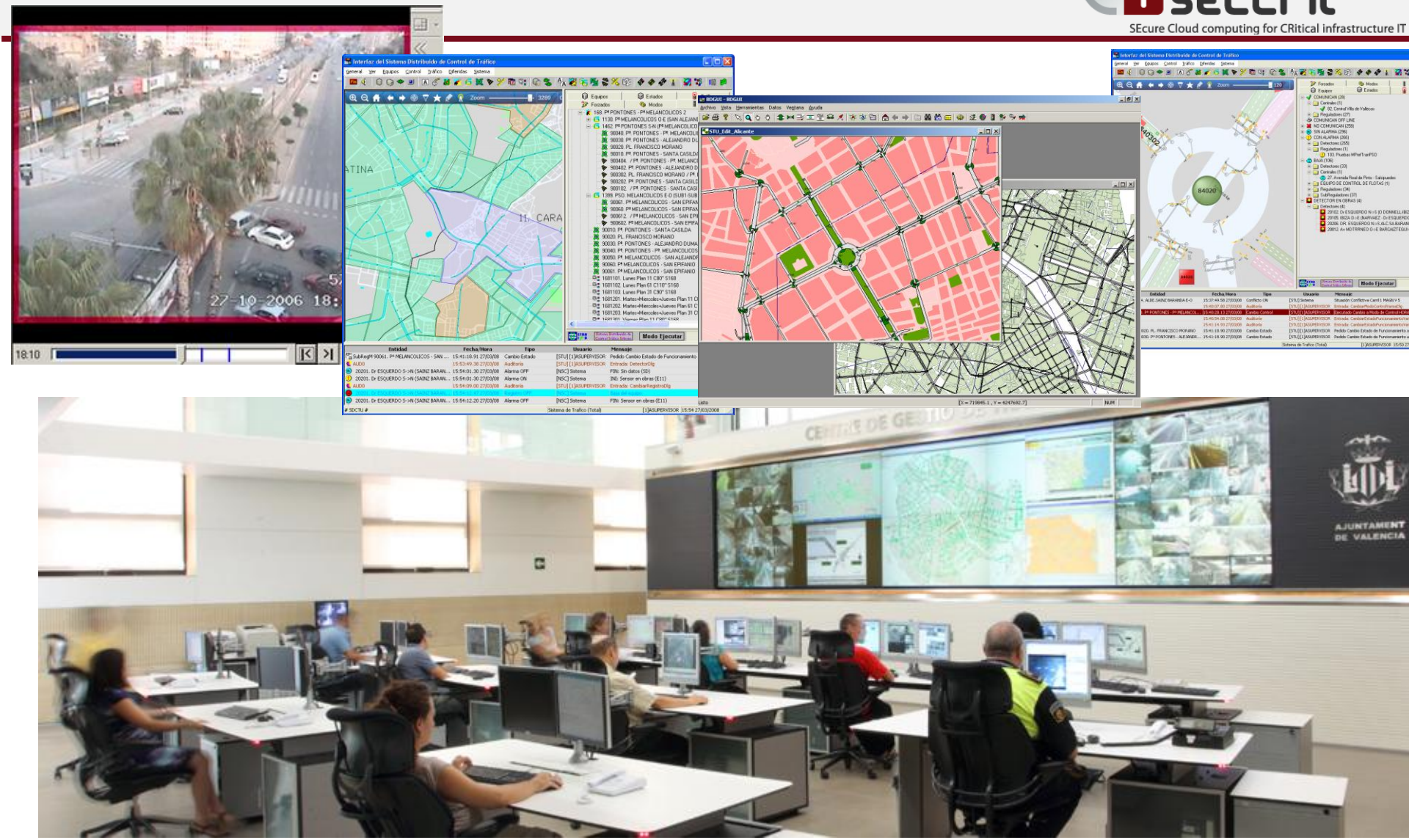
SEcure Cloud computing
for CRitical Infrastructure IT

Exploitation Plans

Santiago Cáceres
ETRA Research and Development

AIT Austrian Institute of Technology • ETRA Investigación y Desarrollo • Fraunhofer Institute for Experimental Software Engineering IESE • Karlsruhe Institute of Technology • NEC Europe • Lancaster University • Mirasys • Hellenic Telecommunications Organization OTE• Ayuntamiento de Valencia • Amaris

SECCRIT
SEcure Cloud computing for CRitical infrastructure IT



How we worked…

AJUNTAMENT DE VALÈNCIA
PREMISES

etra
SUPPORT

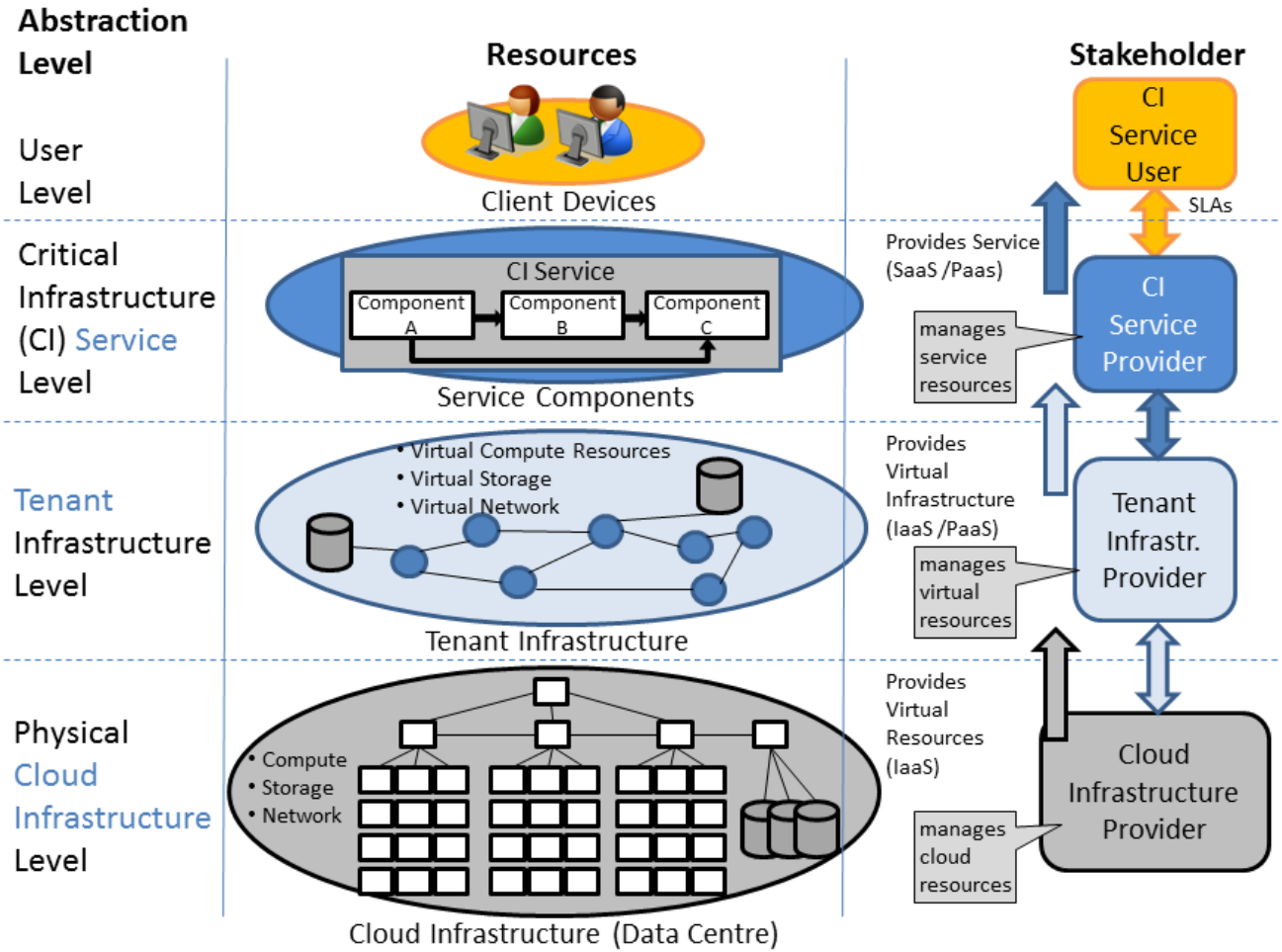
Everything goes as a service…

AJUNTAMENT DE VALÈNCIA

- Outsource hardware-related maintenance tasks
- Ease the deployment and of new functionalities by taking advantage of cloud elasticity
- Implement effective server-backup policies
- Enhance resilience and minimize service downtime

etra

- Develop the Traffic Management System as a SaaS
- Lower budget and rapid availability



AJUNTAMENT DE VALÈNCIA

etra

etra

OTE Amaris

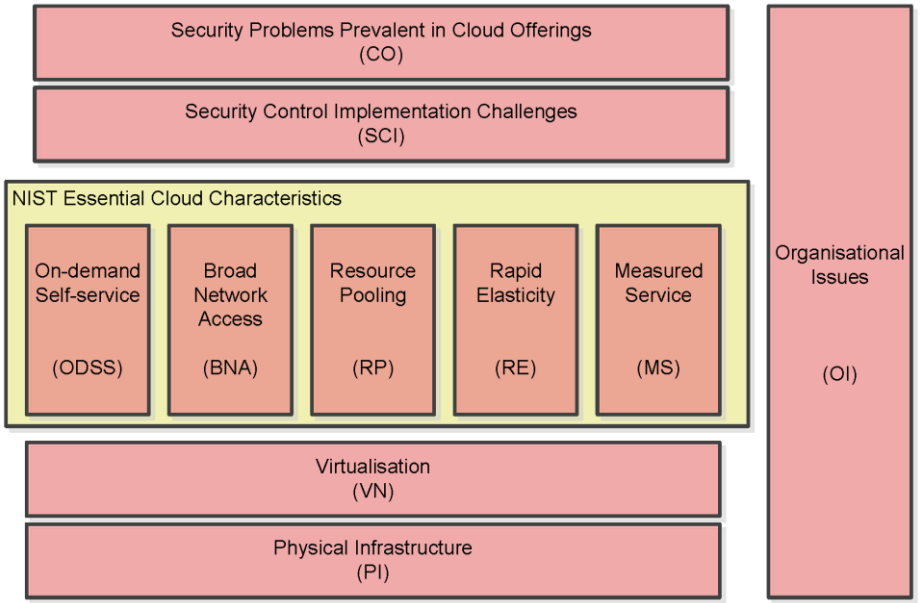
- New actors playing. Cloud provider and ISP

Amaris OTE

- Risks to cyber attacks have been increased (broad network exposure)

The SECCRIT Threat and Vulnerability Catalogue

- Organised items into categories – NIST's essential characteristics of cloud computing at the core
- Identified impact type, i.e., CIA, and references when possible



The catalogue can be downloaded from https://seccrit.eu

Table 7: Rapid elasticity-related vulnerabilities and

Rapid Elasticity		
ID	Description	Type
RE-1 to 3	Insufficient underlying (1) compute, (2) network and (3) storage resources for **scaling-up**	Vu
RE-4 to 6	Insufficient underlying (1) compute, (2) network and (3) storage resources for **scaling-out**	Vu
RE-7	Scaling-out leads to performance issues be- cause networ are not	Th
RE-8	Scaling ciated	
RE-9	Scaling pender or malf	
RE-10	Failure data ce	
RE-11	Failure cloud c gration	
RE-12	Virtual cepted infrastr EU.	
RE-13	Redun to the s ject to	

Table 10: Organisational issues-re

Organisatio	
ID	Description
OI-1	Malicious insiders in the cloud in provider
OI-2	Poor information security processe by the cloud infrastructure provider
OI-3	Inadequate incident-response m processes by the cloud infrastructur
OI-4	Issues emerging because of poor S cation
OI-5	Contractual issues that emerge b bankruptcy and potential switching
OI-6	Failure of a sub-contractor, which the primary "obligor," i.e., a cloud in provider
OI-7	Vulnerabilities emerging from a lac of software versions and APIs

Once in the cloud…

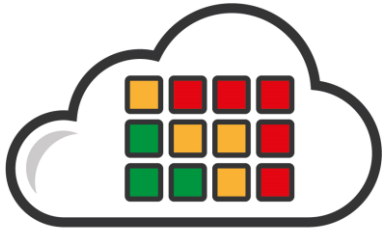
- Increase
  - Resilience
  - Measures against cyberattacks
- Mechanisms to control
  - Cloud provider fulfillment of the SLA
  - ISP fulfillment of the SLA

SECCRIT OUTCOMES

resilience framework including anomaly detection in the cloud

techno-legal guidance

tools for audit trails and root cause analysis



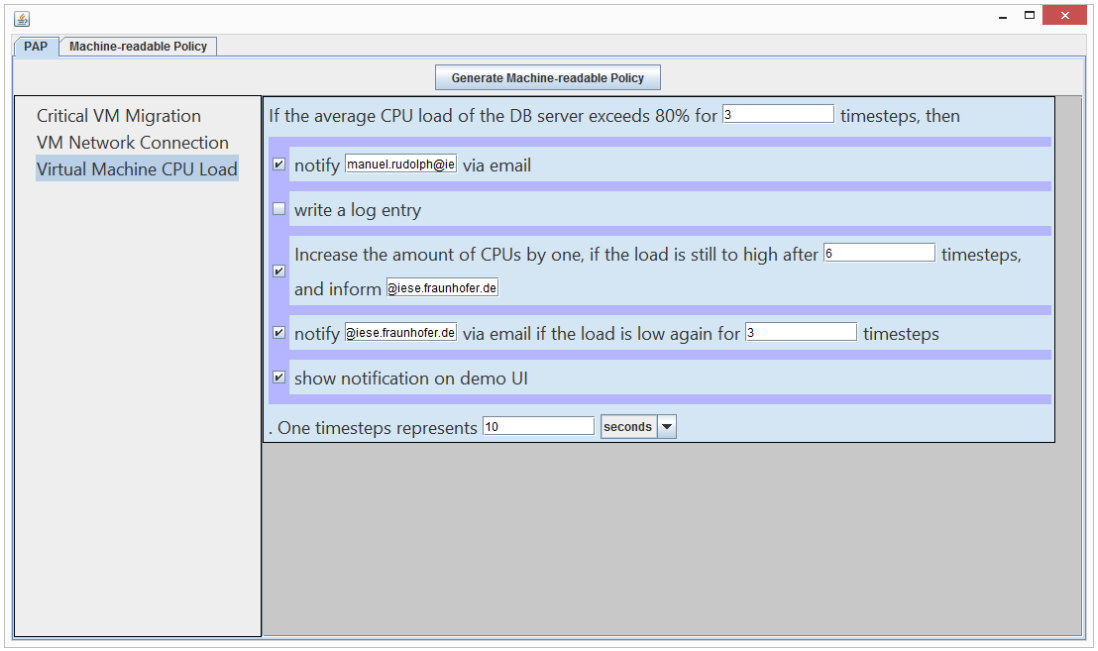
risk assessment

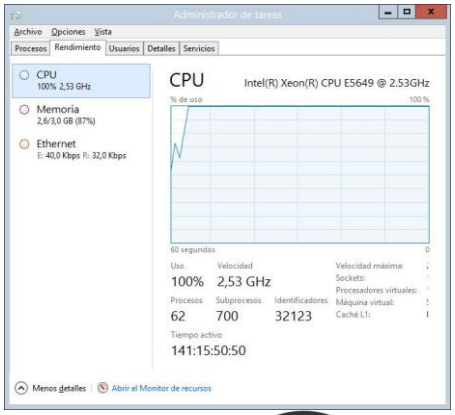
policy specification, decision and enforcement

cloud assurance profile

model driven security guidelines

- Allow translation of **high level availability requirements** (as stated in the SLA) **into low level policies that the framework can implement and monitor**



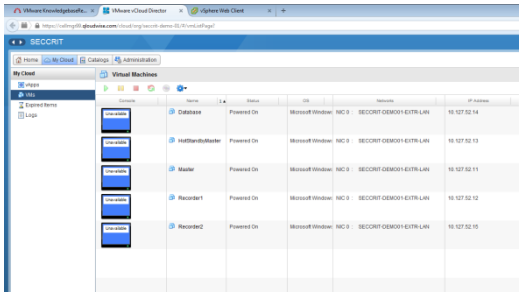


policy specification, decision and enforcement

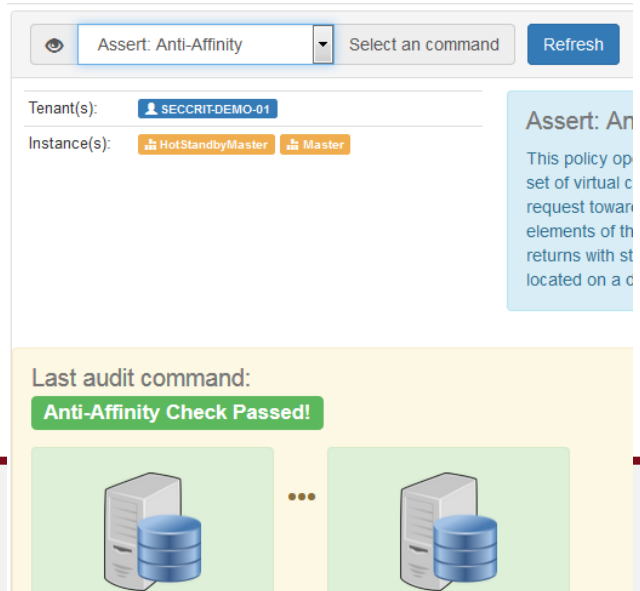
- Allow independent view of logs and events information

- Disruption of service results on a fine (SLA)
- How to prove what went wrong when you are in the cloud?

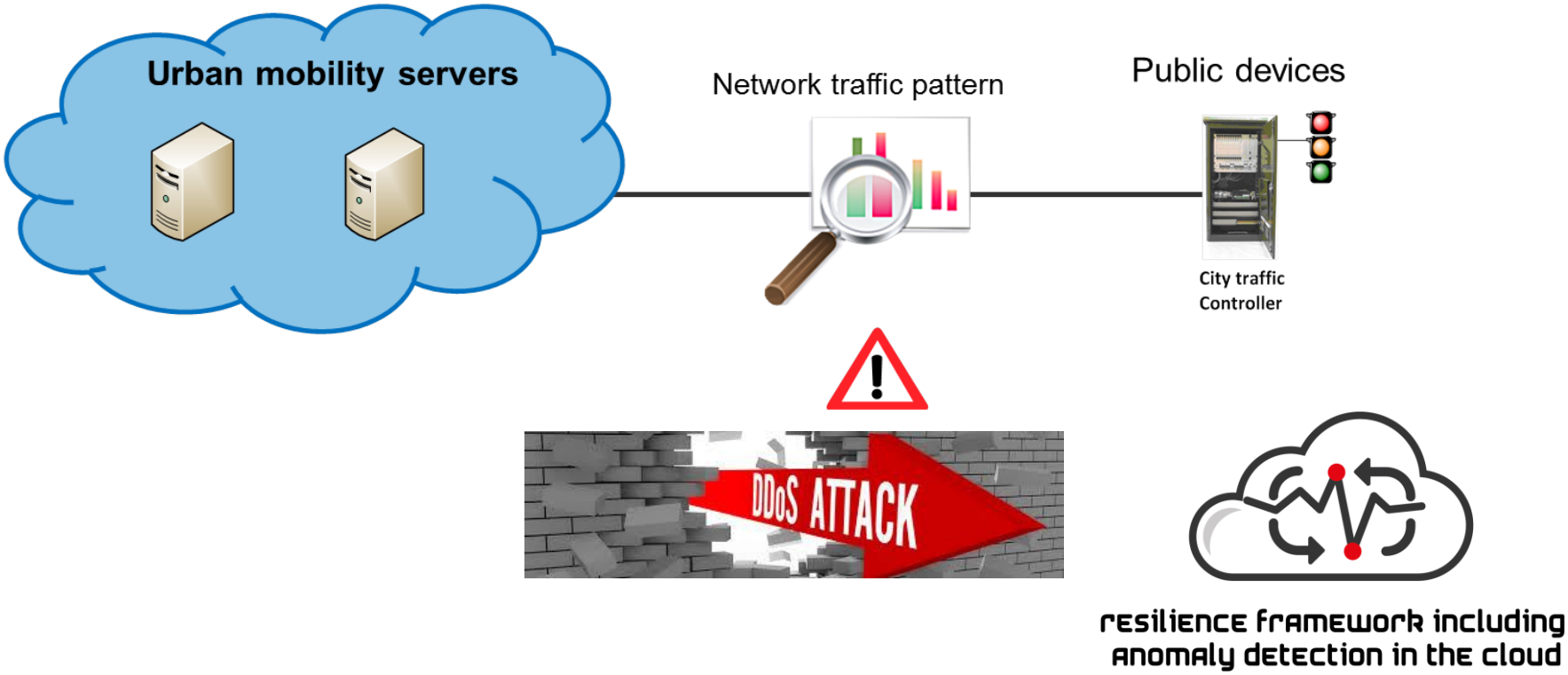
Tenant View - VMWare



Tenant View - CloudInspector



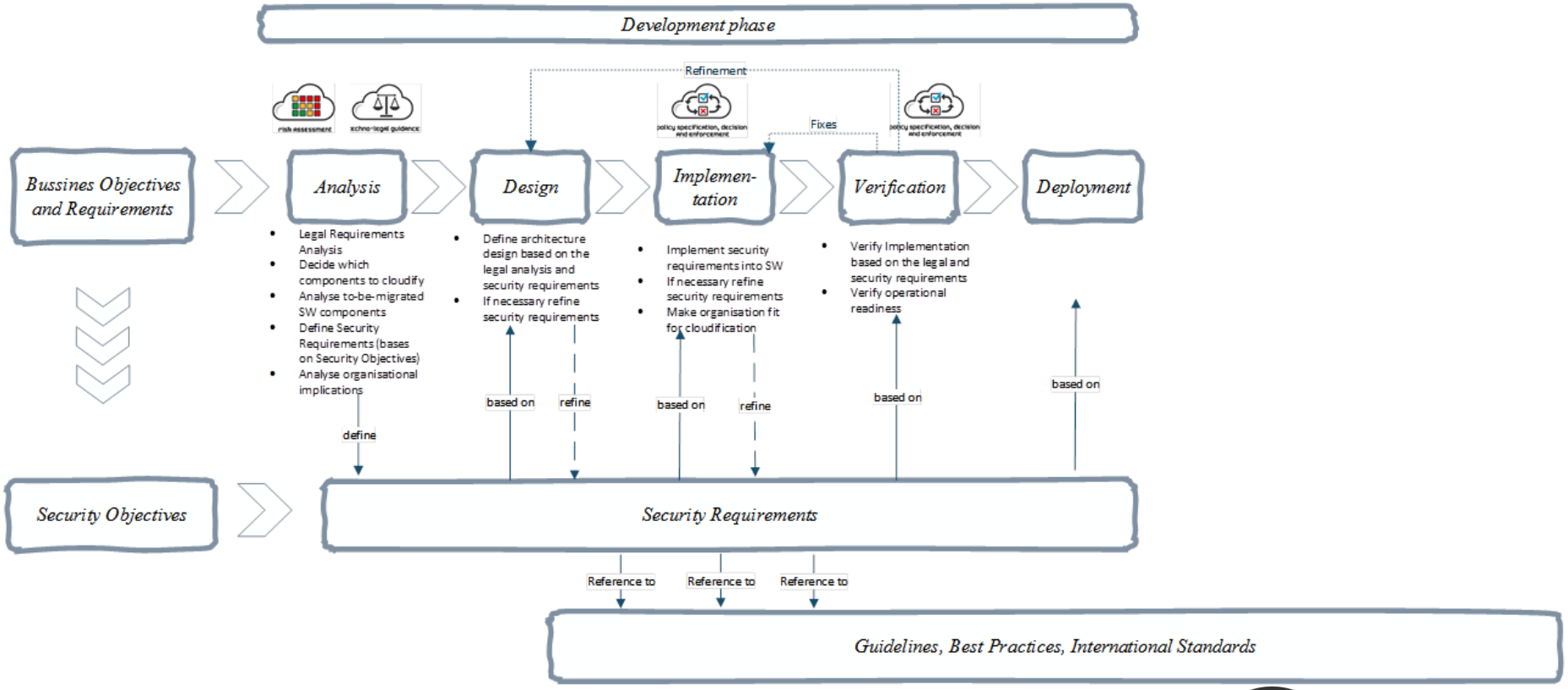
- Monitor pre-defined parameters of the cloud (network traffic, storage usage…) and trigger alerts in the event of a deviation of the normal behavior of the system



- **Continuous assessment** of security properties across the cloud architecture

Class	Security Property Name
INTEGRITY	System/Service Integrity
	Information Consistency
	Error Correction
CONFIDENTIALITY	Password rotation
	Concurrent Session Control
	Strong encryption

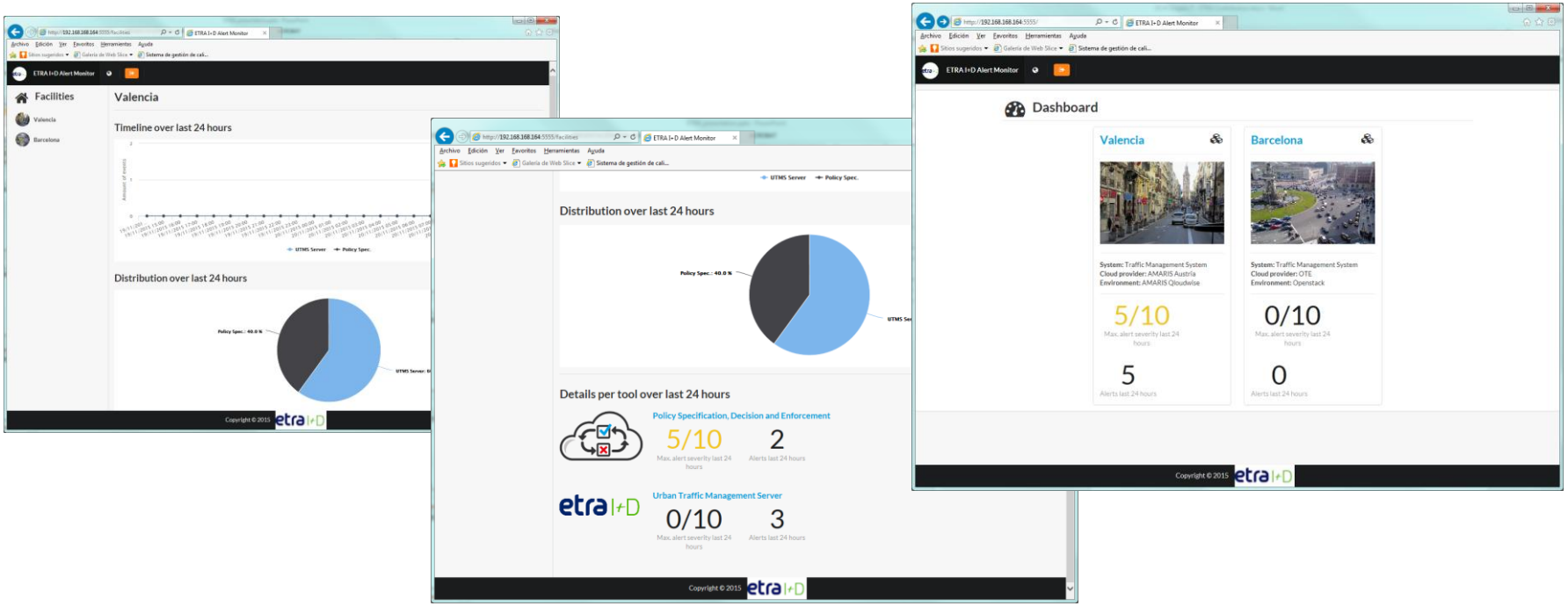
cloud assurance profile



model driven security guidelines

How we use all of these…

- We have a central element to gather all information
- Support tool for IT equipment
- Information correlation among SECCRIT tools with ETRA applications



SEcure Cloud computing for CRitical Infrastructure IT

SEcure Cloud computing for CRitical infrastructure IT

Thanks for your attention

Santiago Cáceres

etra I+D

AIT Austrian Institute of Technology • ETRA Investigación y Desarrollo • Fraunhofer Institute for Experimental Software Engineering IESE • Karlsruhe Institute of Technology • NEC Europe • Lancaster University • Mirasys • Hellenic Telecommunications Organization OTE• Ayuntamiento de Valencia • Amaris