Global Cybercrime Certification

Yves Vandermeer
ECTEG chair
yves.vandermeer@ecteg.eu

Funded by
European Commission

Way to a new IT crime ecosystem

- Standard Operation Procedures and Education docs
  - *ACPO - Good Practice Guide For Digital Evidence (2012)*
  - *Council Of Europe - Electronic Evidence Guide (2013)*
  - *ENISA – Strategies for incident Response and Cyber Crisis cooperation (2016)*
  - *S.D. Brown - Investigating and Prosecuting Cyber Crime (2015)*
  - *Ivar A. Fashing – The Making of an Expert Detective (2016)*
  - *ISO 27037 (2015)*
- Tools
  - features taxonomy from "EVIDENCE" project (*2016*)
    http://wp4.evidenceproject.eu/dft.catalogue/dftc.home.php
  - FREETOOL project (I & II)
- Career path within profiles matrix
  TCF by EC3, ECTEG and CEPOL (2015)
- Course packages coherent and structured
- Practitioners certification procedures
  TOT project - *Universidad Autónoma de Madrid (2016)*

Some IT forensics principles

- Only « accredited » experts are allowed to handle « traces »
- «Chain of Custody»
  - Trace integrity => evidence in front of court
  - WWW : **W**ho ? **W**hen ? ho**W** ?
  - Chronological and accurate reporting
- Allows reproducibility
  - Rights of the defence
  - Original seized “item” still available
  - All actions are motivated (**W**hy)

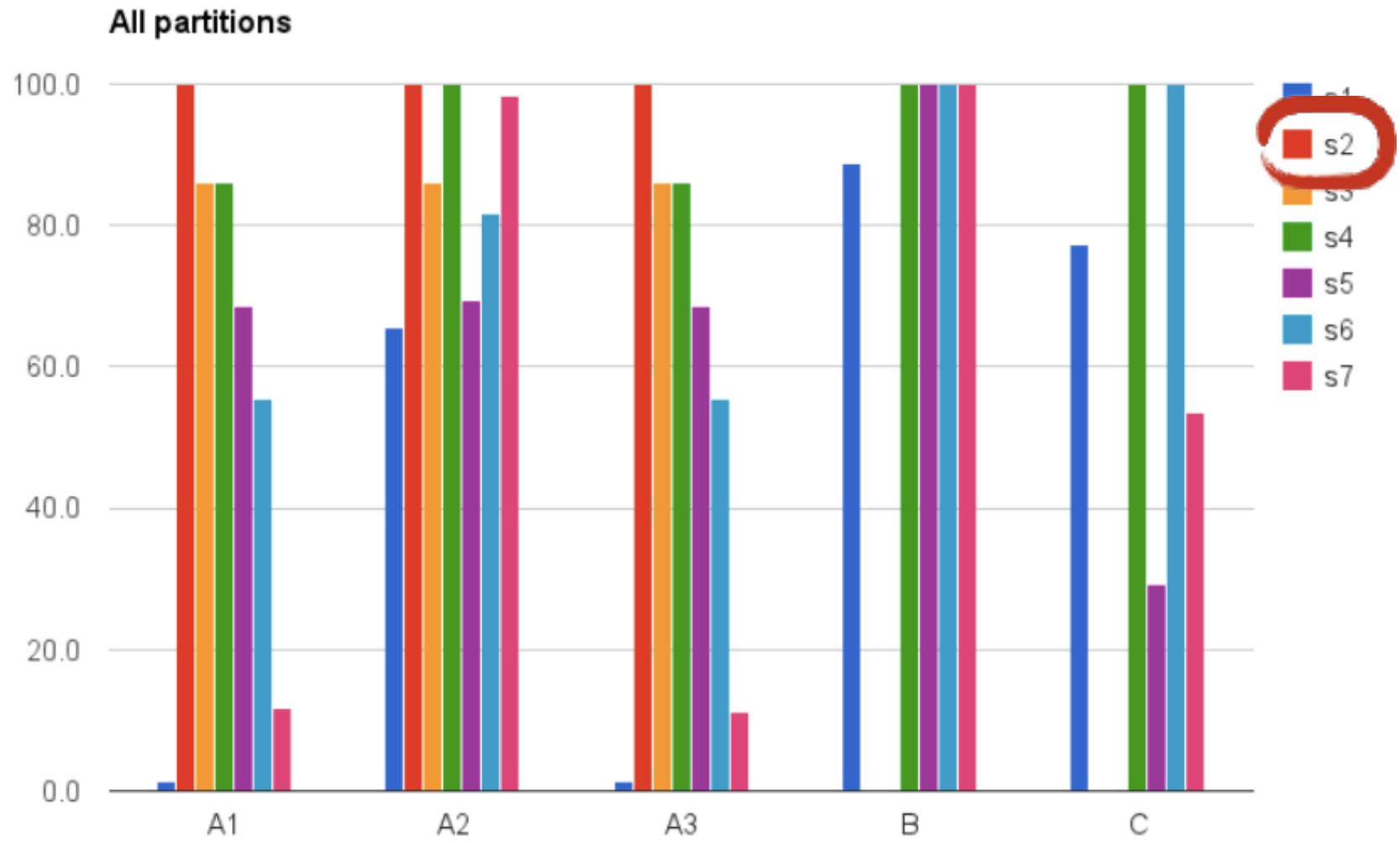
ENFSI
NTFS « state of art » challenge :
Evaluation criteria

- A1 : correct MD5
- A2 : correct full path
- A3 : correct MD5+full path

100 %

- B : unwanted files recovered
- C : files from older version recovered

0 %


All partitions
100.0
80.0
60.0
40.0
20.0
0.0
A1
A2
A3
B
C
s2
s4
s5
s6
s7

Lessons learned

- Only 7 « entities » to address the challenge
- Most participants uses only 1 (commercial) forensic tool
- Only 2 cross-check results (validation ?)
- Only 1 entity got the full mark
- All entities have “something like” a certification or accreditation

A bit more than forensic tools ?

- Capacity building is linked with tasks / operations
  - No need for experts for all tasks
  - But need for experts for some tasks to
    - coordinate forensics (transversal approach)
    - solve what can not be solved by tools (R&D)
    - check and validate tools results
    - present and comment findings in front of the Court
- Avoid to be « tool-dependent »
  - Improve efficiency and accuracy
  - Allows decision makers to change strategy
  - Improve costs management and sustainability
- Keep specialised and trained investigators motivated
  - Recognition
  - Raise expertise level


BIG
DATA
STORAGE
PROCESSING
DECISION
VOLUME
VARIETY
VELOCITY
INFORMATION
INTERNET OF
THINGS
Bit
Byte
Kilobyte
Megabyte
Gigabyte
Terabyte

Expertise AND tools ?

- First responders
  - Identify and gather traces
- Specialisation
  - Search and document traces
  - Validate trace in the investigation
    - Using several *different* tools
- Expertise
  - Traces interpretation
  - Hypothesis

Looking to commercial tools …

- *« EnCase Forensic preserves data in an evidence file format with an unsurpassed record of court acceptance. »*
  (Encase - Guidance Software)

- « court cited solution »
  (FTK - Access Data)

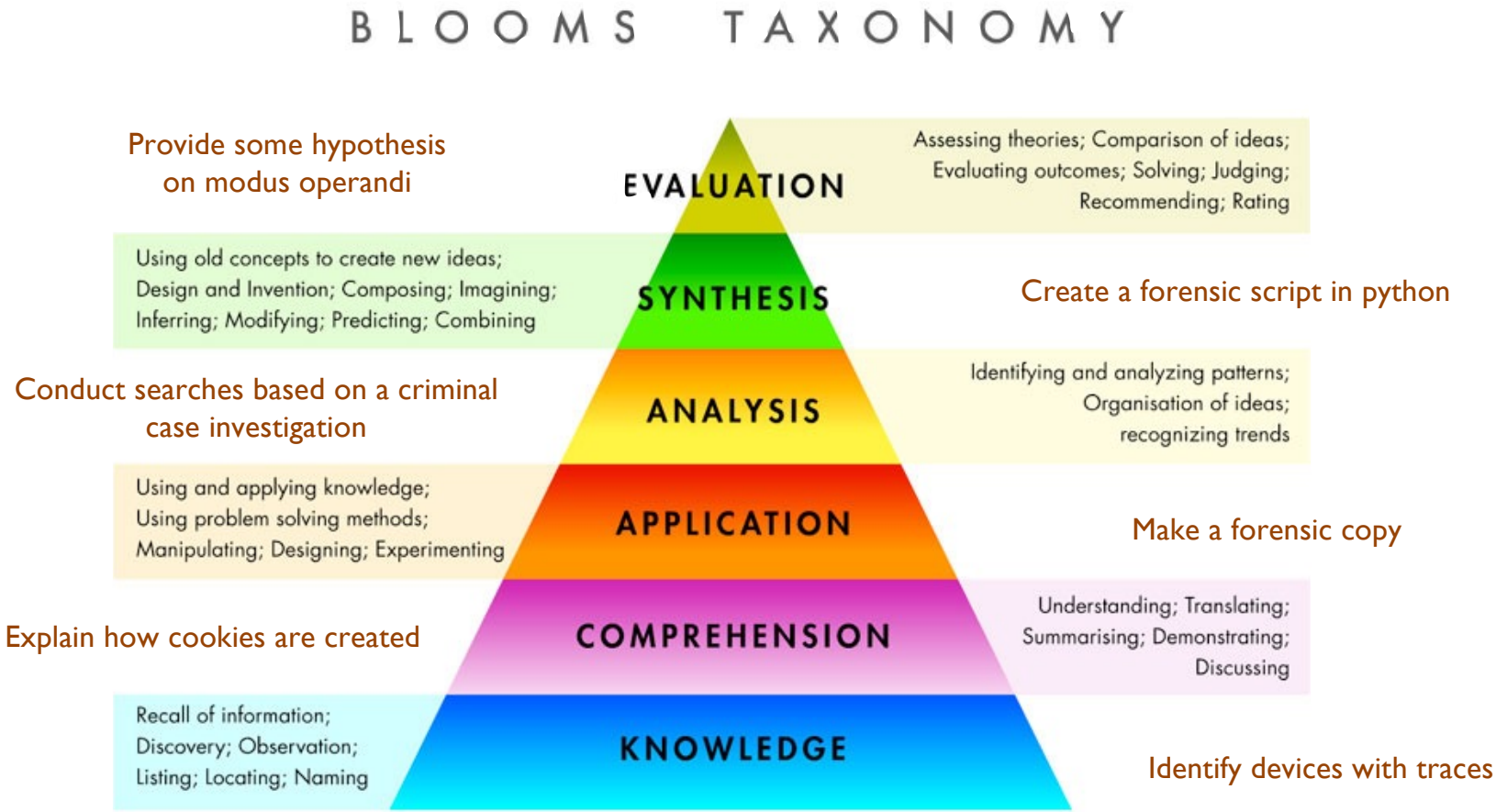
- *« The "engine" that runs the PALADIN Toolbox is a combination of applications that have been used by forensic examiners and investigators for years and have withstood scrutiny of many courts of law »*
  (Paladin - Sumuri)

Do we need specialists ?

- To explain « How »
  - To investigation lead and magistrate
  - To react to cyber attacks
  - In front of court and jury
- To keep “in house” excellence
  - Following IT evolution
  - Be part and contribute in a network
- To explain “Why”
  - Suspects profiling
  - In front of court and jury

Intuition ?

intuitum, de *intueor,* look with attention



Education to intuition ?

- Process, regulations and standards
- Profiles with skills and competences
- Capacity building strategy

courses

= specialist

+ intuition

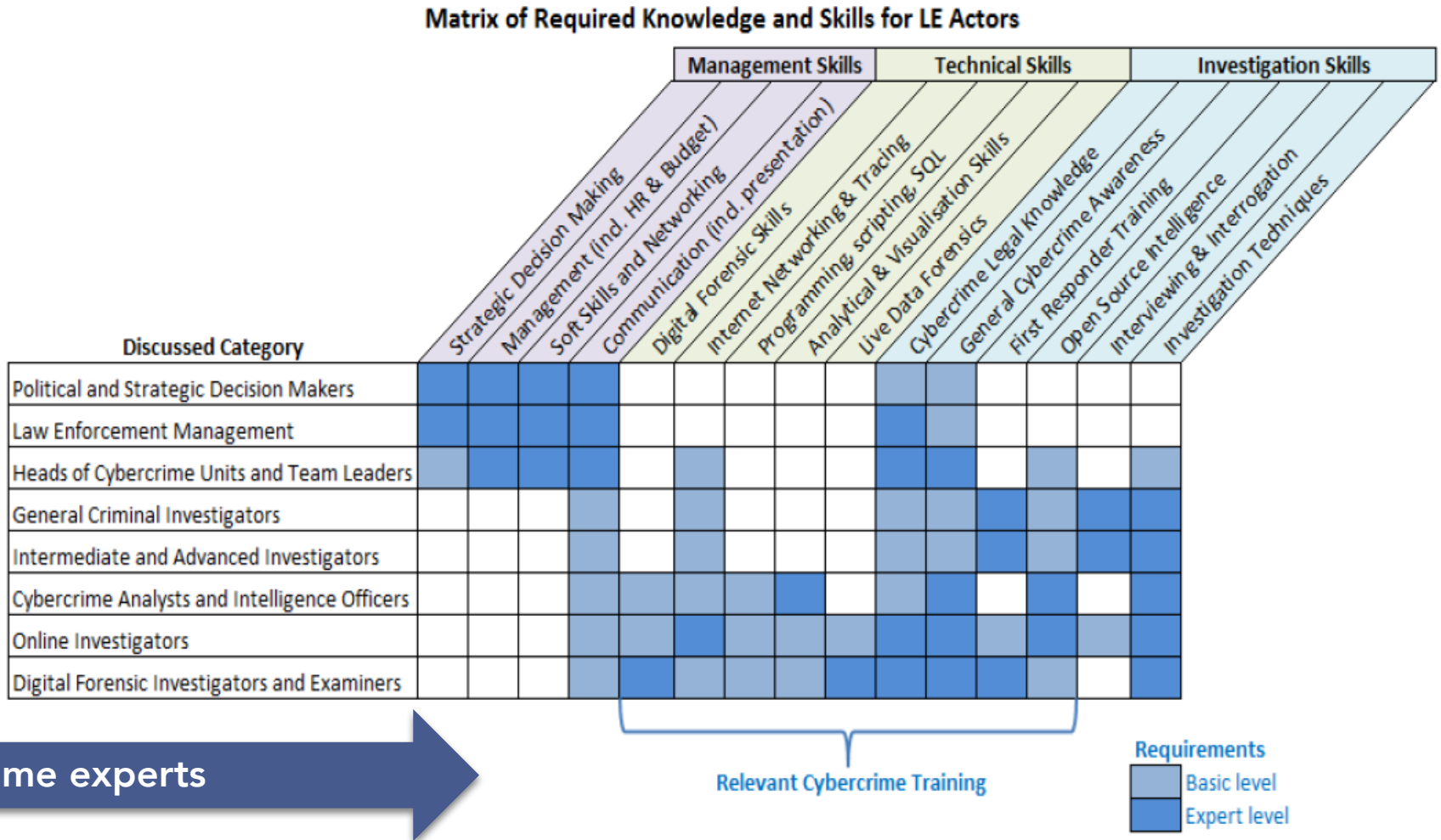
- Experience based
- Shared and validated by an expert networks

Continuous education

But certification are already existing !

- Or tool based
- Or Linked with a course (payment)
- Often presented as profiles framework

Training Competency Framework



Cyber crime experts

First responders

Five components:

- Training based on needs
- Addressing soft skills
- Create a sustainable expert network
- Collaboration with the academic world
  - Research and Development
  - Detect new trends
  - Validate competences by certification
- Implementation of a quality process

The digital evidence is an exception

- Difference between technical evidence and expert evidence ?
  - Live data forensics needs to take decisions
  - Chip-of is sometimes destructive
  - Cloud storage and IoT challenges
  - Cyber attacks and networks
- Reproducibility is not possible anymore
- Traces without interpretation are often useless
- How many DF certified labs ?

Certification challenges

- How to certify IT forensic labs or methods ?
  - Technology is always a challenge
  - JTAG or Chip-Of and destructive methods
  - Live data forensics becoming a standard especially for cyber-crime investigations

Only “good practices” can be defined and frequently updated.

Way to practitioners certification

"good practices" can be defined and have to be frequently updated.

We have to work on how good practices are applied :

- dissemination and training
- assessing practitioners
  - competences
  - skills

Way to practitioners certification

Existing national level recognition :

- only a few countries
- quickly outdated

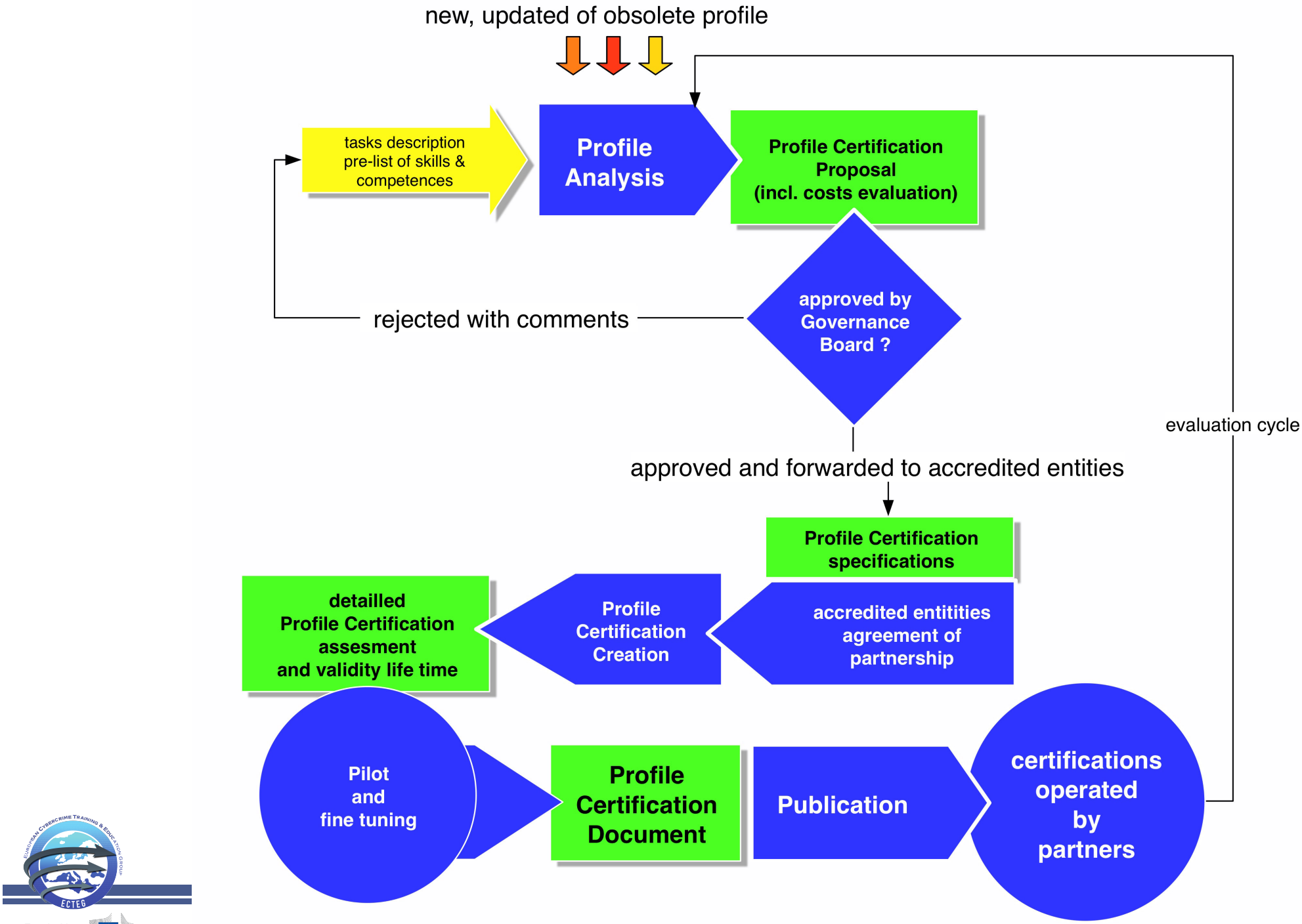
Existing "international" certifications :
(the rich driver license paradox)

- Based on "tool" knowledge
- Based on course attendance
- Competition model

Certification, registration and assessment of digital forensic experts
Peter Sommer (2011)

Practitioners certification model

- Using Training Competency Framework as backbone (profile based certification)
- Unlinked from the training
- Checking competences and skills
  - Theory & practice by academic partners
  - Internship for some profiles
- Limited validity 5 ≃ 3 years
- Transition from exiting ones
- Compatible with academic degrees (bachelor, master)
- Model created by TOT project (2014-2016)
  - Prosecutors, investigator judges, law enforcement, academics
  - Support from Europol, Eurojust and ECTEG



Funded by
European Commission

Global Cybercrime Certification Project

- Using Training Competency Framework as backbone (profile based certification)
- Unlinked from the training
- Checking competences and skills
  - Theory & practice by academic partners
  - Internship for most profiles
- Limited validity 5 ≃ 3 years
- Transition from exiting ones (i.e. IACIS)
- Compatible with academic degrees (bachelor, master)

Advantages

- Mutual recognition of expertise levels
- Valorisation of practitioners
- Harmonisation through EU
  - Profiles harmonisation
  - Defining procedures and standards
  - Practitioners network
  - Career path
  - Training attendees prerequisites
- Support to national structures
  - Addressing capacity building issues

Step forward – model implementation

- Already advised when :
  - Creating new profiles
  - Creating new training packages
- Governance board
  - Europol, CEPOL, Eurojust, ECTEG, EUCTF, …
  - Certifying body
  - Accreditation bodies organising certifications
- Certification organised by accredited bodies :
  - Implementation checked by governance board members

- First implementation 2017-2018 :
  Global Cybercrime Certification project
  including pilots

BACKGROUND: THE TOT PROJECT

- EU funded (2014-2016)
- Support from Europol, Eurojust and ECTEG
- UAM coordinator of the project, with other 5 institutions
- One of the results: **Framework for Certification.**

  - Cybercrime investigators and judicial authorities
  - Prosecutors, investigating judges, law enforcement, academics.
  - Basis for the development of a pool of professionals capable of correctly dealing with the transnational problems of cybercrime.
  - Taking into account different European countries (civil and common law).

THE PARTNERS

UNIVERSIDAD AUTONOMA DE MADRID

EUROPEAN CYBERCRIME TRAINING & EDUCATION GROUP
E.C.T.E.G

CNTI

UCD DUBLIN

Hochschule Albstadt-Sigmaringen University of Applied Sciences

* With the support of the Spanish Cybercrime Prosecutor's Office

ADDED VALUE

- Mutual recognition (all practitioners)
- EU (global?) harmonisation
- Well adapted to technology evolution
- Tool (vendor) and training neutral
- Partnership with academic world
- International database of experts

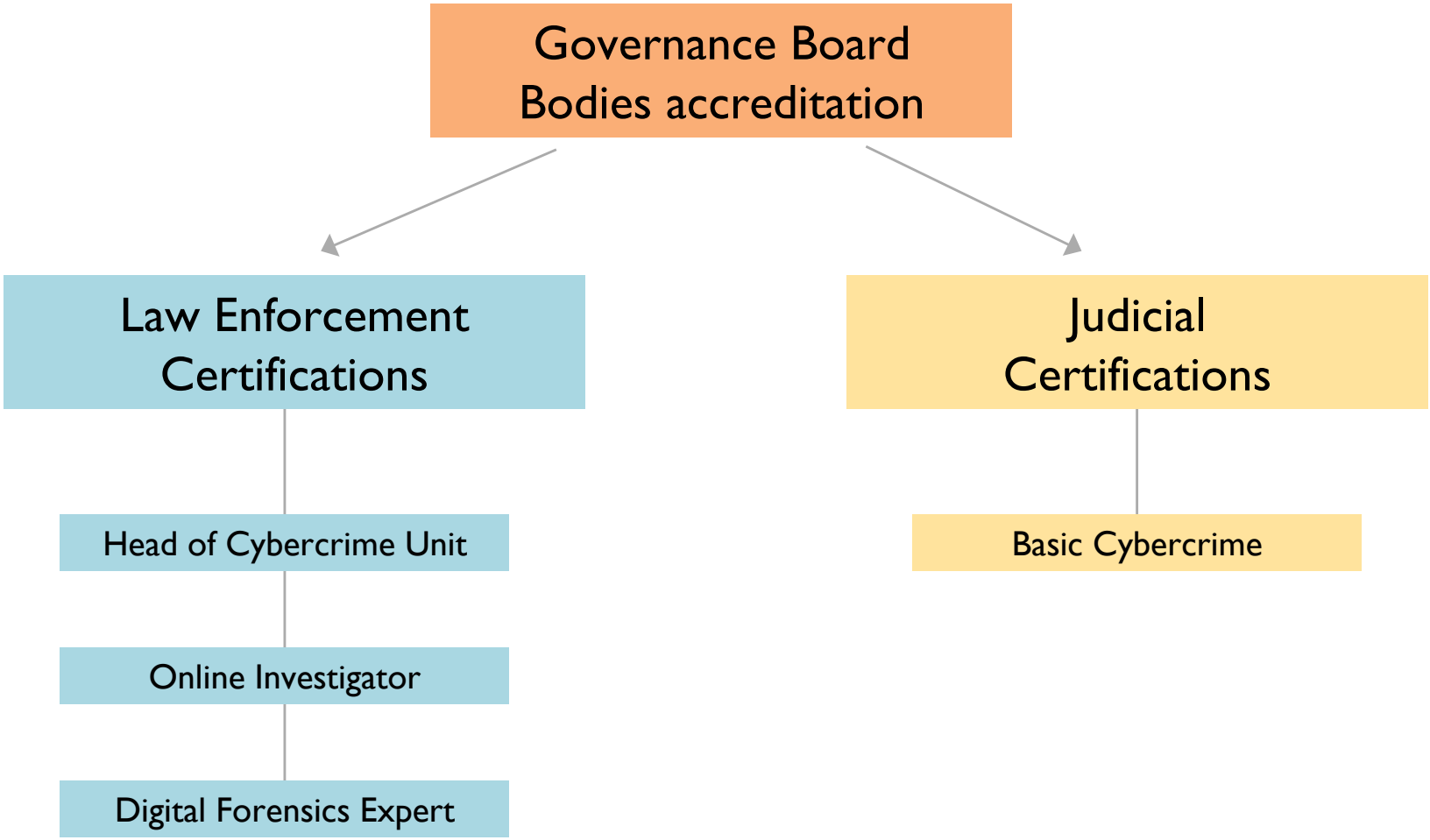
PRINCIPLES

- The certification will **not** be linked to any specific trainings, nor will the project deliver any training.

- The cost of certification is to be as cost-effective as possible.

- Given that the certificates will be competency-linked then assessment should be at pass/fail only.

STRUCTURE OF THE PROJECT

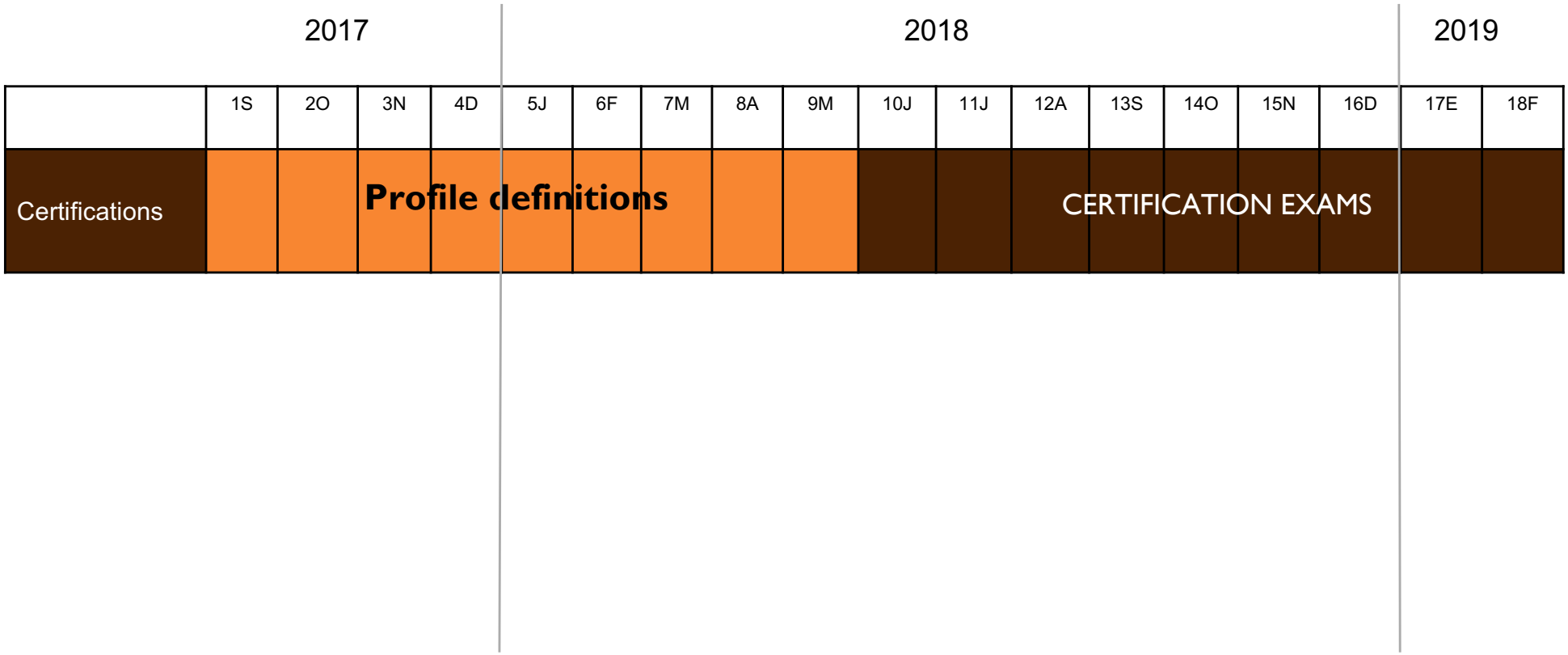


PILOTS

Certification	Duration	Travels Funded	Format	Editions
Head of Cybercrime Unit	One day	Yes	In-person	3 x12 participants
Online Investigator	Three days	No	In-person	3 x 5 participants
Digital Forensics Expert	One day	No	In-person	5 x 10 participants
Judicial Basic	One day	No	Online	3 x 20 participants

- All exams will be free of charge
- The exams will take place in different European countries

TIMELINE


2017
2018
2019
1S
2O
3N
4D
5J
6F
7M
8A
9M
10J
11J
12A
13S
14O
15N
16D
17E
18F
Certifications
Profile definitions
CERTIFICATION EXAMS

PROCESS FOR APLICATION

- The profile descriptions/requirements will be published
- Period for registering will be opened

- Acceptance of attendees
- Period for sending required documents will be opened
- Attendance to certification exams
- The results will be communicated and certifications granted

contact data

European Cybercrime Training and Education Group

- Yves Vandermeer
  yves.vandermeer@ecteg.eu
  twitter : @ecteg