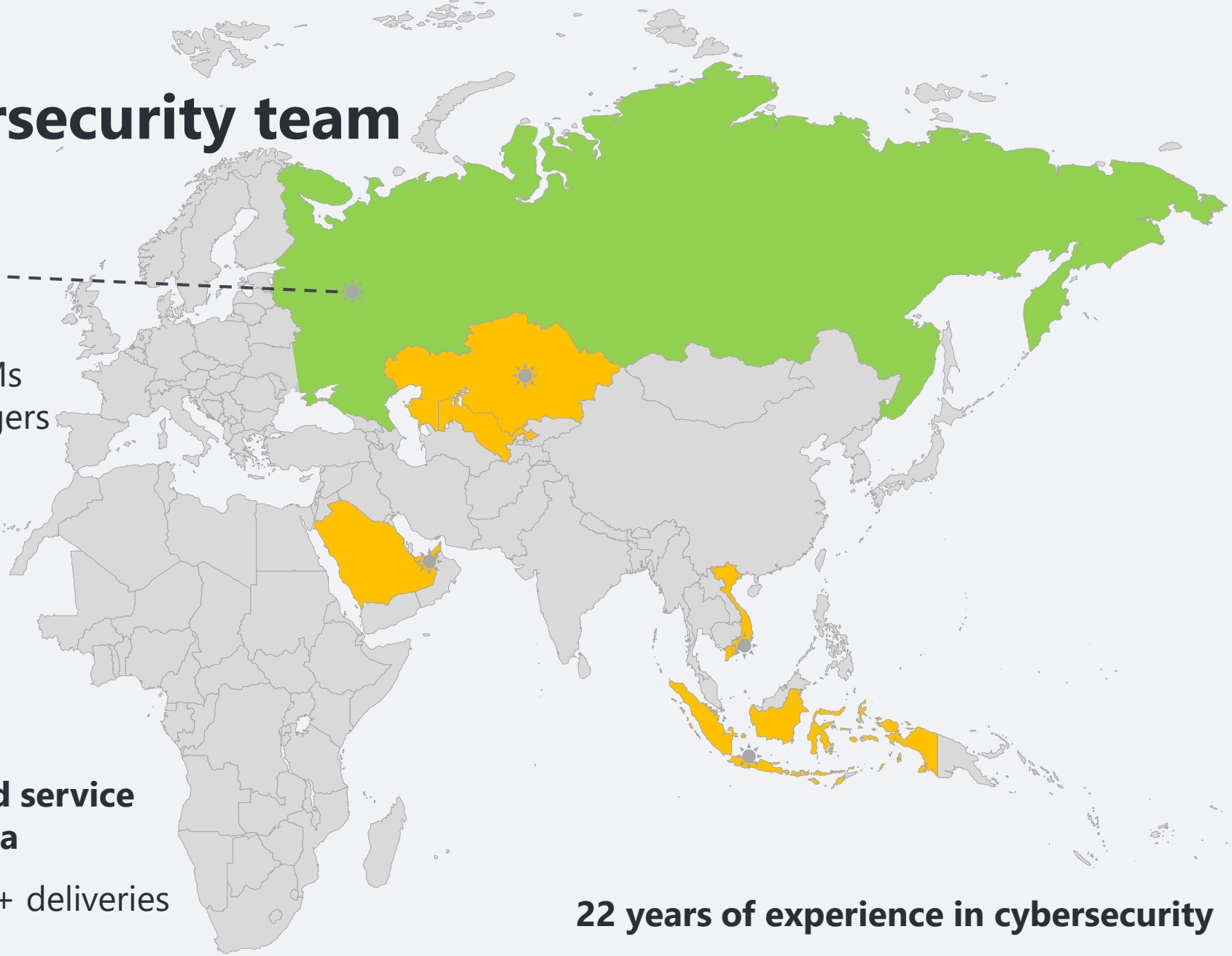
Dmitriy Vasilev

Head of cybersecurity business unit

Softline and cybersecurity team

Headquarter

- 637 account-managers
- 75 cybersecurity solution sales
- 43 technical solution sales & BDMs
- 257 engineers and project-managers
- 66 developers
  - SOC
  - CyberDef
  - CyberPolygon
  - Awareness platform
- 25 offices
- 270+ vendors in portfolio



1st position among integrators and service providers in cybersecurity in Russia

Each year we do more than 20 300+ deliveries & 450+ projects

22 years of experience in cybersecurity

Story #1
Smart hotel without electricity
or
how hard to catch incident without SOC Security Operation Center

Cybersecurity investigation: IOT under attack

Hackers

One very smart hotel with ★ ★ ★ ★ ★

Has been hacked:

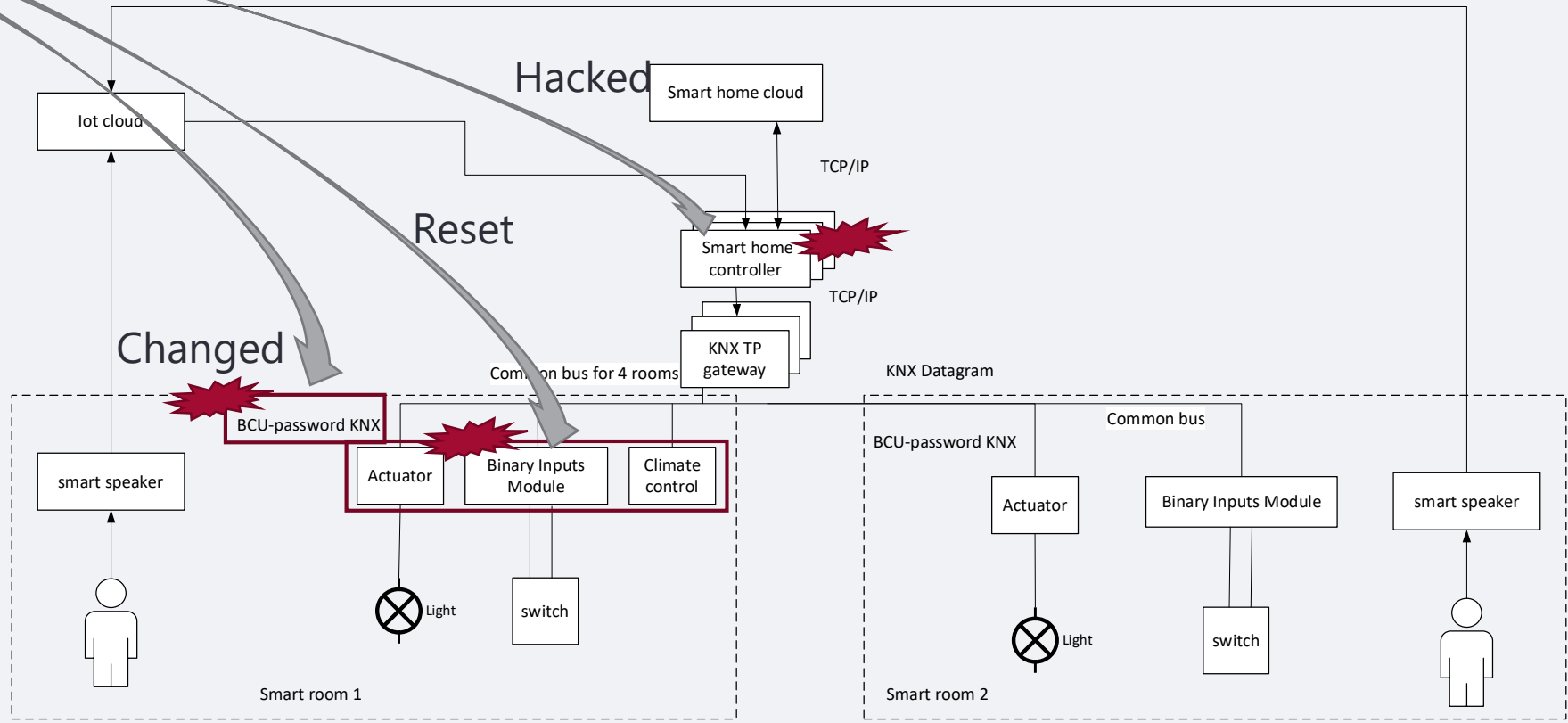
1. Smart controller = Ubuntu OS
2. Old BCU Password bruted
3. New BCU Password enforced
4. Devices firmware reset
5. Asked huge redemption

Business impact

The lights/air conditioning/curtains stopped working in all the rooms

Problem

- Devices can only be re-flashed at the factory
- Brute force could takes a few years



Solution

- Urgent negotiation with device vendor = non-public soft
- Hard reset all devices = 10 days non stop working
- Communications with guests

SOC as a first step in mature cybersecurity MSSP model

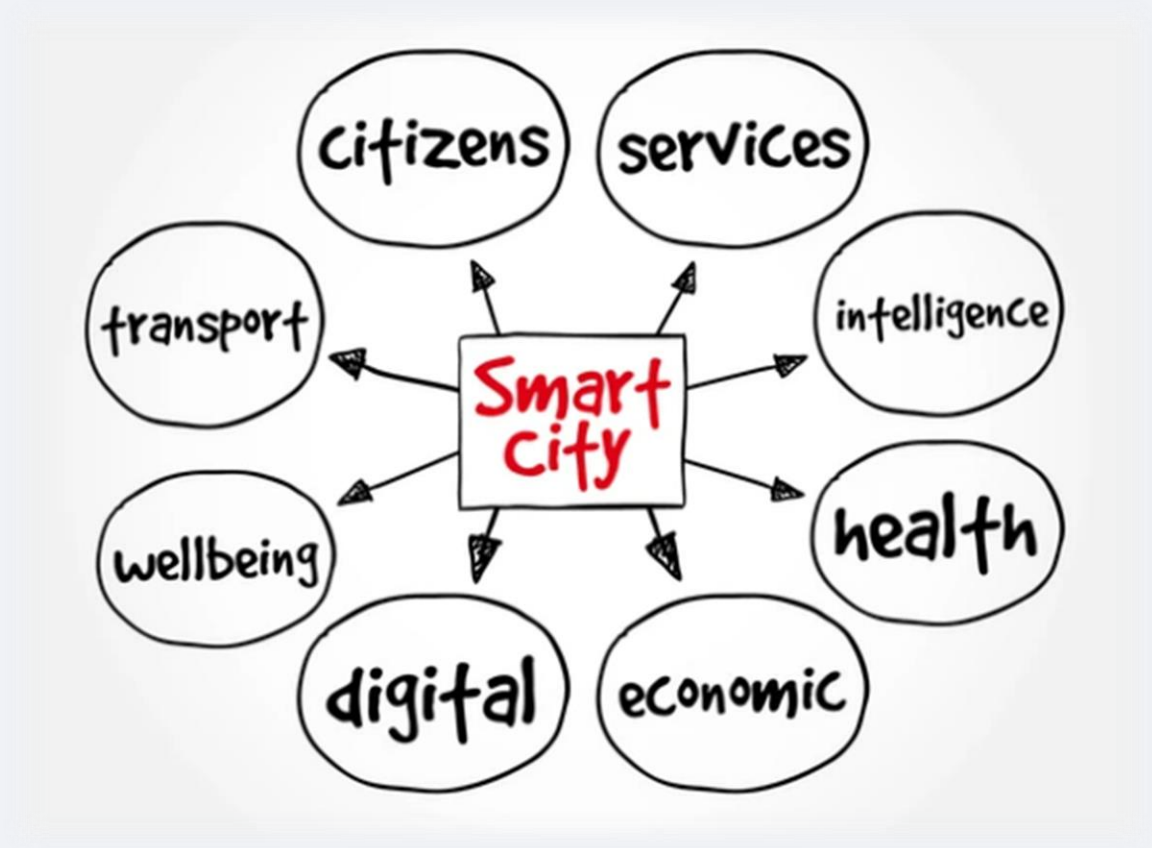
SOC:
- First touch
- Identifying IS GAPs
- Increase trust
- Create value

Moment X

1st Year	2nd Year	3rd Year	4th Year
SOC service: • MS Servers • Linux • Workstations • NGFW • EDR	Technical support contract SOC service: • MS Servers • Linux • Workstations • NGFW • EDR • Cloud providers • Network Devices • RDBMS • PAM	IS consulting contract Technical support contract SOC service: • MS Servers • Linux • Workstations • NGFW • EDR • Cloud providers • Network Devices • RDBMS • PAM • 40+ Business applications	Delivery&Support: • NTA • DAG • DRP • MFA Technical support contract SOC service: • MS Servers • Linux • Workstations • NGFW • EDR • Cloud providers • Network Devices • RDBMS • PAM • 40+ Business applications

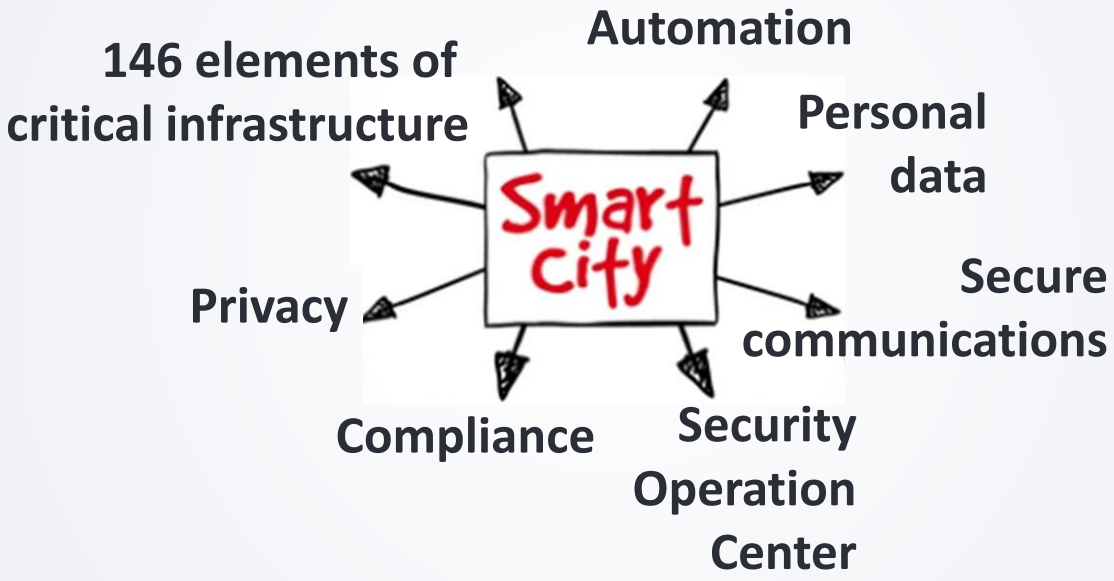
Story #2
Smart city with our SOC

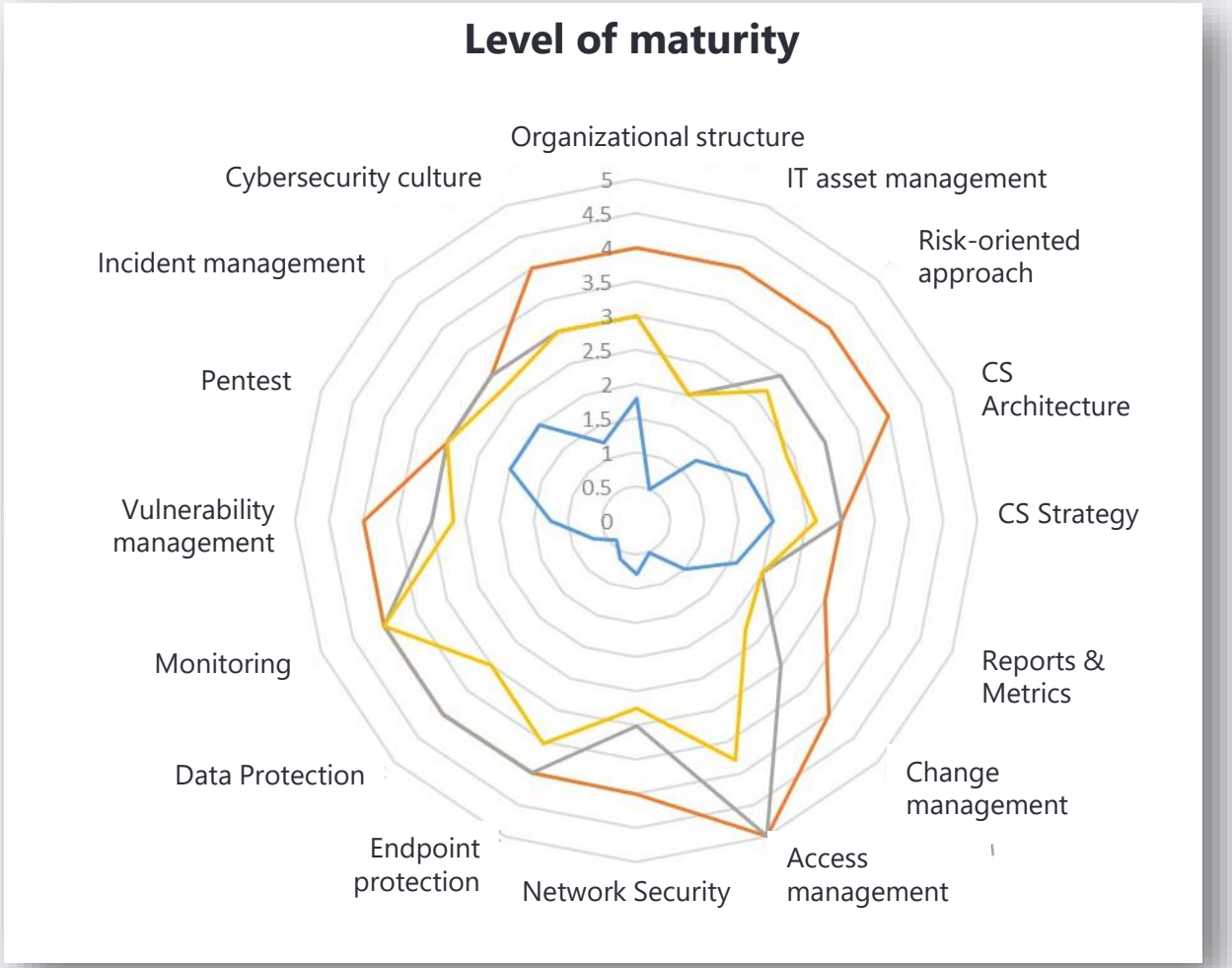
One side of smart city



- 4,61 square kilometers
- 66 500 citizens and 70 000 workplaces
- Smart home & key-less access
- Predictive safety systems
- Central cooling systems
- Dedicated metro-station
- Reflection surface for roads and roof
- Energy-efficient modeling as a foundation
- Automation on all layers
- Smoke-less technologies with low CO2 and NOx
- Waste sorting
- Parks takes 33% of territory

The other side of smart city



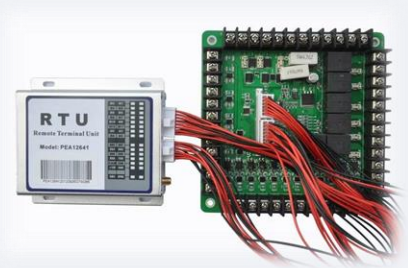


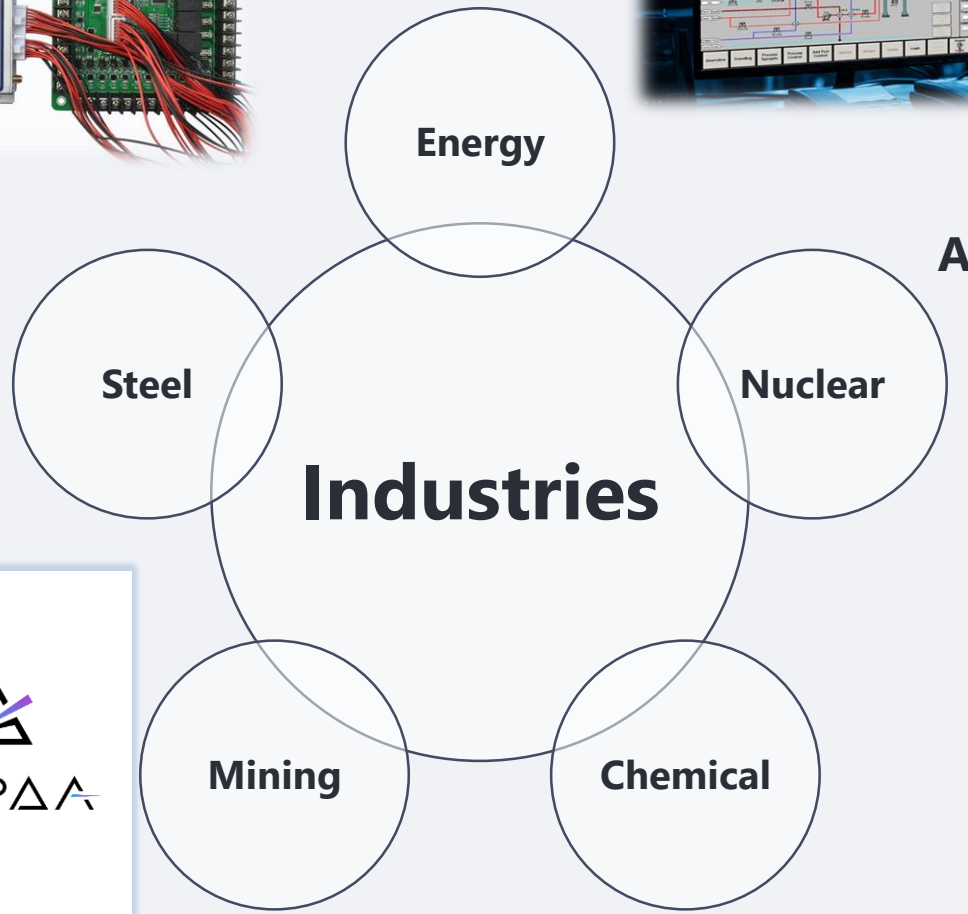
Story #3
Critical infrastructure protection

Critical Infrastructure – 11 years experience

State Energy Corporation
89 branch offices
~1200 locations
1500+ objects of critical infrastructure

1. Audit & categorization
2. Defining requirements
3. Creating documentation
4. Projecting complex cybersecurity management
5. Solution implementation & modernization





Machinery

Assembly lines

RTUs

HMIs

SCADA

PLCs

Modbus

kaspersky
SOLAR
КИБЕР ПРОТЕКТ
КОД безопасности
INFOWATCH
EFROS DEFENCE OPERATIONS
ГАРДА
PT POSITIVE TECHNOLOGIES

Modern heavy industry

22,4M$ & 4 years

Why cybersecurity so important?

- Highly critical production processes
- The need to protect critical information infrastructure facilities
- The need to protect intellectual property
- Requirements for technological process continuity
- The importance of industrial safety
- Reducing the risk of production downtime
- Minimizing financial losses from information security incidents

We must keep in mind that:

1. We are working with high-risk industries
2. Software failure can stop all company
3. Performance is the key - cybersecurity does not have allowance to decrease it
4. Most of OT devices and controllers has a long life with update cycle 10-20 years
5. We need to catch technological “window” for changes

What kind of solutions will be implement:

- Next gen firewall
- Encrypted channels
- Web application firewall
- Endpoint protection
- Vulnerability management
- Network Traffic Analysis
- Multi-factor authentication
- Privileged Access Management
- Data leak protection
- Systems against unauthorized access
- Security Information and Event Management
- Protection for virtualization system
- Threat intelligence

kaspersky · UserGate · INFOWATCH · АЙТИБАСТИОН · positive technologies · КОД безопасности

Digital Transformation. Successful. Effective.

Story #4
Back to business in 2 weeks
or
how it could be much better with business continuous plan & disaster recovery plan

Cybersecurity incident happens…

A software development company (600+ developers) with a distributed geography, broad network of subsidiaries, large number of remote employees. Low cybersecurity maturity.

- The entire infrastructure has been compromised, numerous IoCs detected
- To contain the incident, management has decided to disconnect infrastructure from the Internet and isolate key services within the internal network
- As a result, most of operations (i.e. software development) have been suspended
- An investigation has been initiated, but there is no clear understanding of how to restore business operations without the risk of being re-compromised again
- **There is no defined action plan, available resources are clearly insufficient to address the situation**

softline® SOFL

2 weeks to restore operations and gain confidence

A crisis management team has been set up (15 core + 10 support members)

- Two «green zones» have been deployed:
  - a cloud environment for publishing external resources
  - an internal infrastructure segment with domain services
- Essential security tools have been (re)deployed: EPP / EDR, NGFW / VPN, MFA combined with basic network segmentation and hardening + SOC
- Secure access gateways to critical infrastructure have been deployed
- Minimal business operations have been restored + 6 months action plan prepared
- Long-term cybersecurity strategy development has been kicked-off

Story#5
How to keep team qualified in cybersecurity and ready for incidents?

Training platform for one of the biggest Russian metallurgical holding

Aim

- Train for devOps, IT and cybersecurity teams
- Help with coordination exercises to become a one team
- Identify and train leader in each direction

Tasks

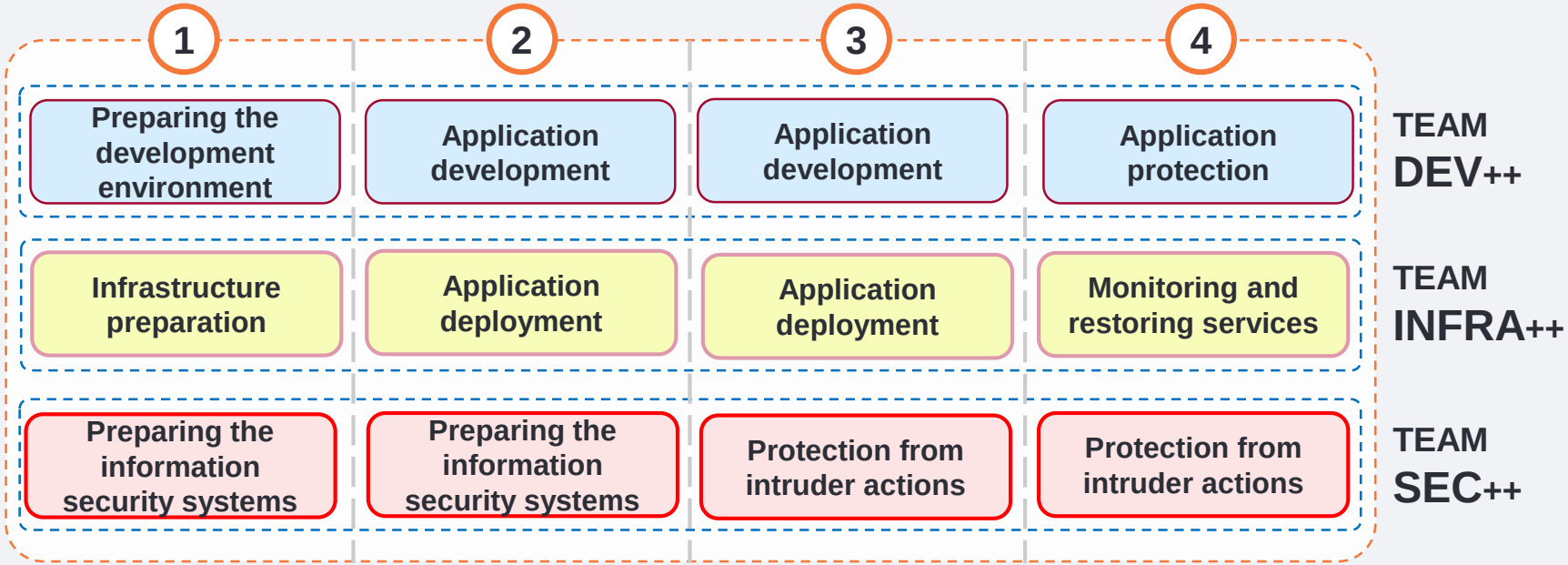
- To train practical cyber exercises against malicious attacks
- To collaboration between departments
- To make recommendations for improving cybersecurity

Results:

Employees gained practical experience in reaction on cybersecurity incidents:

- IT specialists managed to ensure uninterrupted network operation during the attack.
- Cybersecurity specialists managed to stop the intruders in their steps inside customers infrastructure.
- The development team successfully completed the release of software to close the vulnerabilities.

General view what teams are doing



Main responsibilities of participants		
TEAM DEV++	**TEAM INFRA++**	**TEAM SEC++**
✓ **They design and develop** a software product that is critical to the company's business, which must be hosted on the **test site's IT infrastructure** and published online.	✓ **Prepare the IT infrastructure** for the deployment of the developed business-critical software product; ✓ Provide **technical support** to developers **during its publication;** ✓ **Ensure the operation** and development of the basic IT infrastructure.	✓ **Define special requirements** for the software product and IT infrastructure; ✓ **Ensure control** over the implementation of these requirements; ✓ **Research and protect** the deployed IT infrastructure and developed software product; ✓ **Provide access** to the infrastructure of adjacent teams.

Main story SOFTLINE

Digital Transformation. Successful. Effective.

What do we bring to Indonesia cybersecurity market

Based on practice

Critical infrastructure Best practice

Based on Russian vendors

Phishman

Awareness

Own courses

Gamification

Trainings Cyber-polygon

Red, blue, purple team

Web, internal & external

Red teaming & Pentest

Social, wi-fi, mobile, code

Use-cases Automation

Security operation center

Building from scratch

Own service CyberDef

Digital Risk Protection

Looking for local partners

Cybersecurity strategy based on Russian vendors

+79030160870
dm.vasilev@softline.com

Dmitriy Vasilev

Head of cybersecurity business unit