aramis by aizoOn

Know, Protect, Empower. Don’t learn malware.

aizOn® USA
TECHNOLOGY CONSULTING

aramis

Know, Protect, Empower. Don't learn Malware

- Executive Summary
- Market considerations
- Problem with current offering
- Aramis and its 4 pillars
- Details
- Conclusions: Know, Protect, Empower!

Executive summary

- The quantity and sophistication of malware requires a new and more effective approach to threat detection and determination.
- aizoOn has joined two independent fields of intense academic and applied research, one on the use of Bayesian network analysis to determine risk profiles, the second on pre-attentive communication to alert a person's intuition.
- aramis is a cloud based, artificial intelligence solution, enabling organizations to reduce dwell time to one day (industry average 205 days) in detecting and determining the cyber threat.
- aramis is available as a platform for organizations with skilled security analysts, or as a service for those companies that focus on a different core business.

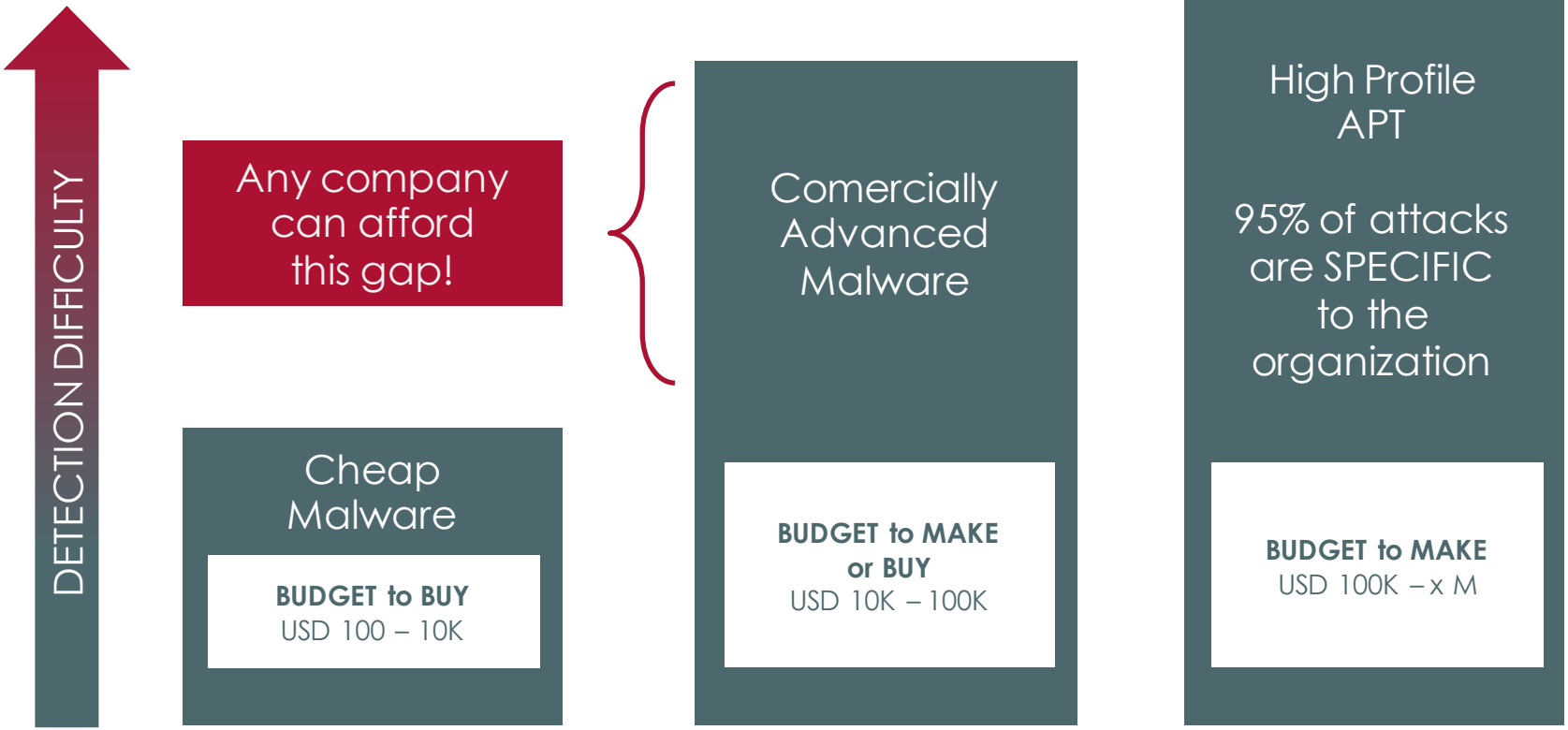
Cyber: war and crimes

- Inexpensive malware is freely available on the internet for all to grab and use to develop more sophisticated attacks.
- Individuals, organized crime and rogue nations have three distinct advantages:
  - Huge number of attacks from near and far, from friends and foes
  - Lack of judicial ability to pursue criminals, domestically and internationally
  - Encryption technology, privacy legislation and social networks combined
  - Fear of organizations in sharing attacks because of brand and penalty damages
  - Element of surprise when devising new forms of attacks
- $425bln lost annually the damage to global economy.
- Data Theft is being replaced by Physical Disruption on infrastructures, machines, plants.

The attackers' key success factors

- Current **defensive technologies** and procedures are just **partly effective**
- The importance of **security awareness** is often **underestimated**
- Motivated attackers **have a high likelihood of breaching**
- Criminals often manage to **escape justice**
- Effective attacking tools and techniques are **economically viable**

Malware is affordable



aizoon® USA TECHNOLOGY CONSULTING

aizoOn experience

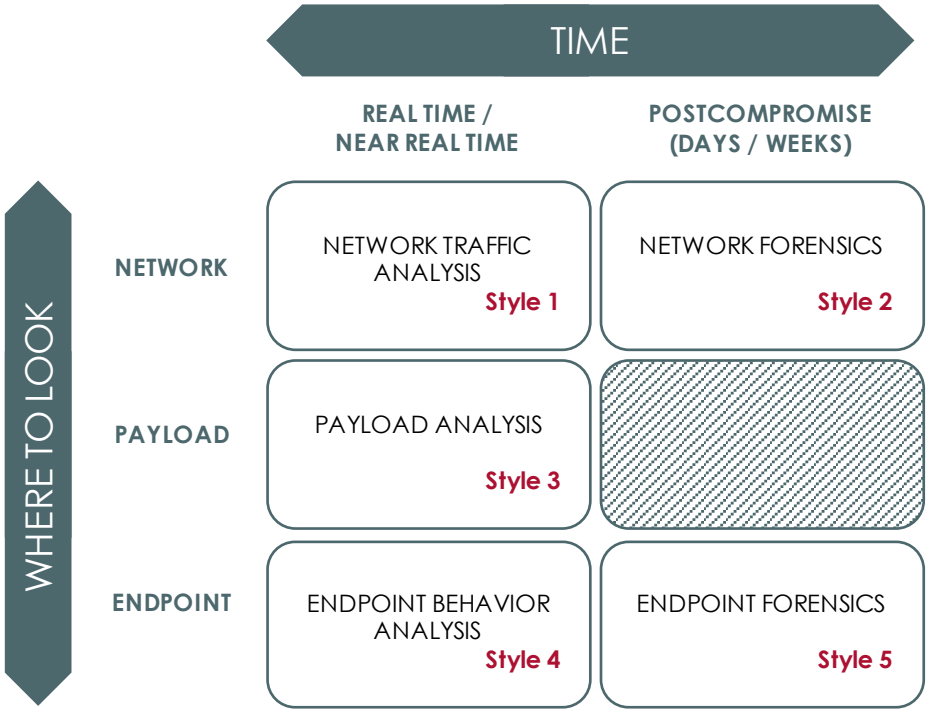
> *We are very proud of our "fake malware"*
> *– that currently comprises about 20 different "base" versions –*
> *because it was able to avoid the anti-apt detection*
> *with a success rate of 98%.*
>
> *Danilo Massa - aizoOn CyberSec Leader*

- We have been asked multiple times to produce «fake malware» to TEST the EFFECTIVENESS of corporate ANTI-APT SOLUTIONS.
- Whereas the most basic samples are usually detected, the more COMPLEX ONES ELUDE DETECTION almost every time.
- Advanced MALWARE IS PACKED WITH FEATURES designed to elude detection and operate silently.

Market offering has problems

PROBLEM 	Targeted Attacks and APTs are sophisticated, rapidly evolving and hard to detect.	Targeted Attacks and APTs are sometimes discovered after days, when it's already too late.	Understanding targeted Attacks and APTs, requires a deep, specific knowledge of technology and malware.
SOLUTION 	aramis does not rely on signatures; it highlights the presence of targeted attacks and APTs with intuitive, pre-attentive graphics	aramis' proprietary logic is designed to reduce to hours the «dwell time» passing from the infection to the malware identification and eradication.	Detection process does not require technology-specific or malware knowledge. The key factor is the knowledge of your environment.

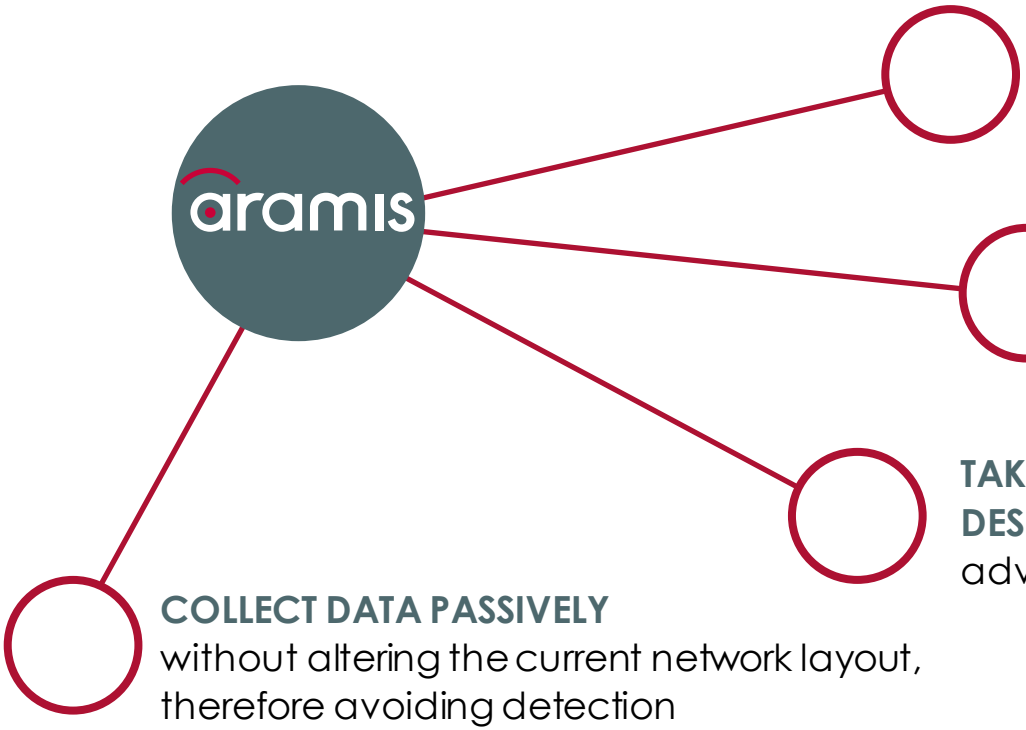
Different approaches to the same problem



GARTNER (August 2013) - Five Styles of Advanced Threat Defense - "Lawrence Orans, Jeremy D'Hoinne"

4 pillars for Aramis

Aramis is an advanced malware identification system designed to:



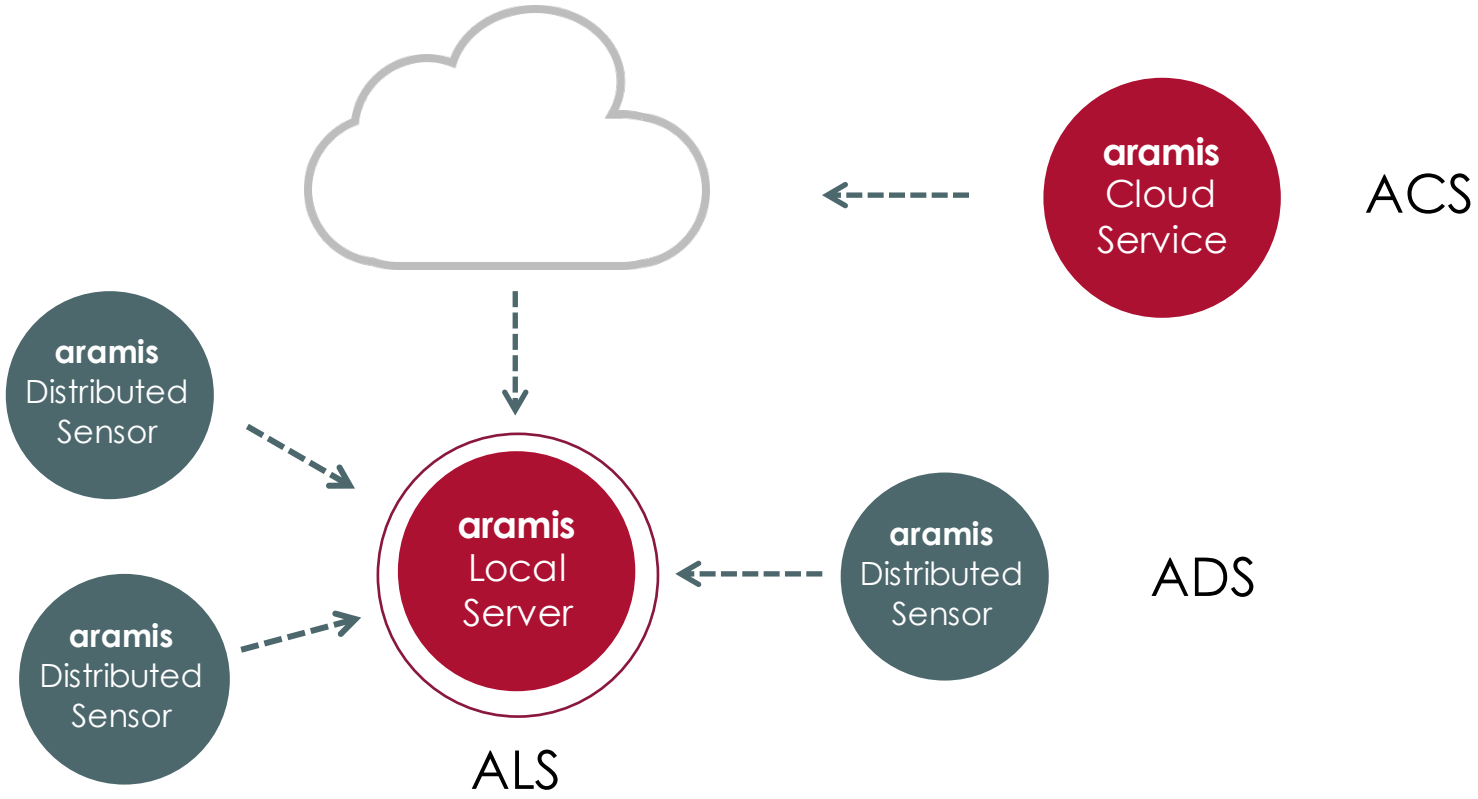
IDENTIFY THREATS inside a network by highlighting the deviations from its normal behavior

FOSTER HUMAN ANALYSIS using proprietary pre-attentive dashboards and graphics

TAKE ADVANTAGE OF SPECIFICALLY DESIGNED BAYESIAN analysis engines and advanced deterministic rules

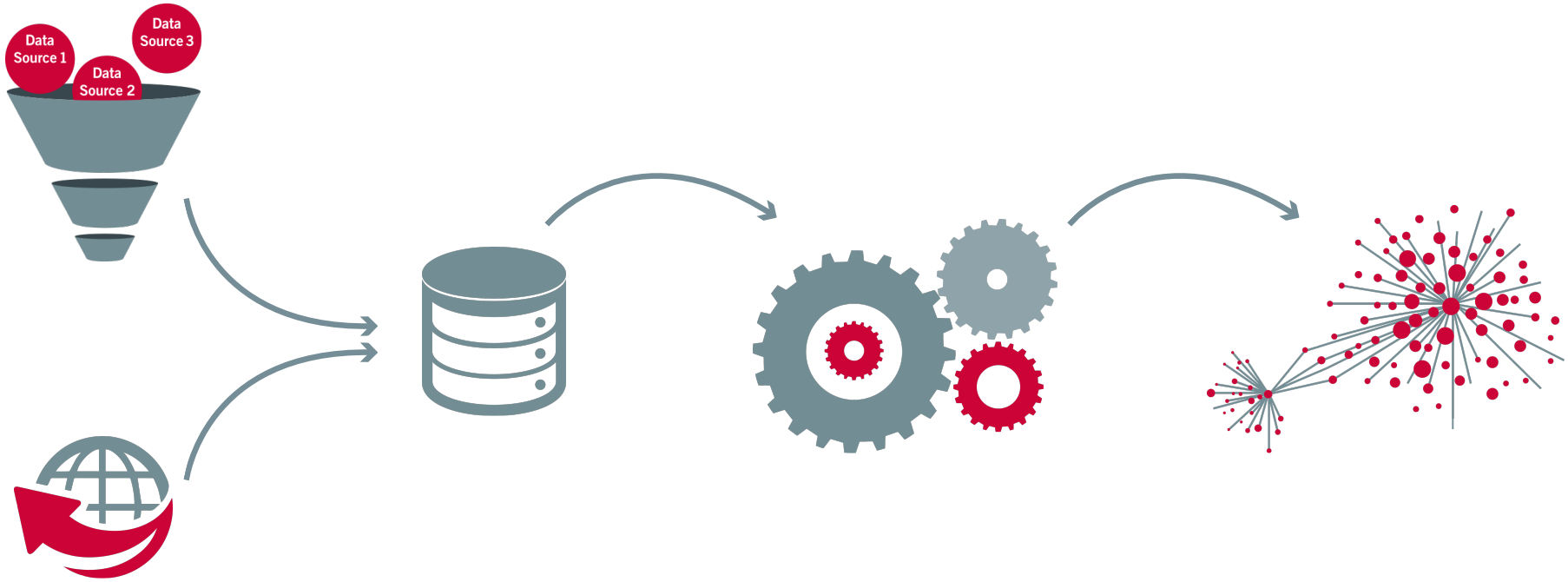
COLLECT DATA PASSIVELY without altering the current network layout, therefore avoiding detection

Aramis Architecture



aizon USA
TECHNOLOGY CONSULTING

Aramis Workflow



aizon® USA
TECHNOLOGY CONSULTING

Bayesian network self-learning engine

Evaluate consistency in the network using ad hoc Bayesian network analysis.
The consistency shows the level (between 0 and 100) of normality of the information in the data flow.

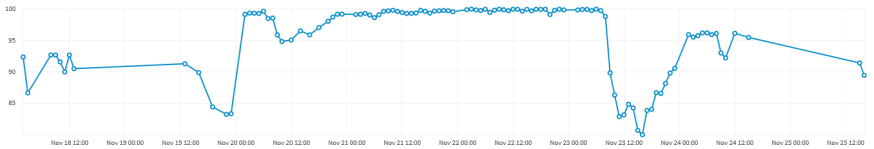
The Bayesian network analyze different dimensions:

- HTTP requests and replies
- FTP activity
- SSL sessions
- SSL certificates used
- SMTP traffic on a network
- DNS activity on a network
- Connections
- Network activity on non-standard ports
- Files transmitted over the network
- Unexpected protocol-level activity

Single Event Consistency

CONSISTENCY	NUMBER OF EVENTS	DESTINATION PORT	ADS	PROTOCOL	DESTINATION MACHINE	SOURCE PORT	DURATION	BYTE TRANSMITTED	CONNECTION STATE		BYTE RECIVED	SERVICE
78.80%	2478	31%	100%	100%	46%	99%	100%	98%	100%	100%	100%	56%

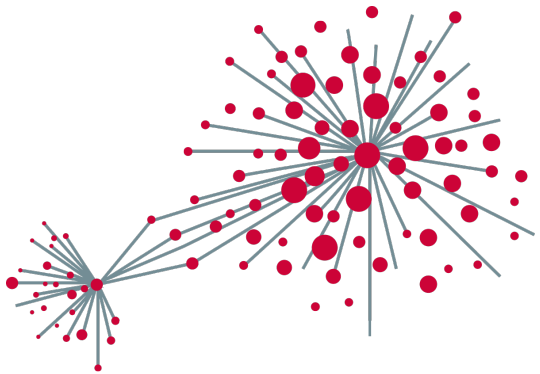
Overall Consistency trend



aizon® USA TECHNOLOGY CONSULTING

Pre-attentive

The *aramis* Risk Visualizer collates the information in pre-attentive dashboards, because in certain cases a person can understand and **react faster** than a computer.



aramis gives the analyst the right tools to be aware of what is going on, in **real time**

Know, Protect, Empower
Don't learn Malware

KNOW

Detection process does not require vendor-specific or malware knowledge. The key factor is the knowledge of your environment trends and behavior

PROTECT

Aramis proprietary logic is designed to reduce the "dwell time" passing from the infection to the identification and eradication of malware to hours instead of days or weeks

EMPOWER

Aramis does not rely on signature triggering; it highlights the presence of malicious behavior, enabling the analyst to immediately identify and classify threats by collating the data presented in the pre-attentive dashboards

KNOW
change the game pay-off

PROBLEM

Attackers can choose organizations that are more easily compromised and provide **greater returns** on "investments"

aramis gives you a **fine-grained picture** of the organization's current risk status and addresses your **protective efforts** where they can make the **difference**

SOLUTION

PROTECT
react sooner

PROBLEM

Targeted Attacks and APTs
are sometimes discovered after many days, when it's already too late.

aramis proprietary logic is designed to reduce to hours the "**dwell time**" passing from the infection to the malware **identification** and **eradication.**

SOLUTION

aizoon® USA
TECHNOLOGY CONSULTING

EMPOWER
recognize, not just identify

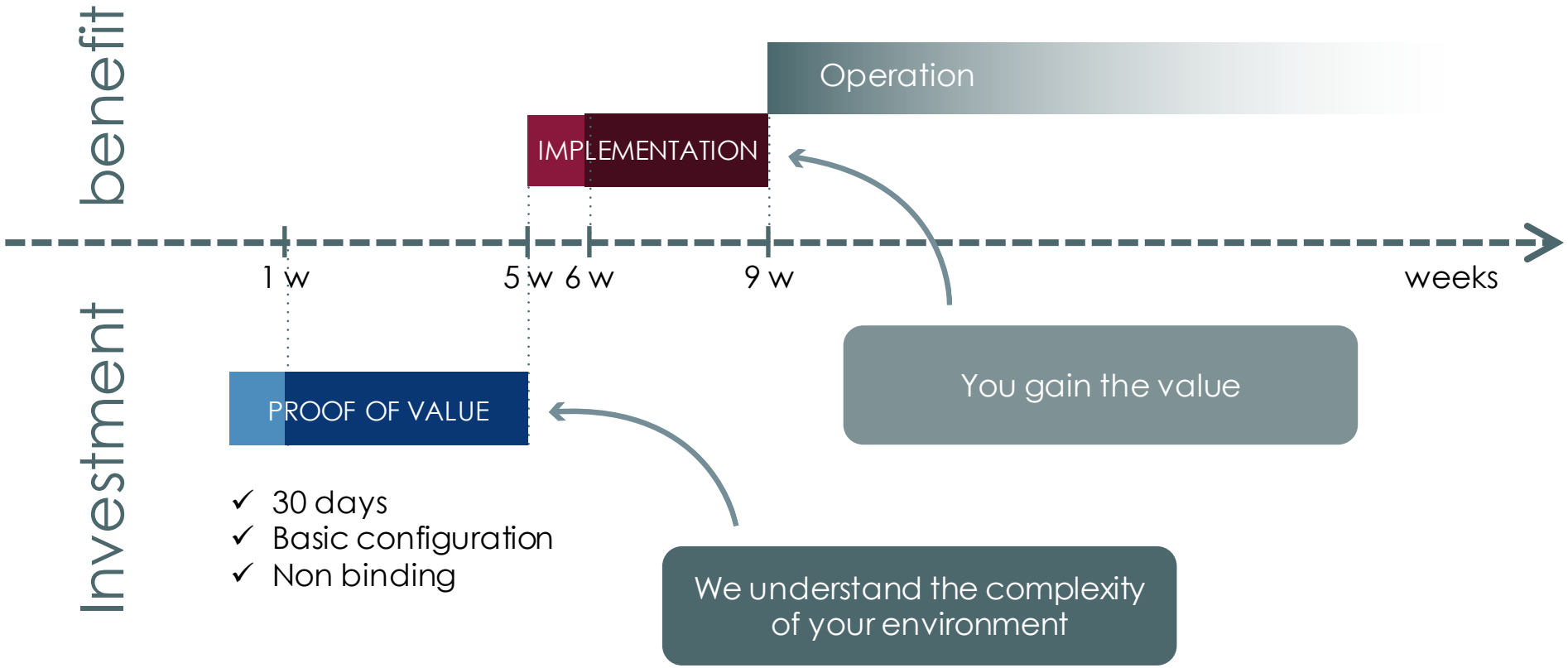
PROBLEM

Targeted Attacks and **APTs** are sophisticated, rapidly evolving and hard to detect.

*aramis does not rely on signature triggering, it **highlights** the presence of targeted attacks and APTs to enable human **pre-attentive** and intuitive **mind processes** to identify them by pure observation.*

SOLUTION

Aramis in action: value & time



Aramis in action: Platform vs. Service ?

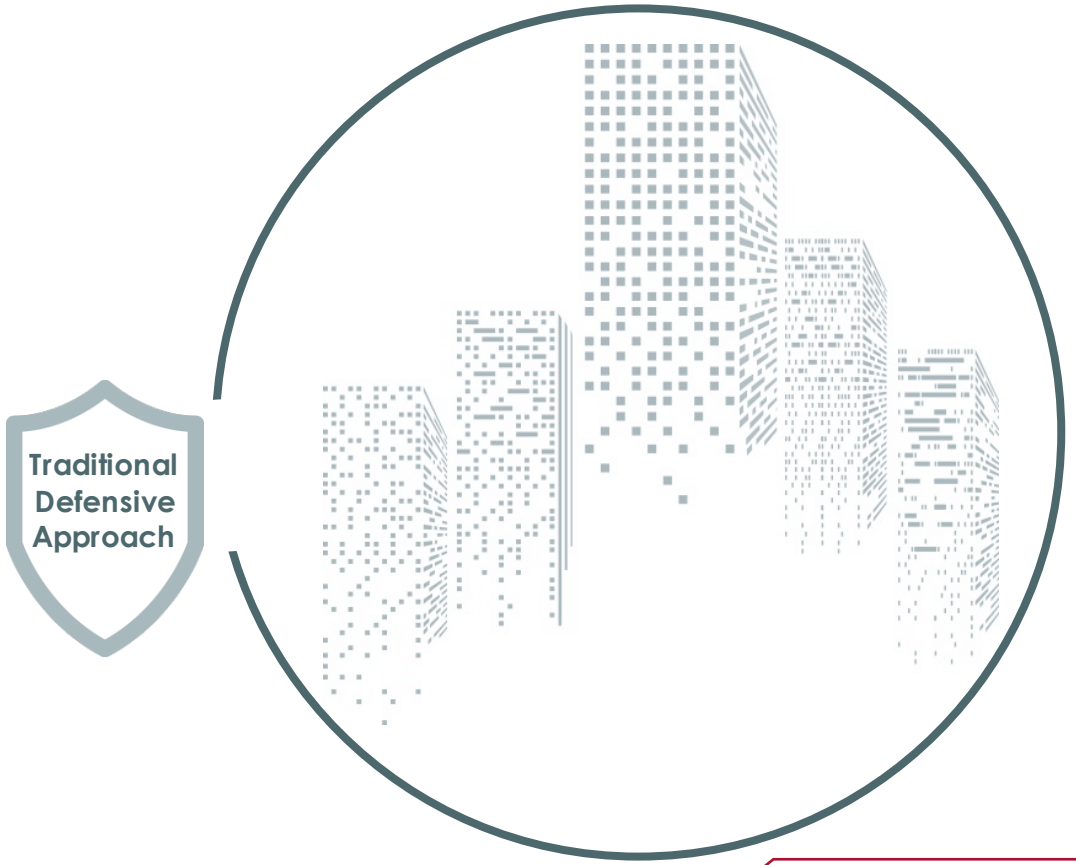
- We provide the training
- Your data stays in your premises
- Develop critical skillsets
- Use your own hardware

VS.

- Easily scalable
- Maximum flexibility
- No training required
- Expert support from day one
- Service Level Agreements

The **classic** friend / foe assessment

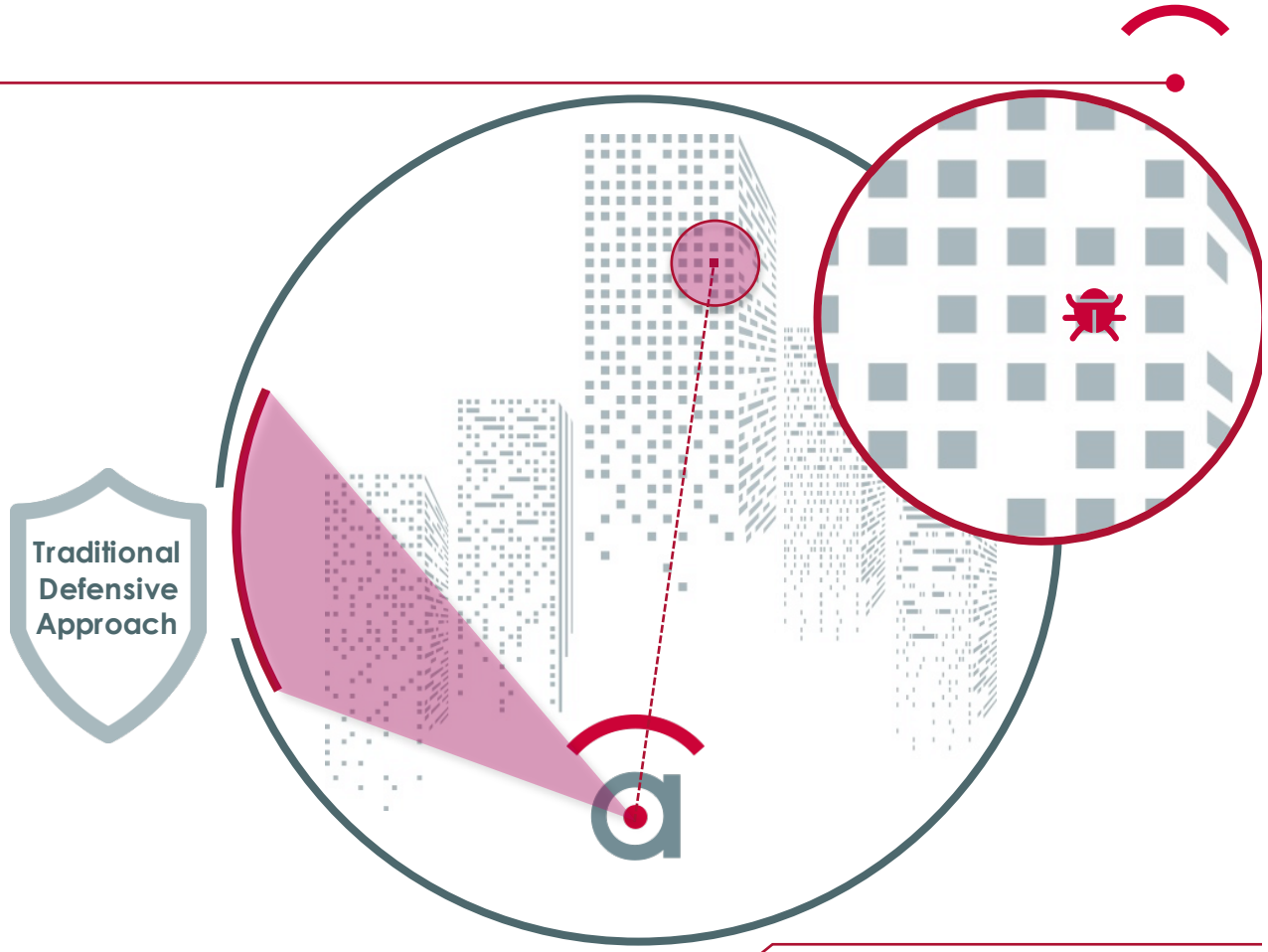
- One time assessment
- Assessing criteria fairly known to attackers
- Standardised approach
- Human knowledge and experience not crucial to the assessment
- Binary outcome



aizon® USA
TECHNOLOGY CONSULTING

The **aramis** approach

- Continuous assessment
- Passive, undetectable solution
- Custom, business-centric assessment criteria
- Human knowledge and experience key to decision
- Risk based results



aizon® USA
TECHNOLOGY CONSULTING