

# SEcure Cloud computing for CRITICAL Infrastructure IT



## Exploitation Plans

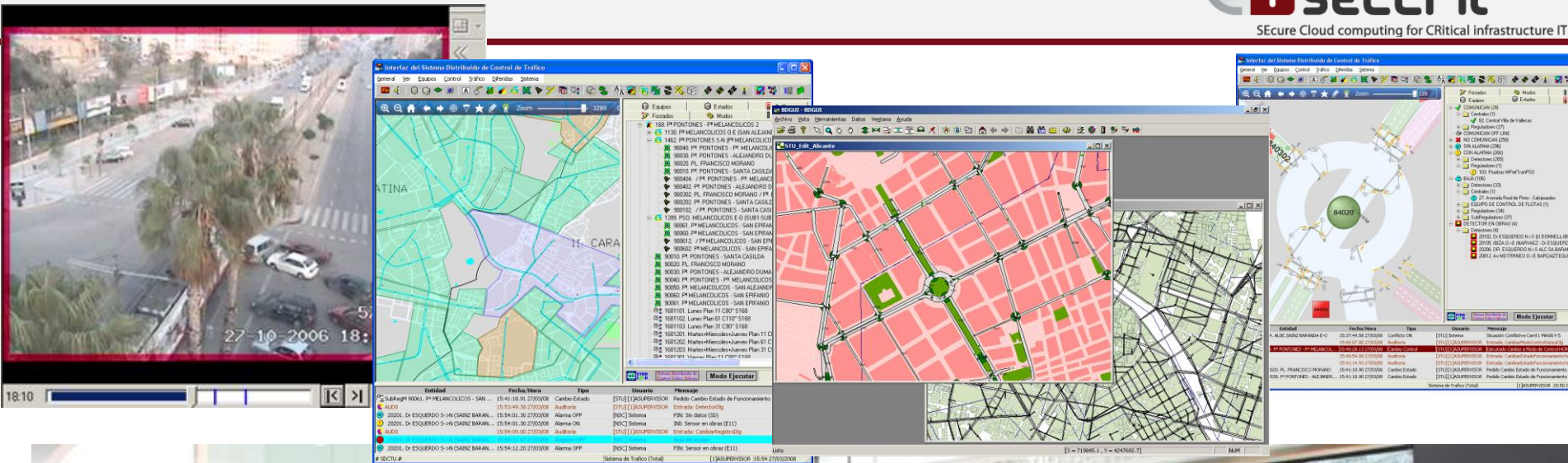
Santiago Cáceres  
ETRA Research and Development



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









# How we worked...



**AJUNTAMENT  
DE VALÈNCIA  
PREMISES**



**etra**  
SUPPORT



**AJUNTAMENT  
DE VALÈNCIA**

**etra**

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

**Abstraction Level**

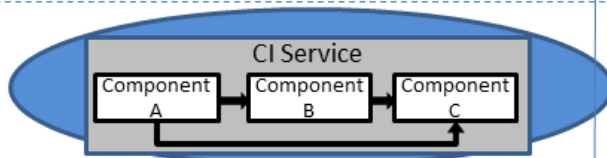
User Level

**Resources**



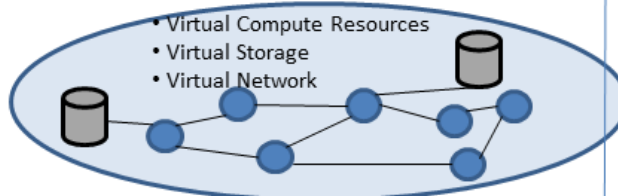
Client Devices

Critical Infrastructure (CI) Service Level



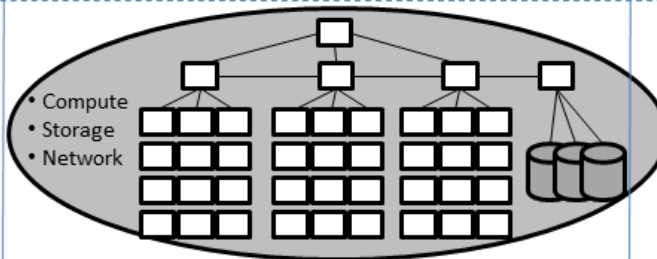
Service Components

Tenant Infrastructure Level



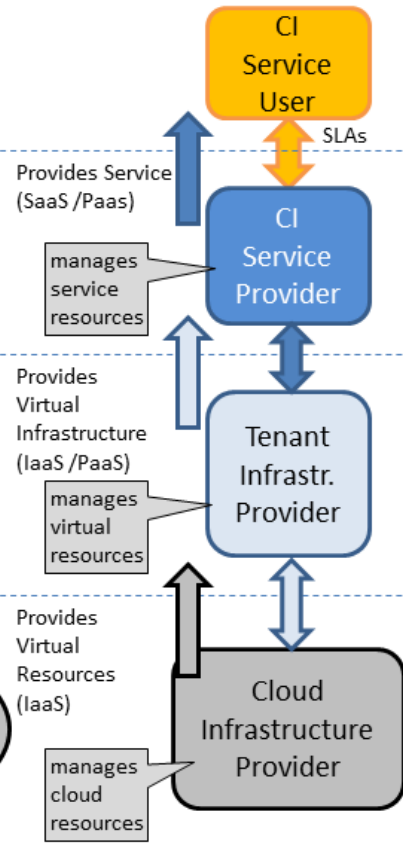
Tenant Infrastructure

Physical Cloud Infrastructure Level



Cloud Infrastructure (Data Centre)

**Stakeholder**



**AJUNTAMENT DE VALÈNCIA**

**etra**

**etra**



**Amaris**



- New actors playing. Cloud provider and ISP

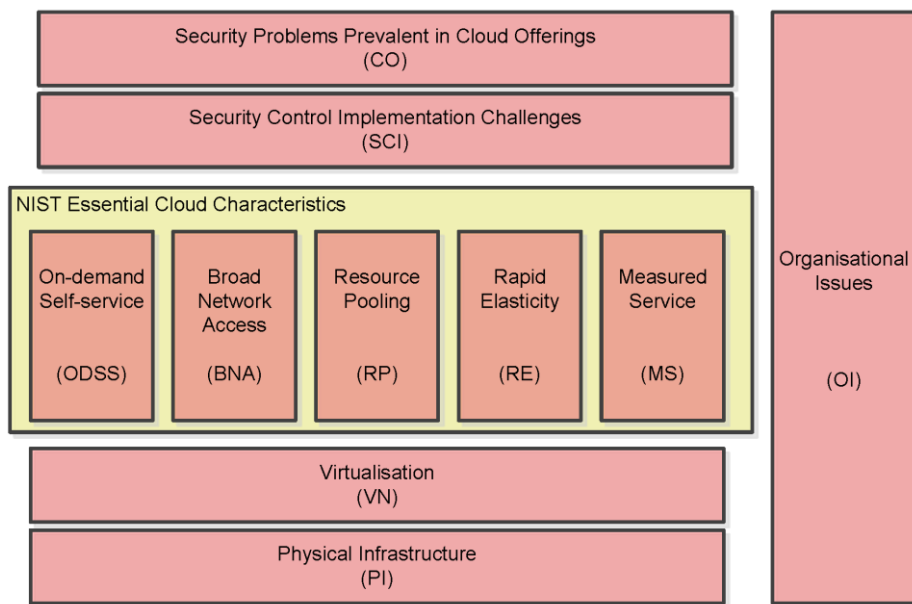
Amaris



- 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 <b>scaling-up</b>	Vu
RE-4 to 6	Insufficient underlying (1) compute, (2) network and (3) storage resources for <b>scaling-out</b>	Vu
RE-7	Scaling-out leads to performance issues because virtualized services that require certain network	Th

Table 10: Organisational issues-re

Organisational Issues		
ID	Description	Type
RE-8	Scaling related	
RE-9	Scaling pender or mal	
RE-10	Failure data ce	
RE-11	Failure cloud d gration	
RE-12	Virtual cepted infrastr EU.	
RE-13	Redun to the s ject to	
RE-14		
RE-15		
RE-16		
RE-17		
RE-18		
RE-19		
RE-20		
RE-21		
RE-22		
RE-23		
RE-24		
RE-25		
RE-26		
RE-27		
RE-28		
RE-29		
RE-30		
RE-31		
RE-32		
RE-33		
RE-34		
RE-35		
RE-36		
RE-37		
RE-38		
RE-39		
RE-40		
RE-41		
RE-42		
RE-43		
RE-44		
RE-45		
RE-46		
RE-47		
RE-48		
RE-49		
RE-50		
RE-51		
RE-52		
RE-53		
RE-54		
RE-55		
RE-56		
RE-57		
RE-58		
RE-59		
RE-60		
RE-61		
RE-62		
RE-63		
RE-64		
RE-65		
RE-66		
RE-67		
RE-68		
RE-69		
RE-70		
RE-71		
RE-72		
RE-73		
RE-74		
RE-75		
RE-76		
RE-77		
RE-78		
RE-79		
RE-80		
RE-81		
RE-82		
RE-83		
RE-84		
RE-85		
RE-86		
RE-87		
RE-88		
RE-89		
RE-90		
RE-91		
RE-92		
RE-93		
RE-94		
RE-95		
RE-96		
RE-97		
RE-98		
RE-99		
RE-100		
RE-101		
RE-102		
RE-103		
RE-104		
RE-105		
RE-106		
RE-107		
RE-108		
RE-109		
RE-110		
RE-111		
RE-112		
RE-113		
RE-114		
RE-115		
RE-116		
RE-117		
RE-118		
RE-119		
RE-120		
RE-121		
RE-122		
RE-123		
RE-124		
RE-125		
RE-126		
RE-127		
RE-128		
RE-129		
RE-130		
RE-131		
RE-132		
RE-133		
RE-134		
RE-135		
RE-136		
RE-137		
RE-138		
RE-139		
RE-140		
RE-141		
RE-142		
RE-143		
RE-144		
RE-145		
RE-146		
RE-147		
RE-148		
RE-149		
RE-150		
RE-151		
RE-152		
RE-153		
RE-154		
RE-155		
RE-156		
RE-157		
RE-158		
RE-159		
RE-160		
RE-161		
RE-162		
RE-163		
RE-164		
RE-165		
RE-166		
RE-167		
RE-168		
RE-169		
RE-170		
RE-171		
RE-172		
RE-173		
RE-174		
RE-175		
RE-176		
RE-177		
RE-178		
RE-179		
RE-180		
RE-181		
RE-182		
RE-183		
RE-184		
RE-185		
RE-186		
RE-187		
RE-188		
RE-189		
RE-190		
RE-191		
RE-192		
RE-193		
RE-194		
RE-195		
RE-196		
RE-197		
RE-198		
RE-199		
RE-200		
RE-201		
RE-202		
RE-203		
RE-204		
RE-205		
RE-206		
RE-207		
RE-208		
RE-209		
RE-210		
RE-211		
RE-212		
RE-213		
RE-214		
RE-215		
RE-216		
RE-217		
RE-218		
RE-219		
RE-220		
RE-221		
RE-222		
RE-223		
RE-224		
RE-225		
RE-226		
RE-227		
RE-228		
RE-229		
RE-230		
RE-231		
RE-232		
RE-233		
RE-234		
RE-235		
RE-236		
RE-237		
RE-238		
RE-239		
RE-240		
RE-241		
RE-242		
RE-243		
RE-244		
RE-245		
RE-246		
RE-247		
RE-248		
RE-249		
RE-250		
RE-251		
RE-252		
RE-253		
RE-254		
RE-255		
RE-256		
RE-257		
RE-258		
RE-259		
RE-260		
RE-261		
RE-262		
RE-263		
RE-264		
RE-265		
RE-266		
RE-267		
RE-268		
RE-269		
RE-270		
RE-271		
RE-272		
RE-273		
RE-274		
RE-275		
RE-276		
RE-277		
RE-278		
RE-279		
RE-280		
RE-281		
RE-282		
RE-283		
RE-284		
RE-285		
RE-286		
RE-287		
RE-288		
RE-289		
RE-290		
RE-291		
RE-292		
RE-293		
RE-294		
RE-295		
RE-296		
RE-297		
RE-298		
RE-299		
RE-300		
RE-301		
RE-302		
RE-303		
RE-304		
RE-305		
RE-306		
RE-307		
RE-308		
RE-309		
RE-310		
RE-311		
RE-312		
RE-313		
RE-314		
RE-315		
RE-316		
RE-317		
RE-318		
RE-319		
RE-320		
RE-321		
RE-322		
RE-323		
RE-324		
RE-325		
RE-326		
RE-327		
RE-328		
RE-329		
RE-330		
RE-331		
RE-332		
RE-333		
RE-334		
RE-335		
RE-336		
RE-337		
RE-338		
RE-339		
RE-340		
RE-341		
RE-342		
RE-343		
RE-344		
RE-345		
RE-346		
RE-347		
RE-348		
RE-349		
RE-350		
RE-351		
RE-352		
RE-353		
RE-354		
RE-355		
RE-356		
RE-357		
RE-358		
RE-359		
RE-360		
RE-361		
RE-362		
RE-363		
RE-364		
RE-365		
RE-366		
RE-367		
RE-368		
RE-369		
RE-370		
RE-371		
RE-372		
RE-373		
RE-374		
RE-375		
RE-376		
RE-377		
RE-378		
RE-379		
RE-380		
RE-381		
RE-382		
RE-383		
RE-384		
RE-385		
RE-386		
RE-387		
RE-388		
RE-389		
RE-390		
RE-391		
RE-392		
RE-393		
RE-394		
RE-395		
RE-396		
RE-397		
RE-398		
RE-399		
RE-400		
RE-401		
RE-402		
RE-403		
RE-404		
RE-405		
RE-406		
RE-407		
RE-408		
RE-409		
RE-410		



# 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



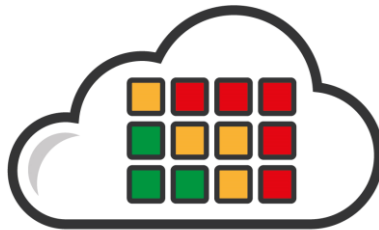
**resilience framework including  
ANOMALY detection in the cloud**



**techno-legal guidance**



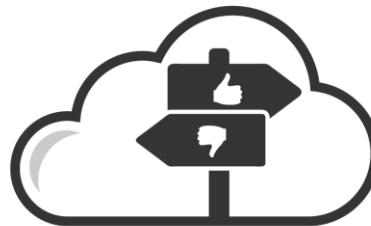
**tools for AUDIT trails AND  
root CAUSE ANALYSIS**



**risk ASSESSMENT**



**cloud ASSURANCE profile**

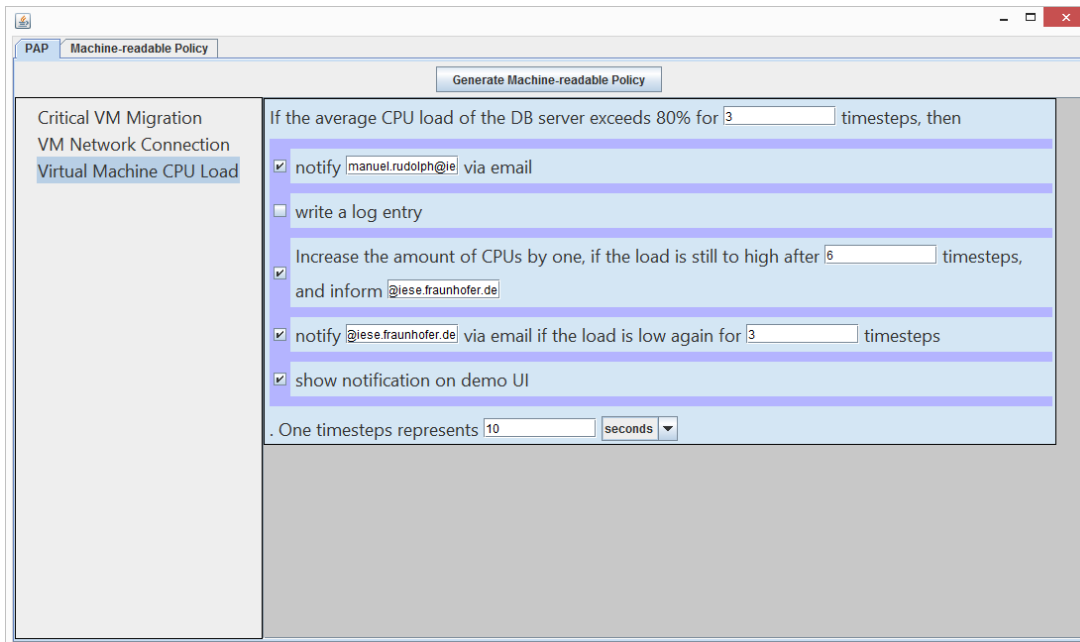


**model driven security guidelines**



**policy specification, decision  
AND enforcement**

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



PAP Machine-readable Policy

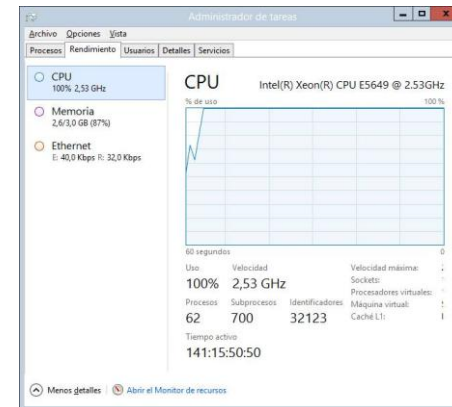
Generate Machine-readable Policy

Critical VM Migration  
VM Network Connection  
Virtual Machine CPU Load

If the average CPU load of the DB server exceeds 80% for 3 timesteps, then

- notify `manuel.rudolph@e` via email
- write a log entry
- Increase the amount of CPUs by one, if the load is still to high after 6 timesteps, and inform `@iese.fraunhofer.de`
- notify `@iese.fraunhofer.de` via email if the load is low again for 3 timesteps
- show notification on demo UI

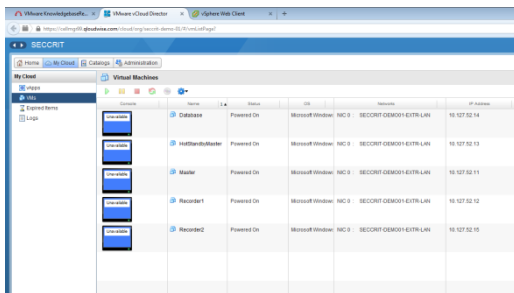
One timesteps represents 10 seconds



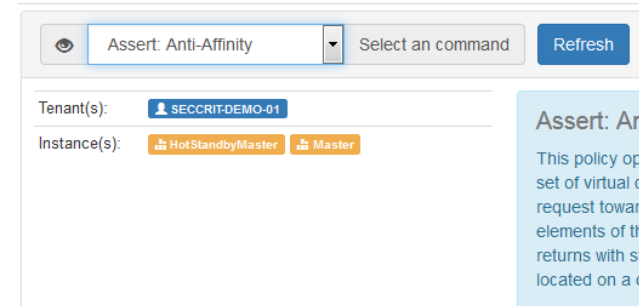
**policy specification, decision  
AND enforcement**

- 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



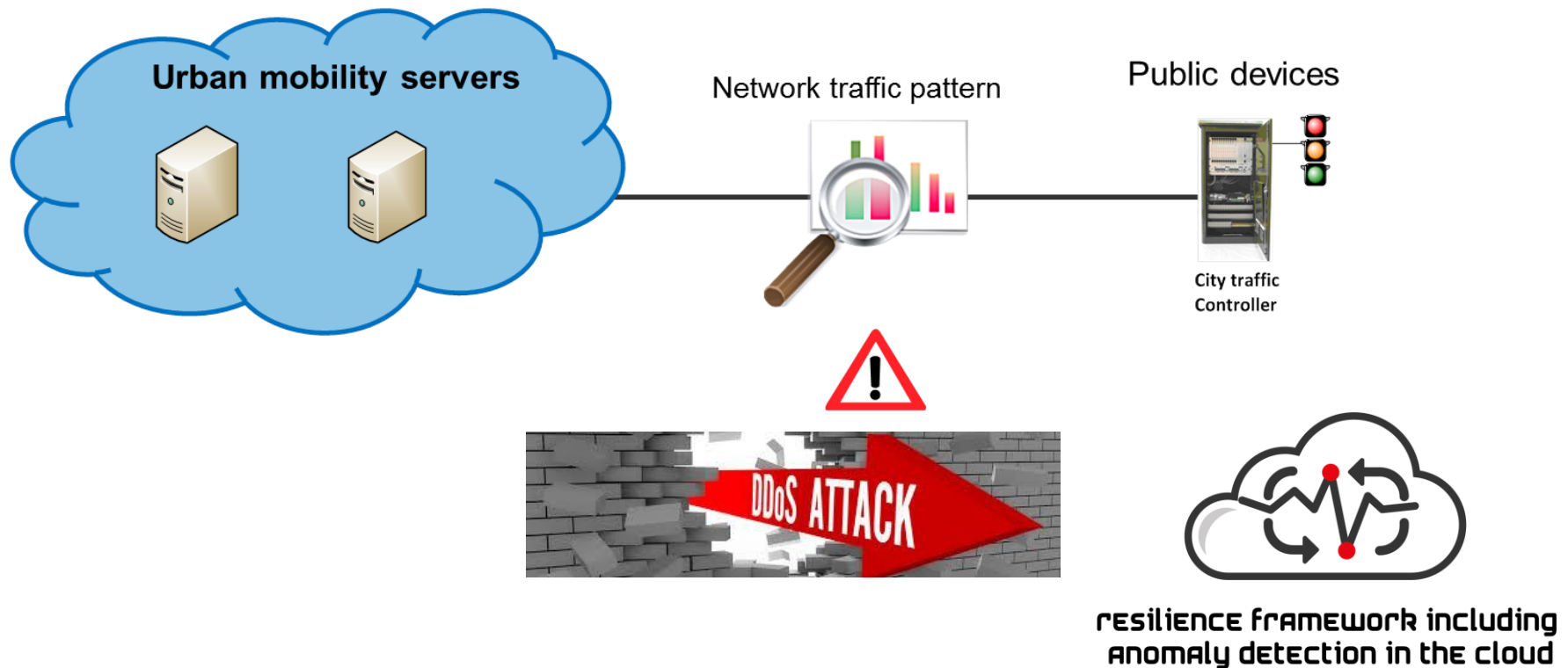
tools for audit trails and  
root cause analysis

Last audit command:

Anti-Affinity Check Passed!



- 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





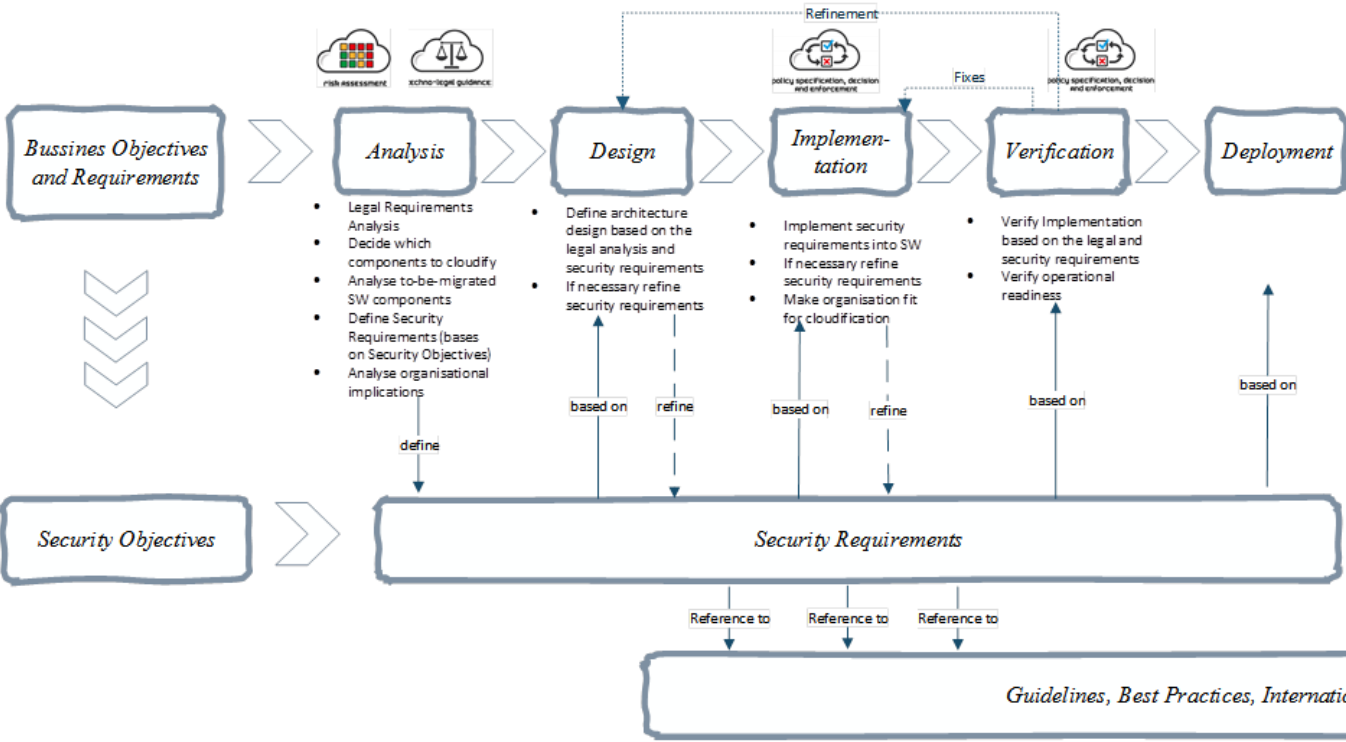
- **Continuous assessment** of security properties across the cloud architecture

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



**cloud ASSURANCE profile**

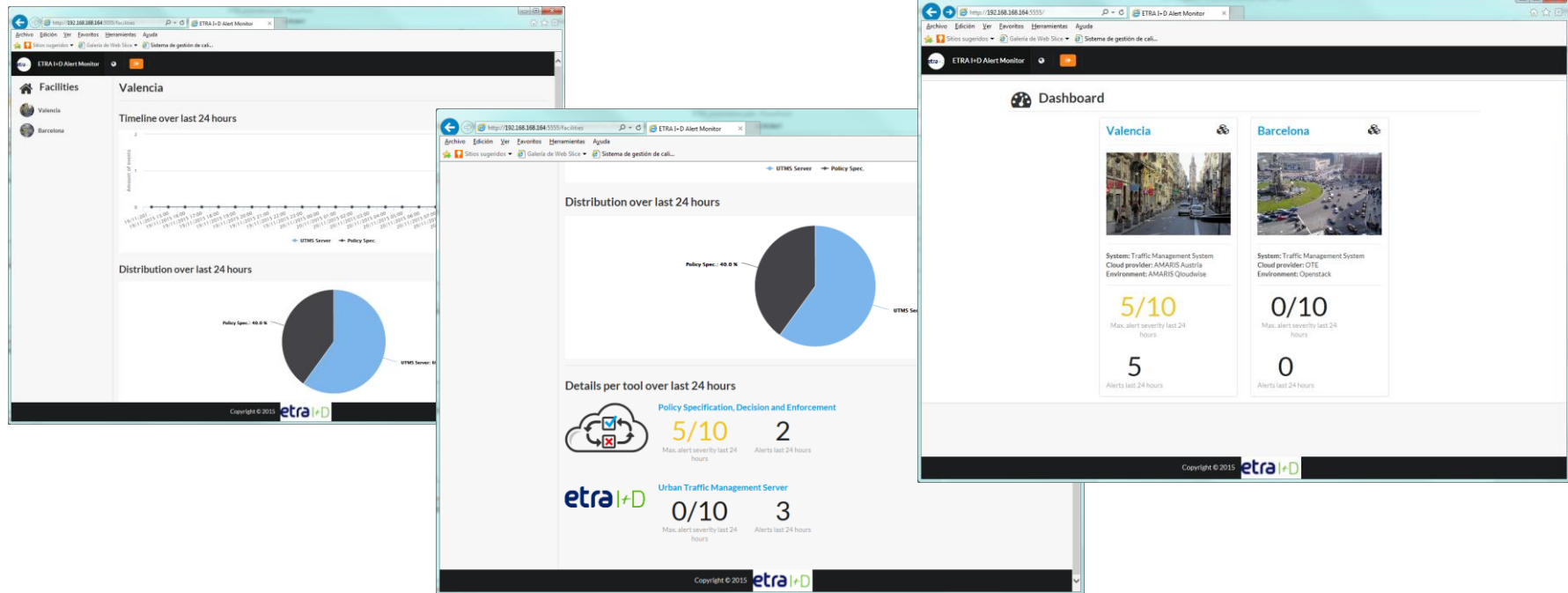
*Development phase*



**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



**Thanks for your attention**

Santiago Cáceres



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

