cloud security alliance
EMEA Congress 2013
25-26th September 2013 // Edinburgh

Cyber Risks and Opportunities in the Cloud

Edinburgh Napier UNIVERSITY

Edinburgh Napier UNIVERSITY

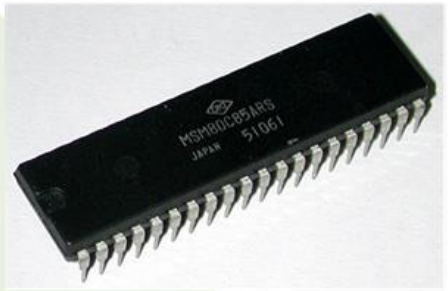
Risk, The Future and Trust

Towards The Next Generation

Prof Bill Buchanan (Twitter: @billatnapier, Web: asecuritysite.com)

Microchip

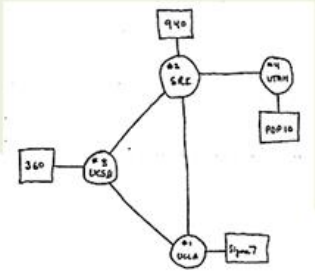
Transistor



Microprocessor

The Cloud

The Personal Computer



THE ARPA NETWORK

DEC 1969

4 NODES

The Internet

Cloud Computing

Cloud

Disruptive Techology

Terminals

Mainframe

Stand-alone computers

Computers connect to services (SoA)

Computers connected to servers

Servers

Edinburgh Napier UNIVERSITY

Cloud: The Future, Risk and Training

Introduction

Prof Bill Buchanan

Edinburgh Napier UNIVERSITY

Large demand for IT graduates

We architecture, we design, we analyse, we build, and we test

Why IT/Cloud?

There's lots of different jobs

- Networking.
- Security.
- Software Development.
- Media Design
- Mobile Devices
- Web Development.

New areas every day ...

- Cloud Computing.
- Big Data.
- Mobile Devices.

Edinburgh Napier UNIVERSITY

Data increases every day:

- 12TB of Tweets.
- 90% of all data in the Cloud produced in the last two years.
- 2,500,000,000,000,000 bytes of data produced every data 2.5 Quintillion Bytes – 1 billion hard disks

It's part of every aspect of our lives...

Why IT/Cloud?

Everything Is dependent on the Internet

- Banking.
- Oil and Gas.
- E-Commerce.
- Transport.
- … virtually everthing

It's all going digital:

- Data.
- Voice.
- Video/Images
- Sensors.

Edinburgh Napier UNIVERSITY

Areas:

- Networks.
- Operating Systems.
- People/Motivations.
- Application Software.
- Encryption/Identity.
- Mobile Devices.
- Wireless ...

It's about understanding everything ...

Computer Security and Digital Forensics

Every changing field

- New applications.
- New threats.
- Cloud and Mobility makes it an every great challenge.
- Lots of opportunities for different careers.

It's all going digital:

- Banking.
- On-line shopping.
- Media/News.
- Government.
- Health.

Edinburgh Napier UNIVERSITY

Tech Companies

It's part of most companies ...

Why Computing?

Finance Industry

... and lots of others

Edinburgh Napier UNIVERSITY

Strategic Big Data

- 12TB of Tweets.
- 90% of all data in the Cloud produced in the last two years.
- 2,500,000,000,000,000 bytes of data produced every data 2.5 Quintillion Bytes – 1 billion hard disks

Mobile Device Battles

In-memory Computing

Gartner Trend

Personal Cloud

Enterprise App Stores

Hybrid IT and Cloud Computing

Mobile Apps and HTML 5

Integrated Ecosystems

Internet of Things

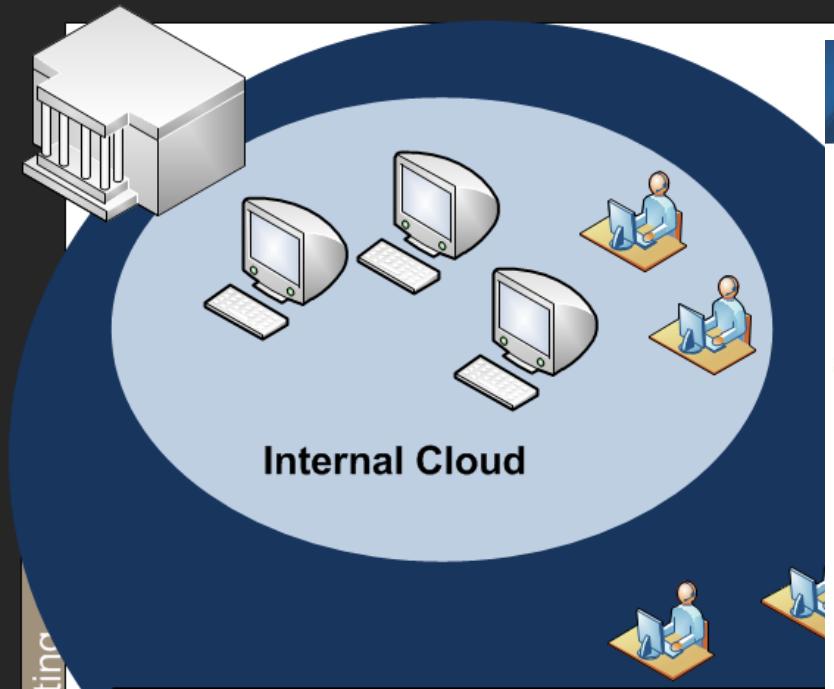
- All devices addressable

Edinburgh Napier UNIVERSITY

Cloud: The Future, Risk and Training

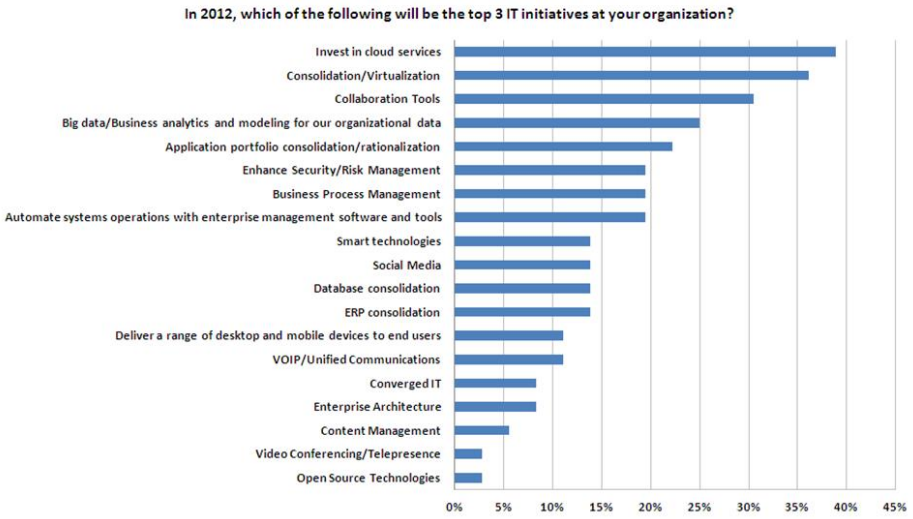
Risk

Prof Bill Buchanan



Top IT Initiatives for 2012

IDC Analyze the Future



Source: IDC CIO Agenda Survey, November-December, 2011
Data shows % of respondents who listed as a top 3 initiative. n= 36

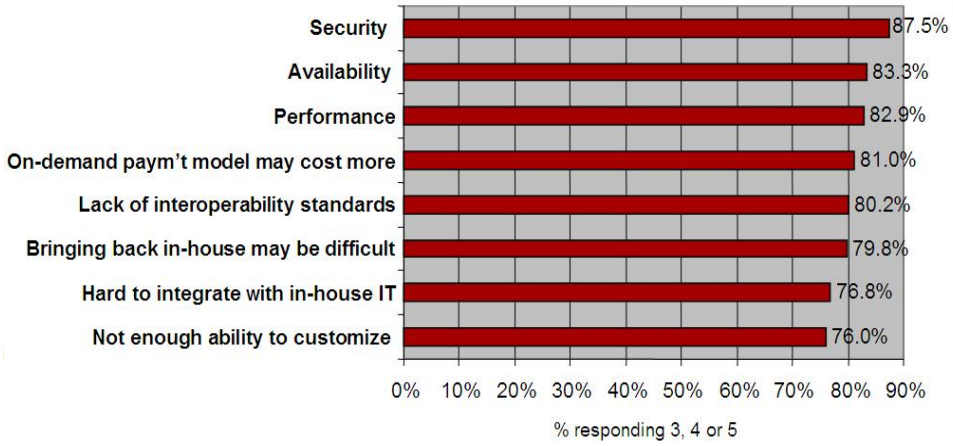
Feb-12 1

Cloud Computing

Cloud

Q: Rate the challenges/issues of the 'cloud'/on-demand model

(Scale: 1 = Not at all concerned 5 = Very concerned)



Source: IDC Enterprise Panel, 3Q09, n = 263

Audit/compliance

Can I be compliant with statutory and regulatory requirements?

- Where is my data stored?
- Who handles breach notifications?
- How long is my data stored for?
- How is eDiscovery handled?

Issues in the Cloud

Understanding Risk

What is … a threat … a risk … a vulnerability … the motivation?

- Wide range of threats to organisations.
- Organisations now highly dependent on their information infrastructure.
- Real-time threat analysis needed to cope with threats.

Risks

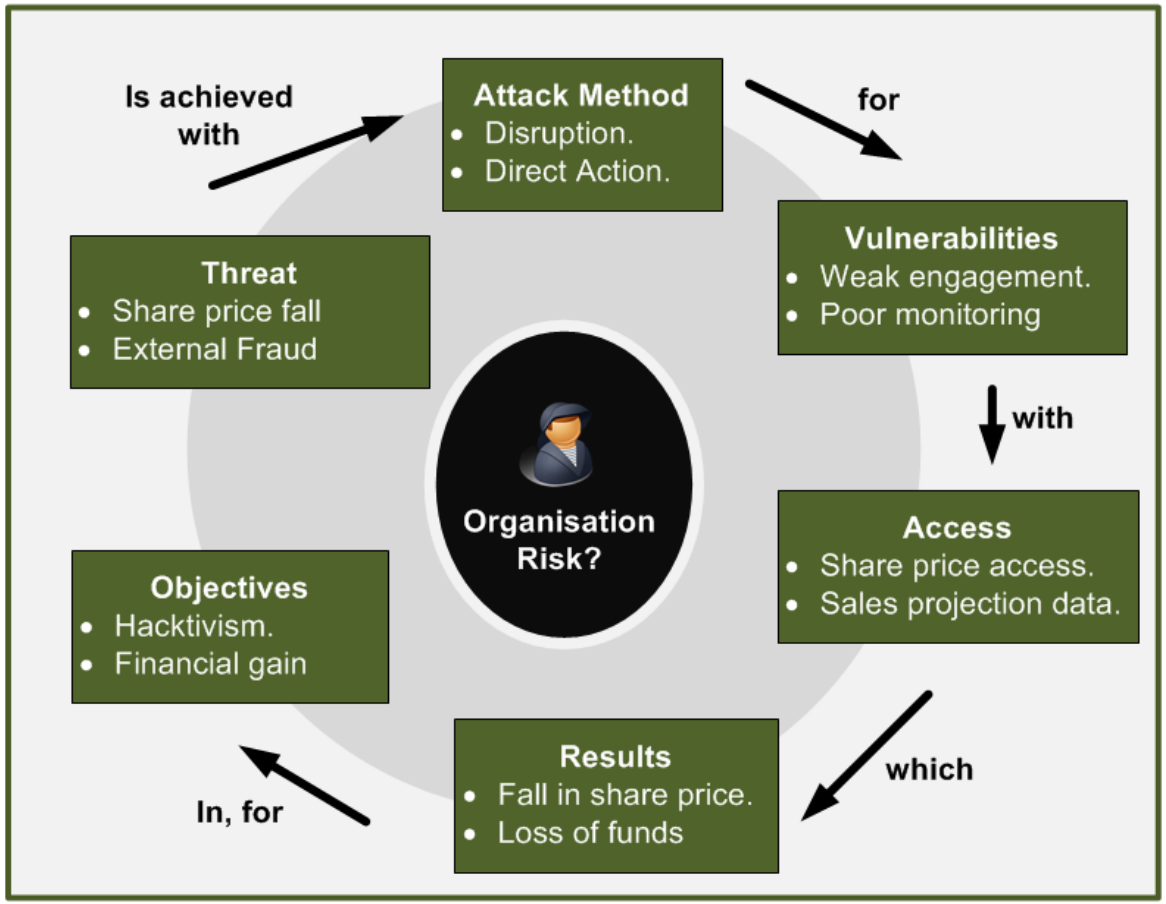
New Threats?

Risks … threats … vulnerabilities

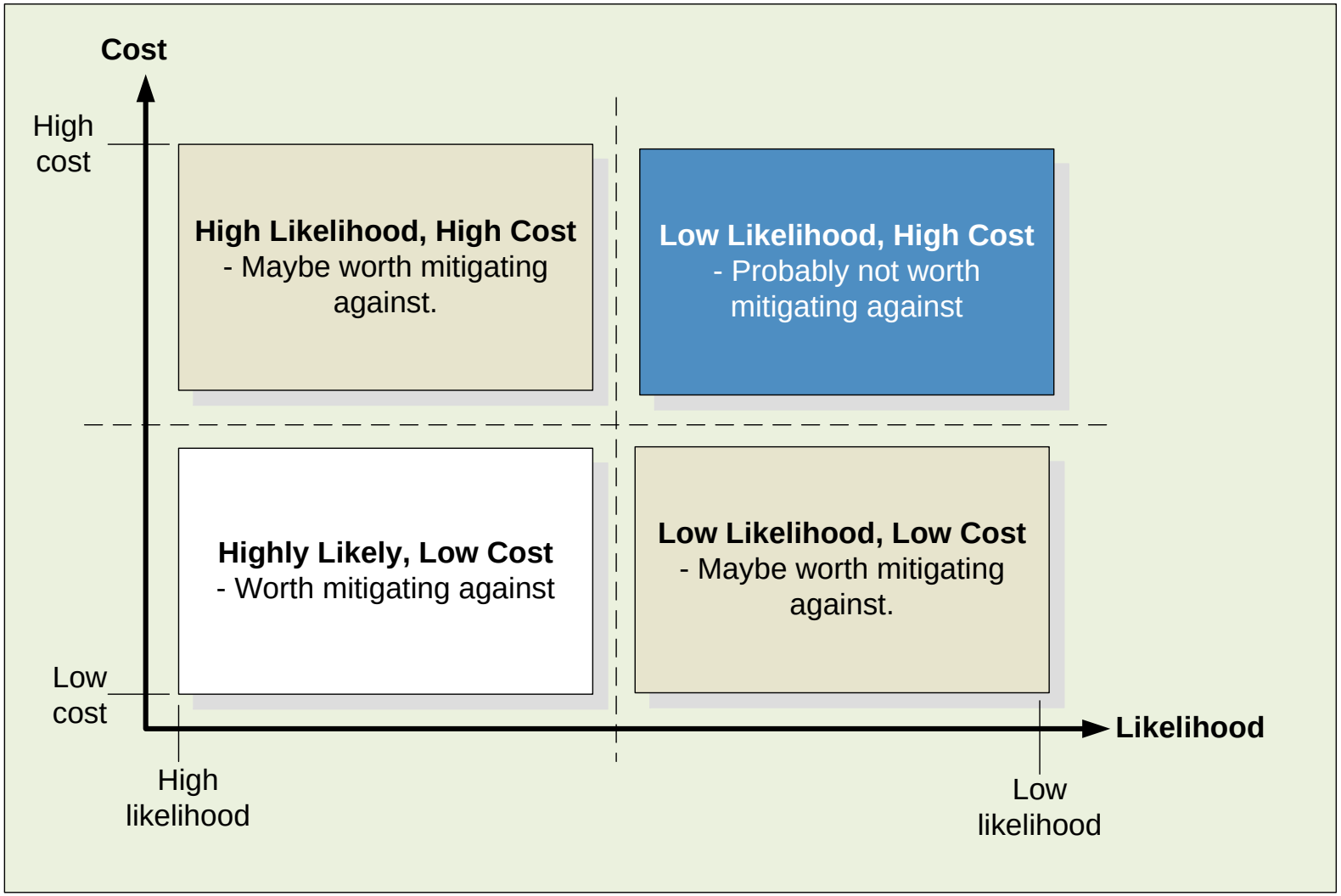
Understanding Risk

What is … a threat … a risk … a vulnerability … the motivation?

- Risk Taxonomy/Ontology required within the organisation.
- Business and Technical staff struggle to communicate on risk.



Get two risk management experts in a room, one financial and the other IT, and they will NOT be able to discuss risk. Each has **different context** ... **different vocabularies**, **definitions**, **metrics**, **processes** and **standards** (Woloch, 2006)

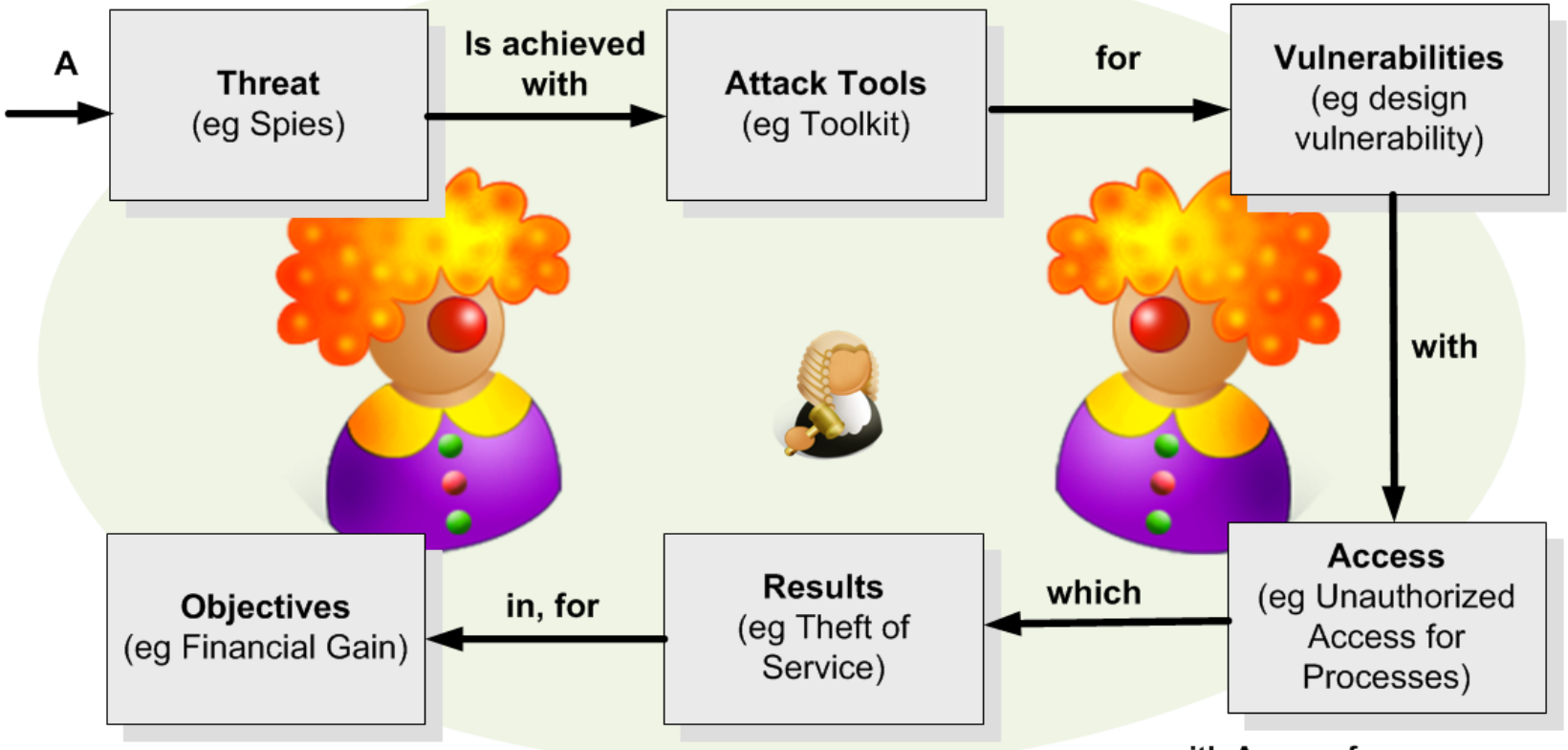


Author: Prof Bill Buchanan

A Threat:
- Hacker.
- Spies
- Terrorists.
- Corporate Raiders.
- Professional Criminals.
- Vandals.
- Military Forces.

is achieved with Attack Tools:
- User command.
- Script or program.
- Autonomous Agent.
- Toolkit
- Distributed Tool.
- Data Tap.

for Vulnerabilities:
- Implementation vulnerability.
- Design vulnerability.
- Configuration vulnerability.



for Objectives:
- Challenge/Status.
- Political Gain.
- Financial Gain.
- Damage.
- Destruction of an Enemy.

which Results in:
- Corruption of Information.
- Disclosure of Information.
- Theft of Service.
- Denial-of-Service.

with Access for:
- Files.
- Data in transit.
- Objects in Transit.
- Invocations in Transit.

Author: Prof Bill Buchanan

A cause or a fight?

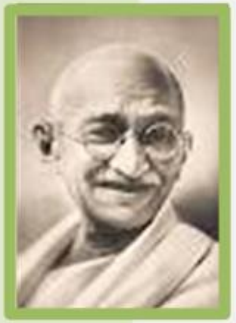
Who? … Why? …
Where? … When?

- One person's freedom fighter is another's terrorist.
- One person's cause is another person's fight.

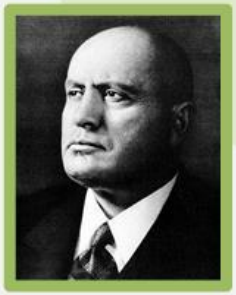
Martin Luther King

Che Guevara

Dalai Lama



Mahatma Gandhi



Benito Mussolini

Adolf Hitler

Cyber Hacktivism

Hacktivism

Who? … Why? … Where? … When?

- Attacks against an organisation for political reasons.
- Who?
- Why?
- Where?
- When?

2012 /2013

- New York Times brought down by Syrian EA hacktivist.
- Anonymous focus on India on censorship.
- Virgin Broadband over PirateBay block.
- SOCA (Serious and Organised Crime Agency) over arrests, also Norwegian Lottery and Bild.
- Home Office sites over Gary McKinnon case.

2009. Climate Research Unit of East Anglia University

Why: Emails published showed conspiracy to suppress data that contradicted their conclusions on global warming (Russian FTP server)

2011, HBGary

Why: HBGary were going after Anonymous
Reward: Emails published, Web site defaced.

2010, Mastercard and Visa

- Why: Decision to stop processing payments to the whistle-blowing site Wikileaks,
- Result: DDoS attacks on Visa, Mastercard, om.nl and politie.nl

2010, Australian Government.

Why: Australian Government's attempt to filter the Internet.

2012. Department of Justice and the FBI. Denial of service attack

2011, Tunisian government websites

- Why: Censorship of the Wikileaks documents
- Result: DDoS attacks against sites. Some Tounisians assisting in these attacks.

2011. Sony's PlayStation Network.

- Why: Sony were suing Geohotz, who jailbroke the PlayStation 3.
- Result: Afterwards, a group of hackers claimed to have 2.2 million credit card numbers from PSN users for sale

A few examples ...

Hacktivism

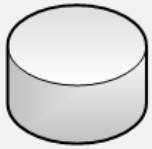
Who? … Why? …
Where? … When?

- Attacks against an organisation for political reasons.
- Who?
- Why?
- Where?
- When?

HBGary Federal CEO Aaron Barr to unmasked Anonymous with a list
HBGary contacts with NSA, Interpol, McAfee, and many others

Hbgaryfederal used CMS and comprised by:

http://www.hbgaryfederal.com/pages.php?pageNav=2&page=27



Username, passwords (stored as hash values), email database

Passwords broken by Rainbow tables

"ranger12"
"martin12"

CEO Aaron Barr and COO Ted Vera had weak passwords (six characters and two numbers) – which were easily broken

Passwords found for CEO and COO

A few examples …

Hacktivism

Who? … Why? …
Where? … When?

- Attacks against an organisation for political reasons.
- Who?
- Why?
- Where?
- When?

"ranger12"

"martin12"

CEO Aaron Barr and COO Ted Vera used the same password for a range of systems: Twitter, email, Linked in, and so on.

twitter LinkedIn Gmail by Google

Support.hbgary.com

Remote login to support.hbgary.com from Ted Vera's account

Flaw exploited in system to escalate privilege

Gigabytes of research and backup data

Aaron was a System Administrator for their Gmail Apps Hbgary account

Gmail by Google

Complete control of company email

A few examples …

Hacktivism

Who? … Why? …
Where? … When?

- Use strong passwords.
- Never re-use passwords (30% of users do).
- Patch systems.
- Watch out for social engineering.
- Beware of unchecked Web sites.
- Get an SLA from your Cloud provider.
- Don't store emails in the Cloud.
- Restrict access from outside.

Now for another site owned by Greg Hoglund, owner of HBGary

Social Engineering … to gain root password for Greg's site

Web site taken offline and user registration database published

A few examples ...

Edinburgh Napier UNIVERSITY

Cloud: The Future, Risk and Training

Training

Prof Bill Buchanan

Security policy

Organisation of information systems

Asset management

Human resources security

Critical Control 1: Inventory of Authorized and Unauthorized Devices
Critical Control 2: Inventory of Authorized and Unauthorized Software

Communications and Operational Management

Access Control

Critical Control 3: Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers
Critical Control 12: Controlled Use of Administrative Privileges
Critical Control 15: Controlled Access Based on the Need to Know

Physical and Environment Security

Critical Control 5: Malware Defenses
Critical Control 19: Secure Network Engineering

Information System Acquisition, Development and Maintance

Business Continuity Management

Compliance

Critical Control 8: Data Recovery Capability
Critical Control 17: Data Loss Prevention

Critical Control 4: Continuous Vulnerability Assessment and Remediation

Critical Control 20: Penetration Tests and Red Team Exercises

Critical Control 9: Security Skills Assessment and Appropriate Training to Fill Gaps

Author: Prof Bill Buchanan

Pen. Testing

Threats

Good...

... Bad

White Hat

Blue Hat

Grey Hat

Black Hat

Cracker

motivated by financial gain, and has criminal intent

Script kiddies

does not have many skills, and use standard scripting tools

Software Cracker

reverse engineer software applications

Phreakers

hacks telephone systems

Hacktvist

has a political agenda

Whacker

focuses on wireless LAN and WANs

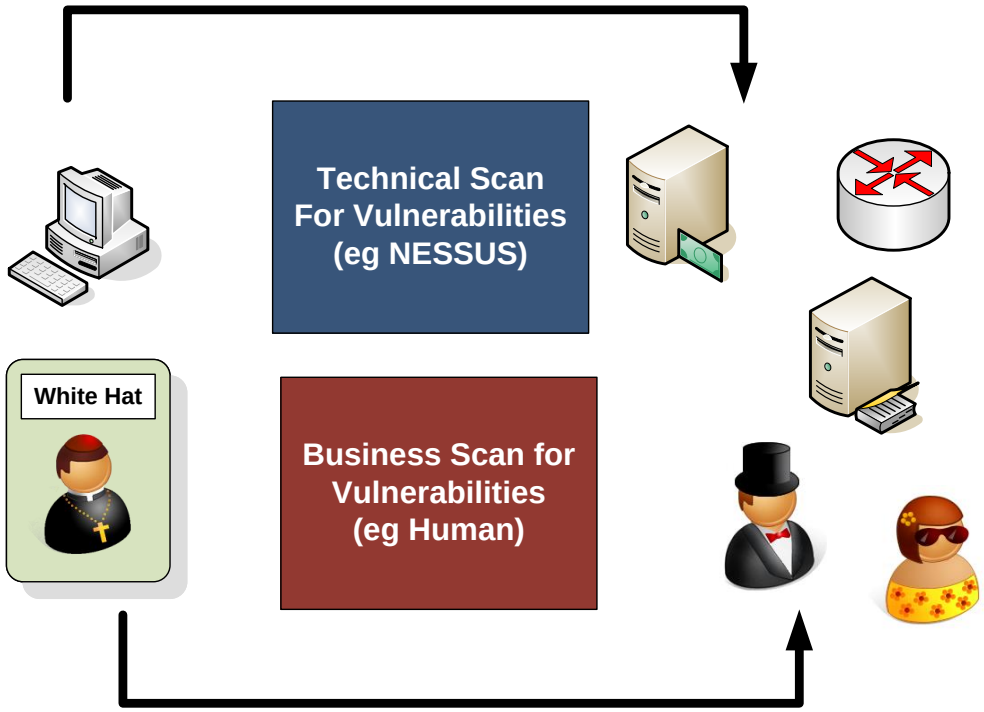
Author: Prof Bill Buchanan

Vulnerability

Threats

Automated Testing

- Port scanning.
- Malware detection.
- SQL Database Exploits.



Adversarial Role

- Social Engineering.
- Password Cracking.
- Data Theft.

Risks

Adverse Disclosure
Service Availability
Business Disruption
Damage to or Modification to Assets
Fraud/E-Crime
Reputational Damage
Legal and Regulatory Censure

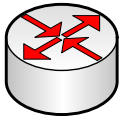
Threats

Malware
Hacking
Social
Misuse
Physical
Error
Environmental

Actor

Internal
External
Trusted Partner

Author: Prof Bill Buchanan



Technical Scan For Vulnerabilities (eg NESSUS)

Business Scan for Vulnerabilities (eg Human)

Adversarial Role

Adversarial Role

- Social Engineering.
- Password Cracking.
- Data Theft.

Vulnerability

Threats

Denial of Service

User Account Breach

Password Cracking

Physical Attack

Database Breach

Email Breach

SNMP Breach

Malware Install

Web Comprise

Backdoor Install

Spyware Install

SCADA Compromise

VoIP Compromise

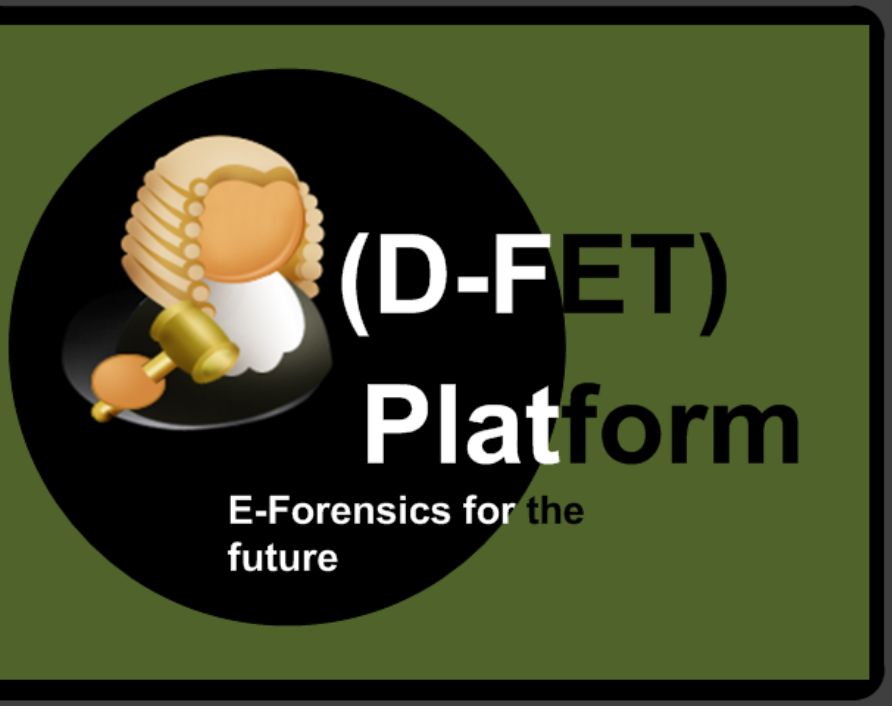
Cloud Compromise

Adverse Disclosure
Service Availability
Business Disruption
Damage/Modification of Assets
Fraud/E-Crime
Reputational Damage
Legal and Regulatory Censure

Risks

Author: Prof Bill Buchanan

Community Cloud



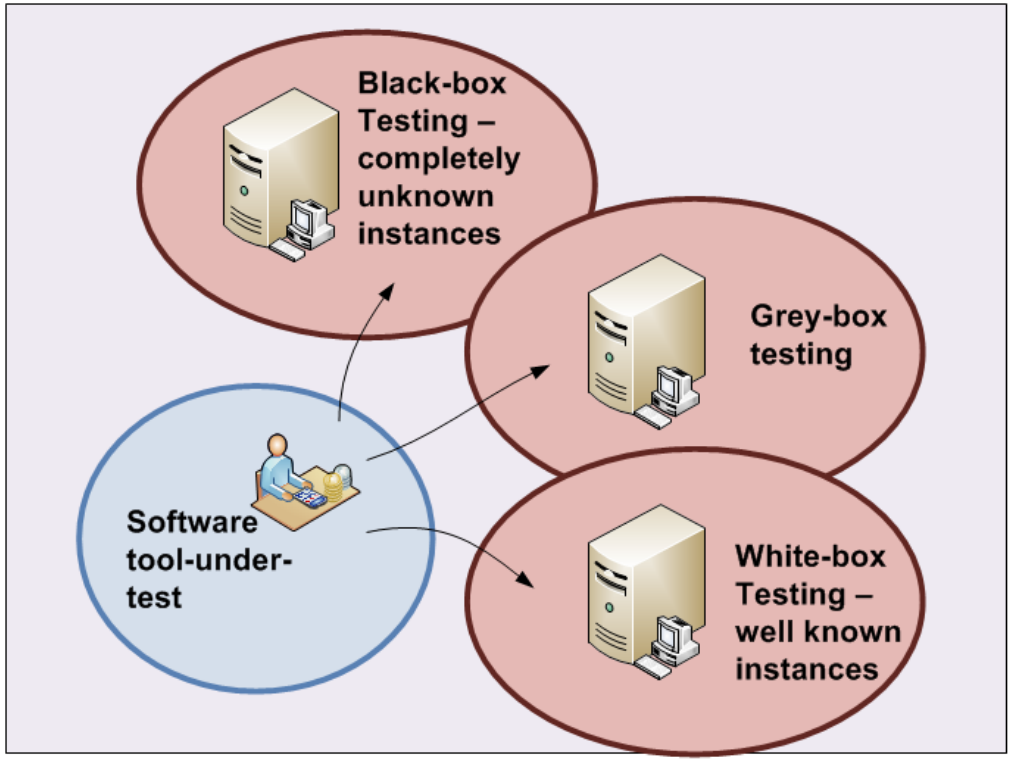
D-FET – A Community Cloud for Enhancing Skills using Virtualised Environments and Cloud-based Infrastructures

> D-FET – A Community Cloud

Author: Prof Bill Buchanan

Training Issues:

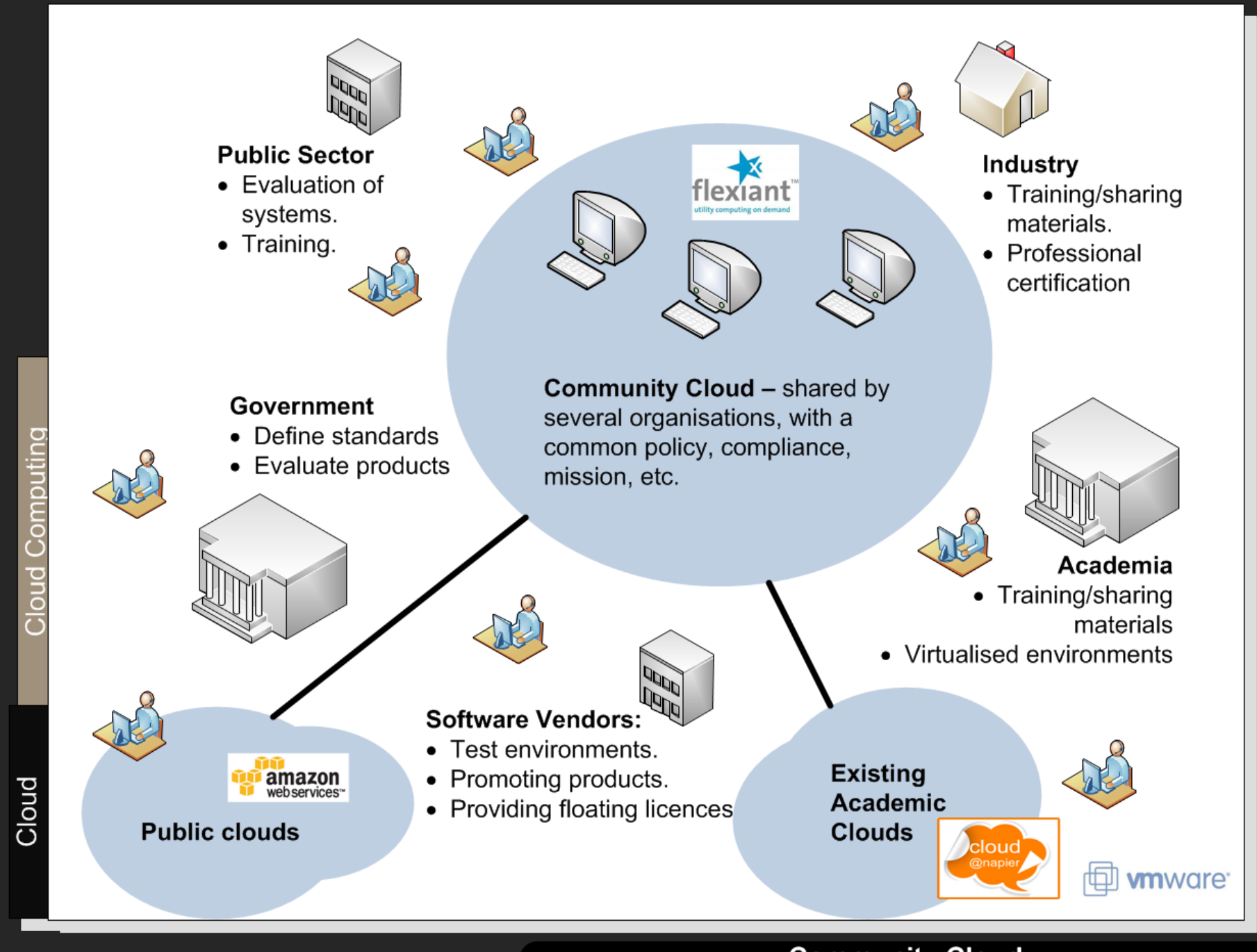
- Lack of standardized images of training.
- Lack of engagement from industry/law enforcement.
- Environment is fairly static and not changing.
- Students not exposed to a wide range of tools and environments.
- Lack on training on real-life environments.
- Physical location can restrict training opportunities.
- And so on.

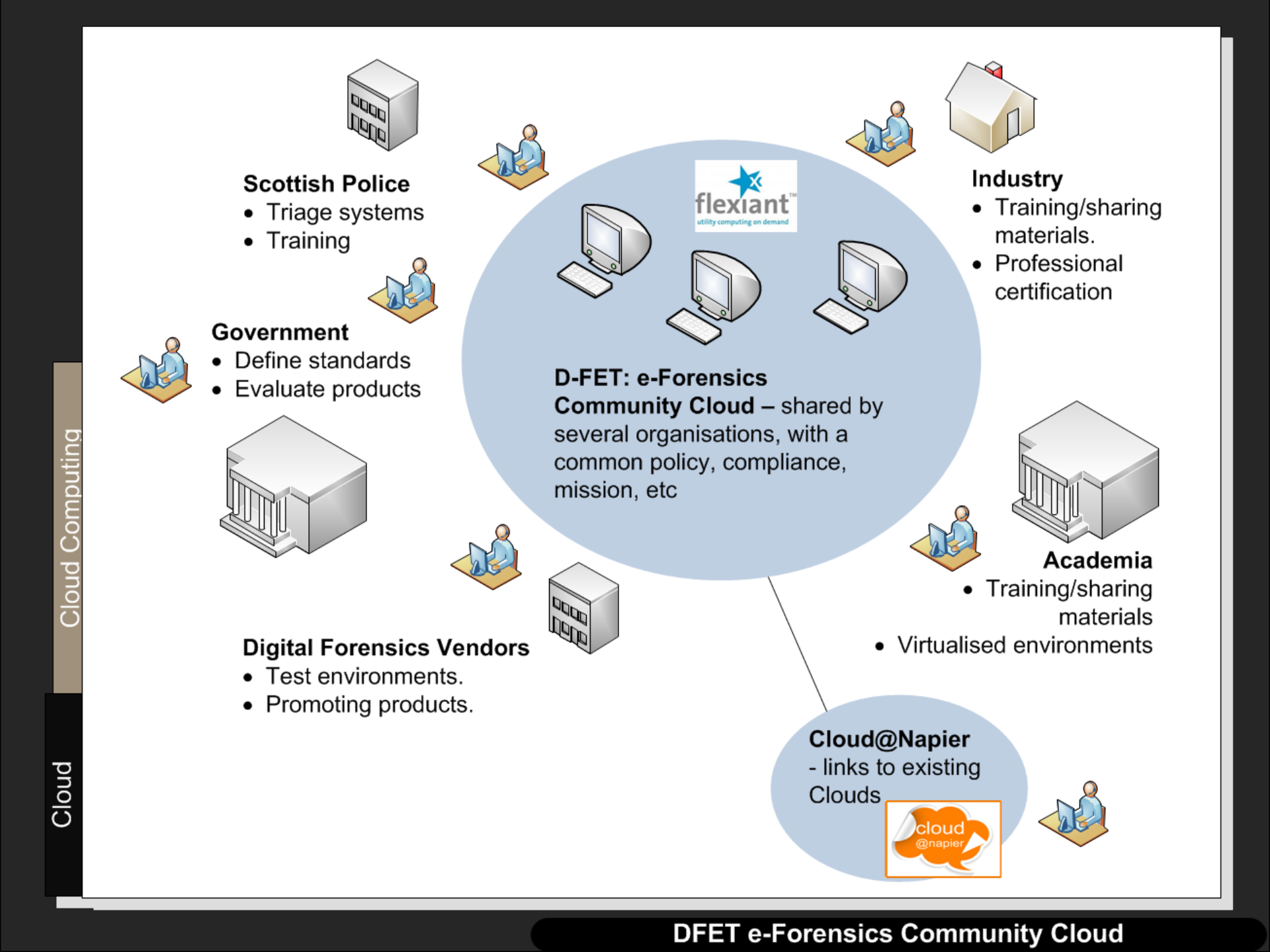


Validation Issues:

- Lack of validation for tools, especially for closed-source ones.
- No standardized framework for evaluation.
- Lack of repeatability.
- No standardization for the quality of digital forensics tools.
- Simulators suffer from not being realist enough.
- And so on.

Some of the issues in tool validation


Cloud Computing
Cloud
Public Sector
• Evaluation of systems.
• Training.
Industry
• Training/sharing materials.
• Professional certification
flexiant
utility computing on demand
Community Cloud – shared by several organisations, with a common policy, compliance, mission, etc.
Government
• Define standards
• Evaluate products
Academia
• Training/sharing materials
• Virtualised environments
Software Vendors:
• Test environments.
• Promoting products.
• Providing floating licences
amazon web services
Public clouds
Existing Academic Clouds
cloud @napier
vmware
Community Cloud


Cloud Computing
Cloud
Scottish Police
• Triage systems
• Training
Government
• Define standards
• Evaluate products
flexiant
utility computing on demand
D-FET: e-Forensics Community Cloud – shared by several organisations, with a common policy, compliance, mission, etc
Industry
• Training/sharing materials.
• Professional certification
Academia
• Training/sharing materials
• Virtualised environments
Digital Forensics Vendors
• Test environments.
• Promoting products.
Cloud@Napier
- links to existing Clouds
cloud @napier
DFET e-Forensics Community Cloud

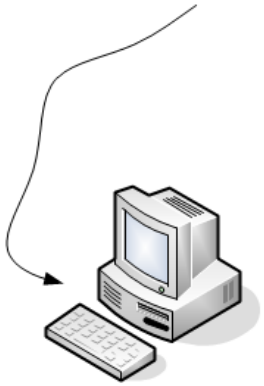
White Hat

Good...

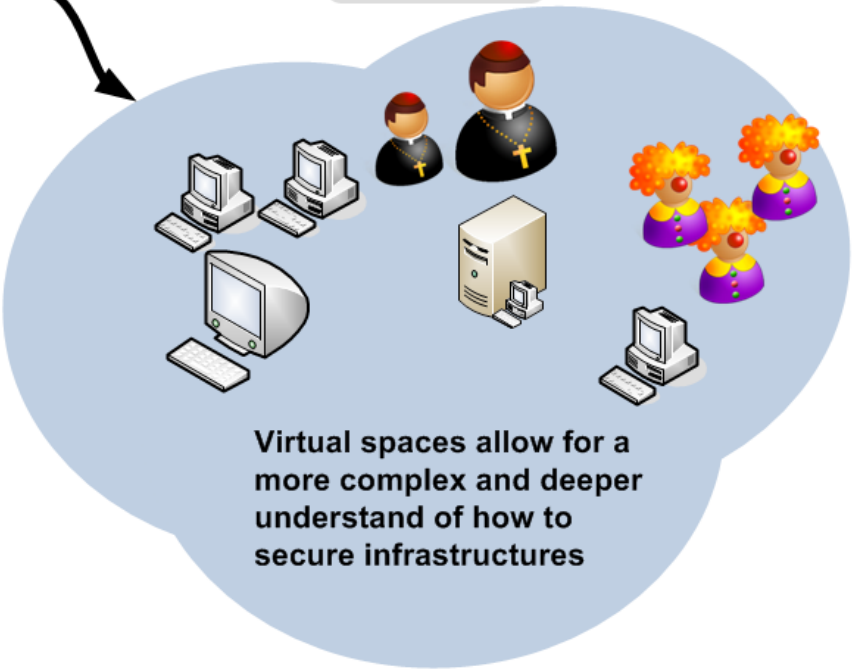
... Bad

Black Hat

Grey Hat



Difficult to use many of the techniques within a real-life space

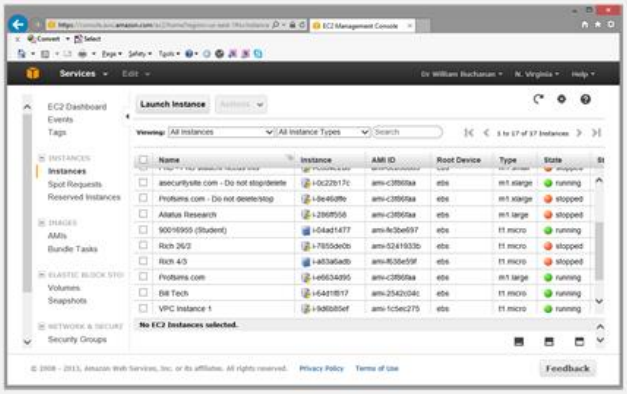


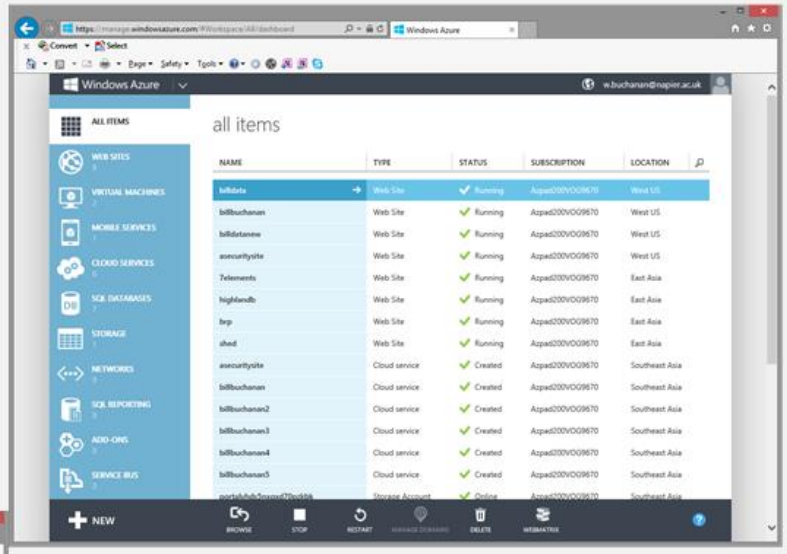
Virtual spaces allow for a more complex and deeper understand of how to secure infrastructures

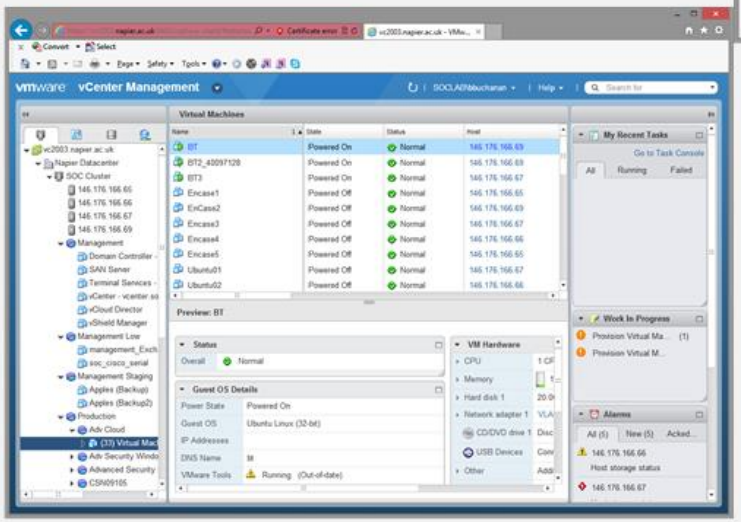
Demands on professional certification

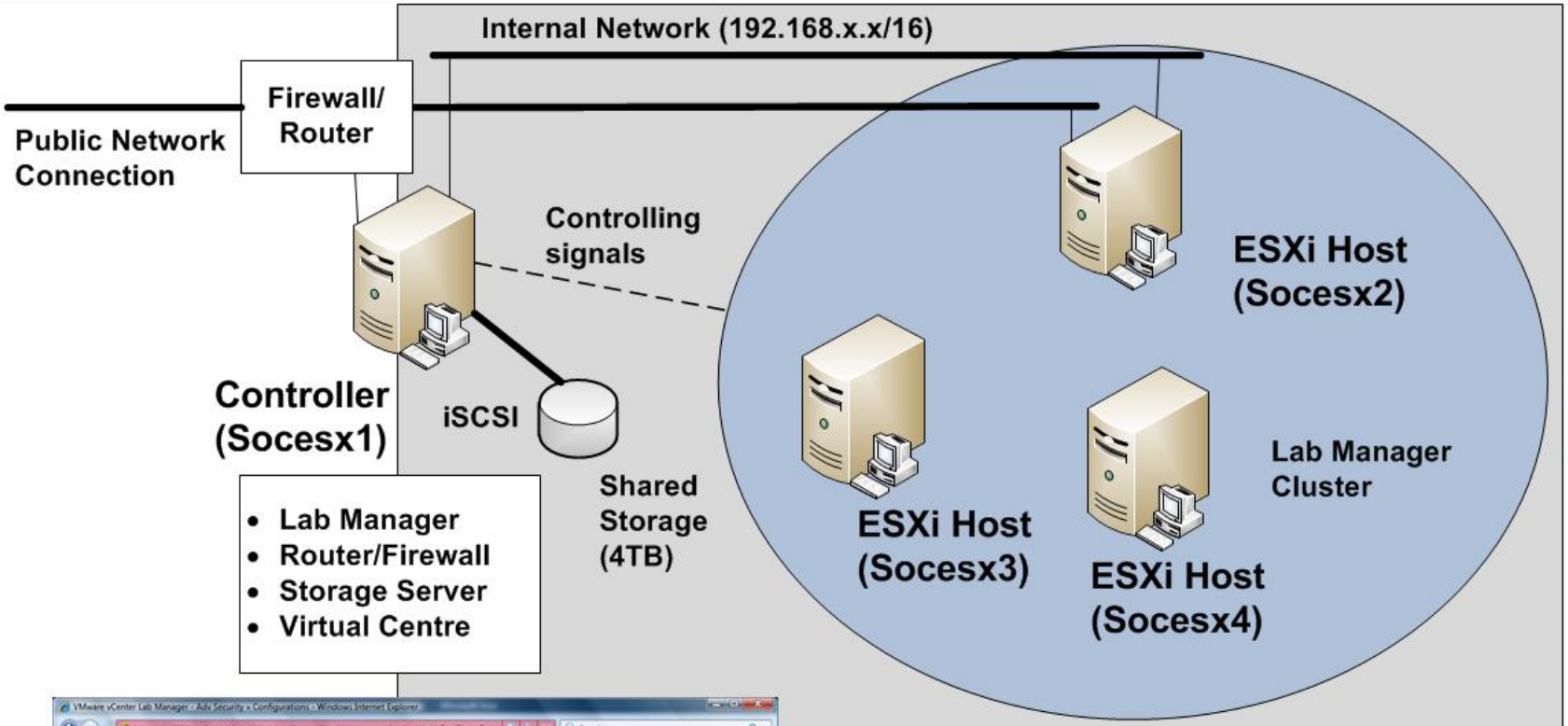
Employers now require in-depth knowledge and a range of skills

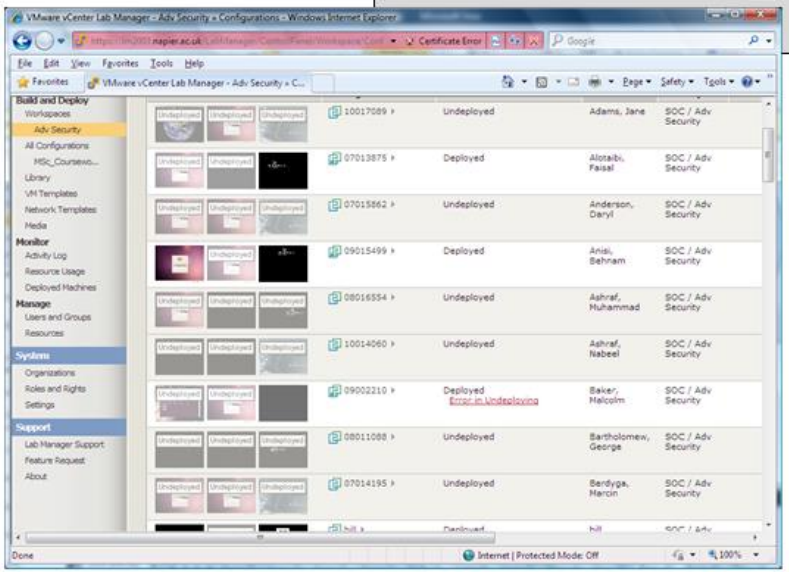
Edinburgh Napier UNIVERSITY











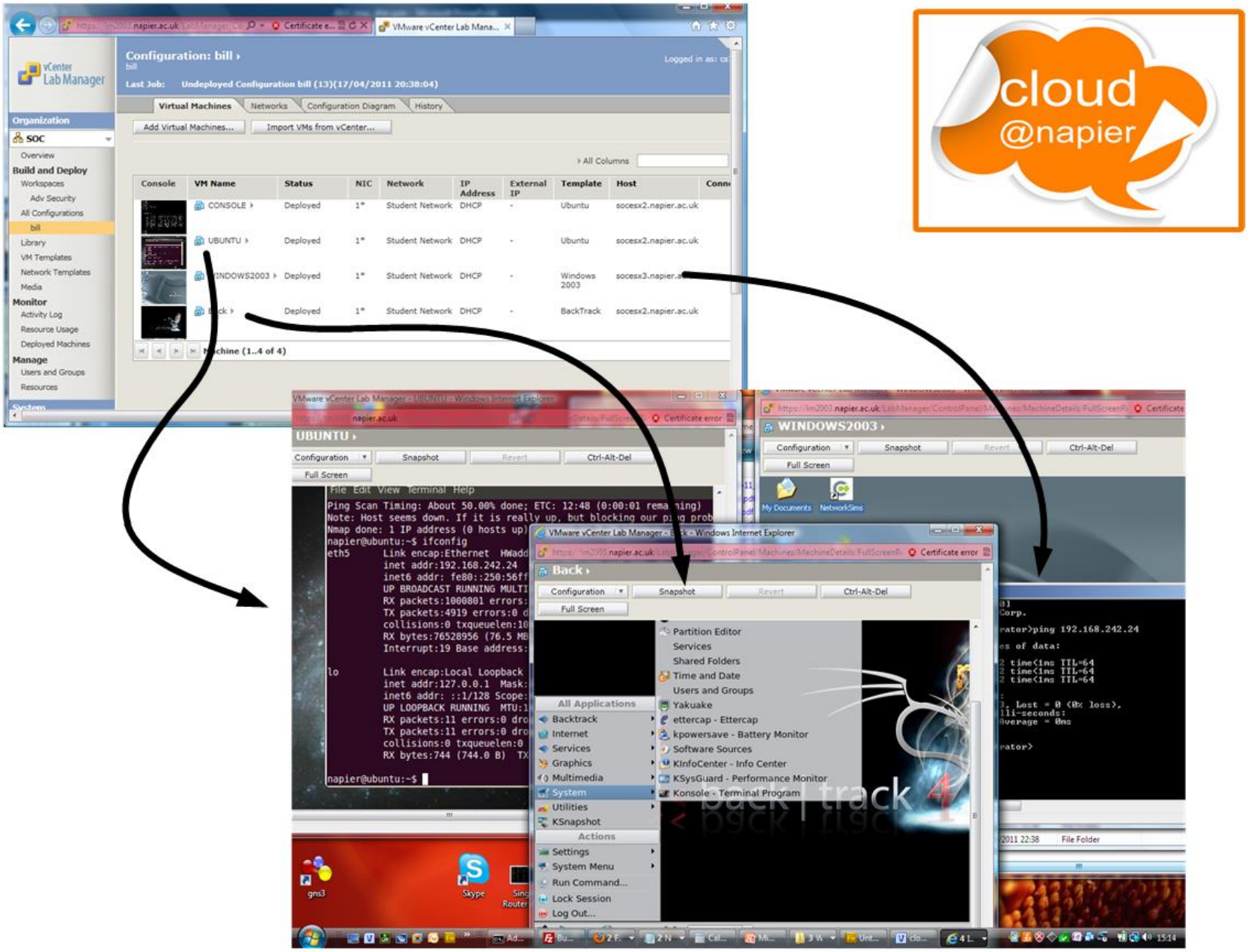
vCenter

Cloud

vmware

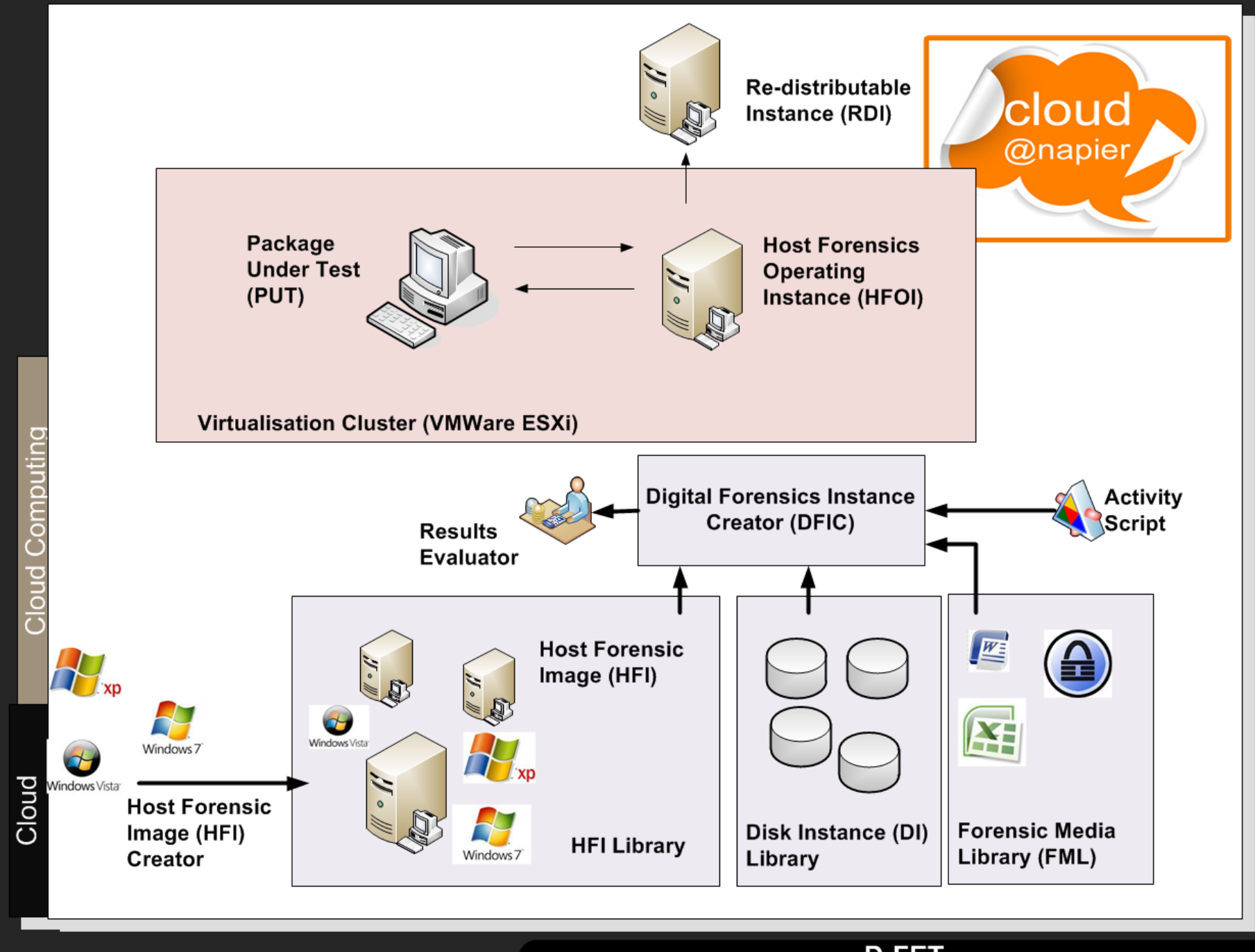
cloud
@napier

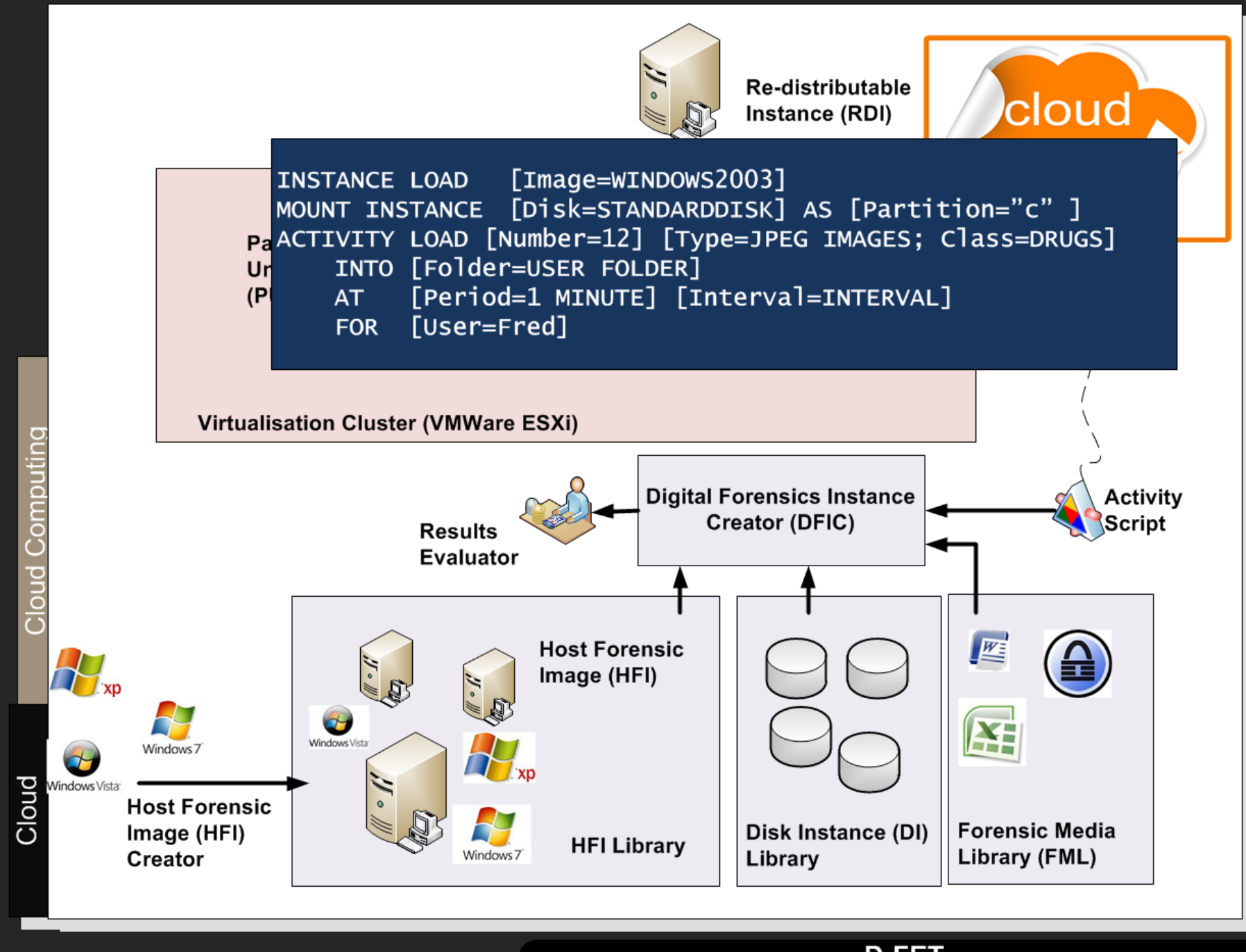
Napier vCenter infrastructure

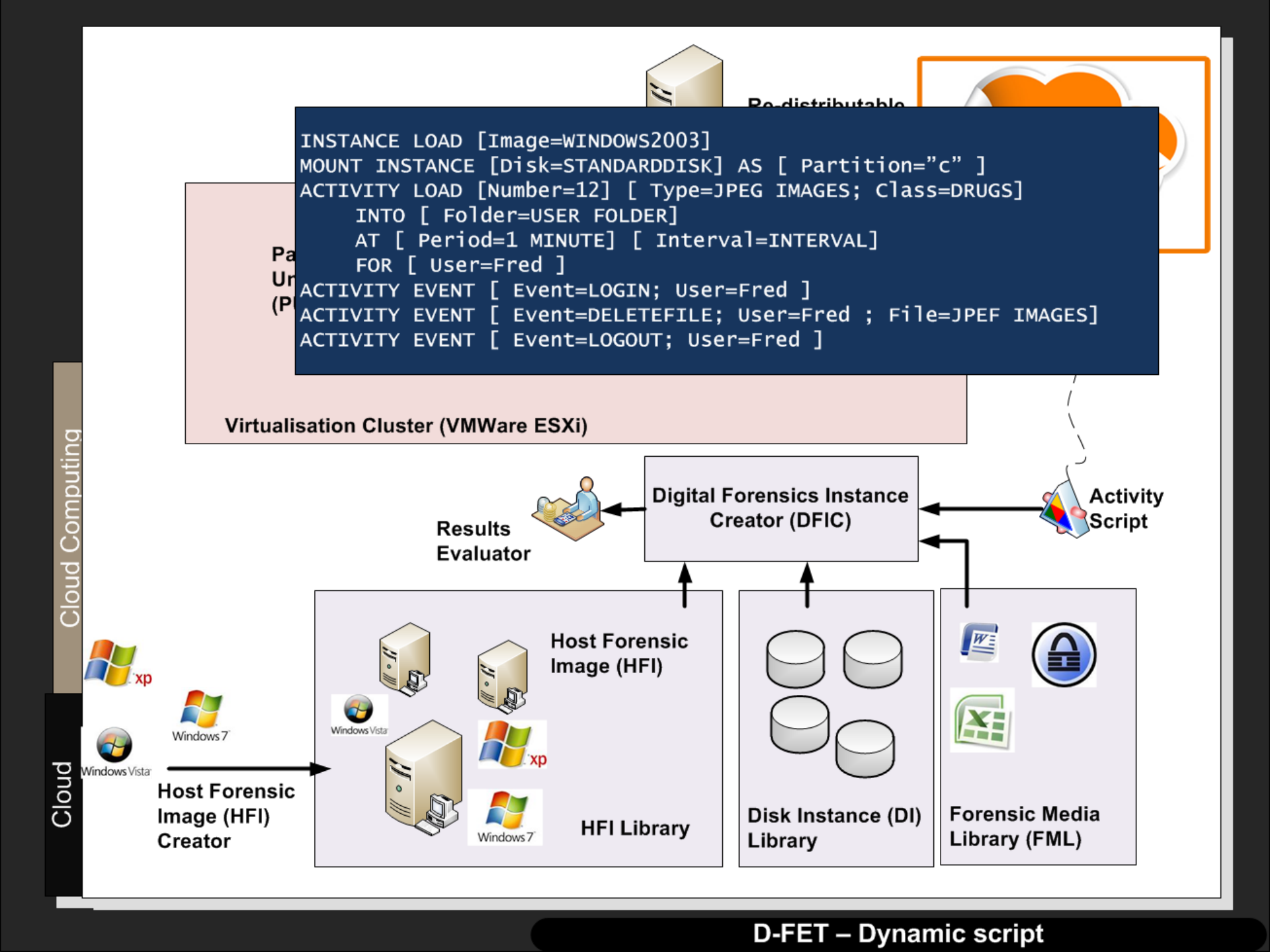


Cloud Computing

Cloud


Re-distributable Instance (RDI)
cloud @napier
Package Under Test (PUT)
Host Forensics Operating Instance (HFOI)
Virtualisation Cluster (VMWare ESXi)
Cloud Computing
Results Evaluator
Digital Forensics Instance Creator (DFIC)
Activity Script
Host Forensic Image (HFI)
Windows Vista
xp
Windows 7
Windows Vista
Host Forensic Image (HFI) Creator
HFI Library
Disk Instance (DI) Library
Forensic Media Library (FML)
Cloud
D-FET


Re-distributable Instance (RDI)
cloud
INSTANCE LOAD [Image=WINDOWS2003]
MOUNT INSTANCE [Disk=STANDARDDISK] AS [Partition="c"]
ACTIVITY LOAD [Number=12] [Type=JPEG IMAGES; Class=DRUGS]
INTO [Folder=USER FOLDER]
AT [Period=1 MINUTE] [Interval=INTERVAL]
FOR [User=Fred]
Virtualisation Cluster (VMWare ESXi)
Digital Forensics Instance Creator (DFIC)
Activity Script
Results Evaluator
Cloud Computing
Cloud
xp
Windows 7
Windows Vista
Host Forensic Image (HFI) Creator
Host Forensic Image (HFI)
HFI Library
Disk Instance (DI) Library
Forensic Media Library (FML)

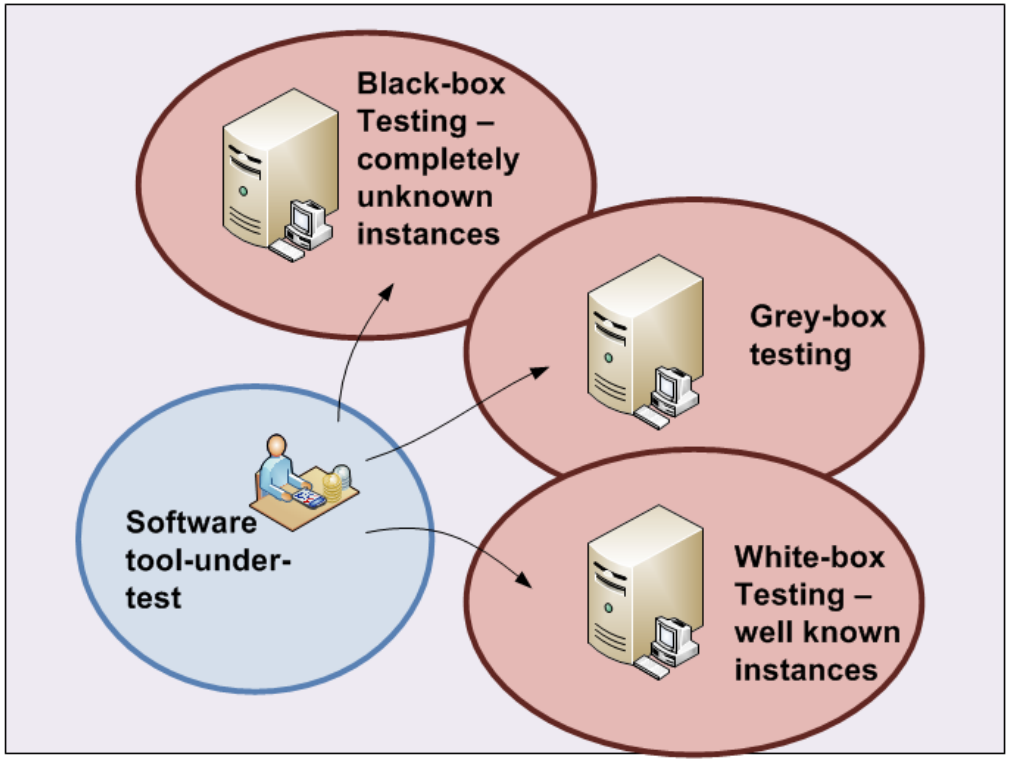


D-FET – Dynamic script

Forensics Quality Evaluator (Speed of response, CPU utilitzation, memory footprint, thread utilization, and so on)

cloud @napier

Evaluation report



Forensic Quality Metrics

- Presence of known illicit images
- Presence of known illicit movies
- Evidence of accessing/viewing/uploading/ downloading illicit material
- Evidence of moving/copying/burning/printing illicit material to other locations
- User accounts – number and names
- Presence of filesharing software
- Filesharing history vs known bad files
- Presence of counter-forensics software
- ...
- Hidden files (unallocated space) - recovery
- Deleted files - recovery
- String searches for ASCII strings
- String searches for UNICODE strings

Cloud Computing

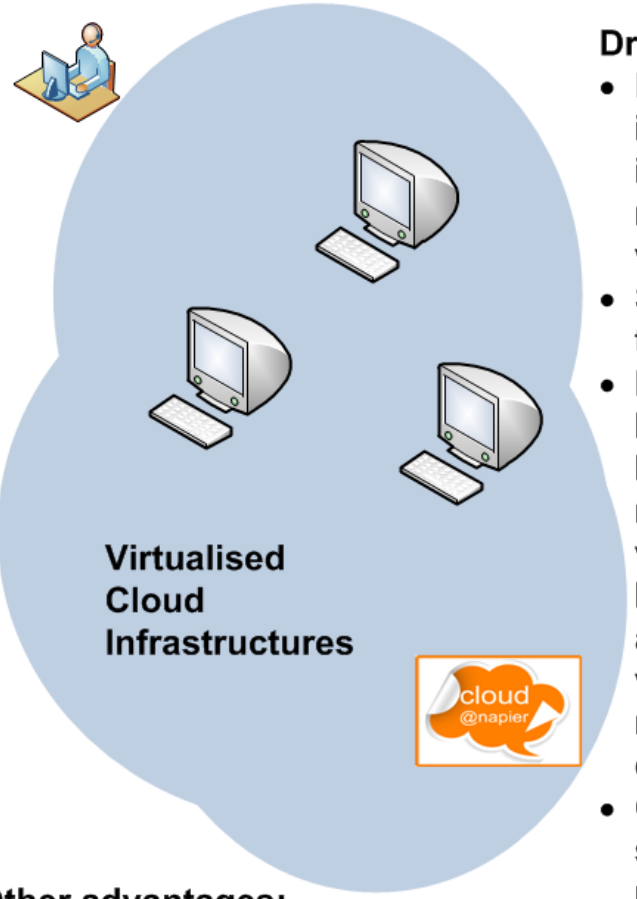
Cloud

Tool validation:

- Supports a wide range of tool validation.
- Ever changing environment for a range of testing.

Skills:

- Allows students to remotely complete labs.
- Students training on state-of-the-art infrastructures.
- Different labs can be created for different situations (DF Tools/OSs/etc).
- Supports remote/distance learning.
- Infrastructure can be ring-fenced.
- Supports group work in an isolated environment.
- In-depth analysis of infrastructures.
- Students can build systems from scratch.
- Students can update their own infrastructure/tools, as required.
- Seems to engage the students, and show them a wide potential.
- Encourages students to continue work after the lab/tutorial.
- Time windows of labs/tutorials can be carefully controlled.
- Extensive and complex infrastructures assessed within a sandboxed environments.



Drawbacks:

- Requires an investment in time in creating and maintaining the virtual image.
- Students can avoid the lab situation.
- Possibly requires a backup strategy for labs (if using network-based virtualisation – but has advantages that a standalone version does not need a network connection).
- Goes against the stand-alone machine philosophy.

Other advantages:

- Easy for teaching team to update.
- Helps with franchised colleges.
- Easy setup for classroom demonstrations.
- Infrastructure can be ring-fenced.
- Produces repeatable labs.
- Not dependent on Napier/network infrastructure.
- Time windows of labs/tutorials can be carefully controlled.

Edinburgh Napier UNIVERSITY

Cloud: The Future, Risk and Training

Towards the Next Generation

Prof Bill Buchanan