We support you to improve your security

ADVANCED THREAT INSPECTION

A holistic service for assessing vulnerabilities and risks of software, hardware and services

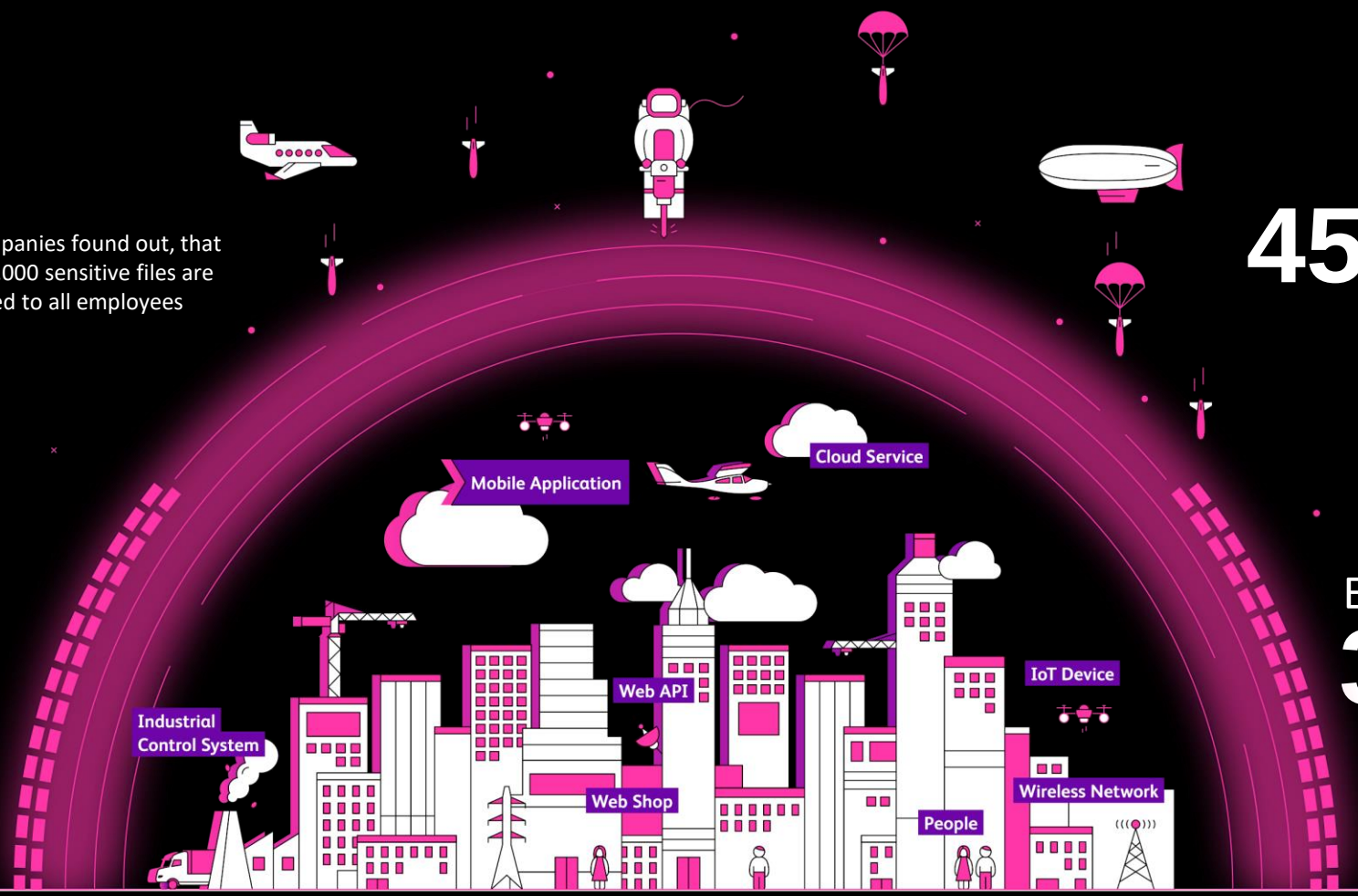
BearingPoint®

53% of companies found out, that over 1.000 sensitive files are exposed to all employees

450.000 new malware types are discovered day by day

2.000% increase in OT attacks year-over-year since 2018

Every **39** seconds, public-facing services are attacked on average



Your business is under attack!

Are your doors locked?

BearingPoint®

More than a pentest

Advanced Threat Inspection gives you an independent security verification of your digital products and services

	Regular Pen Test	Advanced Threat Inspection
(Automated) Vulnerability Scanning	✓	✓
Vulnerability Report	✓	✓
Vulnerability Rating	✓	✓
Remedition guide for known vulnerabilities	✓	✓
Standardized procedure model		✓
Secured flight recording		✓
Post execution cleanup process		✓
Custom exploit development		✓
Proof of exploitation (video, screen captures)		✓
20+ page technical report		✓
Client-specific recommendations on resolution		✓
Individual debriefing with security engineer		✓
Executive summary		✓
Possible Add-Ons+		
Custom phishing campaign		✓+
Cloud security compliance assessment		✓+
Code security review		✓+
OWASP ASVS Testing		✓+
Resolution support for identified vulnerabilities		✓+

Special Features

20+ pages technical report

including vulnerability and exploitation details and recommendations on resolution

Custom exploit

Development and proof of exploitation for realistic, client-specific impact analysis

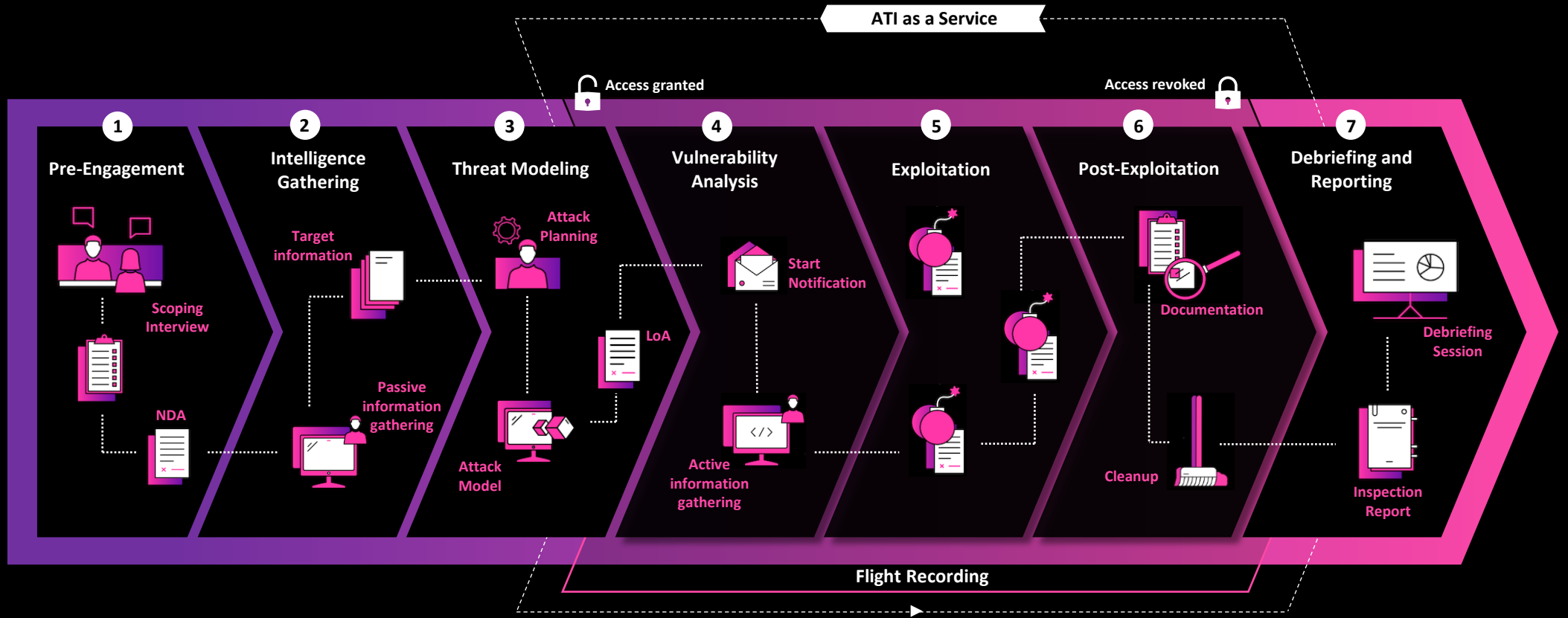
Individual Debriefing

Individual debriefing session with security engineers and target client audience (developers, operations,...)

BearingPoint®

Security with System

Our systematic approach ensures effective and careful execution for every inspection



Targets, objectives and general conditions are defined during a scoping interview.

Information about the targets is passively collected and used to identify possible attack vectors.

All gathered information is consolidated and used to create a customized attack model which gets approved by the client within the „Letter of Authorization“.

Active information gathering is performed through automated and manual scans for vulnerabilities and additional system properties.

Customized exploits are developed and executed, and findings documented.

The findings are analyzed, documented and rated, and all activity traces on the targets removed.

The inspection report is generated and the findings and recommendations are explained in a personal debriefing session.

BearingPoint®

Pricing

Depends on your individual needs

Our security inspections are customized to the requirements of our clients and cater to their specific needs.

That is why a price can typically be provided after a first discussion about scope, width and depth.

To give an indication, here are three anonymized real-life projects and their cost.

Recurring inspections can be done more efficiently due to lower organisational overhead, and the cost savings are passed on to our clients.

European waste management company

Execution time: 2 weeks

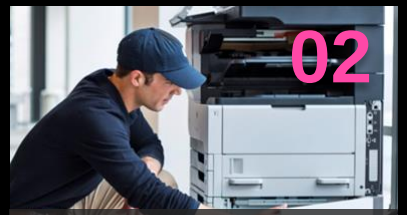
Cloud-hosted customer web portal + API

Service fee: **EUR 7.800,00** *per inspection*

Value for the client:

- In-depth grey box inspection by OSCP-certified security professionals
- Identification of several critical vulnerabilities and independent risk rating
- 20+ page report with proof of exploitation and impact demonstration (video)
- Personal debriefing with software developers and resolution guidance

EUR 10.000,00



Global consulting company

Execution time: 4 weeks

Enterprise printing solution for 5.000 users

One-time fee: **EUR 18.000,00**

Value for the client:

- In-depth black box inspection by OSCP-certified security professionals
- Identification of man-in-the-middle exploit usable for data leakage
- 30+ page report and resolution support with manufacturer (patching)
- Security due diligence for equipment acquisition

EUR 20.000,00

Leading global electronics manufacturer

Execution time: 7 weeks

Attack surface testing for 10 public IPs

Service fee: **EUR 26.000,00** *per inspection*

Value for the client:

- In-depth grey box inspection by OSCP-certified security professionals
- Identification of business critical data leaks and high risk vulnerabilities
- 40+ page report and resolution support for vendors and operations teams
- Recurring security audit for certifications and hardening of attack surface

EUR 30.000,00

BearingPoint®

Some of our projects in the last 12 months

International automotive OEM supplier

Challenge
Inspection of the public attack surface

What we found out
Full supplier database extracted through custom exploit using SQL injection

European insurance spin-off

Challenge
Inspection of full cloud-based service environment

What we found out
Full access to source code, API tokens and credentials and ability to modify and deploy code as unauthorized user

Austrian utilities software company

Challenge
Inspection of web application and APIs

What we found out
Full customer data extracted through API and acquired admin privileges

Scandinavian fashion company

Challenge
Inspection of web shop and staff intelligence gathering

What we found out
Employee data acquired through social engineering as basis for phishing attacks

German manufacturing software developer

Challenge
Inspection of web application hosted on cloud platform

What we found out
Access to personal user data through an unprotected API endpoint

International software development company

Challenge
Inspection of SaaS application hosted on AWS

What we found out
Remote shell access acquired through corrupted template and local file content leakage

„The identified potential for optimisation was underpinned through their vast technical know-how to demonstrate various risk scenarios.

Thanks to these findings we can now better protect our products and develop them in a more secure way going forward.“

Member of the executive board, CMO
Saubermacher Dienstleistungs AG

BearingPoint®

Think digital – Act agile – Manage innovation

- **Consulting**
- **Technology**
- **Services**

- Management Consulting
- Digital Transformation
- Agile Advisory
- Software Engineering
- Business Services

Austrians largest management and technology consulting firm

With more than 500 employees in Austria we develop innovative strategies for new and existing business models and design and implement digital solutions and services for leading companies and public institutions.

With our competencies in management consulting, agile transformation, technology-based business services and smart BearingPoint software solutions, we develop innovative business models together with our clients and partners.

Among BearingPoint's clients are Austrias leading companies and organisations. The global BearingPoint network with more than 10.000 employees supports clients in more than 75 countries and actively engages with them for measurable and long-lasting business success.

BearingPoint®