A few stories from Softline

Short sketches about cybersecurity

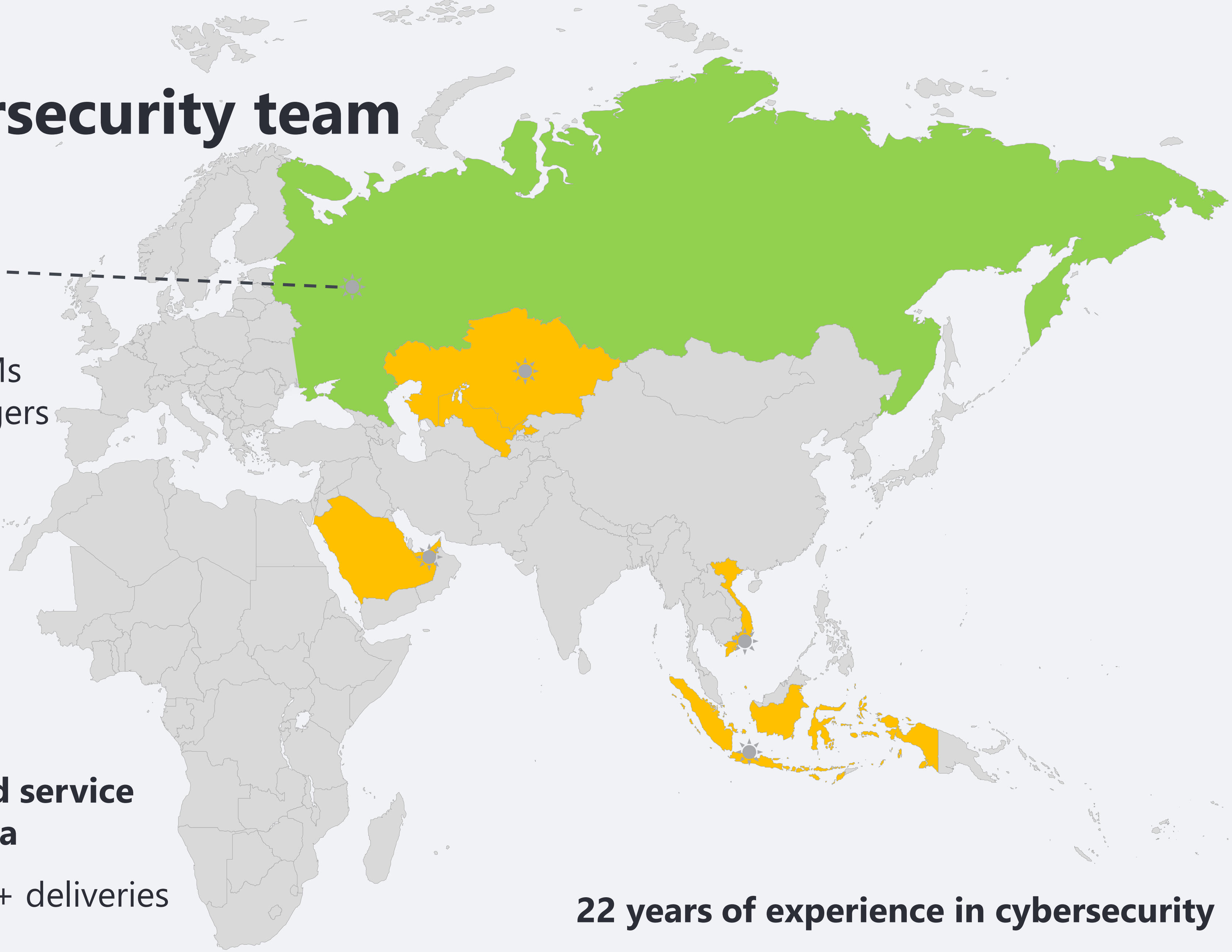
Dmitriy Vasilev

Head of cybersecurity business unit

Vladimir Tashkeev

Head of cybersecurity consulting
CISA CISSP ISO27LA

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
Security Operation Center

Cybersecurity investigation: IOT under attack

Hackers

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

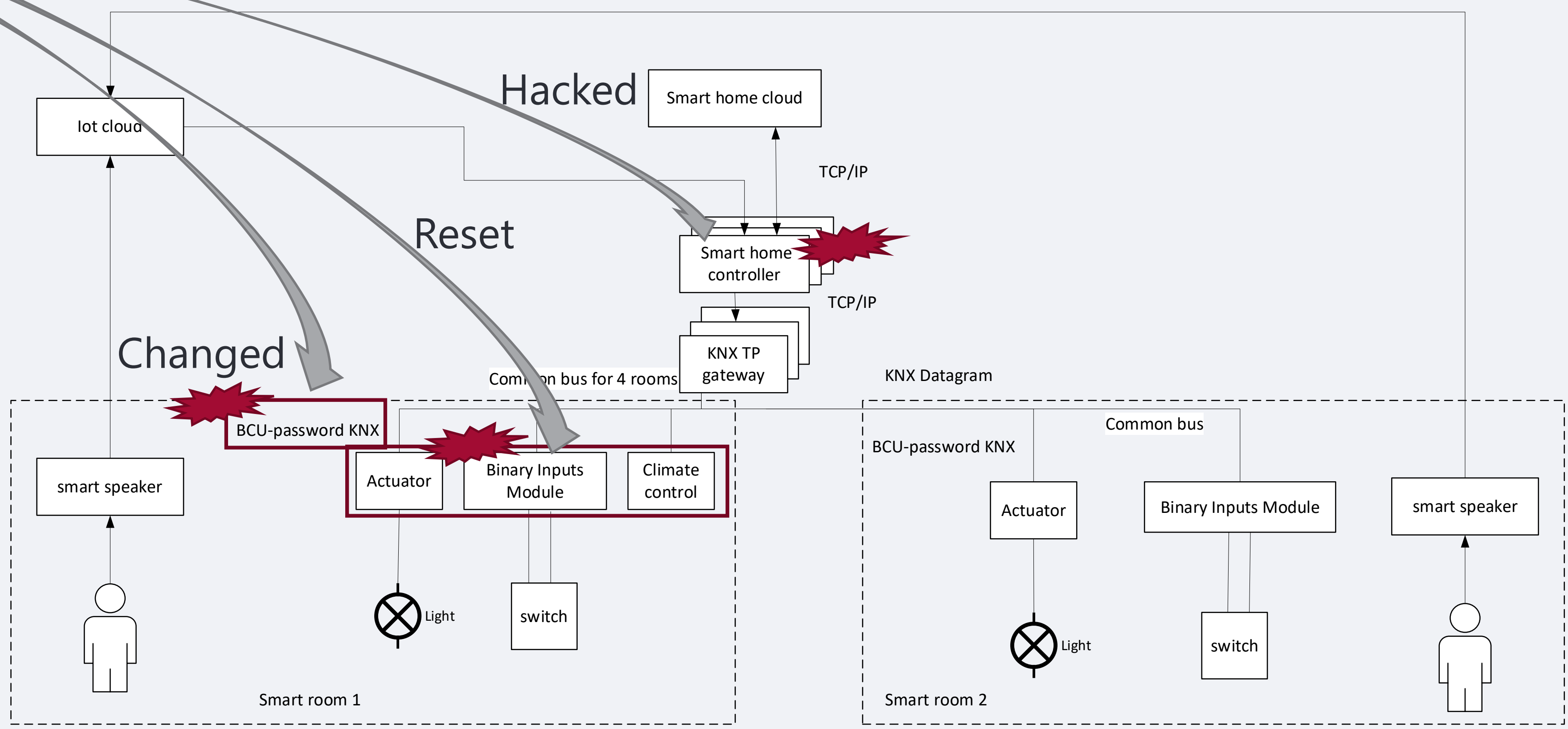
Business impact

The lights /AC /curtains stopped working in all the rooms

Problem

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

One very smart hotel with ★ ★ ★ ★ ★



Solution

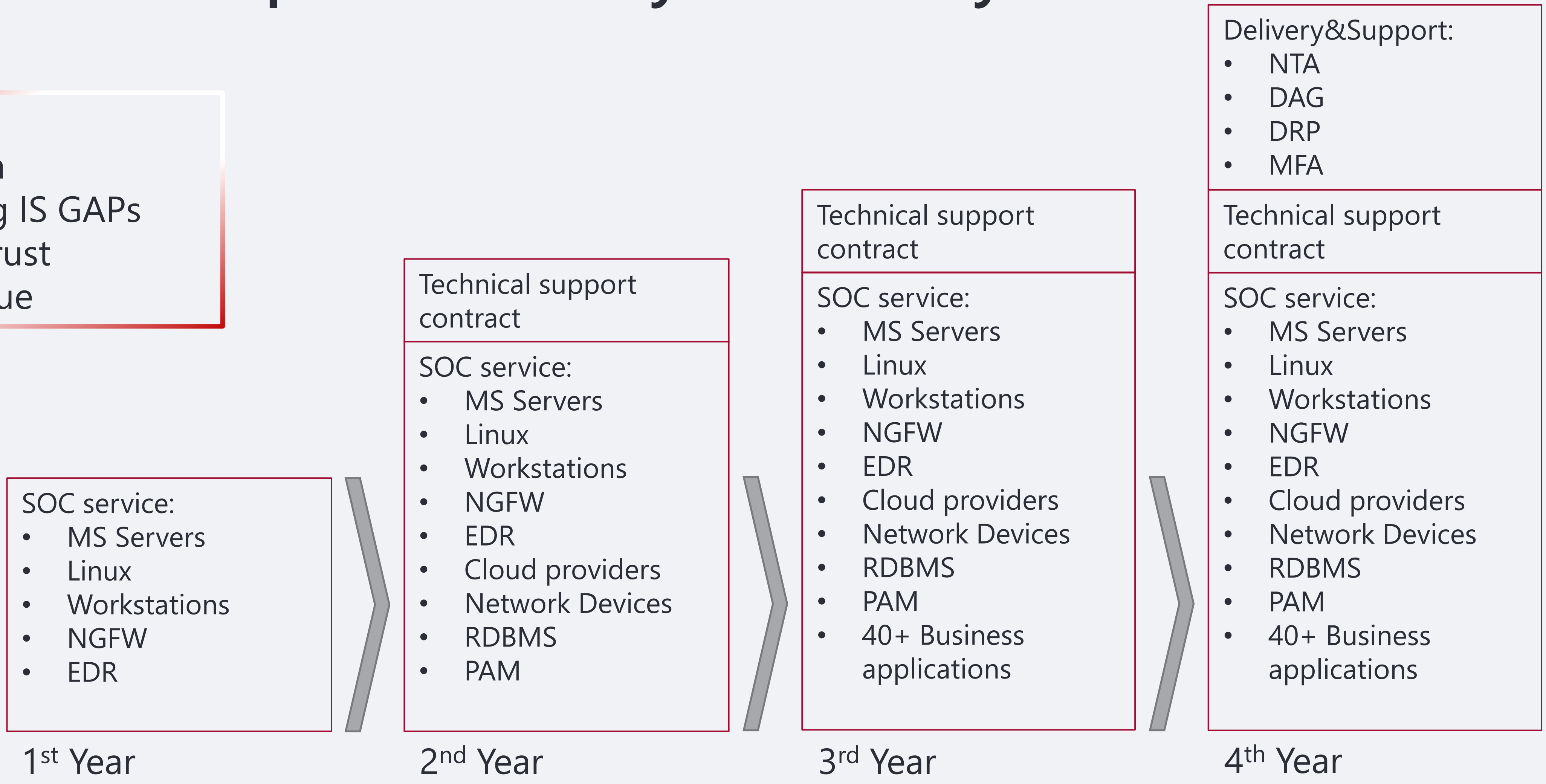
- Urgent negotiation with device vendor = non-public soft
- Hard reset all devices = 10 days non-stop working
- Communications with guests

SOC as a first step in mature cybersecurity MSSP model

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

Moment

X



SOC service:
- MS Servers
- Linux
- Workstations
- NGFW
- EDR

1st Year

Technical support contract

SOC service:
- MS Servers
- Linux
- Workstations
- NGFW
- EDR
- Cloud providers
- Network Devices
- RDBMS
- PAM

2nd Year

Technical support contract

SOC service:
- MS Servers
- Linux
- Workstations
- NGFW
- EDR
- Cloud providers
- Network Devices
- RDBMS
- PAM
- 40+ Business applications

3rd Year

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

4th Year

What if we deliver proper SOC coverage of what’s worth ahead of _default_ schedule?

(based on another case)

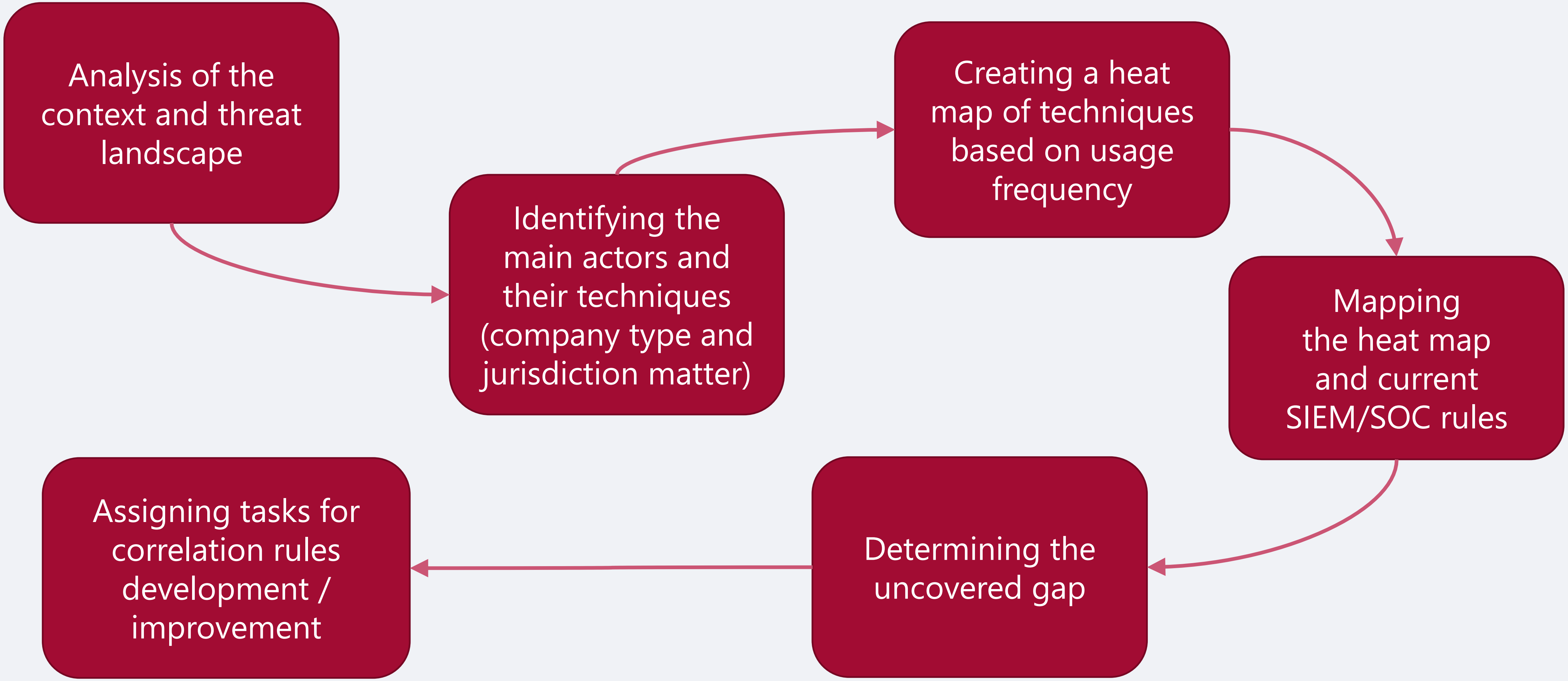
The problem

- Monitoring and response tools are not fully aligned
- Reactive approach for default correlation rules tuning and improvement
- Lack of a unified approach and proper resources for incidents analysis and response
- Insufficient SOC team skills management

What was done

- The roadmap for SOC transformation to a «Defined SOC» level has been prepared
- Proposals for SOC staff development, including calculation of L1/L2 required FTEs, a competency map and L1/L2 interaction process
- **MITRE matrix coverage analysis has been performed to address the gap**

6 steps of practical SOC coverage improvement



Analysis of the context and threat landscape

Identifying the main actors and their techniques (company type and jurisdiction matter)

Creating a heat map of techniques based on usage frequency

Mapping the heat map and current SIEM/SOC rules

Determining the uncovered gap

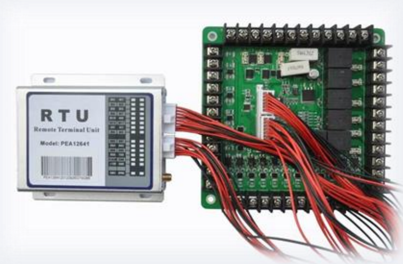
Assigning tasks for correlation rules development / improvement

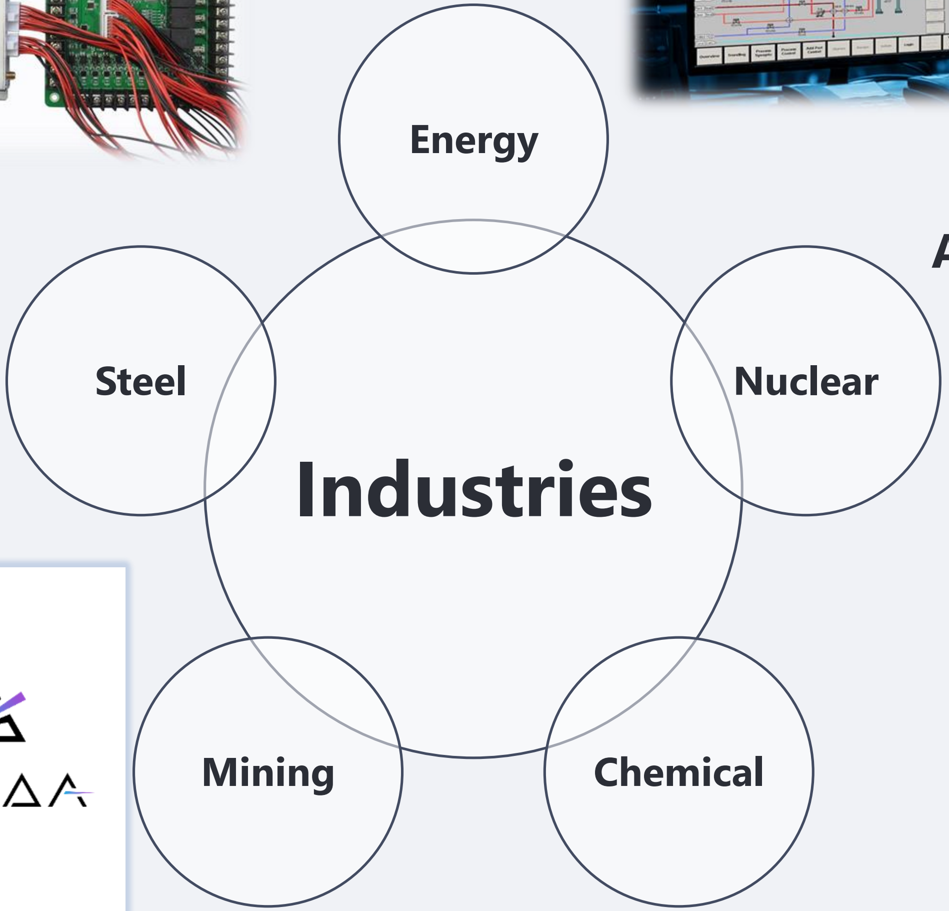
Story #2
Critical infrastructure protection

Critical Infrastructure – 12 years of 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

КОД безопасности

EFROS DEFENCE OPERATIONS

SOLAR

ГАРДА

КИБЕР ПРОТЕКТ

INFOWATCH

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

positive technologies

UserGate

INFOWATCH

АЙТИБАСТИОН

КОД безопасности

Story #3
When vendor ecosystem meets corporate requirements

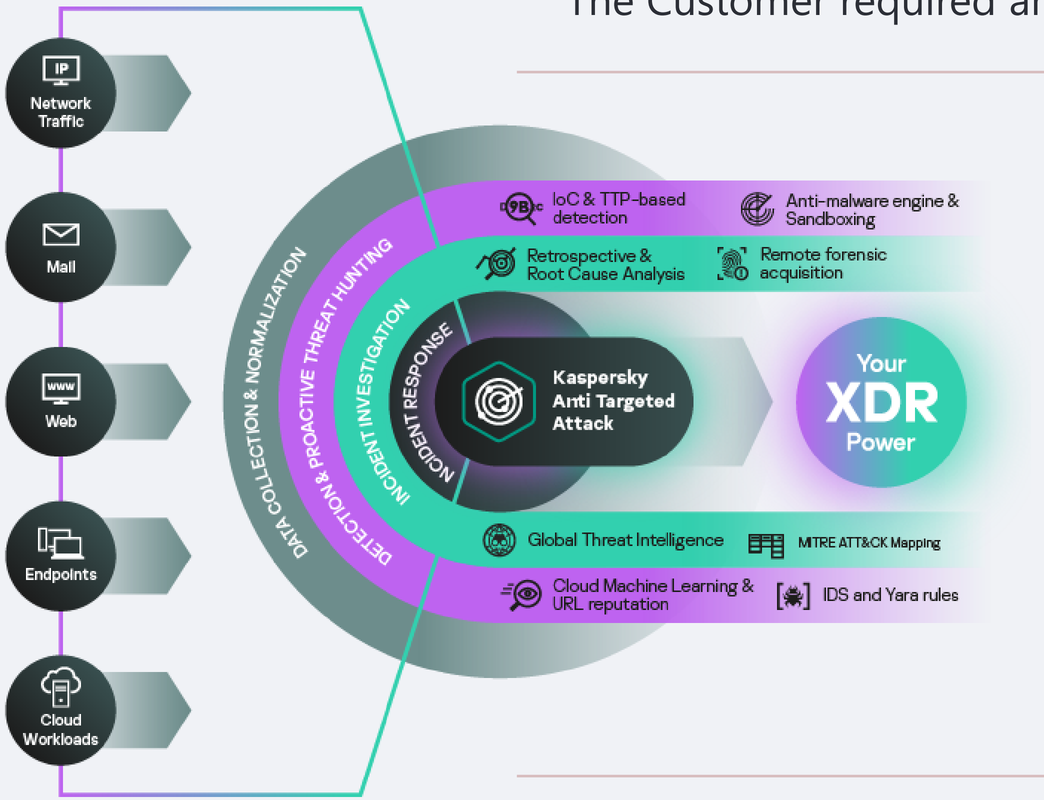
Not a part of global cybersecurity anymore

Project context

Eastern Europe Branch of Global FMCG company

The goal was to migrate from HQ global cybersecurity services to self-hosted solutions.

The Customer required an ecosystem of cybersecurity tools from a single software vendor.


Network Traffic
Mail
Web
Endpoints
Cloud Workloads
DATA COLLECTION & NORMALIZATION
DETECTION & PROACTIVE THREAT HUNTING
INCIDENT INVESTIGATION
INCIDENT RESPONSE
IoC & TTP-based detection
Anti-malware engine & Sandboxing
Retrospective & Root Cause Analysis
Remote forensic acquisition
Kaspersky Anti Targeted Attack
Your XDR Power
Global Threat Intelligence
MITRE ATT&CK Mapping
Cloud Machine Learning & URL reputation
IDS and Yara rules

We proposed implementing following Kaspersky Lab products:

- Kaspersky Anti Targeted Attack (KATA)
- Kaspersky Endpoint Detection and Response (KEDR)
- Kaspersky Secure Mail Gateway
- Kaspersky Security for virtual environment
- Kaspersky Endpoint Security
- Kaspersky Automated Security Awareness Platform (ASAP)

Challenges? Plenty

· A high-availability and geographically distributed architecture

· Hyper-V hardware virtualization which is not officially listed as a recommended platform.

· Complicated load-balancing scenario using HAProxy which is not listed as a recommended option.

· Requirement to transfer the maximum possible settings and security requirements during migration.

· A dedicated test lab was built to recreate the Customer’s infrastructure.

· The KATAP system was deployed in a HA configuration / Active-Passive mode. In the event of a failure, network data sources and managed devices were switched over to the standby configuration via preconfigured connection profiles in KSC.

· Integration of KATAP data sources was completed, including: EDR agents, email traffic from KSMG, and mirrored raw network traffic (SPAN).

· A custom backup mechanism for KATAP system servers was individually designed and tested for the Customer, ensuring integrity of collected telemetry.

· A migration was carried out on more than 3,500 managed endpoints.

· A Disaster Recovery Plan (DRP) was prepared

Above all, project was completed with full vendor participation, commitment and support.

Story #4
Recovery from incident is never enough

In previous episodes…

A large software development company with a distributed geography, 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
- New «green zones» have been deployed and essential security tools have been (re)deployed: EPP / EDR, NGFW / VPN, MFA combined with basic network segmentation and hardening + SOC
- Minimal business operations have been restored + 6 months action plan prepared
- Long-term plan development have been started…

One does not simply develop a strategy

- Trust no one, but that’s all we have:
    - Are we alone in our own IT infrastructure?
    - Once compromised – cast away forever?
    - Why are we so sure «green zones» are really «green»?
- We deal with one bottleneck only to face another:
    - We book the budget to deploy security tools and policies
    - Security tools follow from security architecture definition
    - Security architecture is to be prepared and agreed enterprise-wide
    - Decision making process is something money can’t buy…
- To be continued…

Story #5
Bottom-up towards AI Security

AI Security ≠ LLM security

Common fears when implementing AI:

- Processing of sensitive data by AI
- Chatbots vulnerability to prompt injections
- Generation of false information
- «Poisoning» of model data
- «Eavesdropping» on voice assistants and chatbots

Most of the businesses can’t wait for 100% safe LLM, they’ve already started to implement as-is.

So the real goal is to manage what we can manage.

Threats of AI to business:

- Sensitive data leakage through AI
- Generating malicious instructions on behalf of the Company
- Reputational losses
- Disruption of technological processes
- System compromise
- Financial losses

Steps towards building an AI Security Governance

1 Analysis of AI-based systems

- Analysis of key use cases for AI systems and automated business processes.
- Analysis of the logical and physical architecture of AI systems, identification of critical components (data, model, API, etc.).
- Identification and visualization of sensitive data flows.

2 Threat modeling and assessment of associated risks

- Identification of key attack vectors and risk scenarios (taking into account OWASP, NIST, MITRE ATLAS and DASF frameworks) for AI systems.
- Ranking of risk scenarios (based on quantitative assessment methods).
- Formulation of recommendations for managing identified risks.

3 Building an Enterprise AI Security Framework

- Typification of information security requirements for AI systems.
- Defining a strategic plan for the development of security when using AI in the Company.
- Allocation of responsibilities for AI security issues.
- Taking into account the recommendations of ISO/IEC 42001, 27xxx, and NIST AI RMF for building an AI management system.

4 Creating an AI security roadmap

- Prioritization of information security requirements for AI systems based on the results of threat modeling and risk assessment.
- Setting up security metrics and verification checkpoints.

AI Security: Practical case

Information about the project

Line of business	- FMCG
Size	~ 7000
Number of AI systems	~ 60+

Situation before the project

- A variety of AI systems addressing fundamentally different business use-cases: assistants, copilots, forecasting systems, etc.
- Different stages of AI systems lifecycle: from planning to active operation.
- Lack of understanding of specific threats and attack vectors for AI systems.
- Applicable security requirements have not been defined.
- Lack of clear action plan and first steps

Completed tasks

- An analysis of the Company's AI systems was conducted (use cases, architecture and critical components, key data flows, integrations).
- Key attack vectors and risk scenarios were identified (taking into account NIST, OWASP, and MITRE frameworks), risk scenarios were ranked by criticality.
- Security requirements were developed based on risk scenarios (taking into account NIST, OWASP, and MITRE frameworks).
- Security requirements were standardized for all of the Company's AI systems.
- An enterprise AI security framework was built.

Results

- Risks to the Company's AI systems were prioritized based on the Company's context – focusing resources on what is most important for business.
- AI safety is built into various stages of the SDLC of AI systems: from conception to decommissioning.
- A roadmap for the development of cybersecurity for AI systems (for different planning horizons) was developed.

Main story SOFTLINE

What do we bring to UAE cybersecurity market

Based on practice

Critical infrastructure
Best practice

Top 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 proven vendors

Digital Transformation. Successful. Effective.

softline®