SOFTLINE GROUP Cybersecurity Services

Evgeny Kurtukov, Regional Director MENA

Softline Group

Investment and technology holding company with over 30 years of experience and a broad regional presence in Middle East, Central Asia, South-East Asia and Eastern Europe

Cornerstone of Digital Transformation

25+
Companies in the Group

>5000
Manufacturers

>100 000
Customers

Full range of
Services and solutions

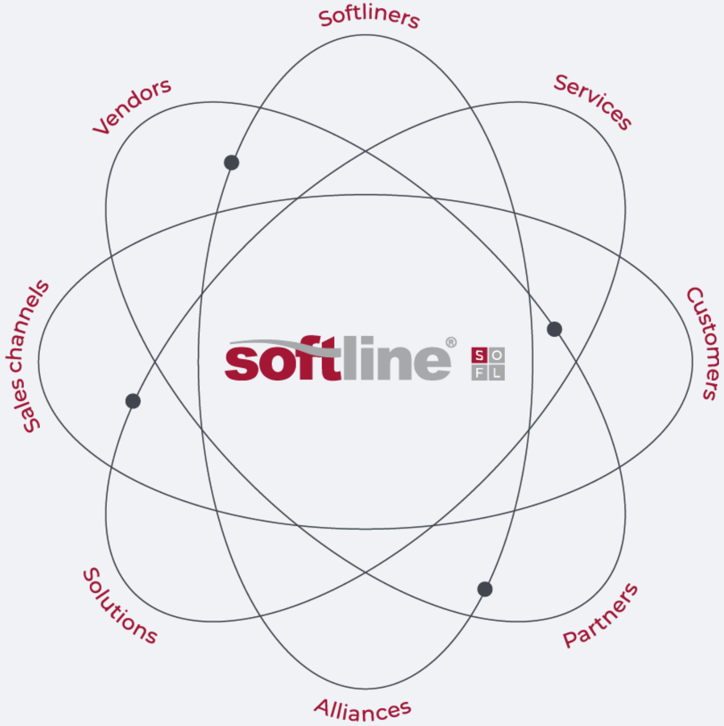
Leading IT Company in Eastern Europe

30+
Representative offices in 6 countries

30+
Years on IT-market

~1.3B USD
Turnover in 2024

>11 100
Employees



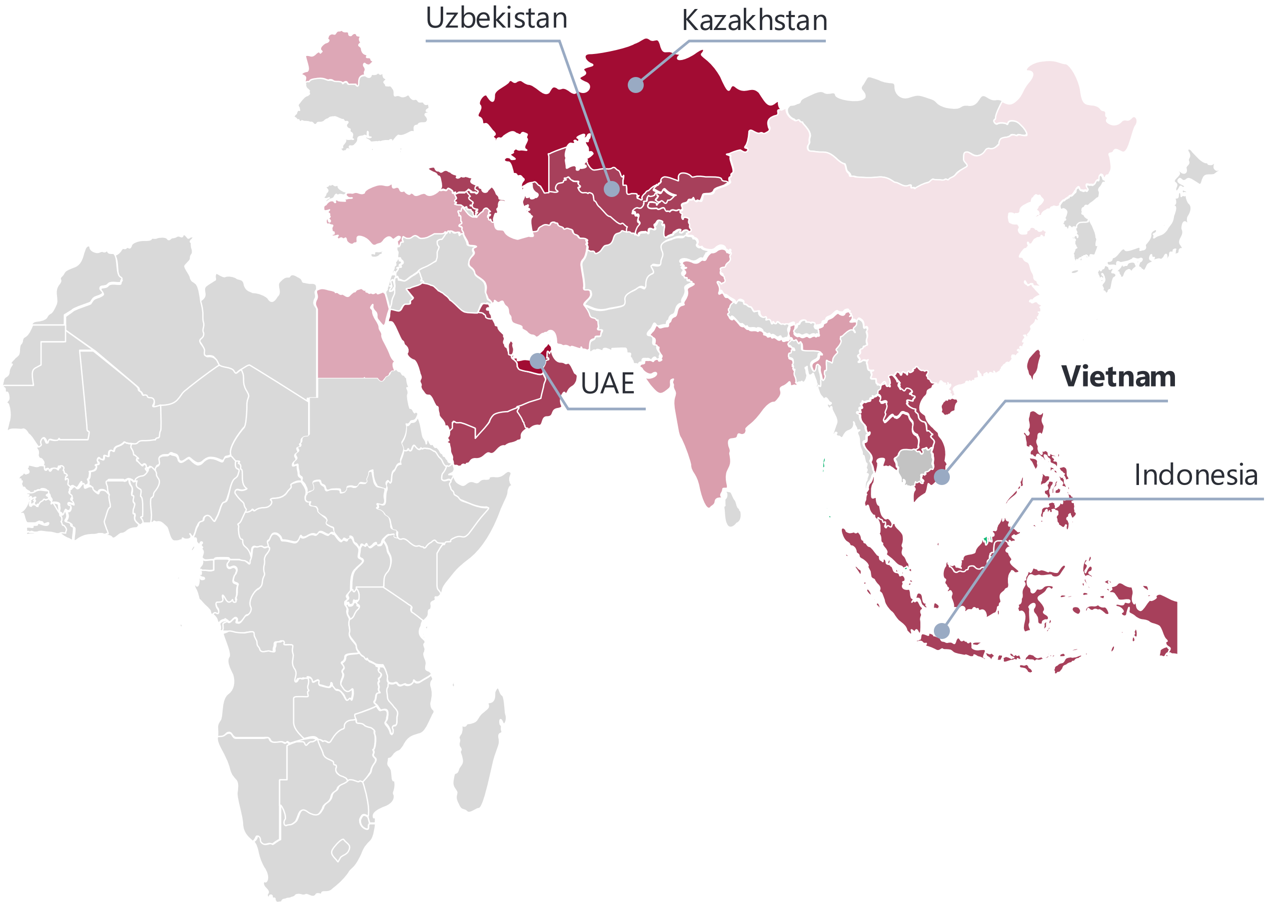
International Strategy

Softline Group is building an IT ecosystem encompassing our own products, industry-specific solutions & services

- 30 years of experience with a wide range of products and solutions from the world's leading software and hardware vendors.

- Successful cooperation with global customers. Understanding the unique business dynamics across various global regions is crucial for our strategic planning and market expansion initiatives.

- Extensive experience, expertise and delivered IT projects in over 64 countries before splitting business with Noventiq



Product and Solution Portfolio

Software & Hardware

Servers, Storages, Laptops and Desktops, POS and Business Solutions (OS, BI, RPA, CV, etc.)

Premier Services

Infrastructure Audit, ITSM and Consulting

System Integration

System Integration and Distribution, including services (implementation, integration and 24/7 technical support)

Industry solutions

QHSE Digitalization solutions based on AI, ML, IoT, Big Data, VR/AR

Custom Development

Own software development team focused on the industrial systems

Cybersecurity

Business Thread Detection Services, DevSecOps, VAPT, SOC, TI, CS Strategy and Consulting

Softline Cybersecurity Center of Excellence

400+
employees in total in the CS Department

300+
Experts (out of total empl.)

1000+
cybersecurity projects annually

Infrastructure Security

- Secure workspace
- Network security (NGFW, IPS, ATP)
- Cloud security (CASB)
- Secure communication channels (VPN)
- Change audit
- Secure content collaboration
- Database protection (DAM)
- Secure mobility (MDM, EMM)
- Integrity monitoring
- Email and web traffic security

CS Management Systems

- Incident management (SIEM, IRP)
- Security Operation Center (SOC)
- International standards and frameworks (ISO 27001, NIST, CIS, etc.)
- Critical Information Infrastructure
- Industrial standards (NIST, IEC)
- Proprietary solutions (CyberDef)

Application Security

- Code analysis
- Application security (WAF)
- Configuration management
- Penetration testing (pentest)

Data Protection

- Employee training/testing (awareness)
- Data protection (DLP)
- Access management (IDM, PAM, 2FA)
- Data encryption

Our Services

- Design & Architecture
- PoC and Demo Zones
- Deployment & Integration
- Technical Support
- Managed Services

Convergence of AI, IoT, CV for QHSE

AI-enabled video analytics are replacing manual safety observations, while unified OT/IT/HSE platforms become the new standard. Modern control rooms are evolving into **decision intelligence hubs** rather than simple monitoring centers.

Edge / Wearable IoT

With Smart Helmets we track personnel location, detect falls, alert to environmental hazards, and provide panic button for immediate assistance call.

Perception (AI Vision)

With video stream we deliver real-time PPE detection, behavior monitoring, zone violation alerts, and detect other deviations through computer vision integration.

Command / Control Center

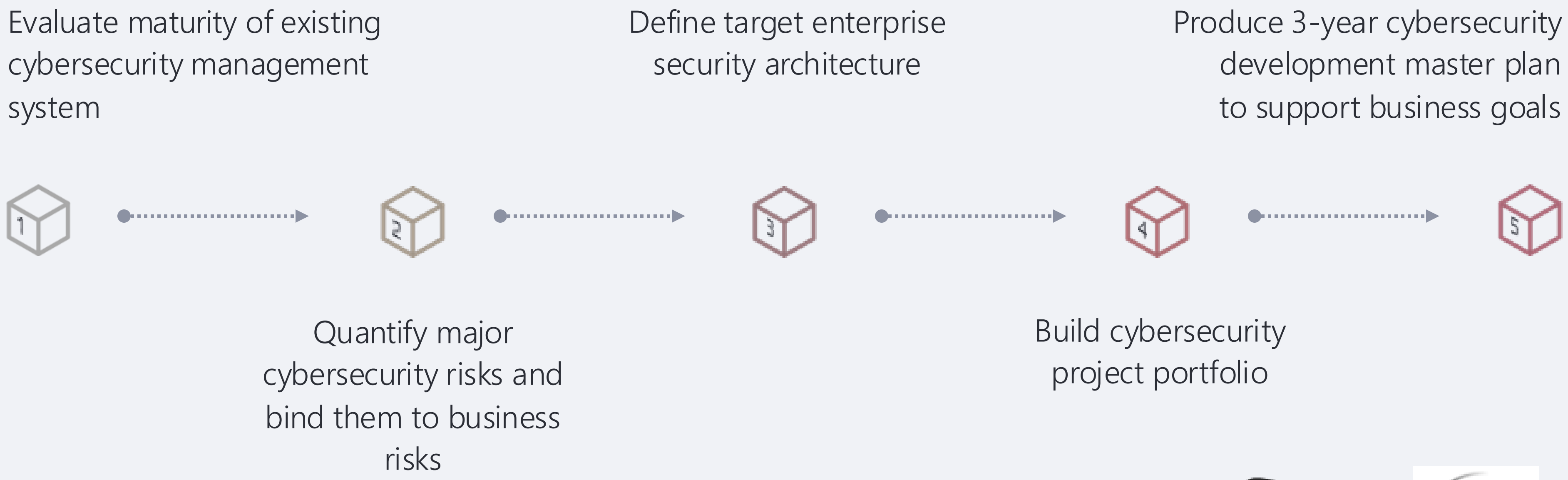
With our Digital platform we offer centralized event management and control, live dashboards, automated incident workflows, and electronic work permits, and more...

We integrate fragmented systems and provide unified control interface with multi-source correlation between existing systems, wearables, and sensors. The architecture scales efficiently for both greenfield and brownfield deployments.

Cybersecurity Services from Softline

Our focus on strategy, architecture, risks and cyber resilience

And it all starts with a master plan



Evaluate maturity of existing cybersecurity management system

Quantify major cybersecurity risks and bind them to business risks

Define target enterprise security architecture

Build cybersecurity project portfolio

Produce 3-year cybersecurity development master plan to support business goals

Everything is considered: business & IT strategy / project portfolio, cybersecurity risk profile, external threat landscape evolution, upcoming regulatory requirements, best-in-class solutions and practices.

Standards and frameworks: ISO27xxx, CIS Controls, NIST CSF, OpenFAIR

Frameworks and Standards

- ISO/IEC 27xxx
- NIST CSF, CIS
- TOGAF, O-ESA
- FAIR, OCTAVE
- SWOT, RICE
- ISO/IEC 22301, 22317

Competences and Certifications

- 27001 LA / LI
- CISA, CISM
- CRISC, CISSP
- PMP

Security maturity assessment and roadmap

Security audit benefits:

- Weaknesses clarification in the security management system
- Assess the current state and define roadmap
- Next steps clarification

Audit aims to determine the cybersecurity maturity level and identify growth areas

Deliverables:

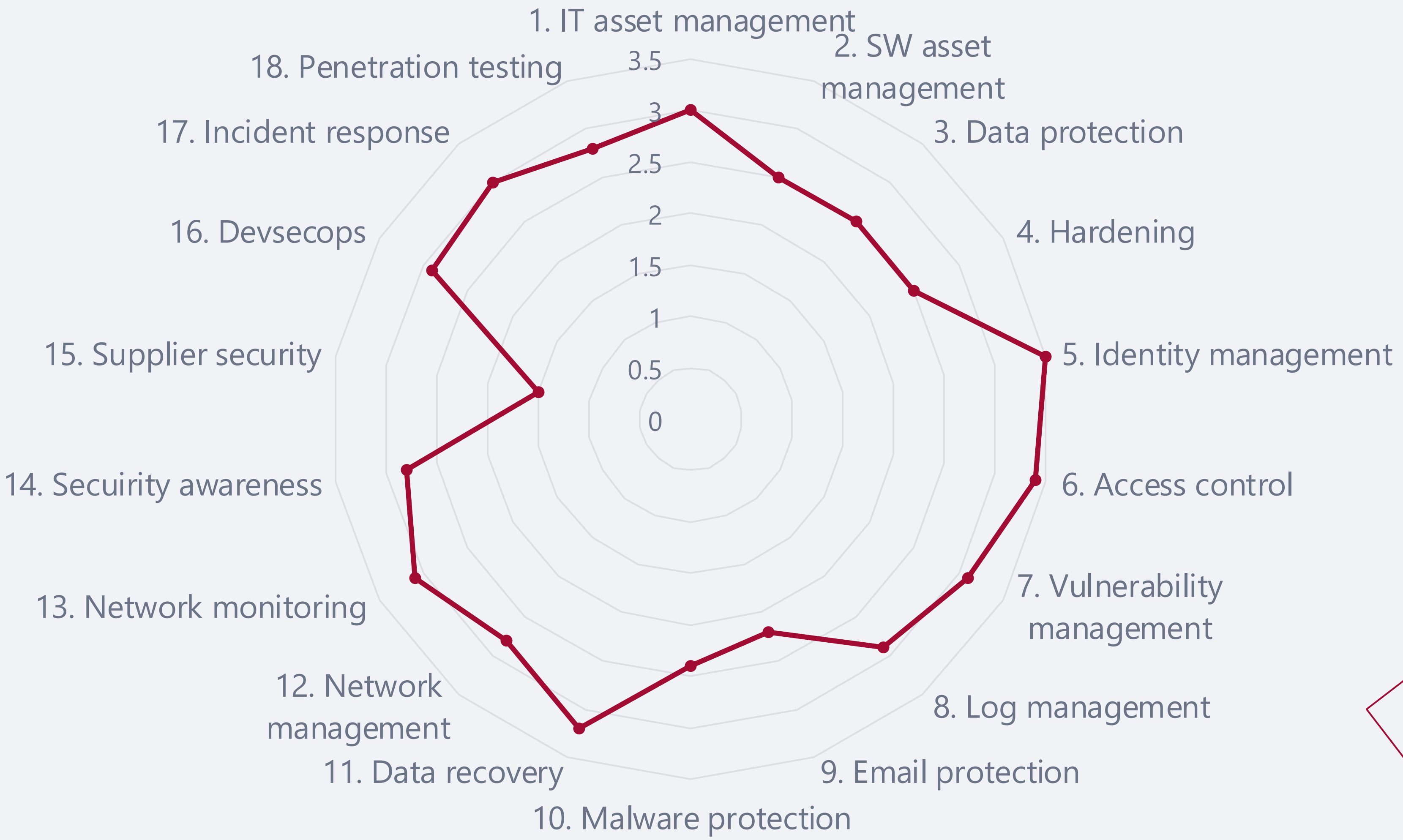
- Current state report
- Roadmap
- Key risks registry and treatment plan
- Brief report with key findings for management

Maturity assessment entails in practical terms:

1. Understanding the Current Posture (technologies, processes)
2. Assessing Capabilities and Weaknesses
3. Roadmap development
4. Providing recommendations and targets

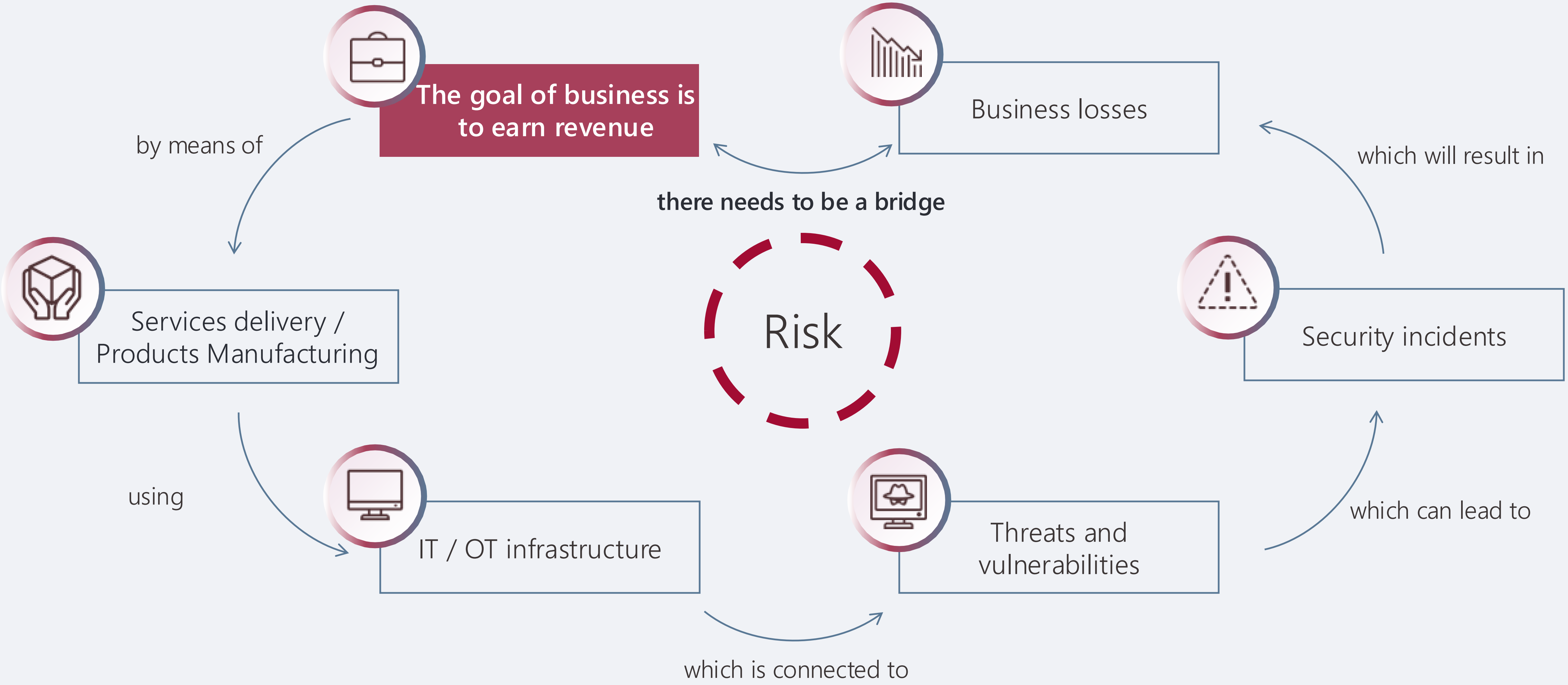
Example of information security assessment based on CIS Controls v8

Maturity level
4
3
2
1



SAMPLE

The goal is to protect business – compliance is not enough



The goal of business is to earn revenue

by means of

Services delivery / Products Manufacturing

using

IT / OT infrastructure

which is connected to

Threats and vulnerabilities

which can lead to

Security incidents

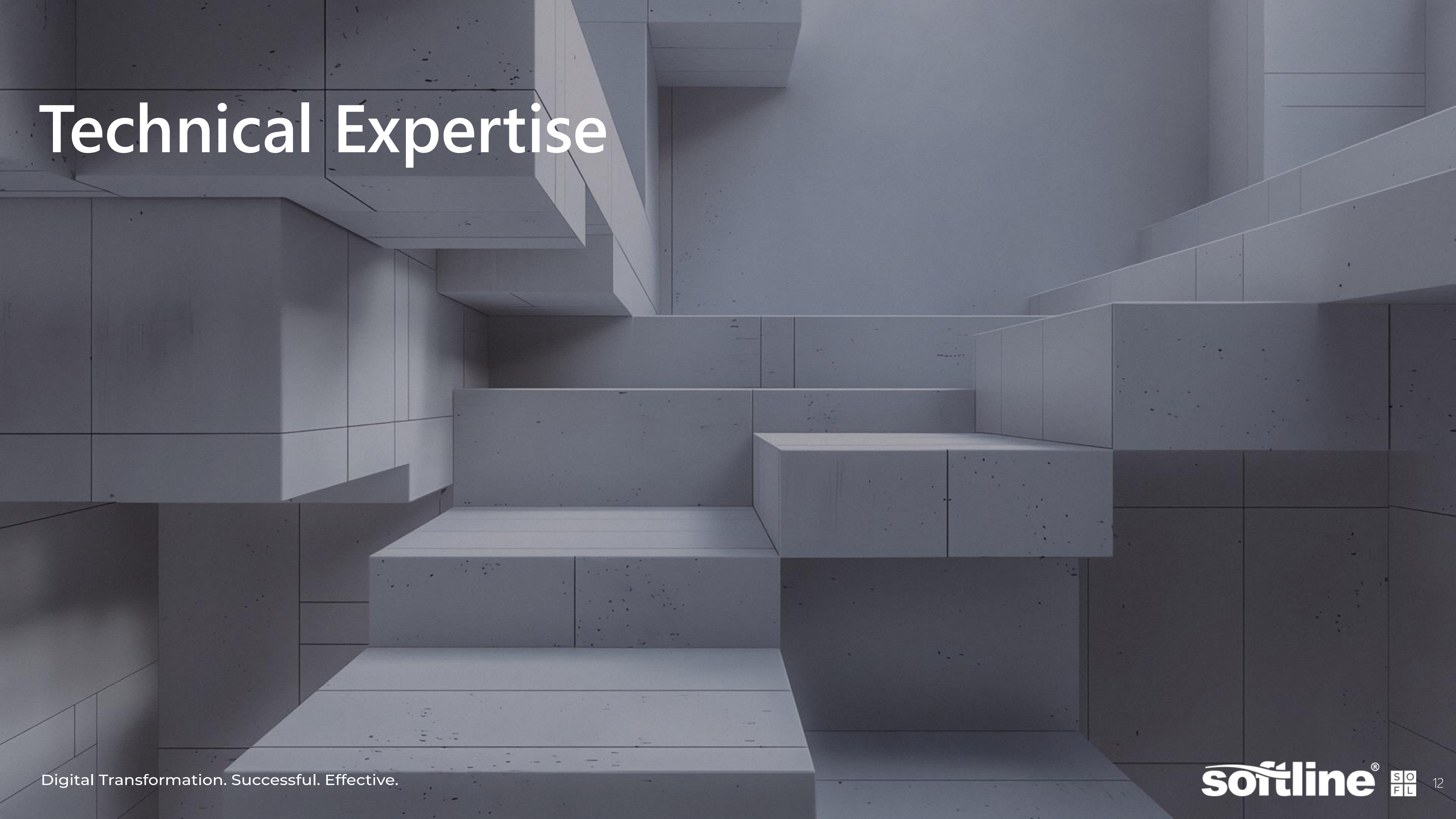
which will result in

Business losses

there needs to be a bridge

Risk

Technical Expertise



Technical assessment and audit services

Possible Problems

- Inefficient use of information security tools
- Downtime of expensive protection software and hardware
- Rapid company growth: more employees, branches and tasks
- Lack of information security specialists for product analysis and implementation

Tasks

- Gathering information about the company's infrastructure, business processes and tasks
- Comparison of operation scenarios with business goals
- Analyze system architecture and configurations
- Test system settings for technical sufficiency
- Survey report provided and approved

Results

- Efficient use of system functions
- Settings aligned with best practices
- Reduced risks from misconfiguration
- Budget savings
- Documented audit recommendations

Design, development and deployment services

Benefits:

Experienced certified engineering team by multiple vendors

Project Manager always in touch

Implementation in accordance with the company's business processes

Deliverables:

Quick and effective configuration of information security tools

Project design and technical documentation

Complex projects (delivery + deployment) by one supplier

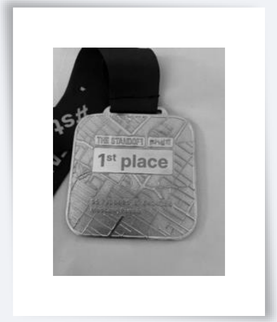
A wide range of services from basic deployment to turnkey implementation

Project entails in practical terms:

1. Site survey and audit
2. Documentation development
3. Architecture development
4. Solution deployment
5. Acceptance test
6. Technical support

Penetration Testing

Team qualifications and achievements



Standoff competitions winners in Codeby team: 2020, 2021, 2022, 2023.

Offensive security certificates

Penetration testing competence (OSCP) and devices audit (OSWP)

Burp Suite Certified Practitioner (BSCP)

Deep knowledge of web vulnerability classes, and the skills required to discover and exploit them

Hacktory Web Security Professional (HWSP)

Certified Red Team Operator (CRTO)

Basic principles, tools, and techniques that are involved within the red teaming tasks

Certified AppSec Practitioner (CAP)

API Security Architect (API Academy)

eLearnSecurity

Practical assessment that simulates real-world penetration testing scenarios

Types of penetration testing

Web application penetration testing

Internal penetration testing

External penetration testing

Social engineering penetration testing

Wireless penetration testing

Mobile application penetration testing

White box penetration testing

Penetration testing reports

Technical report

- Structured description of the obtained data on the target infrastructure
- Description of the vulnerabilities identified
- Description of the attempted penetrations and their results
- Analytical conclusions on the current security level of the target information infrastructure
- List of developed recommendations for increasing the security level

Executive summary report

- Brief report for management, written in non-technical language
- Key findings/recommendations

- The Management Report is developed together with the Technical Report and contains a description of the most critical vulnerabilities and security assessment of test objects

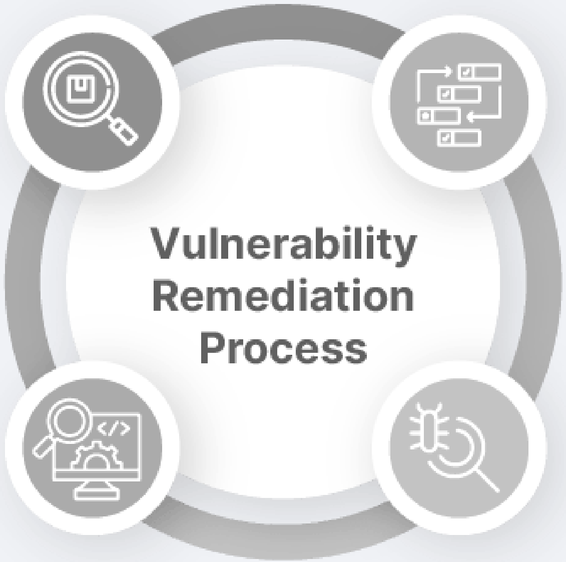
Options

Presentation

Educational webinar

Vulnerability Management Services

Vulnerability management services



01. Detect
Detecting vulnerabilities through scanning and testing

02. Prioritize
Understanding which vulnerabilities pose a real and significant risk

03. Remediate
Patching, blocking, or remediating in real-time

04. Monitor
Real-time alerts and notifications for newly discovered vulnerabilities

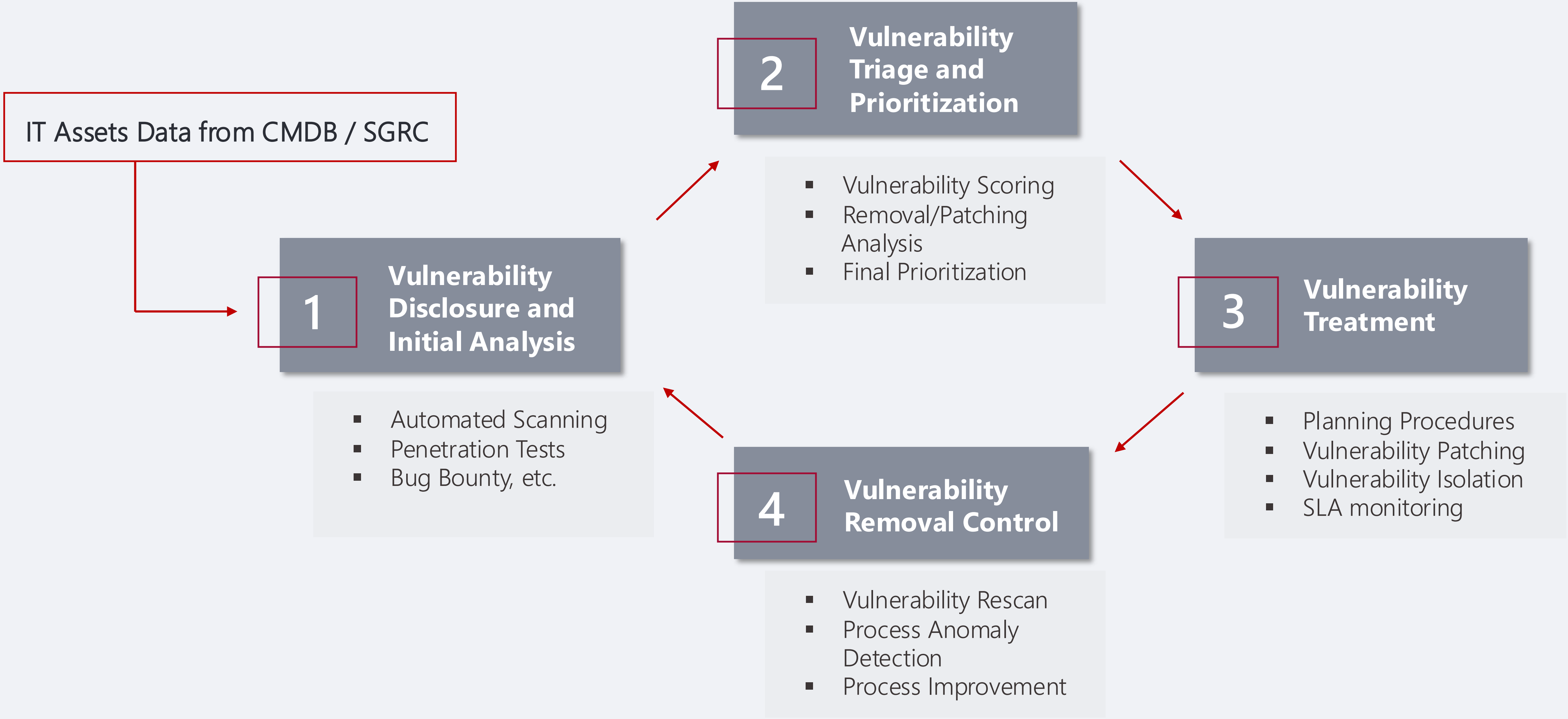
What is it?

- Management process
- Assets discovery and identification
- Vulnerabilities prioritization
- IT and information security interaction (ex. vulnerabilities patching)
- Vulnerabilities elimination monitoring

Where is it?

- ✓ Softline cloud
- ✓ On-premise platform provided and managed by Softline

Vulnerability management process stages



IT Assets Data from CMDB / SGRC

1 Vulnerability Disclosure and Initial Analysis

- Automated Scanning
- Penetration Tests
- Bug Bounty, etc.

2 Vulnerability Triage and Prioritization

- Vulnerability Scoring
- Removal/Patching Analysis
- Final Prioritization

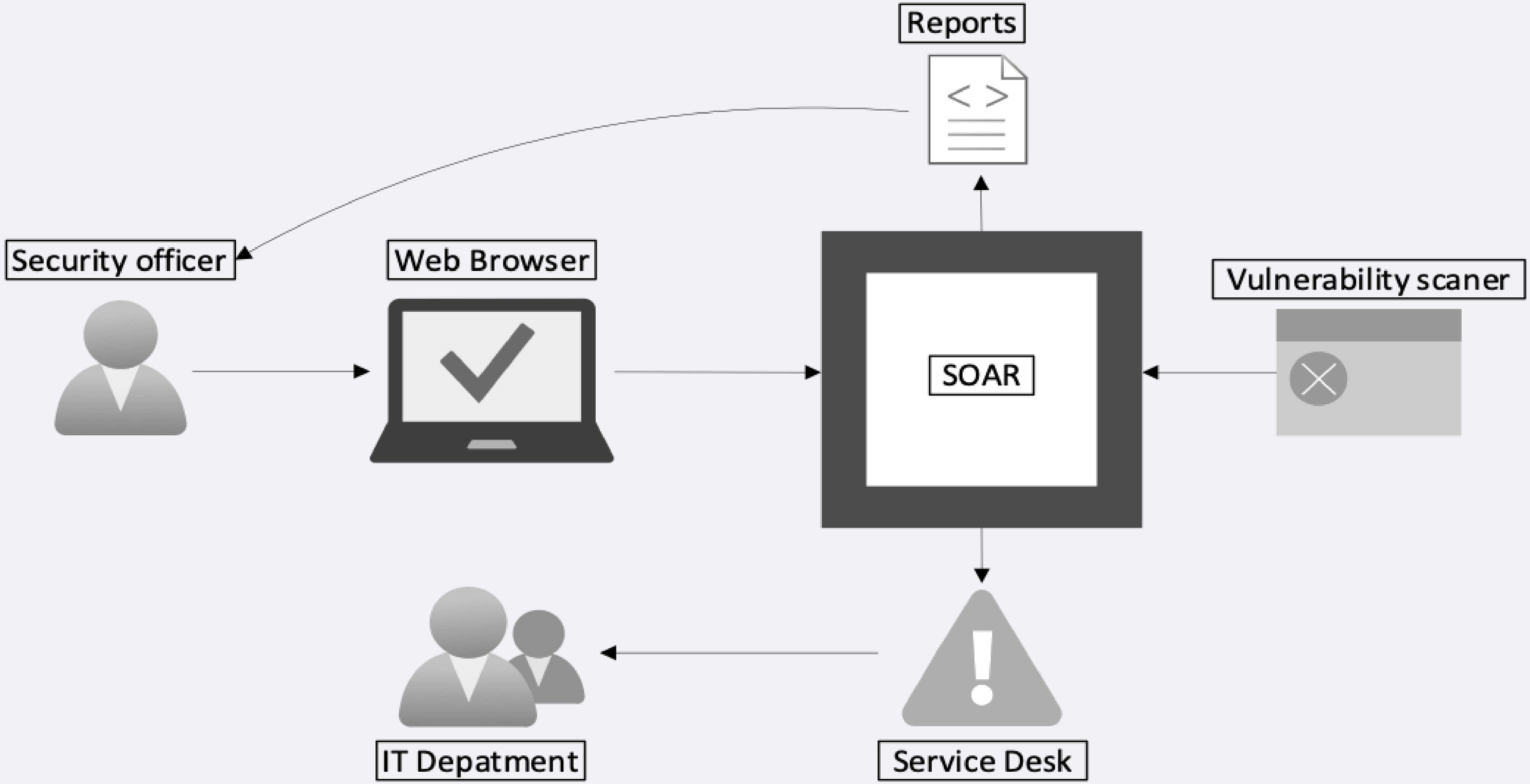
3 Vulnerability Treatment

- Planning Procedures
- Vulnerability Patching
- Vulnerability Isolation
- SLA monitoring

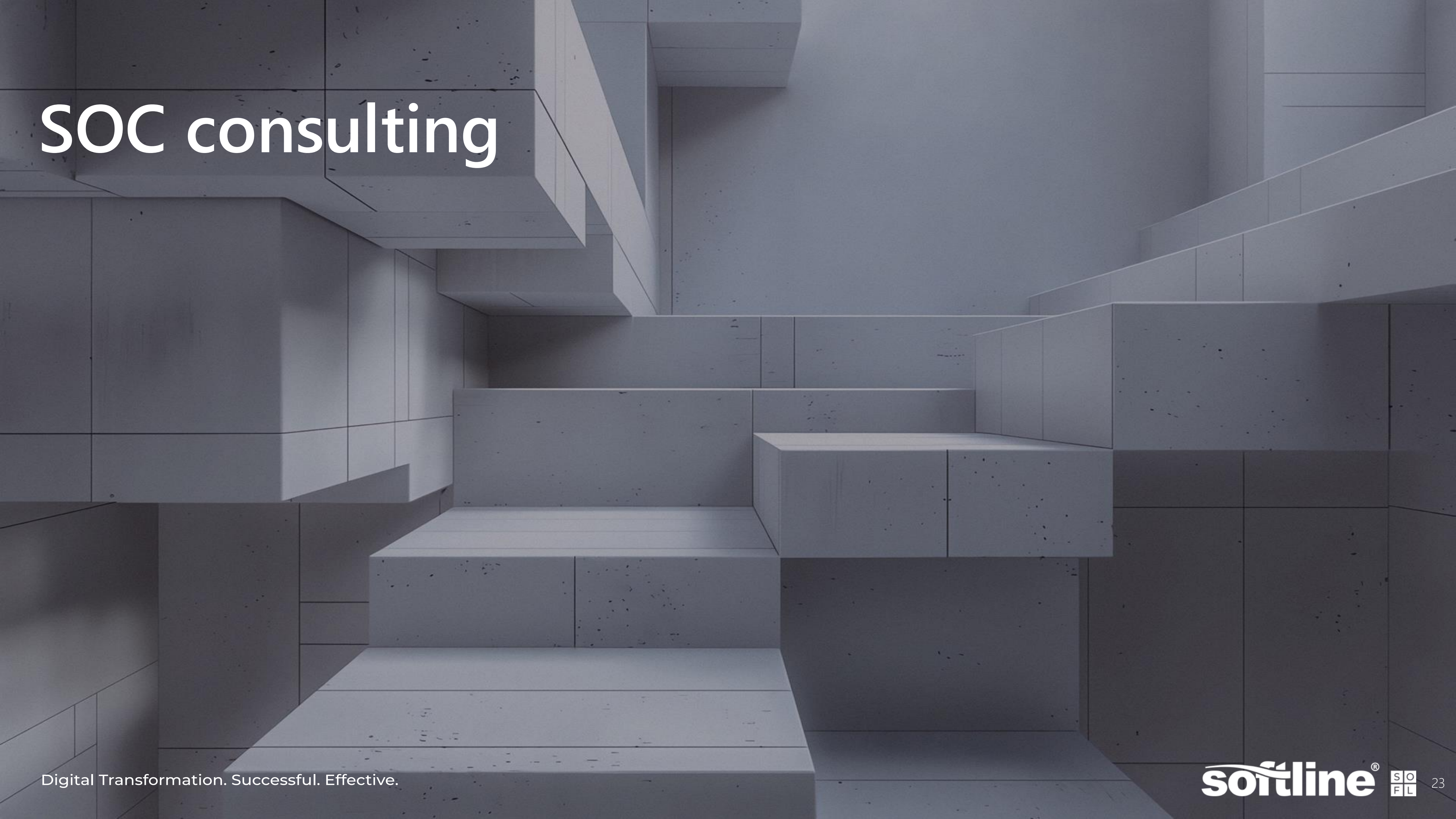
4 Vulnerability Removal Control

- Vulnerability Rescan
- Process Anomaly Detection
- Process Improvement

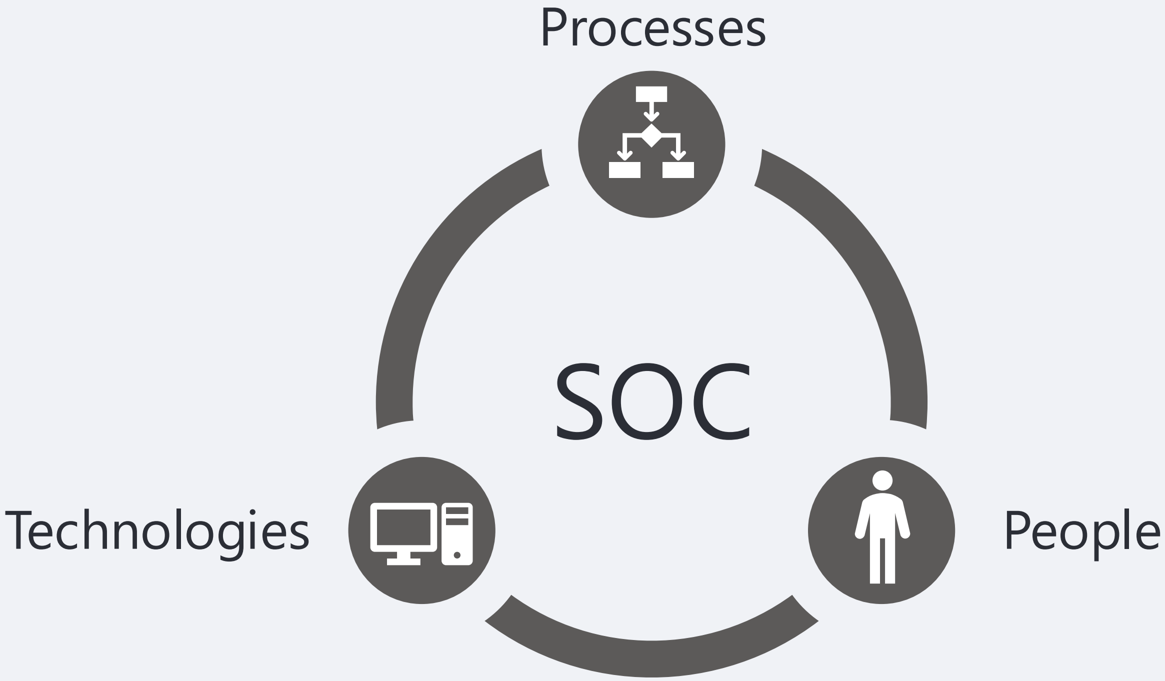
Vulnerability management services



SOC consulting



Security Operation Center planning goals



The main goals of the SOC Planning stage are:

- To define the target state of the SOC
- To outline the principles and methods of achieving the target state of the SOC
- To develop the plan of achieving the target state of the SOC

SOC Project Full Timeline (from Scratch)

Planning

3 months

- Initial Assessment
- SOC Strategy Planning
- Specification Development
- Service Model Planning
- Platform Testing and Selection
- HLD Development
- Target Organizational Structure Development
- Procurement Documentation Development

Implementation

3-6 months

- SOC Staff Hiring and Adaptation
- SOC Base Infrastructure Setup
- SOC Core Deployment
  - SIEM
  - SOAR/IRP
  - TI
- SOC Initial Tuning: integrations, correlation rules, response playbooks, workflows, reports and dashboards
- Regulations, Instructions and Procedures Development
- SOC Trial Operation

SOC Start-Up

3-6 months

- Staff Training
- Rules Fine Tuning
- Playbooks Implementation
- Procedures Improvement
- Duty Shift Planning and Implementation
- Response Exercises and Training
- SOC Commercial Operation

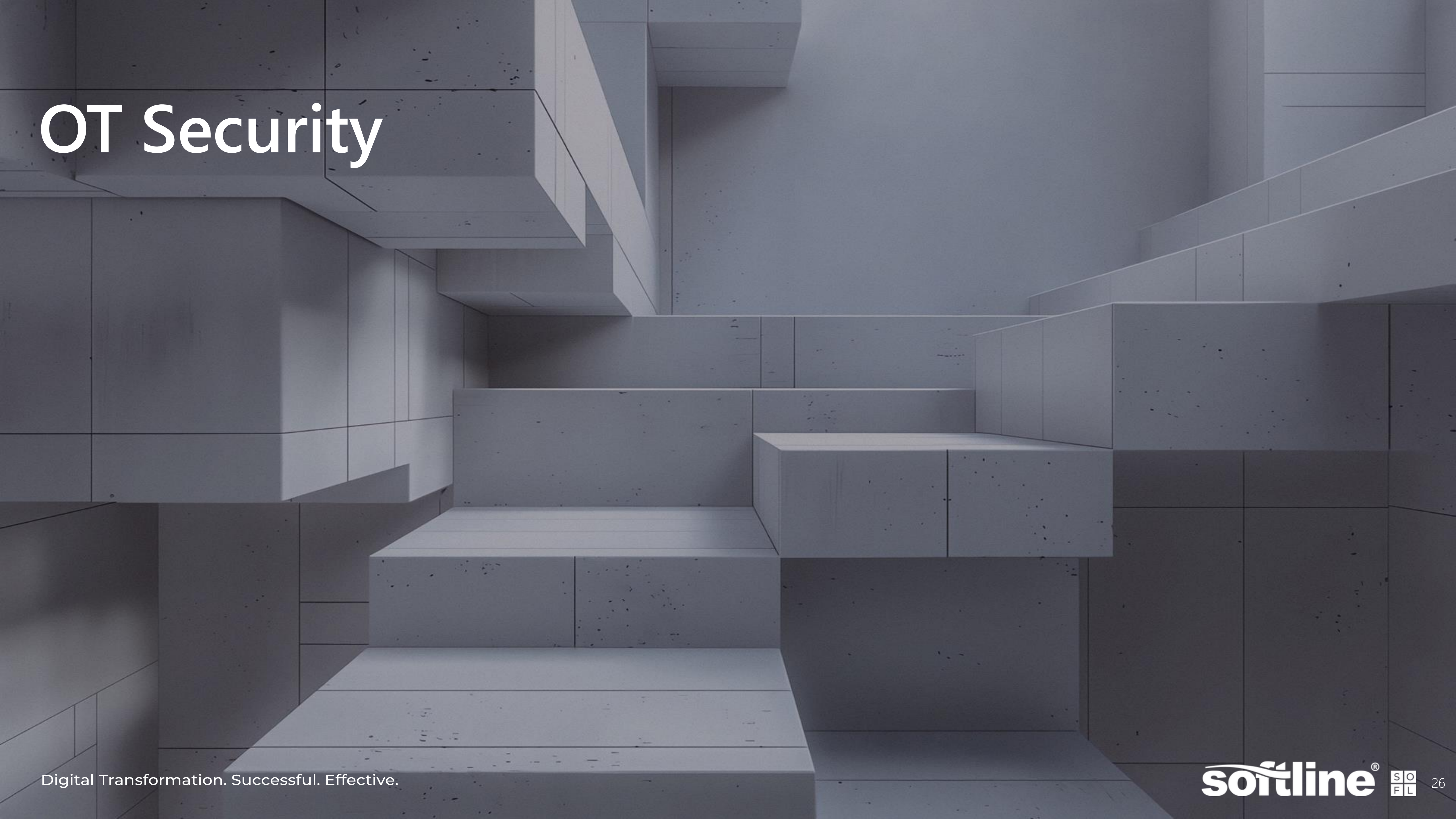
Ops

1-2 years

Improvement

- Processes Optimization
- SOC Maturity Assessment
- KPI and Metrics Revision
- Event Sources Extension (APCS)
- New Features Implementation (Physical Security Control, Fusion Center)

OT Security



Our experience

- Oil & Gas
- Energy
- Chemical Industry
- Mechanical Engineering
- Metallurgy
- Nuclear Energy
- Smart Cities
- Transportation
- Food Industry

- Over 10 industries
- Over 500 projects

- Over 300 experts
- More than 10,000 secured OT systems

Critical infrastructure – 10 years of experience

Technological network

- Segmentation
- Internal communication optimization
- Privileged user control

Remote access

- Remote suppliers control
- MFA
- Privileges control
- Suppliers security

Data transfer

- Mid server for data transferring
- Info-diode solutions
- Technological TVs

Vulnerability management

- Patch management
- Version control
- Vulnerability check

Password management

- Password policy
- Employee awareness
- Default passwords change

Unauthorized devices

- Device control
- Employee awareness

Traffic monitoring

- Limited physical access
- Traffic mirroring (SPAN)

Dedicated demo zone

Dedicated Owned Equipment

We use our own demo equipment and infrastructure to conduct demos and tests for our customers

UI Demonstration and Evaluation

We provide demonstrations of UI usage of all Information Security Solutions deployed in the Demo Zone

Demonstration of Fully Deployed Solutions

We thoroughly demonstrate technical principles and features of complex information security solutions in real-time

Deployed Software and Solutions

We have fully deployed installations of Kaspersky KICS for Nodes and KICS for Networks

Project Portfolio

Practical case: Energy company

Goals

To implement information protection system for the distributed industrial control and monitoring system

The security system implementation allowed to detect and prevent direct Internet access from some parts of customer's ICS

Outcomes

- 30 sites and 1 data center survey
- Installation and commissioning works on sites
- Information protection system implemented and secured
- Documentation developed based on customer requirements and standards

Works performed

- Audit: 30 sites
- Categorization of critical infrastructure
- Information security system design
- Information security system implementation
- Acceptance tests

Practical case: Major retailer company

Goals

To achieve comprehensive protection of corporate email system from cyber threats, hacks and phishing based on the Business Email Protection product

Works performed

- Designed and implemented a mail protection complex
- Configured rules for analyzing mail traffic, implemented a fault-tolerant architecture on-site
- Implemented and customized new functionality of the system, developed specifically at the Customer's request with Vendor support

Outcomes

- Design documentation accepted
- Equipment, software supplied
- System for protecting the Customer's mail traffic implemented and technical support supplied

Practical case: Oil pipeline company

Works performed

- Connected over 1500 event sources of 35 different types (including Oracle, IBM, Red Hat, Huawei)
- Written 20 custom normalization rules for 12 types of unsupported event sources
- Created more than 40 custom correlation rules based on the Customer's Incident List
- Developed technical solutions for connecting 2 types of non-standard sources (business systems) via intermediate CSV files

Outcomes

Improved the level of efficiency of protection of the Customer's IT infrastructure from information security (IS) threats by collecting and processing IS events and identifying IS incidents on the basis of MaxPatrol SIEM

Practical case: Organizer of sporting events

Goals

- To obtaining an independent assessment of the current state of information security of the Customer's information infrastructure against possible attacks by intruders of various types
- To evaluate effectiveness of measures taken to increase employees' information security awareness

Works performed

- WiFi penetration testing
- Internal penetration testing
- Social engineering testing
- Recommendation development

Outcomes

- WiFi network found to have serious security flaws:
  - Insecure network topology
  - Weak password policies
  - Username disclosure
- LAN found to have serious security flaws:
  - Default credentials on services by manufacturer, weak and missing passwords
  - Free access to sensitive information
  - Insecure storage of sensitive information
  - Insecure network topology
  - Vulnerable version of Gitlab software with RCE
- **Unacceptable event:** Gained root access to the DBMS via Reverse Shell possibly leading to data theft or destruction
- **Severe threat:** 20% of employees opened the phishing emails, clicked on a phishing link, and entered their credentials

Q&A