EICAR Minimum Standard for IT-Security Products

RAINER FAHS

CHAIRMAN, EICAR

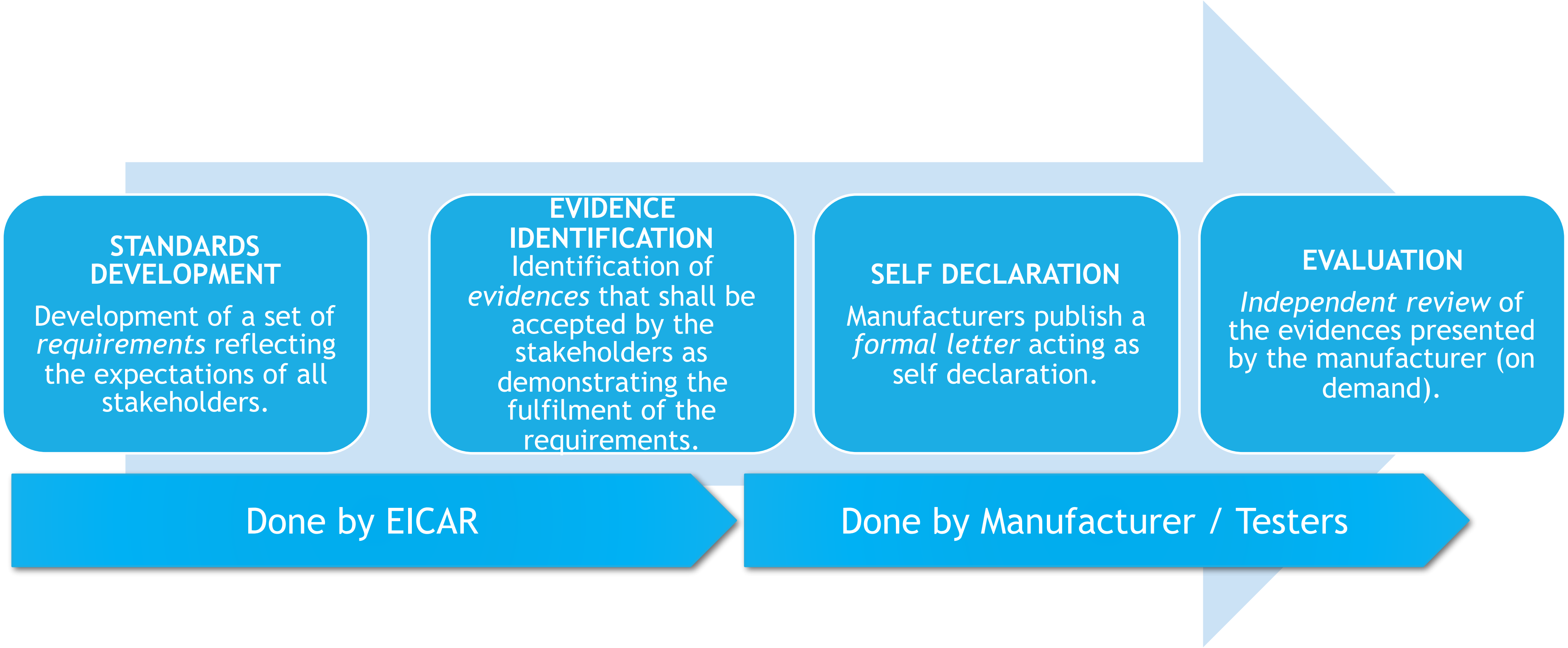
Why a Minimum Standard?

- Need: Enhance the trustworthiness in products supporting IT Security and Data Protection.
- An independent and objective standard for IT Security products is needed.
- The first and most important step is the development of a set of implementation independent trustworthiness standard for IT Security products
  - Beginning with Anti Malware products as the area of our core expertise.
- EICAR as an independent international organisation is in the right position to integrate all requirements and be THE trustful custodian.

The Content

Transparency		Mastery	Trust	Security	Privacy
Commitment	Responsible exchange	Code mastery	No hidden functionality	Secure transfer	User anonymity
Privacy declaration	Transparent functionality	Code control	No third party access	Secure storage of data	No unwanted data transfer
Transparency on data analyzed		Containment of malicious code	Detection of backdoors		No access to user data

The Process



STANDARDS DEVELOPMENT
Development of a set of *requirements* reflecting the expectations of all stakeholders.

EVIDENCE IDENTIFICATION
Identification of *evidences* that shall be accepted by the stakeholders as demonstrating the fulfilment of the requirements.

SELF DECLARATION
Manufacturers publish a *formal letter* acting as self declaration.

EVALUATION
Independent review of the evidences presented by the manufacturer (on demand).

Done by EICAR

Done by Manufacturer / Testers

More Detail

- The Minimum Standard is a kind of „voluntary industrial self-control“.
  - Letter where the vendor signs for his product and commits compliance against the standard.
- The last paragraph of the trustworthiness standard is the agreement that the vendor agrees to be subject to an independent evaluation.
  - The evaluation process is currently under development – see next part of the presentation.
- EICAR closely works together with the MAPPING project (Managing Alternatives for Privacy, property and Internet Governance) and the AV tester community.

Marketing

- In this process we need to work closely with the marketing departements of the vendors that will sign off the Minimum Standard procedure. This will provide a win/win situation as they also will raise trust and exposure.
- So far, interest has been great, **but little commitment from vendors**

eicar
Security checked

TREND MICRO

G DATA

KASPERSKY ANTIVIRUS

F-Secure

Accountability and Trustworthiness using the EICAR Minimum Standard

SACHAR PAULUS

FACULTY OF COMPUTER SCIENCE, MANNHEIM UNIVERSITY OF APPLIED SCIENCES

EICAR SCIENTIFIC DIRECTOR

Accountability and Trustworthiness

Security

„the state of being free from unacceptable risks“

Accountability

“… answerable for the correct and thorough completion of the deliverable… “

Trustworthiness

„… how well a set of functional and non-functional properties is secured…“

Trust

„reliance on another entity“

Source: OPTET Project, Wikipedia

Trustworthy Software (Apps & Internet Services)

Allows for accountability

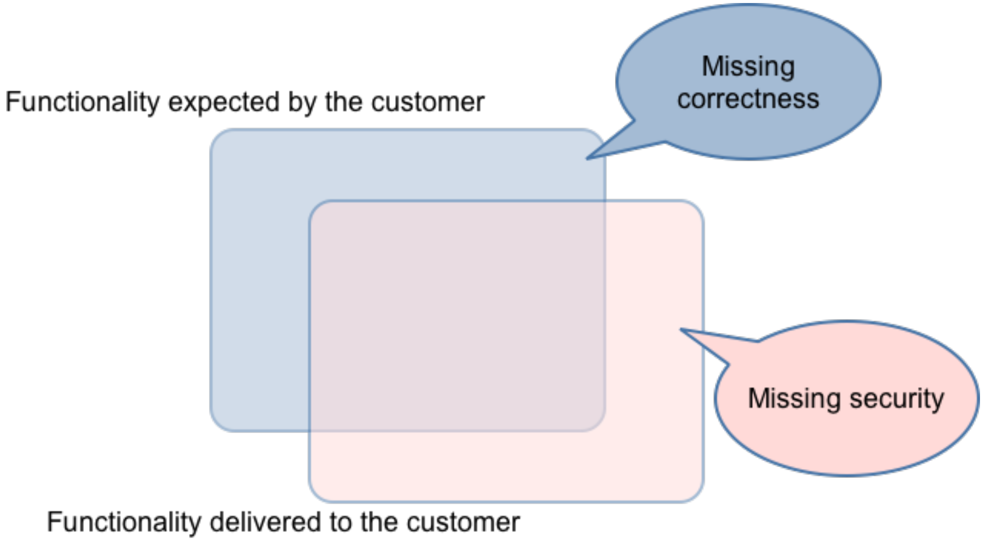
Is managed and operated with transparency

Does what it promises

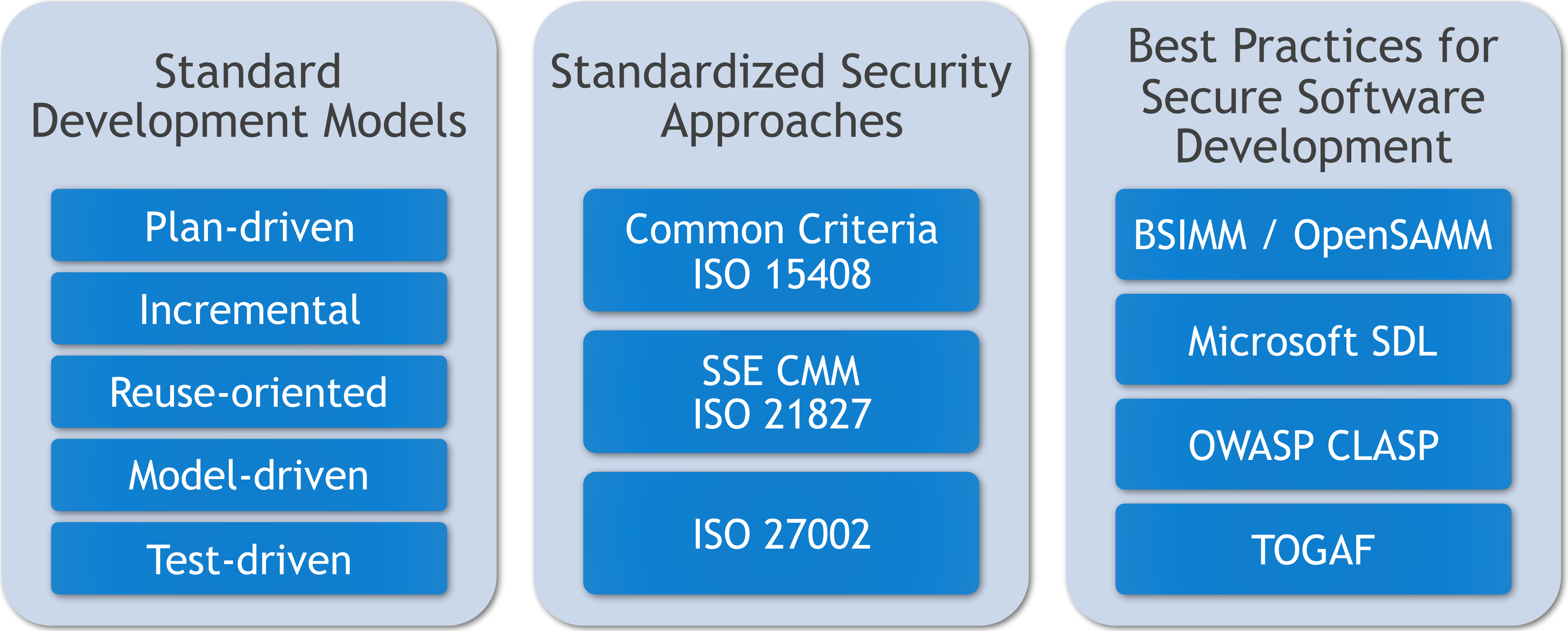
Does nothing else

Proactively respects user‘s interests

Proactively respects user's privacy


Functionality expected by the customer
Missing correctness
Missing security
Functionality delivered to the customer

Existing Approaches to Produc Trustworthy Software



Standard Development Models

- Plan-driven
- Incremental
- Reuse-oriented
- Model-driven
- Test-driven

Standardized Security Approaches

- Common Criteria ISO 15408
- SSE CMM ISO 21827
- ISO 27002

Best Practices for Secure Software Development

- BSIMM / OpenSAMM
- Microsoft SDL
- OWASP CLASP
- TOGAF

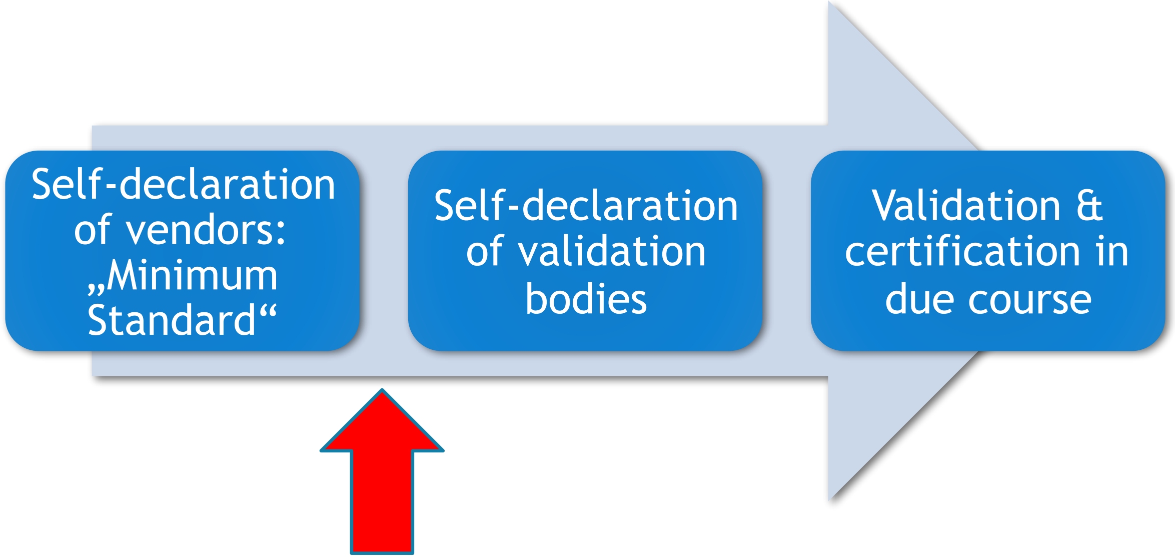
Source: OPTET Project

The EICAR Approach

None of the models presented is able to assure trustworthiness „by design“

New, agile approaches are necessary

Approach of EICAR:

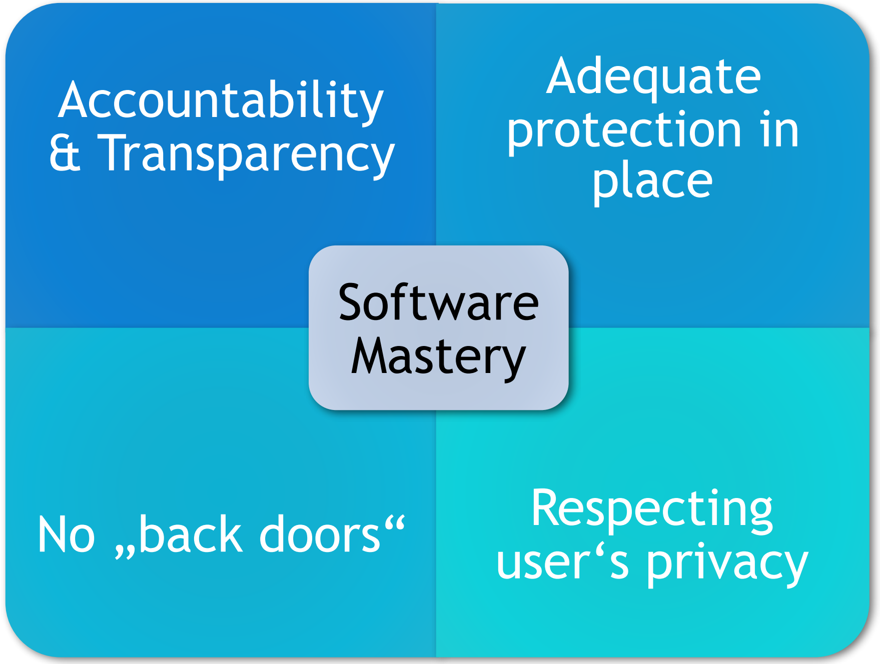


Self-declaration of vendors: „Minimum Standard“

Self-declaration of validation bodies

Validation & certification in due course

The EICAR Minimum Standard covers:



Accountability & Transparency

Adequate protection in place

Software Mastery

No „back doors“

Respecting user‘s privacy

Options for Validation

Customer Audits

- Include Minimum Standard into contracts
- Grant customers audit rights

Independent Validation

- Define criteria covering the minimum standard
- Independent bodies perform validation

Industry Standard

- Standards body working group develops criteria
- Certification by established organizations

EICAR‘s approach

Customer Audits

- Include Minimum Standard into contracts
- Grant customers audit rights

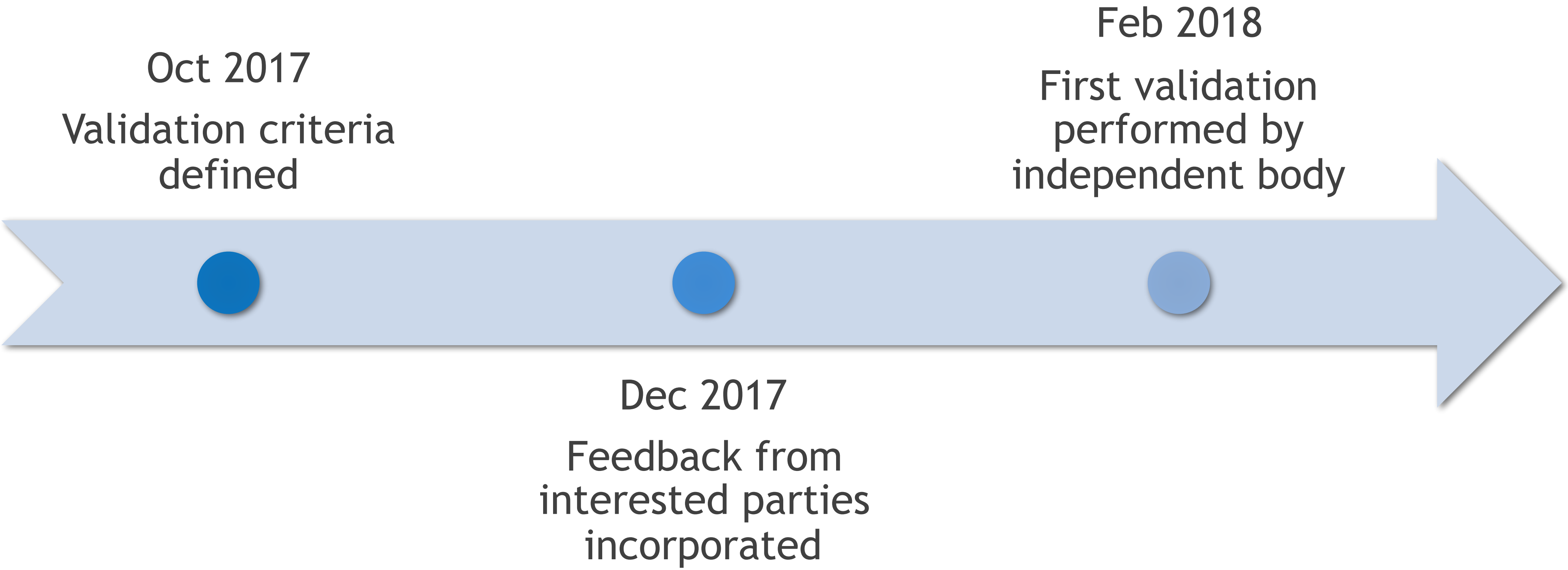
Independent Validation

- Define criteria covering the minimum standard
- Independent bodies perform validation

Industry Standard

- Standards body working group develops criteria
- Certification by established organizations

Timeline



Oct 2017

Validation criteria defined

Dec 2017

Feedback from interested parties incorporated

Feb 2018

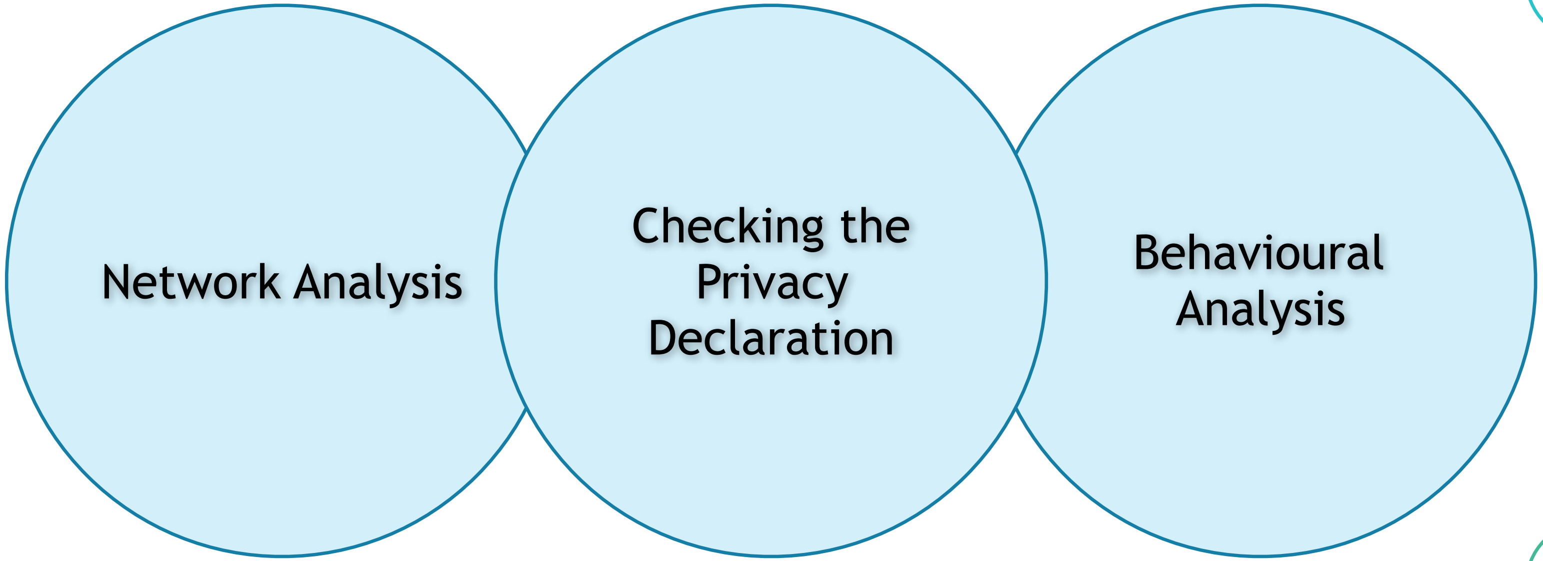
First validation performed by independent body

Trustworthy Security Software How to Validate the EICAR Minimum Standard

MARCEL EBERLING

FACULTY OF COMPUTER SCIENCE, MANNHEIM UNIVERSITY OF APPLIED SCIENCES

Validation Categories

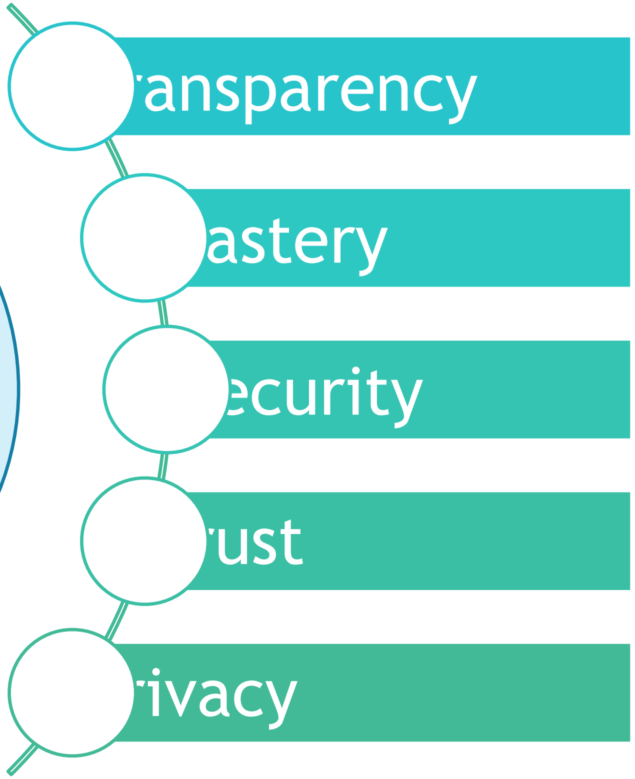


Network Analysis

Checking the Privacy Declaration

Behavioural Analysis

DONE



ansparency

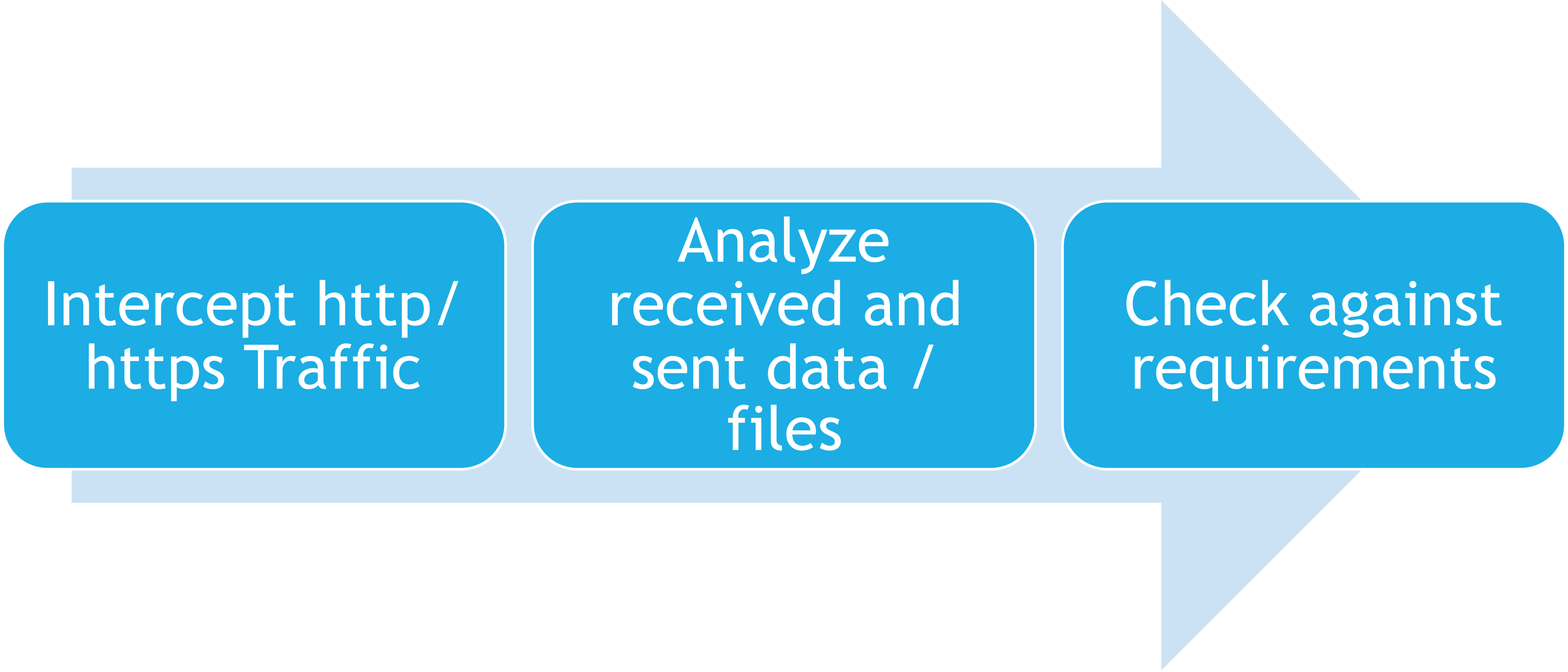
astery

ecurity

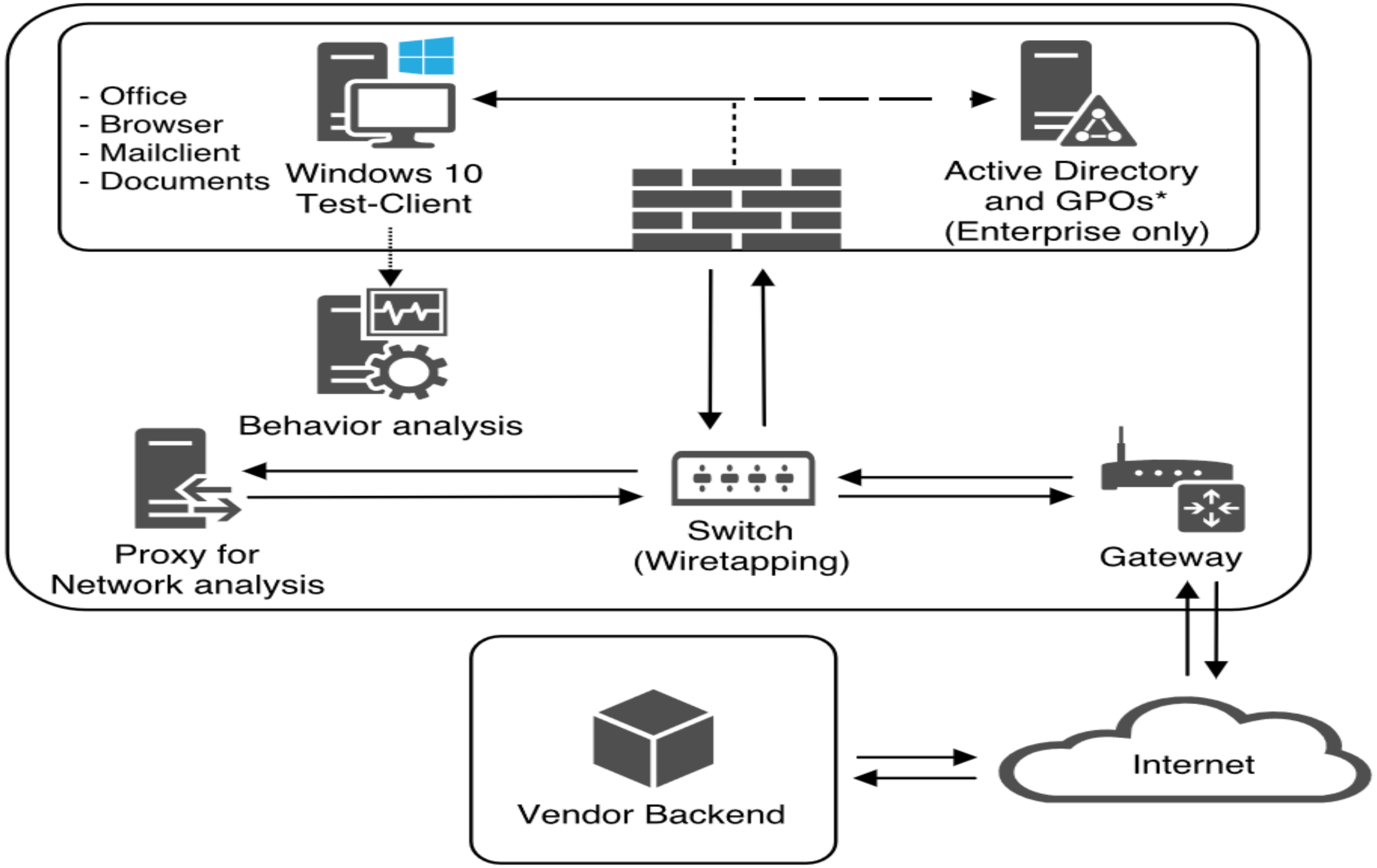
ust

ivacy

Network Analysis


Intercept http/ https Traffic
Analyze received and sent data / files
Check against requirements

Network Analysis Setup



Network Analysis Validation Results

- 15 products tested for interception / 11 have been testable
- 6 Free / 9 paid licenced programs
- Some use plain HTTP to transfer updates and signatures (!)
- „Cloud Protection“ was turned off
  - Needs to be investigated further (specifically regarding data drain)

- Overall, the approach is valid to test the requirements

Behavioral Analysis Approach

- Goal: to check whether user data / system information is tapped, modified, deleted, copied… without the user‘ consent
- How:
  - Observe read/write operations on file system level
  - Compare with expected behavior
  - Identify potential mismatches
- Success factors:
  - Observation time at least one week (crown jobs etc.)
  - Normal user behavior (to avoid the identification of test mode by potential „malware“)
  - Sample realistic user data

Privacy Declaration Approach

Validation through objective criteria…

- Length of the declatation
- Length of the sentences
- Users consent does not impact privacy rights („too much“)
- Comprehen-siveness, complexity of words chosen
- Sequence of topics, segregation of aspects

… still needs some research

EICAR Minimum Standard for IT-Security Products

THANK YOU