Softline Cybersecurity Services and Expertise

Softline Cybersecurity Center of Excellence

400+
employees in total in the IS Department

300+
Experts (out of total empl.)

1000+
cybersecurity projects annually

Infrastructure Protection

- 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

IS 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

Information Security Consulting Services

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

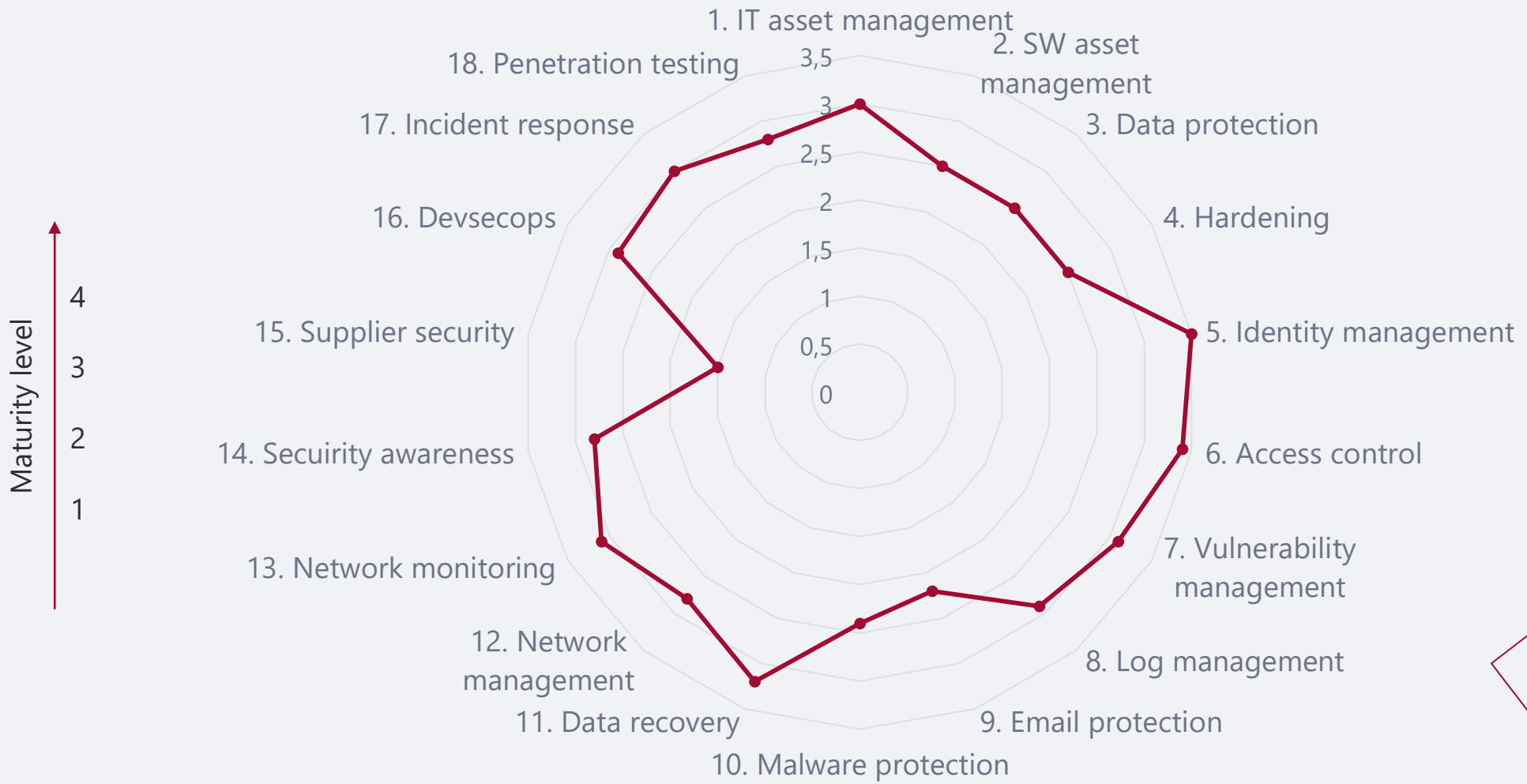
Key risks registry and treatment plan

Brief report with key findings for management

Maturity assessment entails in practical terms:

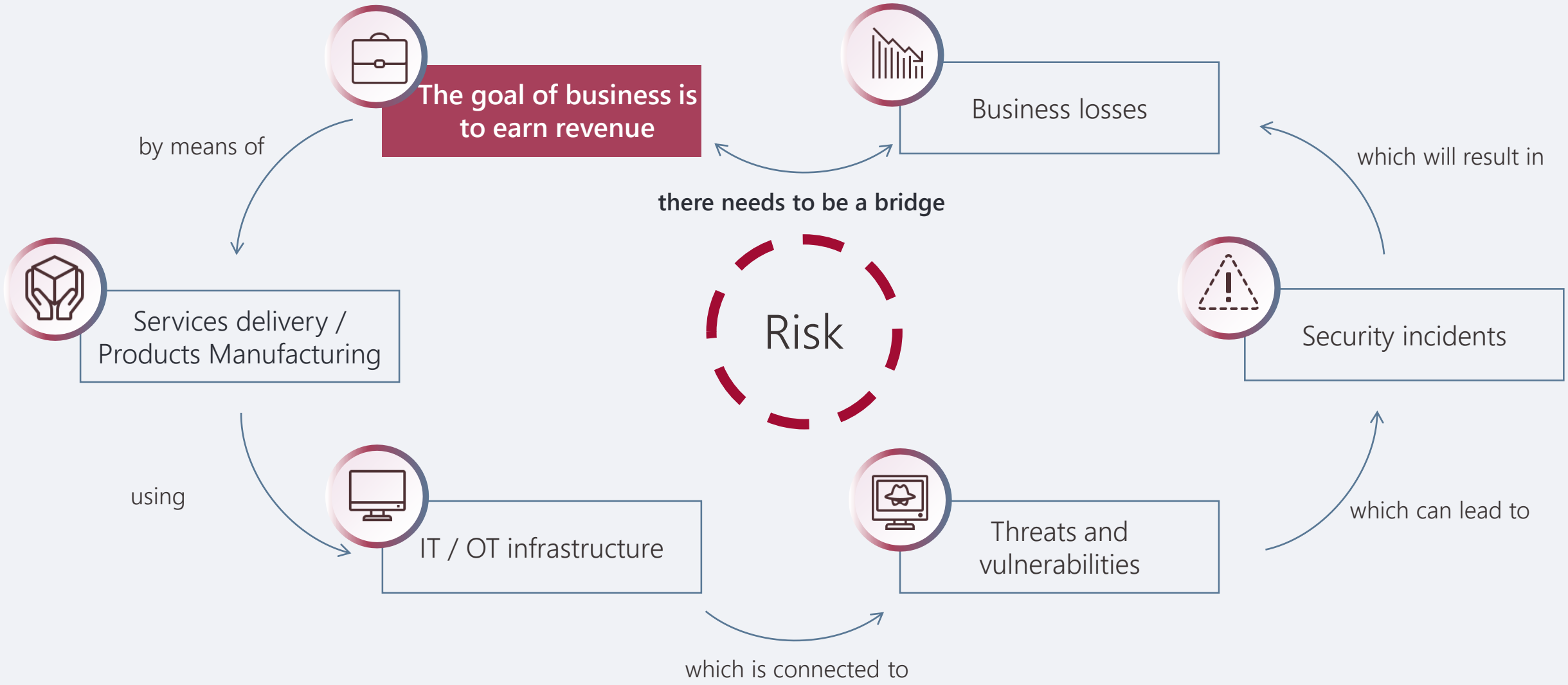
1. Understanding the Current State (technologies, processes)
2. Assessing Capabilities and Weaknesses
3. Roadmap development
4. Providing recommendations and targets

Example of information security assessment based on CIS Controls v8

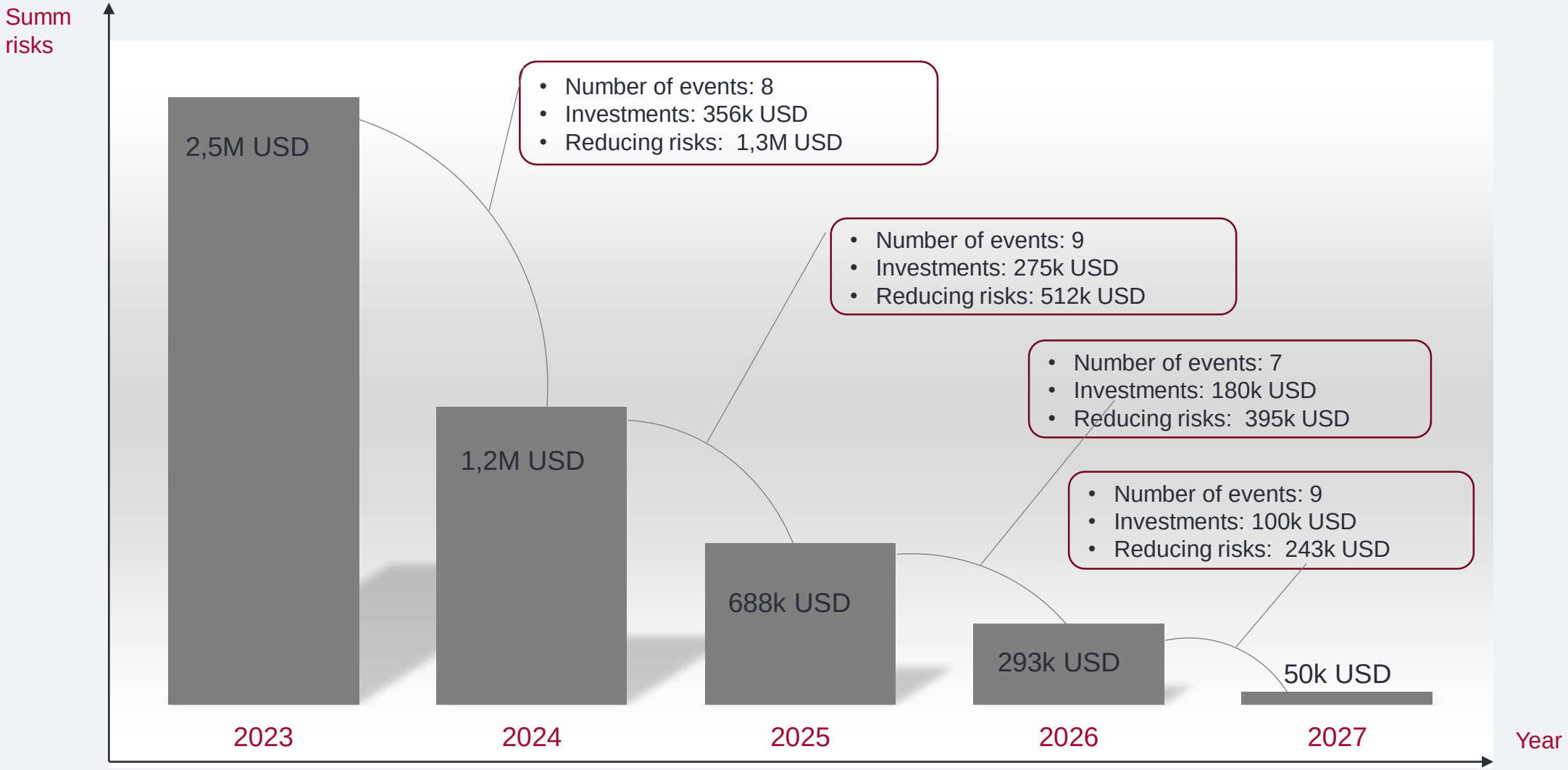


SAMPLE

The goal is to protect business – compliance is not enough



Results (ROI)


Summ risks
2,5M USD
1,2M USD
688k USD
293k USD
50k USD
• Number of events: 8
• Investments: 356k USD
• Reducing risks: 1,3M USD
• Number of events: 9
• Investments: 275k USD
• Reducing risks: 512k USD
• Number of events: 7
• Investments: 180k USD
• Reducing risks: 395k USD
• Number of events: 9
• Investments: 100k USD
• Reducing risks: 243k USD
2023
2024
2025
2026
2027
Year

General approach to IS strategic planning

What is the current state of information security?

Information Security Analysis (AS IS)

Assess current maturity level

What is important for the business?

Risk Identification

Key business risks

What will impact information security in the coming N years?

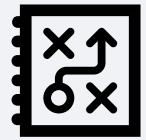
Context Definition

Trends by domain:
- Technology
- Threat landscape
- Compliance

What should information security look like, based on the previous steps?

Target State Definition (TO BE)

Information security strategy

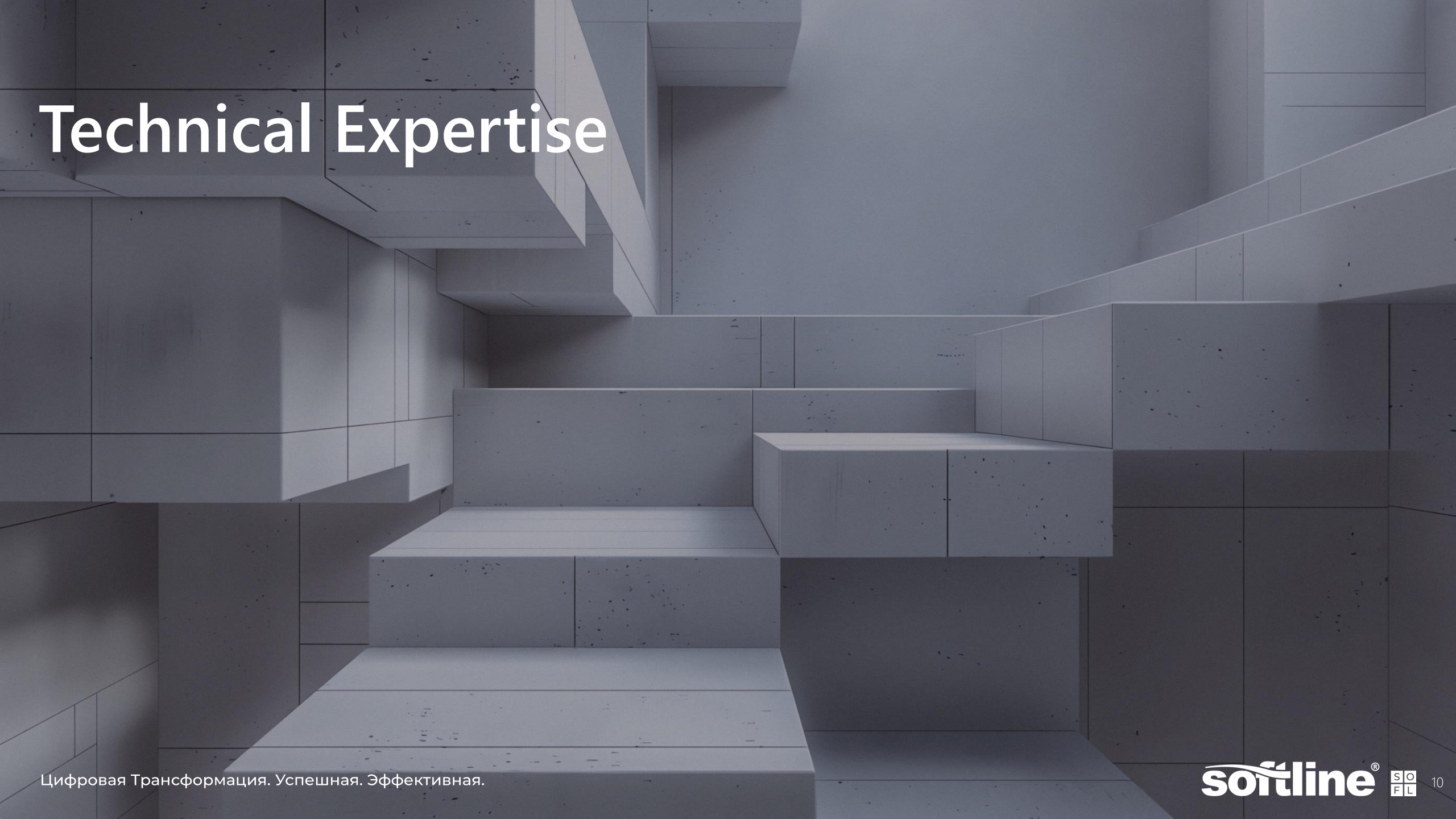


How will we reach the target state?

Transition Planning

Roadmap
Project portfolio

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

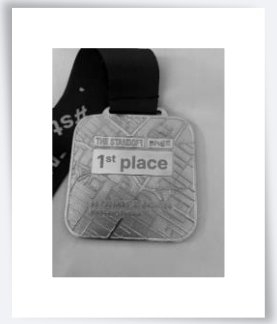
A wide range of services from basic deployment to turnkey implementation

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)

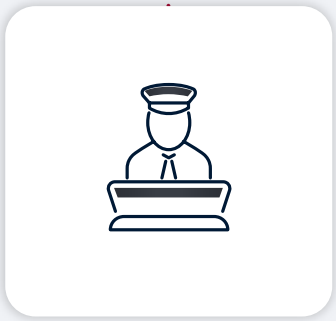
API Security Architect (API Academy)

eLearnSecurity
Practical assessment that simulates real-world penetration testing scenarios

Types of penetration testing

Web application penetration testing

Internal penetration testing

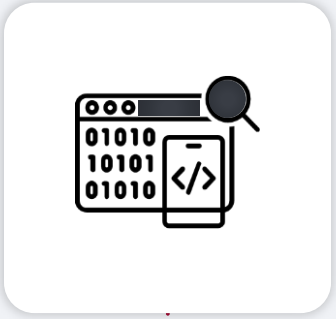


External penetration testing

Social engineering penetration testing

Wireless penetration testing

Mobile application penetration testing



White box penetration testing

Penetration testing reports

Technical report

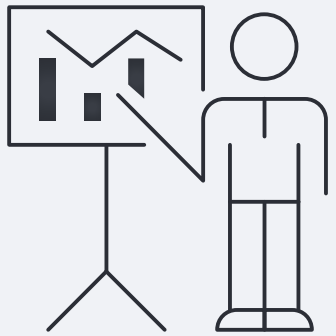
- Structured description of the obtained data on the target infrastructure
- Description of the vulnerabilities identified
- Description of the attempted penetrations and their results
- Analytical conclusions on the current security level of the target information infrastructure
- List of developed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

Executive summary report

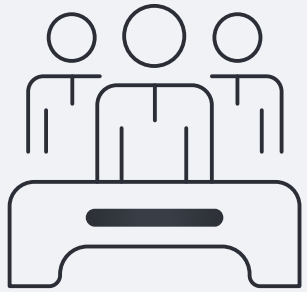
- Brief report for management, written in non-technical language
- Key findings/recommendations

- 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

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

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

What is it?

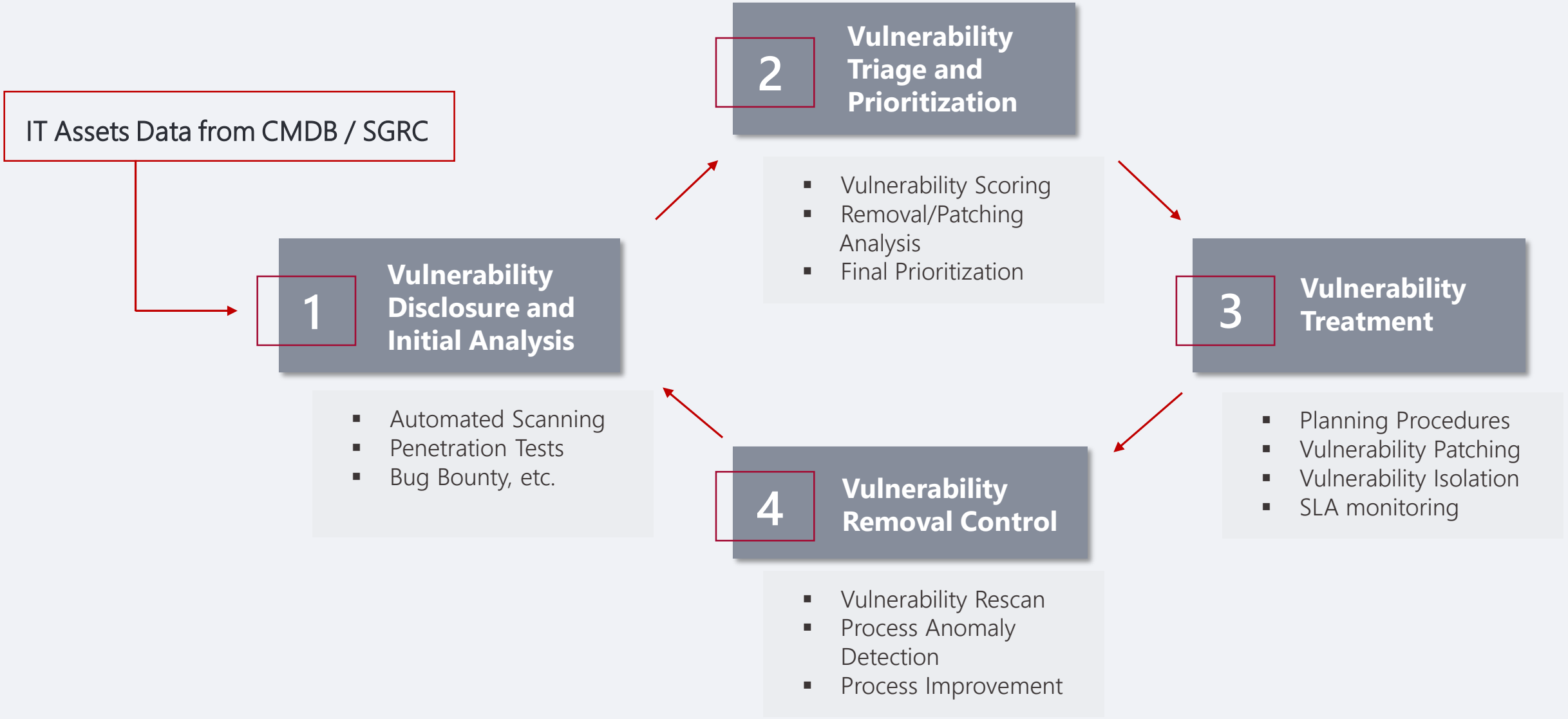
Softline service providing:

- management process
- assets discovery and identification
- vulnerabilities prioritization
- IT and information security interaction (ex. vulnerabilities patching)
- vulnerabilities elimination monitoring

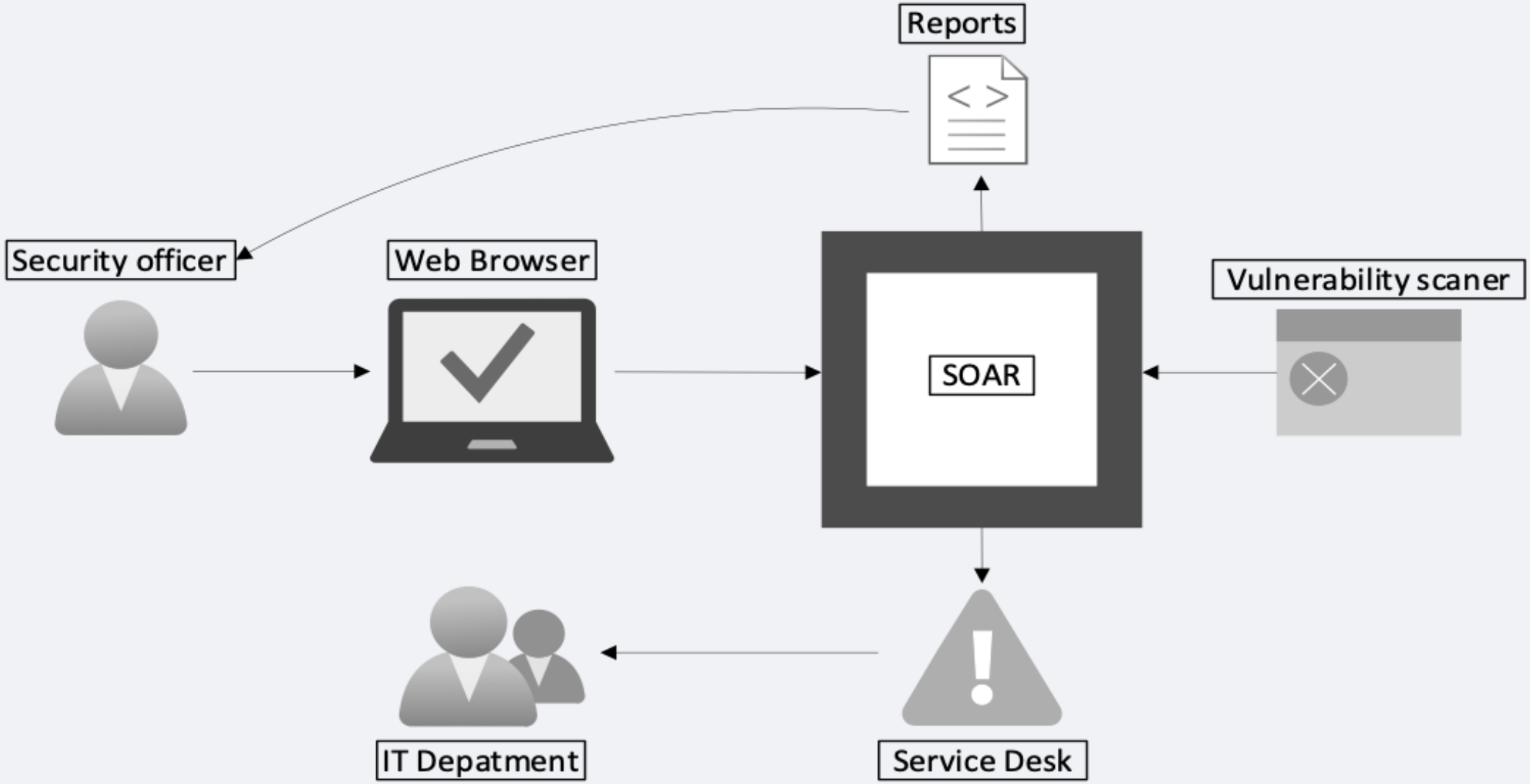
Where is it?

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

Vulnerability management process stages

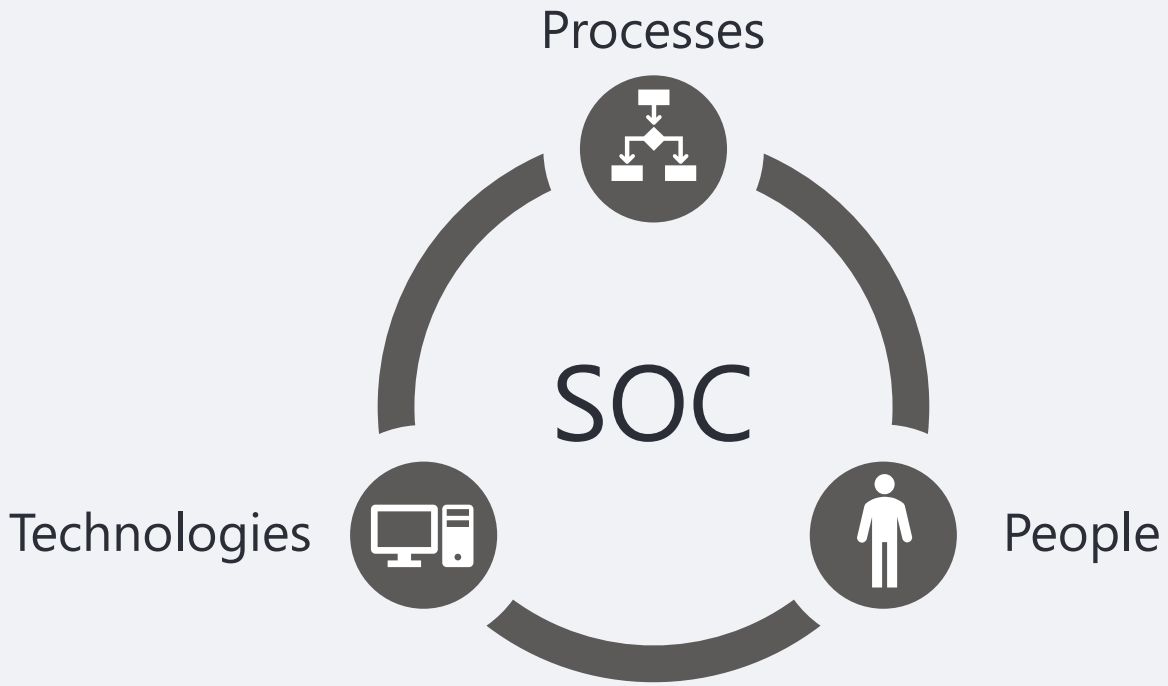


Vulnerability management services



SOC from Scratch

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	Implementation	SOC Start-Up	Ops	Improvement
3 months	3-6 months	3-6 months	1-2 years	

▪ Initial Assessment
▪ SOC Strategy Planning
▪ Specification Development
▪ Service Model Planning
▪ Platform Testing and Selection
▪ HLD Development
▪ Target Organizational Structure Development
▪ Procurement Documentation Development
	▪ 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
		▪ Staff Training
		▪ Rules Fine Tuning
		▪ Playbooks Implementation
		▪ Procedures Improvement
		▪ Duty Shift Planning and Implementation
		▪ Response Exercises and Training
		▪ SOC Commercial Operation
				▪ 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

- Mechanical Engineering

- Smart Cities

- Energy

- Metallurgy

- Transportation

- Chemical Industry

- Nuclear Energy

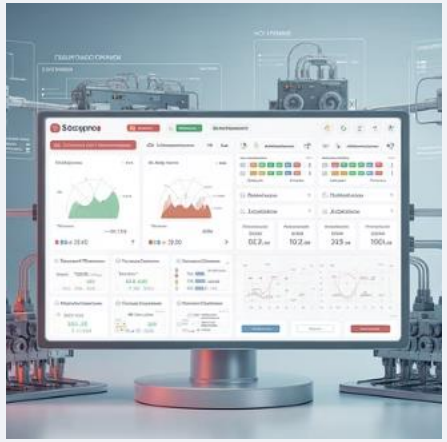
- Food Industry

- Over 10 industries
- Over 500 projects
- Over 300 experts
- More than 10,000 secured OT systems

Key challenges for industrial sector

- Outdated Equipment & Unsupported Software
- Remote Locations & Complicated Logistics
- Non-Stop Production Requirements
- High Fault-Tolerance Demands
- High-Security & Hazardous Facilities
- Ongoing Construction Work
- Unstable Power Supply

What to protect?



Common IT standards

- ISO/IEC 27001
- NIST SP 800-53
- MITRE ATT&CK threat evaluation and modelling

Worldwide-known ICS vendors

- Siemens
- Yokogawa
- Emerson
- Honeywell
- Schneider Electric
- HollySys
- ABB
- Rockwell automation

OT standards

- IEC 62443
- NIST SP 800-82

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 Positive Technologies ISIM, SIEM, VM, NAD, Kaspersky KICS for Nodes and KICS for Networks, Infowatch ARMA and other solutions

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: Major Russian 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