



# Cyber Security and Digital Forensics Training Platform

Adrian Smales and Prof Bill Buchanan

Edinburgh Napier  
UNIVERSITY



ACONITE  
INTERNET SOLUTIONS



POLICE  
SCOTLAND  
Keeping people safe



Stockholm  
University



Institut "Jožef Stefan", Ljubljana, Slovenija



Partially funded by EU DG Home – Prevention Of and Fight against Crime

# DFET Project

- **Outline:** DFET creates new training methods/techniques to support judicial authorities, law enforcement agencies and associated stakeholders in the fight against cybercrime through the development of a virtual (cloud-based) cybercrime training environment to include real life simulation and scenario analysis.
- **Aim:** To improve crime detection rates by providing scenario-based training in line with the dynamic nature of cybercrime. Overall DFET aims to create a training infrastructure which can share cyber training across Europe, and allow access to hands-on environments, no matter the physical location of trainer.
- **Partial Funding:** DG Home – Prevention Of and Fight against Crime.
- **Partners:** Edinburgh Napier University, Joseph Stefan Institute (JSI), Stockholm University, Police Scotland, and Aconite Internet Solutions.
- **Dates:** Jan 2013 – Dec 2015.



# DFET Project Contribution

- Creation of a Cloud-based training infrastructure for Law Enforcement, Industry and Academia.
- Real-life virtualized practical sessions, with on-line support.
- Uses real-life devices, tools and systems.
- Credit rating of training against academic framework.
- Coverage of a range of subjects, including cryptography, network forensics, digital forensics, malware analysis, and so on.

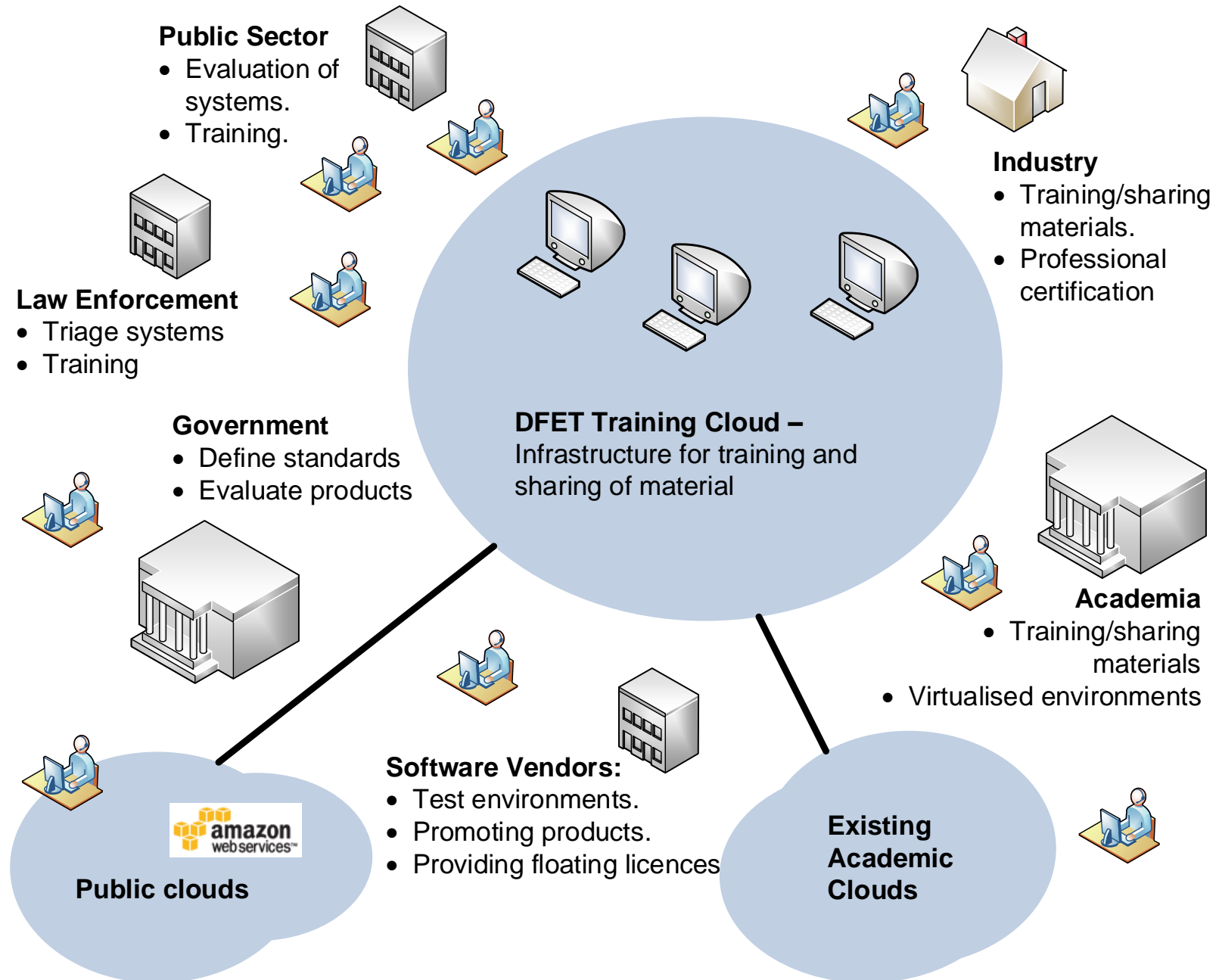


# Cyber Security and Digital Forensics Training Platform

## Vision and Features



# Vision



# Features

- Full coverage of cyber security.
- MSc integration.
- Fully virtualised practical environments.
- On-line lectures/demonstrations.
- Integration with Professional Certification.
- Ever changing challenges.
- Integrated feedback.
- On-site or remote training.



# Forthcoming Events

- Creation of **CyberFET.com** – On-line material with Cloud integration.
- Creation of **The Cyber Academy** (launch 6 May 2015). Supported by a wide range of organisations, including Scottish Government, Standard Life, Lloyds, and many others.
- Roll-out of training material from Sept 2015.





# Cyber Security and Digital Forensics Training Platform Architecture

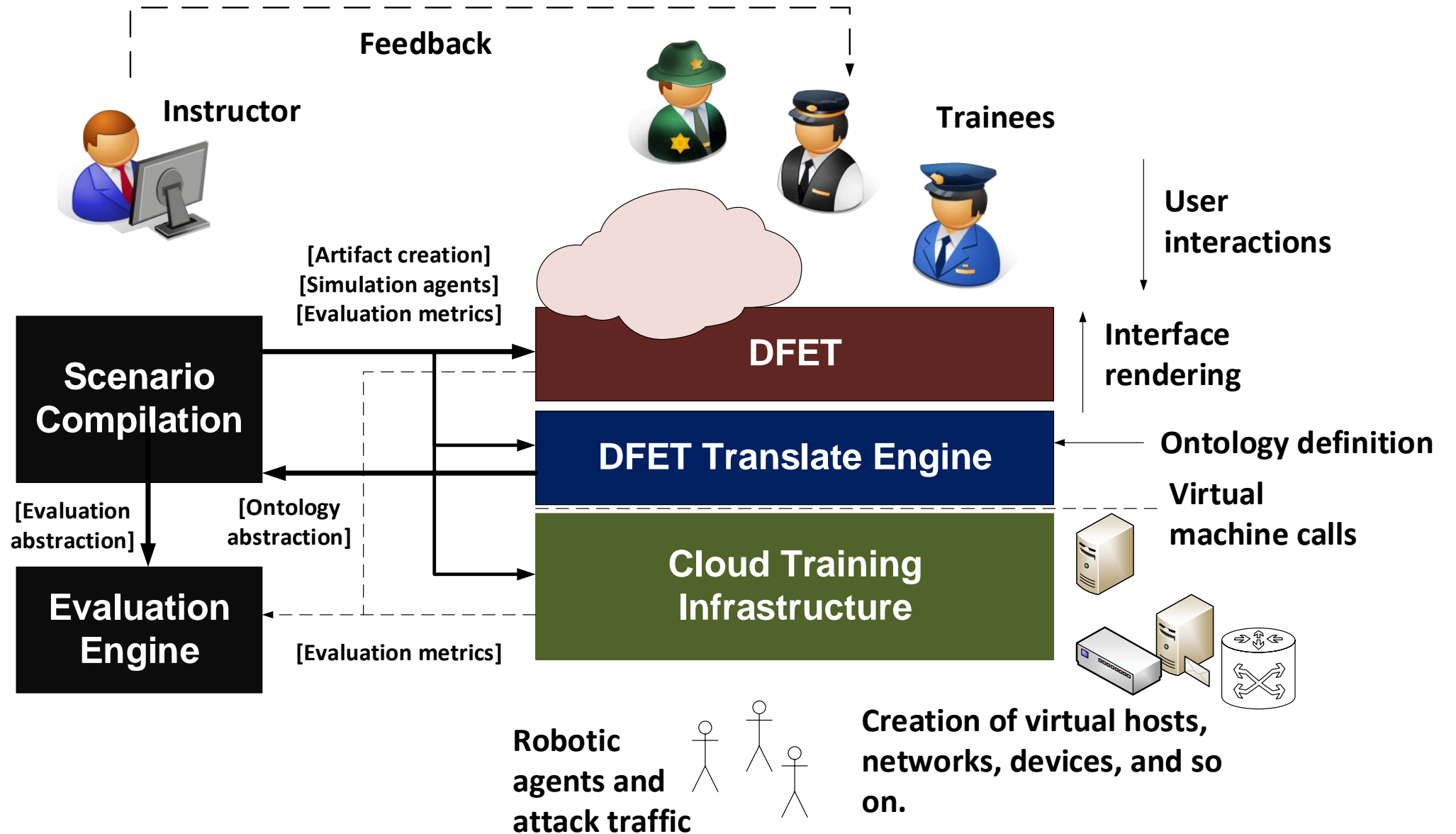


Partially funded by EU DG Home – Prevention Of and Fight against Crime

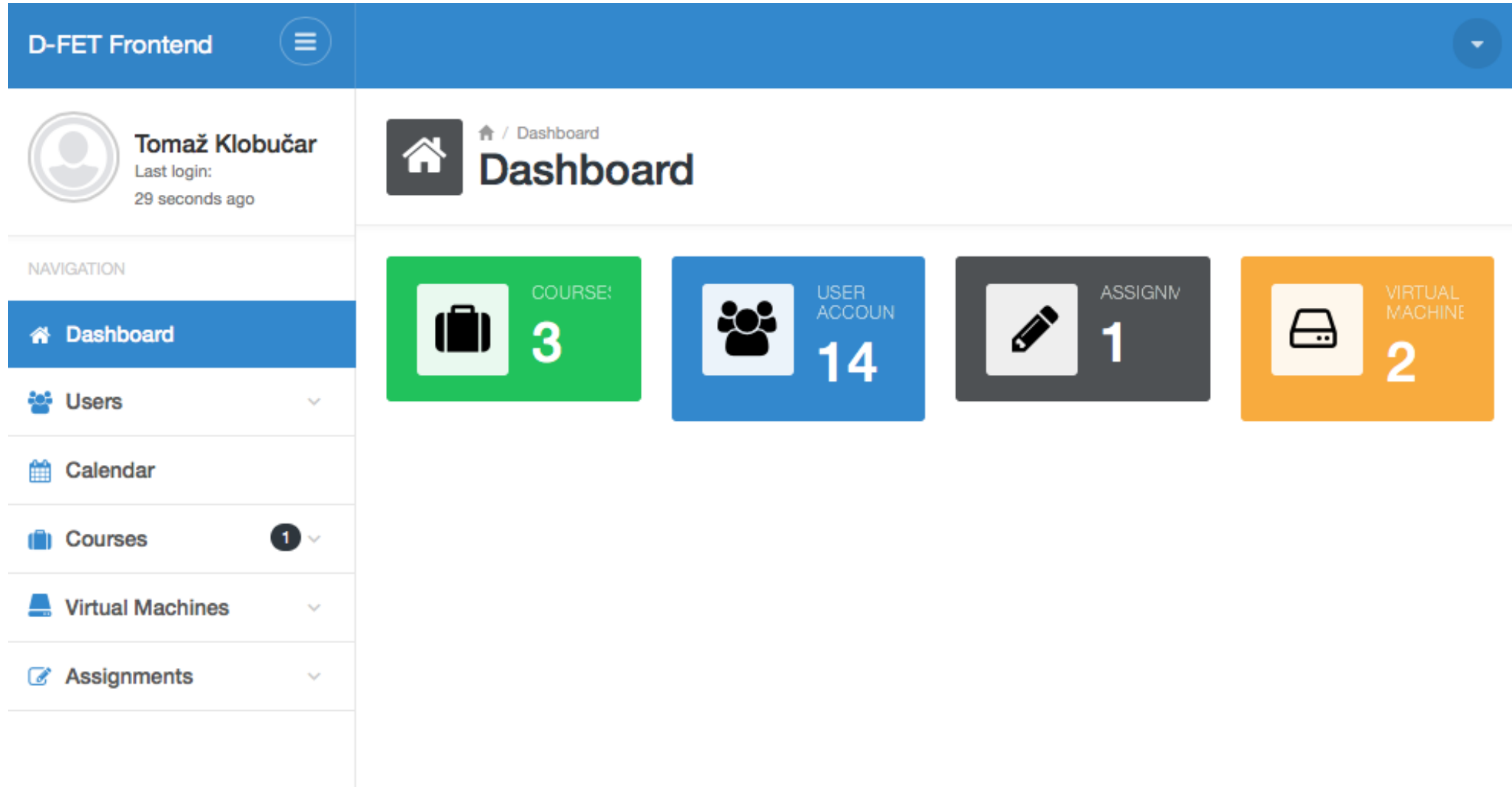




# DFET Architecture



# DFET EDUFORS Platform



**D-FET Frontend**

**Tomaž Klobučar**  
Last login: 29 seconds ago

**Dashboard**

NAVIGATION

- Dashboard
- Users
- Calendar
- Courses **1**
- Virtual Machines
- Assignments

**COURSE!**  
3

**USER ACCOUNT**  
14

**ASSIGNMENT**  
1

**VIRTUAL MACHINE**  
2

# DFET EDUFORS Platform

## Phishing Scenario

[Open Console](#)[Reset Console](#)

 **Note:** Use HD2 Disk in X-Ways.

**Description of attack:** An attacker tried to gain access to the web hosting server using brutforce tool. Through ssh he gained access to the server, where he explored the environment (mysql, apache etc.) for possible useful information. Attacker uploaded website and left it running for a while and gained victims data. At the end he deleted his uploaded data. Find the correct answers below.

- Choose correct attacker IP:
- 133.240.139.53
  - 207.40.75.93
  - 132.253.0.70

- Choose correct date of attack:
- 2010-03-16 10:06:00
  - 2009-11-24 04:46:00
  - 2009-11-24 18:16:00

- Choose stolen data:
- user passwords
  - personal photos
  - credit cards

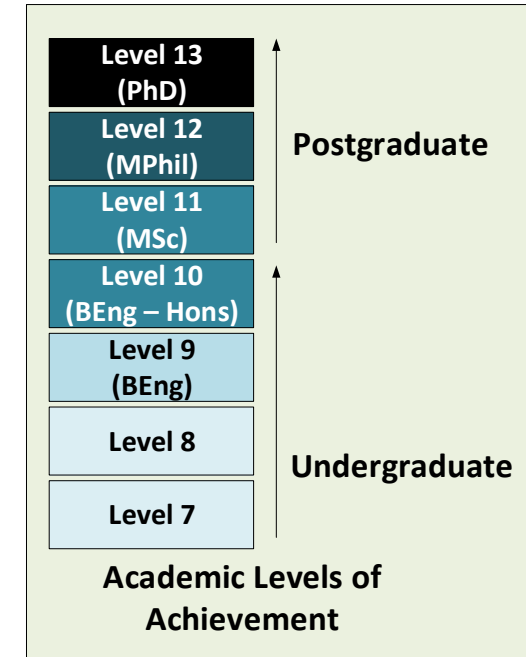
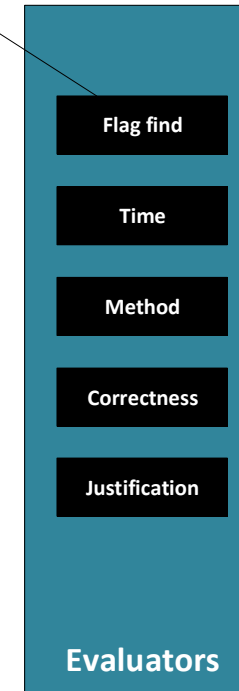
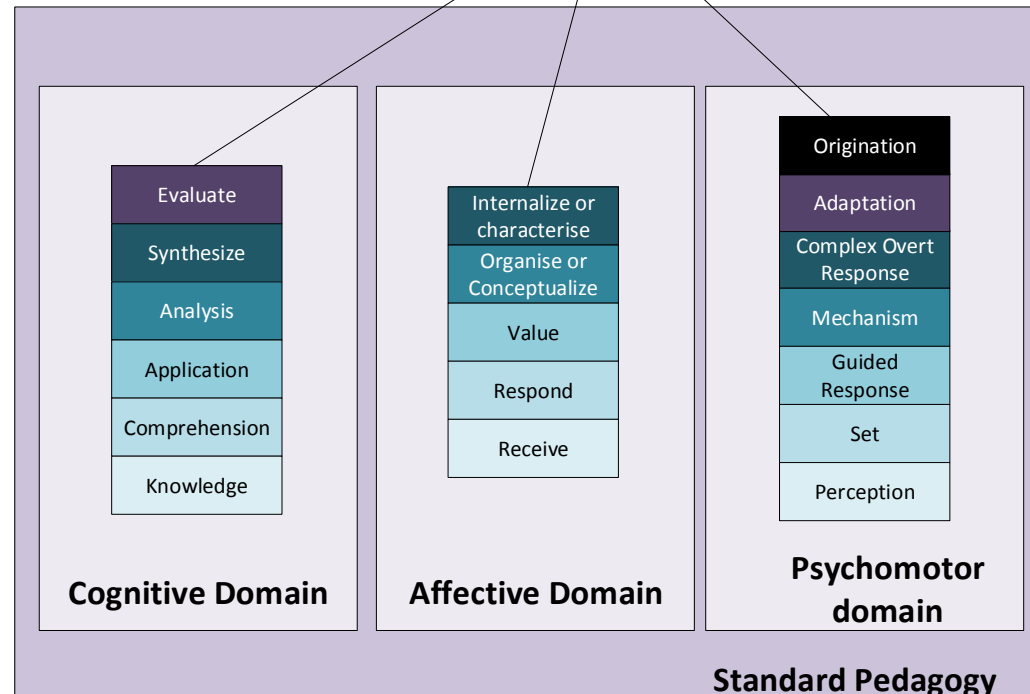
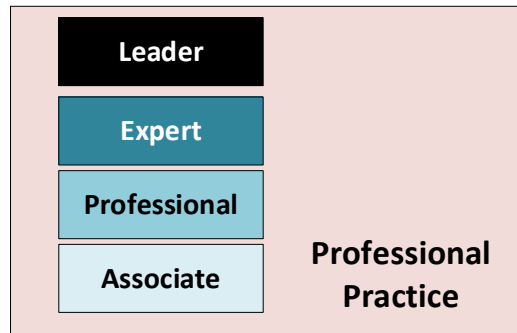


# DFET Pedagogy Mapping



Top-level script definition (Instructor created)

Abstract Pedagogy and Scripting  
 [Scenario] has [Learning Elements] which are assessed by  
 [Metric Evaluators] with [Metric Grades]



# Cyber **FET.com**

## Cyber Security and Digital Forensics Training Platform

Edinburgh Napier  
UNIVERSITY



ACONITE  
INTERNET SOLUTIONS



**POLICE  
SCOTLAND**  
Keeping people safe



Stockholm  
University



Institut "Jožef Stefan", Ljubljana, Slovenija



Partially funded by EU DG Home – Prevention Of and Fight against Crime

# CyberFET.com

- **Subjects:** Network and Live Forensics; Security Fundamentals; Cryptography; Malware Analysis; Security Architectures; Data Loss Prevention; Open Source Investigations; Security Risk and Compliance; Cyber Crime; Host-based Forensics; Mobile Device Forensics; Penetration Testing; Incident Response; and Law and Ethics.
- 14 books released to support on-line material.
- Each subject has six teaching elements. 3 hr training elements. Each element with Lecture, Test and Practical Lab.
- Formal test taking with score fed back to student/instructor.
- Virtualised challenges with ever changing challenges.
- New courses being created: DDoS Investigation, Mac Forensics.





# The Cyber Academy



# Aims

- Integrate **Teaching, Professional Practice** and **Research** into an advanced academic infrastructure.
- Provide **international leadership in Cyber Security**, especially related to education and professional development.
- Support the development of **flexible training programmes**, with academic credits.
- Support **innovation in Cyber Security** from the initial ideas, through funded PhD programs, and onto the end-product.
- Provide a platform for the debate and articulation of **key issues in Cyber Security**.
- Provide access to members to an **advanced and virtualized training infrastructure** for Cyber Security, for both evaluation and training.
- Provide integrated academic support for a range of roles from **Apprentice Cyber Security professionals to Advanced Research-focused levels**.
- Provide a mechanism for **increased interaction** between organisations and students.
- Integrate with the requirements of **law enforcement, industry and the public sector**.





# How will it work?

- **Collaborative and inclusive model.** The **Cyber Academy** is a partnership between academia, law enforcement, industry and the public sector, and aims to collaborate with a wide range of organisations on delivering on the key aims for the benefit of its partners.
- **Membership.** It is free to join the Academy at Associate-level, and which will allow organisations to be part of the infrastructure with support for a strong working relationship. Other levels of membership, such as around research and innovation sponsorship, are available and can be discussed with the team.
- **Dissemination.** The **Cyber Academy** will support a wide range of Conferences, Symposiums and Workshops, each focusing on key topics related to Cyber Security, with a special focus on Innovation, Professional Development and Education.
- **Professional Development.** The **Cyber Academy** integrates with a wide range of professional bodies, and aims to fully integrate academic structures with professional practice and training.





# Cyber Security and Digital Forensics Training Platform In Conclusion



# In Conclusion

- 6 May 2015 launch of **The Cyber Academy**.
- DFET Project looking for partners within the Academy.
- Raid the Flag/EU Cyber Team of the Year On-line Challenge. June 2015.
- October 2015 Symposium of Cyber Security Education – Police College, Tulliallan, Scotland.
- Full roll-out of Virtualised Training in Autumn 2015. Evaluators welcome.





# Cyber Security and Digital Forensics Training Platform

Adrian Smales and Prof Bill Buchanan

Edinburgh Napier  
UNIVERSITY



**POLICE  
SCOTLAND**  
Keeping people safe



Stockholm  
University



Institut "Jožef Stefan", Ljubljana, Slovenija



Partially funded by EU DG Home – Prevention of and Fight against Crime