



**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?**

# 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	✓	✓
Remediation 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		✓
<b>Possible Add-Ons<sup>†</sup></b>		
FOSS (Free & Open Source Software)		✓ <sup>+</sup>
Custom phishing campaign		✓ <sup>+</sup>
Cloud security compliance assessment		✓ <sup>+</sup>
Code security review		✓ <sup>+</sup>
OWASP ASVS Testing		✓ <sup>+</sup>
Resolution support for identified vulnerabilities		✓ <sup>+</sup>

## 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

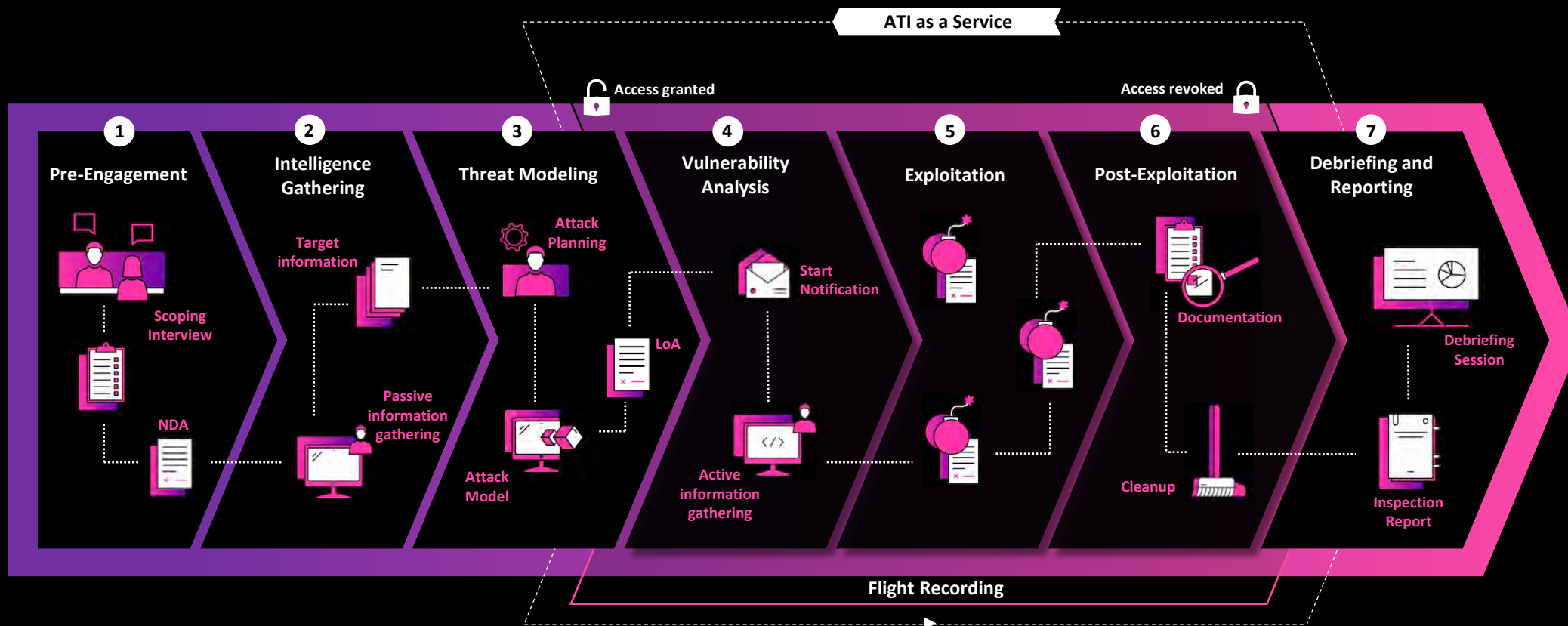


**Individual Debriefing**  
Individual debriefing session with security engineers and target client audience (developers, operations,...)



# 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.

# 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 costs.

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



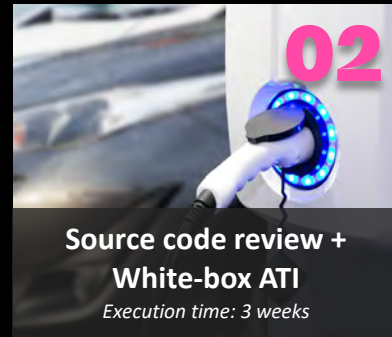
### 10 public IPs with 2 low-complexity webservices

Fee: **EUR 5.600**

#### Key facts:

- In-depth black box inspection by OSCP-certified security professionals
- Testing exposed webservices for OWASP Top 10 & Web security testing
- Identification and verification of vulnerabilities and misconfiguration

EUR 10.000,00



### High-complexity web app + APIs

Fee: **EUR 15.000**

#### Key facts:

- Collaborative source code review based on OWASP ASVS
- Testing web application based on OWASP Top 10 & API testing project
- Active exploitation of vulnerabilities and proof-of-concept demo

EUR 20.000,00



### Headquarter and 5 branch sites

Fee: **EUR 27.000**

#### Key facts:

- In-depth grey box inspection by OSCP/OSWP-certified security professionals
- Simulation of successful employee PC takeover and perimeter breach
- Identification and verification of vulnerabilities and misconfiguration
- Detailed inspection and risk rating for high-value target systems

EUR 30.000,00

# 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®**

# Industrial Security Solution

Introducing the best of OT security on a stand-alone hardware - to push your security to the next level and prepare you for the threats of tomorrow

**We help you prepare for unwanted guests**



# BearingPoint Industrial Security Solution (ISS)

An all-in-one, modular and independent OT security solution that addresses the challenges of tomorrow

## Module X



...and many more

## Module 1



Secure OT Remote Access

## Module 2



OT Asset and Anomaly Detection



## Module 4



Data Analytics for Industry 4.0

## Module 3



Next-Gen OT Firewall



# Security challenges of industrial environments

The industrial and manufacturing industry has become the most attacked sector in recent years, but also faces the most limitations when adapting new security mechanisms

## Visibility



Operators of modern industrial environments require **real-time visibility** of all components, their **potential vulnerabilities and network activities** in order to efficiently protect against cyber threats. The majority of industrial environments today does not have technology in place to quickly identify risks and anomalies.

## Connectivity



**Securing, controlling and auditing remote access** for maintenance and development purposes is one of the key activities to protect against unwanted activities on core components. Many of the used technologies today do not offer sufficient security to **prevent malicious activities or uncontrolled access**.

## Control



The ability to **quickly eliminate new vulnerabilities and risks and control network and automation traffic** in a granular way is a challenging task in industrial environments, where architectural and functional changes can often not be implemented in a timely manner due to availability and safety constraints.

## Flexibility








Industry 4.0 drives the adoption of new technology and service models, but often requires investments in infrastructure. Each new solution demands compute resources and connectivity, but budgets are often tight when it comes to investments for existing plants. Operators are looking for **easy and cost-efficient ways to implement Industry 4.0 use cases** in a flexible and fast manner.



# We only use the best tech on the market

An all-in-one package that combines leading technology in an independent and modern architecture

<p><b>Application Service Chain</b></p>	<div style="display: flex; justify-content: space-around; align-items: center;"> <div style="text-align: center;">  <p><b>CHECK POINT</b></p> <p>Next-Gen OT Firewall</p> </div> <div style="text-align: center;">  <p><b>Cyolo</b></p> <p>Secure Remote Access</p> <p>Secure OT Remote Access</p> </div> <div style="text-align: center;">  <p><b>CLAROTY</b></p> <p>xDome/CTD</p> <p>OT Asset &amp; Anomaly Detection</p> </div> <div style="text-align: center;"> <ul style="list-style-type: none"> <li>▪ Data analytics</li> <li>▪ SDWAN</li> <li>▪ Monitoring</li> <li>▪ ...</li> </ul> <p>Additional services</p> </div> </div>	<ul style="list-style-type: none"> <li>• Leading Next-Gen FW vendor</li> <li>• Leading OT security vendor</li> <li>• Possibility to introduce additional virtualised services later on (high flexibility), or exchange individual components for other vendors</li> </ul>
<p><b>Virtualized Hosting Layer</b></p>	<div style="text-align: center;">  <p><b>ADVA™</b></p> <p>Orchestrator</p> </div>	<ul style="list-style-type: none"> <li>• OpenStack based virtualization layer</li> <li>• Advanced network services</li> <li>• Management &amp; Security features</li> <li>• Extensive NW protocol support</li> <li>• Traffic management &amp; zero touch</li> </ul>
<p><b>Hardware Layer</b></p>	<div style="text-align: center;">  <p><b>ADVANTECH</b></p> <p>uCPE</p> </div>	<ul style="list-style-type: none"> <li>• Leading hardware and electronics vendor with solid reputation</li> <li>• Different appliance options available depending on required feature set (modules, performance, connectivity, ruggedized for challenging environments)</li> </ul>

# Features and capabilities

The combination of powerful feature sets makes ISS the ideal OT security problem-solver



## Secure & Control Remote Access

- Easy and granular approval process for remote connections (assets, time, purpose)
- Supports application tunnel for proprietary protocols (e.g. PLC direct connection)
- File transfer support
- Multi-tenancy support; IEC 62443 compliant

## Usability

- Web-based access (no client required)
- Easy-to-use UI and simple target selection
- Central authentication support (SAML, AD, ...)

## Security

- Reverse-SSL tunnel, no inbound connections
- Multi-factor authentication
- Emergency disconnect option

## Traceability

- Detailed Audit Logs
- Over-the-shoulder monitoring
- Session and video recording



## Asset discovery

- Cloud-based (xDome) or on-premise (CTD) management
- 450+ protocols
- Full visibility across OT environments
- Multiple discovery methods (active/passive)

## Vulnerability & Risk Management

- Discovery, enriches and correlates assets
- Custom risk scoring for easy prioritization
- Integration with 3rd party tools (e.g. SIEM)

## Network Protection

- Automated segmentation policy creation
- Automated policy compliance monitoring
- Integrates with Claroty Secure Remote Access

## Threat Detection

- Custom monitoring for industrial environments
- Threat alerting and false positive elimination
- Identify and remediate attack vectors



## Award-winning security

- Gartner Security leader since 1997
- Forrester Wave Leader for enterprise firewalls
- 20 times NSS labs "Recommended"
- Full feature set in a tiny package

## Lightweight

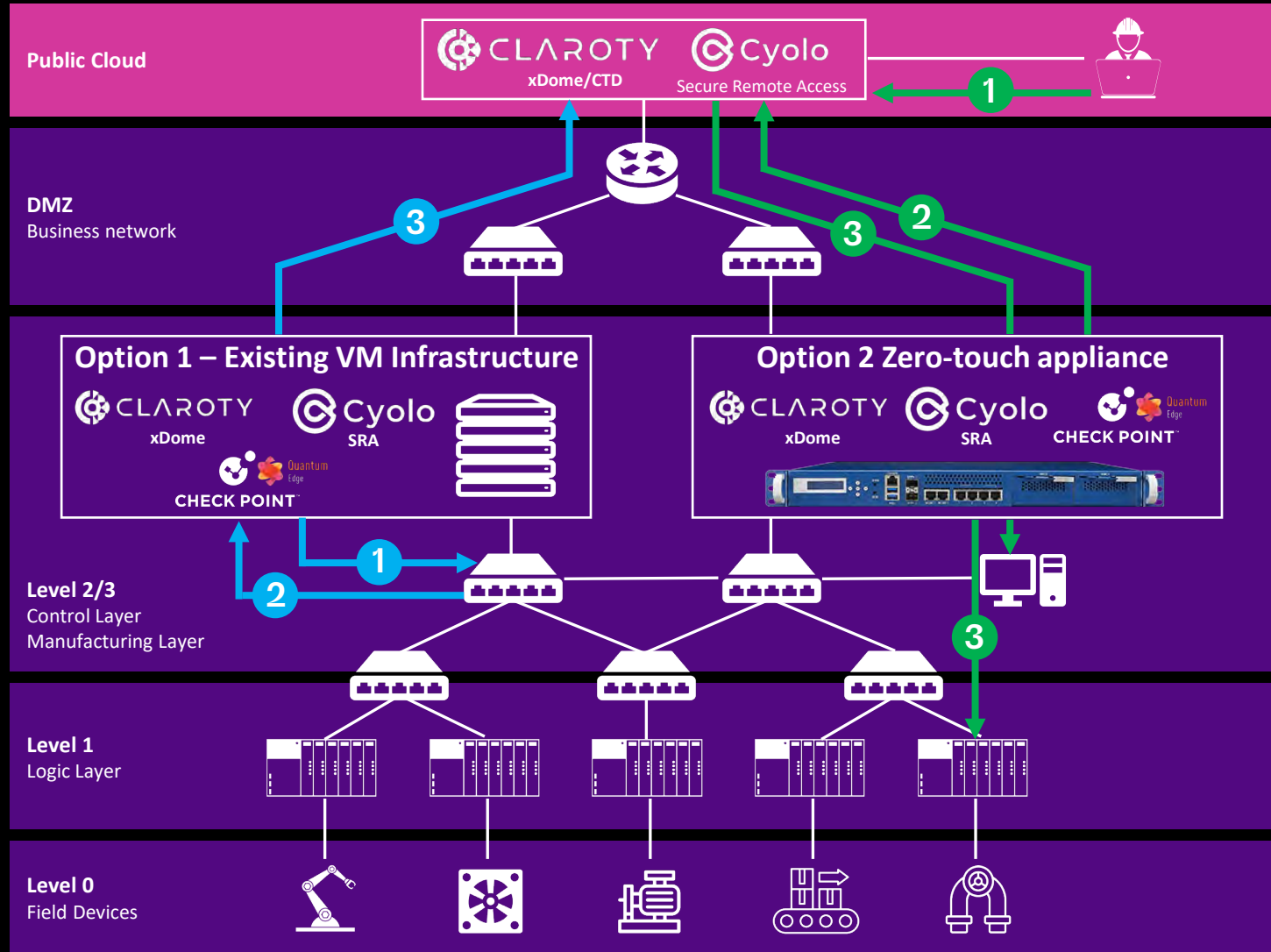
- Virtual machine designed for the WAN edge
- Supports inbound and outbound traffic inspection
- Automated site onboarding

## OT problem-solver

- Virtual patching of vulnerabilities
- Rule-based limitation of traffic flows
- Traffic inspection for OT threats
- Remediation support based on xDome telemetry
- Segmentation and IT/OT separation support
- Cloud-hosted central management support

# Deployment options and data flows

The solution can either be run on independent hardware, or integrated into an existing VM infrastructure



## 1. Asset Discovery

Claroty Edge actively discovers asset information in the OT network

## 2. Traffic collection

A) Mirroring with SPAN ports over multiple switches collects traffic

OR

B) Only Broadcast and Multicast traffic is collected without SPAN ports

## 3. Threat Detection

Collector uploads the consolidated data to the Claroty xDome SaaS portal. Threats, anomalies and risks are presented via the web interface and can be further processed with 3rd party tools.

## 1. Access request

An engineer requests remote access to an asset via the web portal hosted in the cloud or a data center

## 2. Approval and initiation

After review of the request (time, purpose, target assets, etc.) and approval by an operator, the SRA site initiates an outgoing SSL tunnel to the portal. No open ports are required on the site.

## 3. Access

The engineer can access the requested assets and perform actions according to the initial request. All activities are recorded in an audit log and/or through video recording. Activities can be monitored live.

# BearingPoint®

**Think digital.  
Act agile.  
Manage innovation.**

## **Together we are more than business**

BearingPoint is an independent management and technology consulting firm with European roots and a global reach.

We maintain offices in more than 40 locations and with 5500 employees 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. BearingPoint's clients include leading companies and organizations.

The global BearingPoint network with more than 10,000 employees supports clients in over 75 countries and is actively committed to measurable and sustainable business success.



Bernd Koberwein  
Head of Security Services  
BearingPoint AT  
+43 664 81 61 874  
[bernd.koberwein@bearingpoint.com](mailto:bernd.koberwein@bearingpoint.com)

**BearingPoint®**