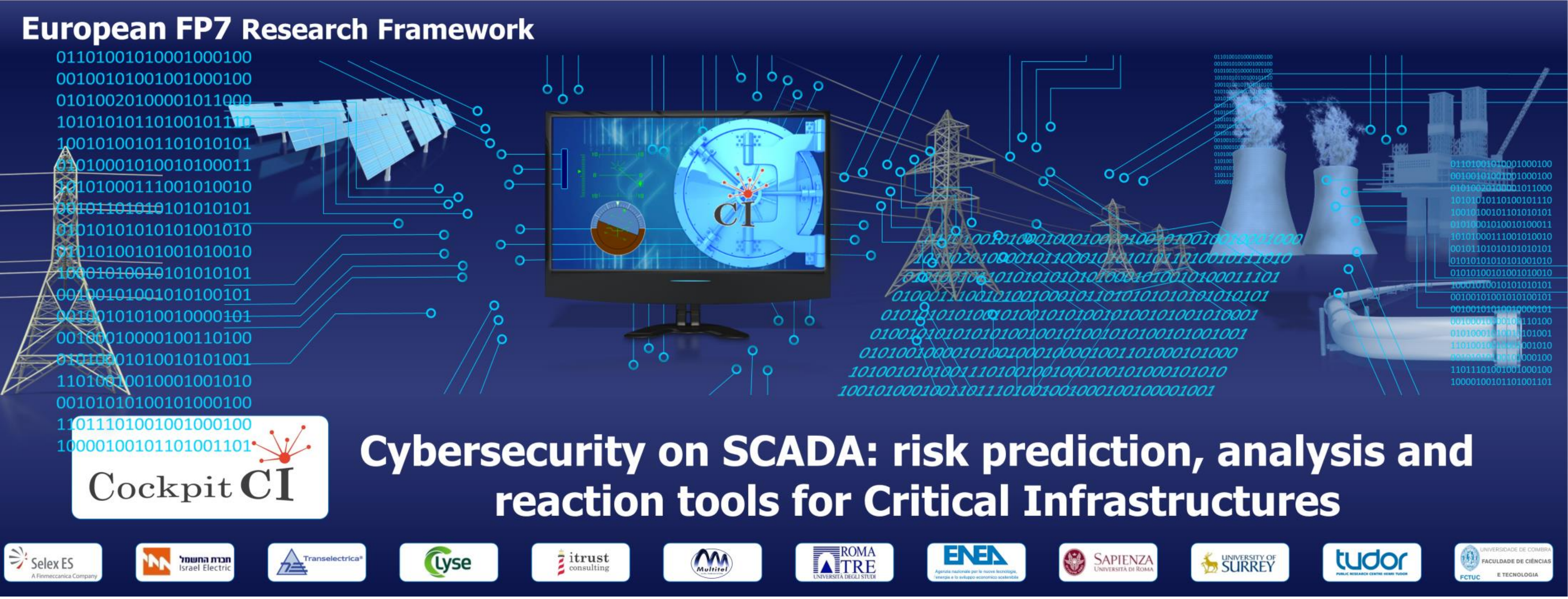

European FP7 Research Framework
Cockpit CI
Cybersecurity on SCADA: risk prediction, analysis and reaction tools for Critical Infrastructures
Selex ES
Israel Electric
Transelectrica
Lyse
itrust consulting
Multitel
ROMA TRE
ENEA
SAPIENZA
UNIVERSITY OF SURREY
tudor
FCTUC

Presentation of specific CockpitCI tools

3rd CockpitCI Workshop (Luxembourg)

M. Aubigny, itrust consulting

Presentation of specific CockpitCI tools

Agenda

1. General presentation
2. Vulnerability assessment solution: Software Checker
    - Overview of the solution of update & vulnerability checker
    - Presentation of the demonstration
    - Deployment design
3. Global antivirus solution: AVCaesar
    - Overview of the solution
    - Presentation of the demonstration
    - Deployment design

Presentation of specific CockpitCI tools

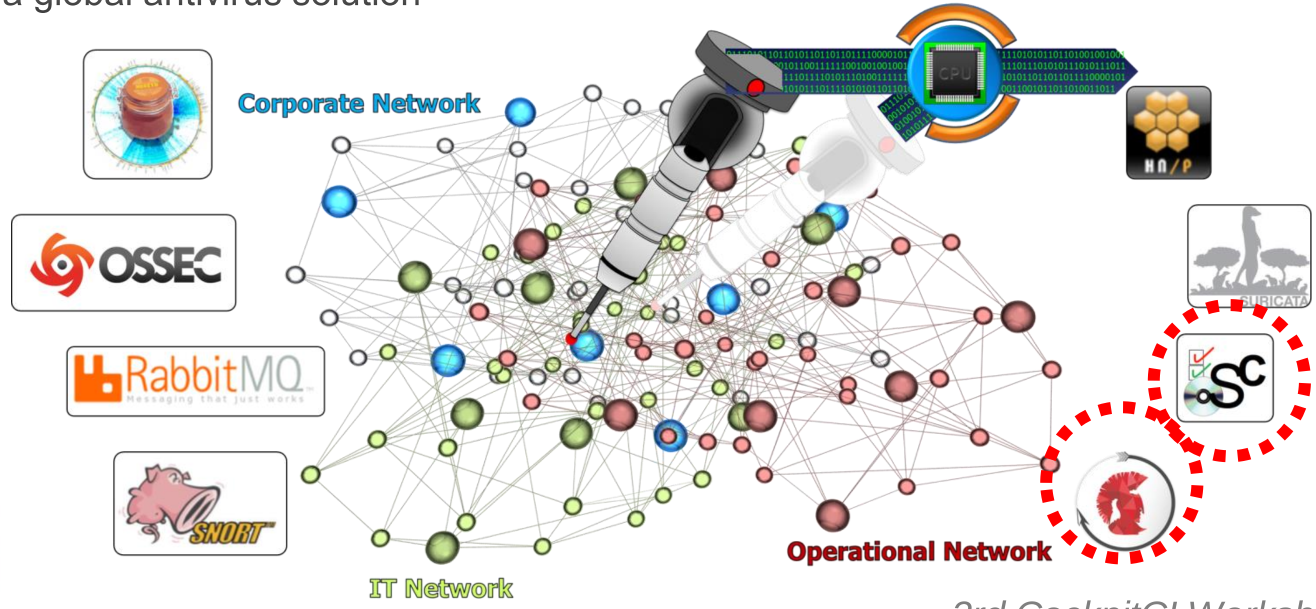
Detection framework overview

The CockpitCI detection framework is a multi-layered detection solution (deployed on the 3 types of networks: ICS, Telco, Corporated) and enables different types of detection tools such as:

- Honeypot
- HIDS & NIDS
- Specific SCADA tools (actually on patent process)

We want to speak about 2 tools developed by itrust in the project framework:

- **Software checker**: a vulnerability assessment solution
- **AVCaesar**: a global antivirus solution



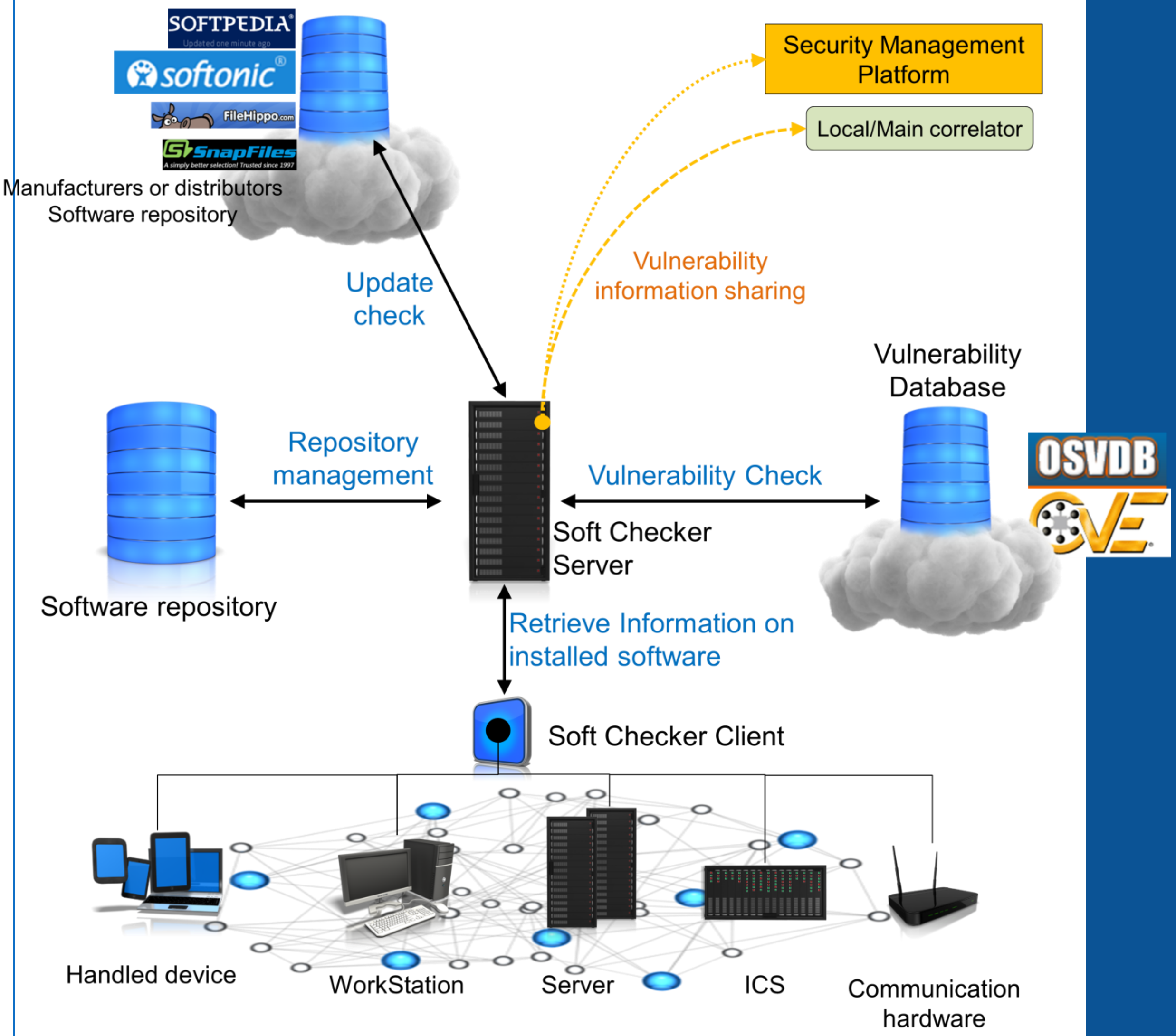
Cockpit CI

Software checker

Update/vulnerability checker overview

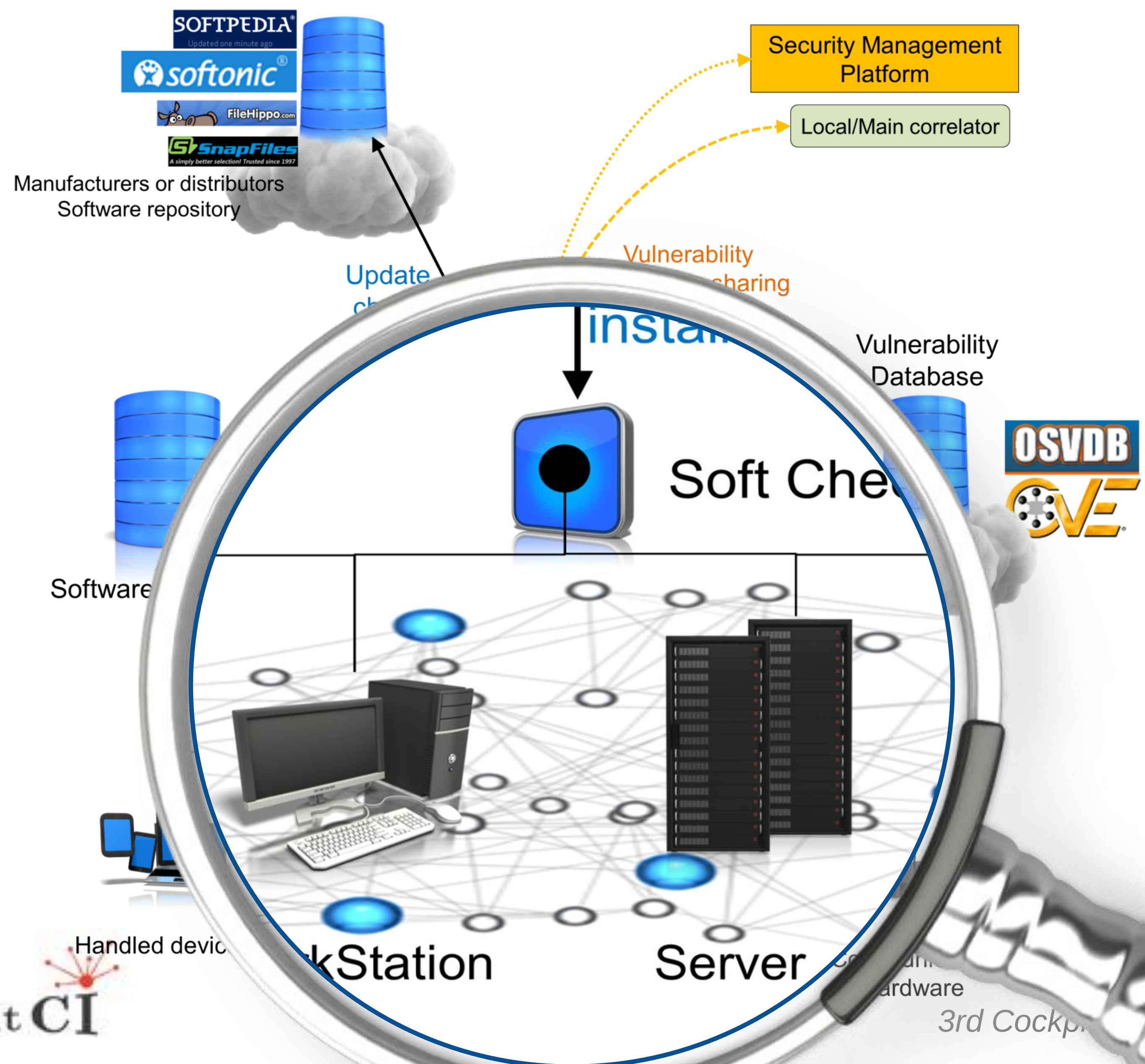
Aim of the update checker

- Retrieve **regularly** information on software deployed on platform: *for example as soon as a components is connected to the network*
- Verify **regularly** the vulnerability state of these software
- Check the **last** update version of software
- Provide in option a central database of **trusted** link for update version.
- Provide a vulnerability assessment to system owner if necessary.
- Provide a central point of vulnerability management

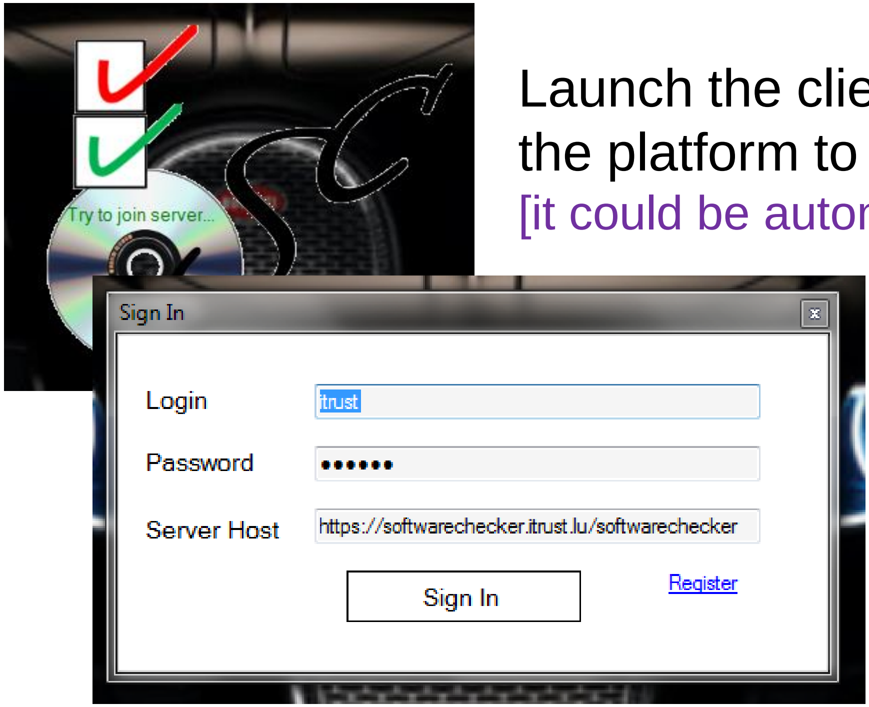


Cockpit CI

Demonstration : Scope of the demo



Demonstration: explanation of the software checker functioning



Sign In

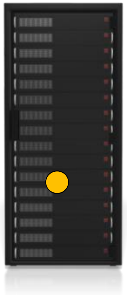
Login: itrust

Password: ••••••

Server Host: https://softwarechecker.itrust.lu/softwarechecker

Launch the client on the platform to test [it could be automatised]

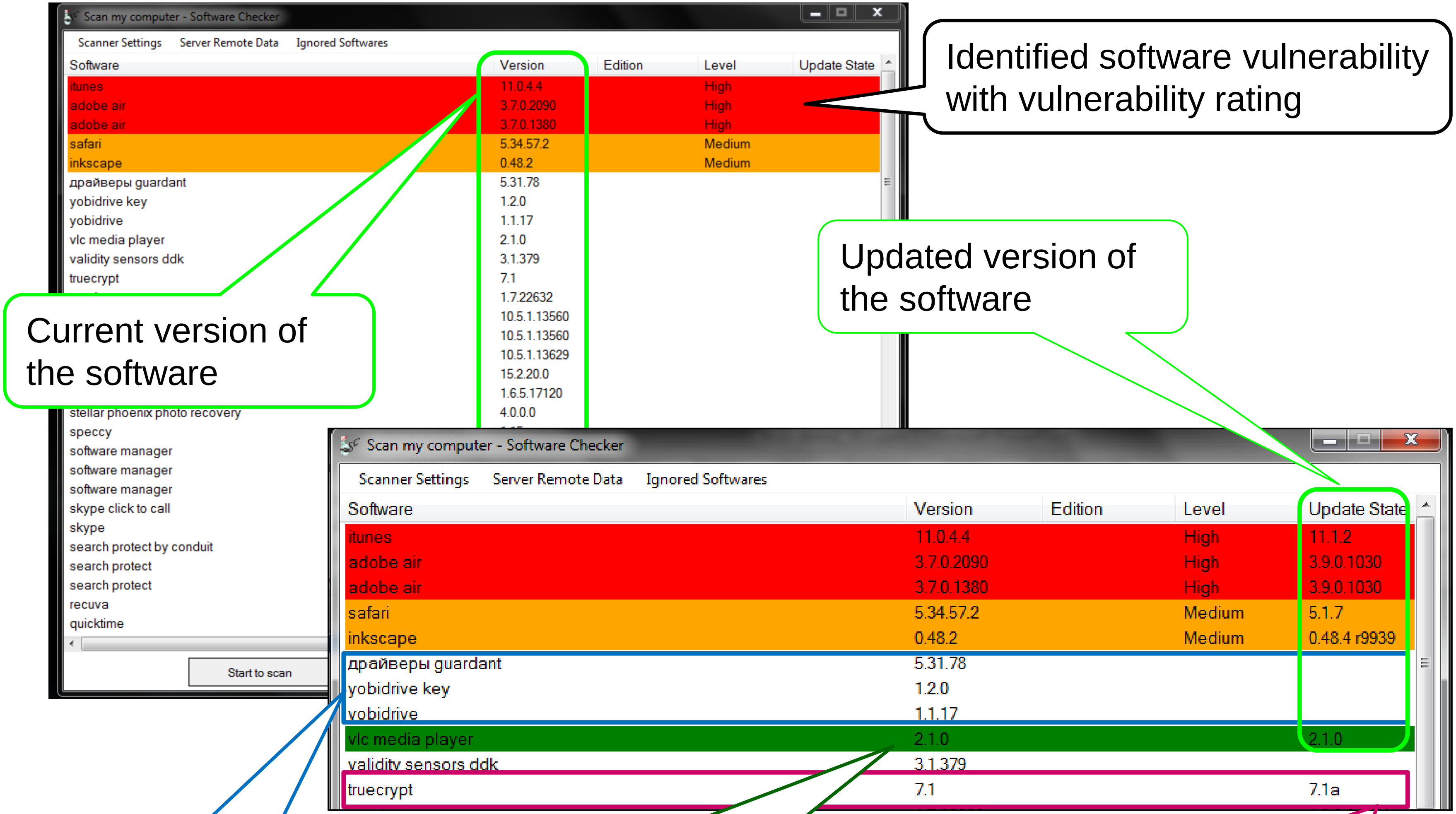
The platform is connected **securely** to the software checker server [it could be deployed in the CI or use internet to connect to third trusted party providing the service]



The tested platform send the information on installed software.

The server check and send the state of vulnerability and the availability of update

Results of the vulnerability assessment



Software	Version	Edition	Level	Update State
itunes	11.0.4.4		High	
adobe air	3.7.0.2090		High	
adobe air	3.7.0.1380		High	
safari	5.34.57.2		Medium	
inkscape	0.48.2		Medium	
драйверы guardant	5.31.78			
yobidrive key	1.2.0			
yobidrive	1.1.17			
vlc media player	2.1.0			
validity sensors ddk	3.1.379			
truecrypt	7.1			
	1.7.22632			
	10.5.1.13560			
	10.5.1.13560			
	10.5.1.13629			
	15.2.20.0			
	1.6.5.17120			
stellar phoenix photo recovery	4.0.0.0			
speccy				
software manager				
software manager				
software manager				
skype click to call				
skype				
search protect by conduit				
search protect				
search protect				
recuva				
quicktime				

Software	Version	Edition	Level	Update State
itunes	11.0.4.4		High	11.1.2
adobe air	3.7.0.2090		High	3.9.0.1030
adobe air	3.7.0.1380		High	3.9.0.1030
safari	5.34.57.2		Medium	5.1.7
inkscape	0.48.2		Medium	0.48.4 r9939
драйверы guardant	5.31.78			
yobidrive key	1.2.0			
yobidrive	1.1.17			
vlc media player	2.1.0			2.1.0
validity sensors ddk	3.1.379			
truecrypt	7.1			7.1a

Identified software vulnerability with vulnerability rating

Current version of the software

Updated version of the software

The software is not known in version database

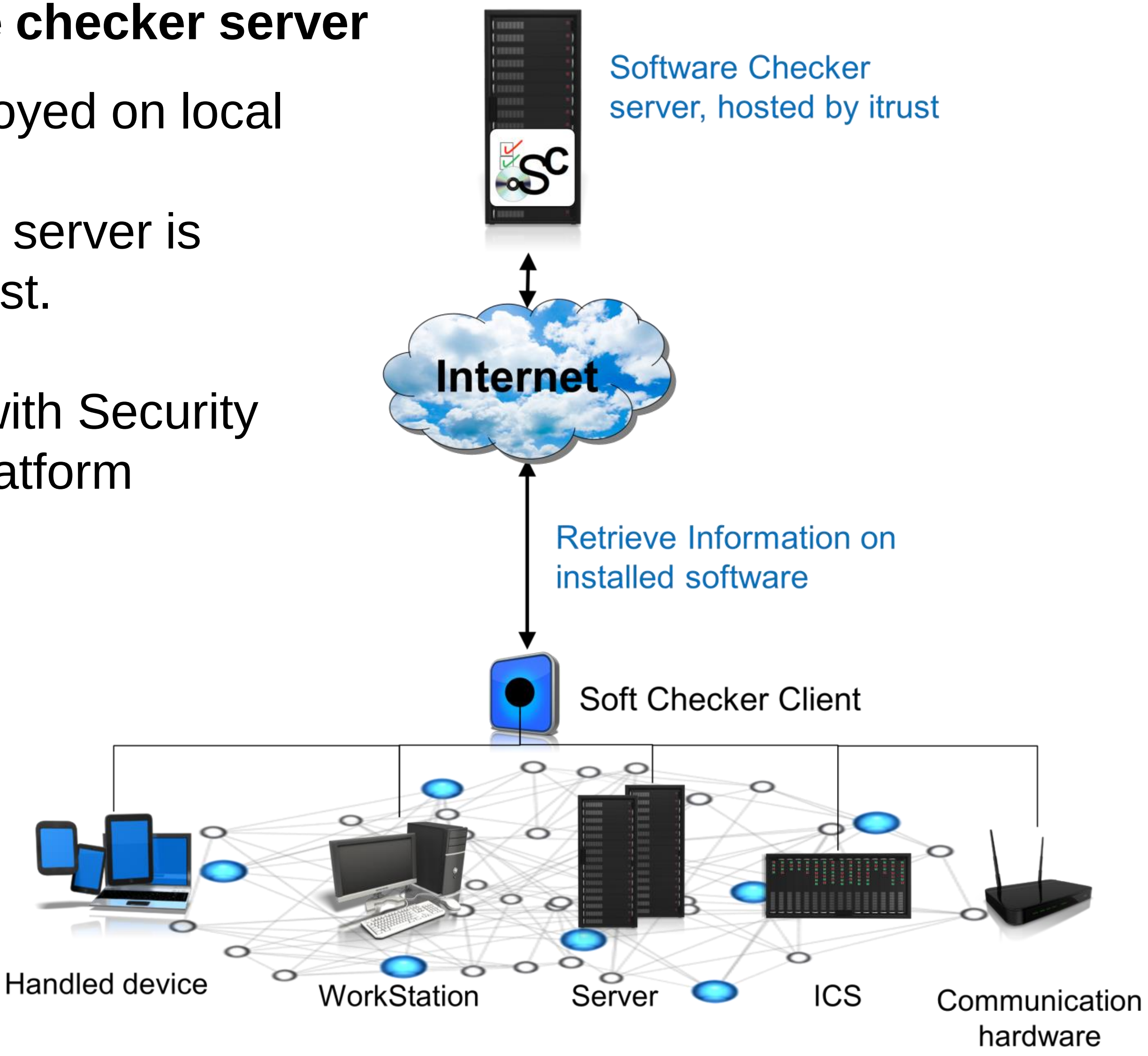
Some vulnerability have been discovered but the version of the software is correct

The software is not updated but the present version is not vulnerable

Deployment Design: Software checker as a service

External Software checker server

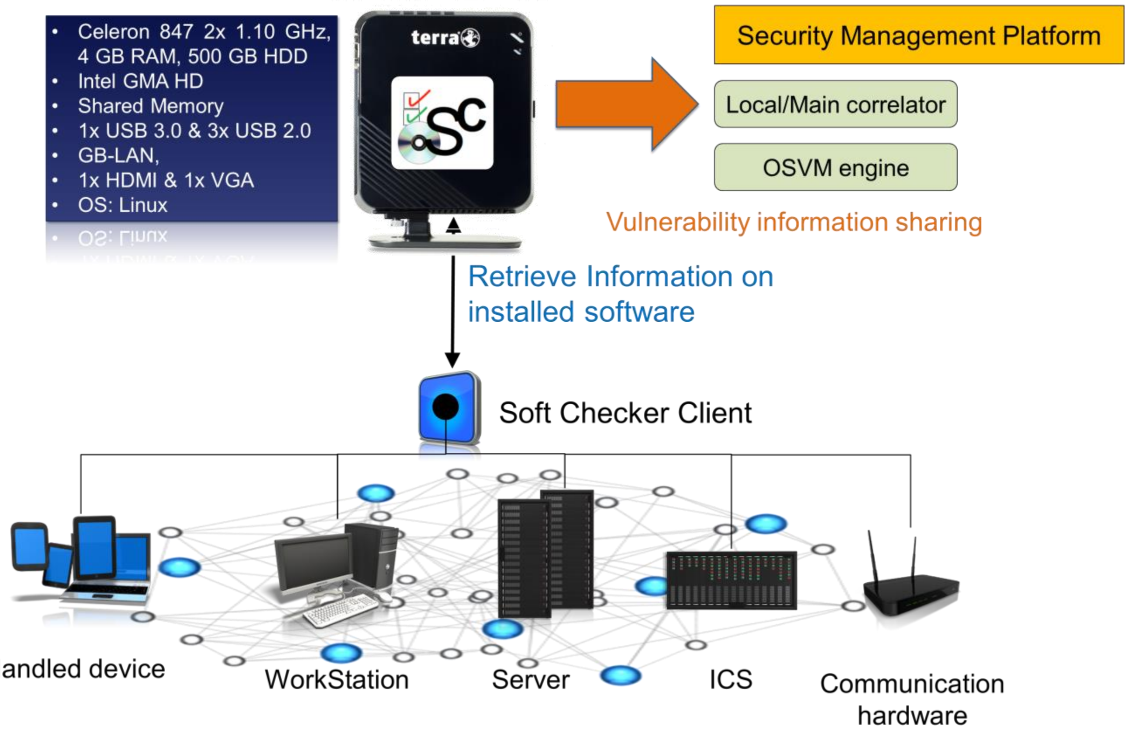
- Clients are deployed on local devices.
- Operation of the server is managed by itrust.
- No connection with Security Management Platform



Deployment Design: Software checker as an appliance

Local Software checker server

- Clients are deployed on local devices.
- The server is deployed and maintained by itrust and operated by the owner (NB: the owner is in charge of server security)
- Possibility to communicate vulnerability information with SMP, LocalMain Correlator and OSVM engine.



- Celeron 847 2x 1.10 GHz, 4 GB RAM, 500 GB HDD
- Intel GMA HD
- Shared Memory
- 1x USB 3.0 & 3x USB 2.0
- GB-LAN,
- 1x HDMI & 1x VGA
- OS: Linux

Security Management Platform

Local/Main correlator

OSVM engine

Vulnerability information sharing

Retrieve Information on installed software

Soft Checker Client

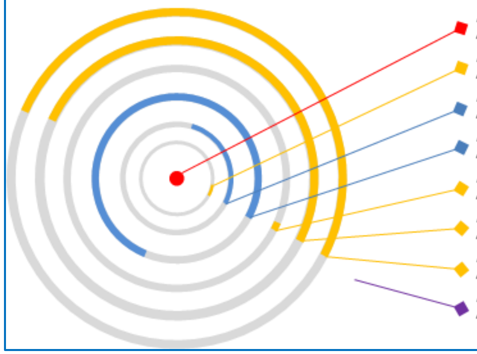
Major outcomes and future works

Major outcomes

- As the vulnerability database is multiple open sources, it allows avoiding manufacturers latency on security vulnerability of their own products and warning CI owner on the level of software vulnerability.

Time-to-response to SCADA Vulnerability

(here Schneider Electric Multiple Products Modbus Serial Driver MBAP Packet Parsing Buffer Overflow)



- 2013/01/05 Vulnerability discovered.
- 2013/01/08 Vulnerability reported to ICSCERT.
- 2013/01/24 Vulnerability acknowledged by Schneider Electric.
- 2013/03/11 Vendor publishes security notification prior to fixes being ready.
- 2013/03/13 ICSCERT provides status update.
- 2013/04/10 Alerts published for OSVDB and RBS VulnDB Service2
- 2013/05/06 Publication of this vulnerability report.
- 2013/05/17 Schneider patch availability.

- If a unknown software is discovered and referenced on the database, it could be send to malware analysis service to deep analysis.

Future issues

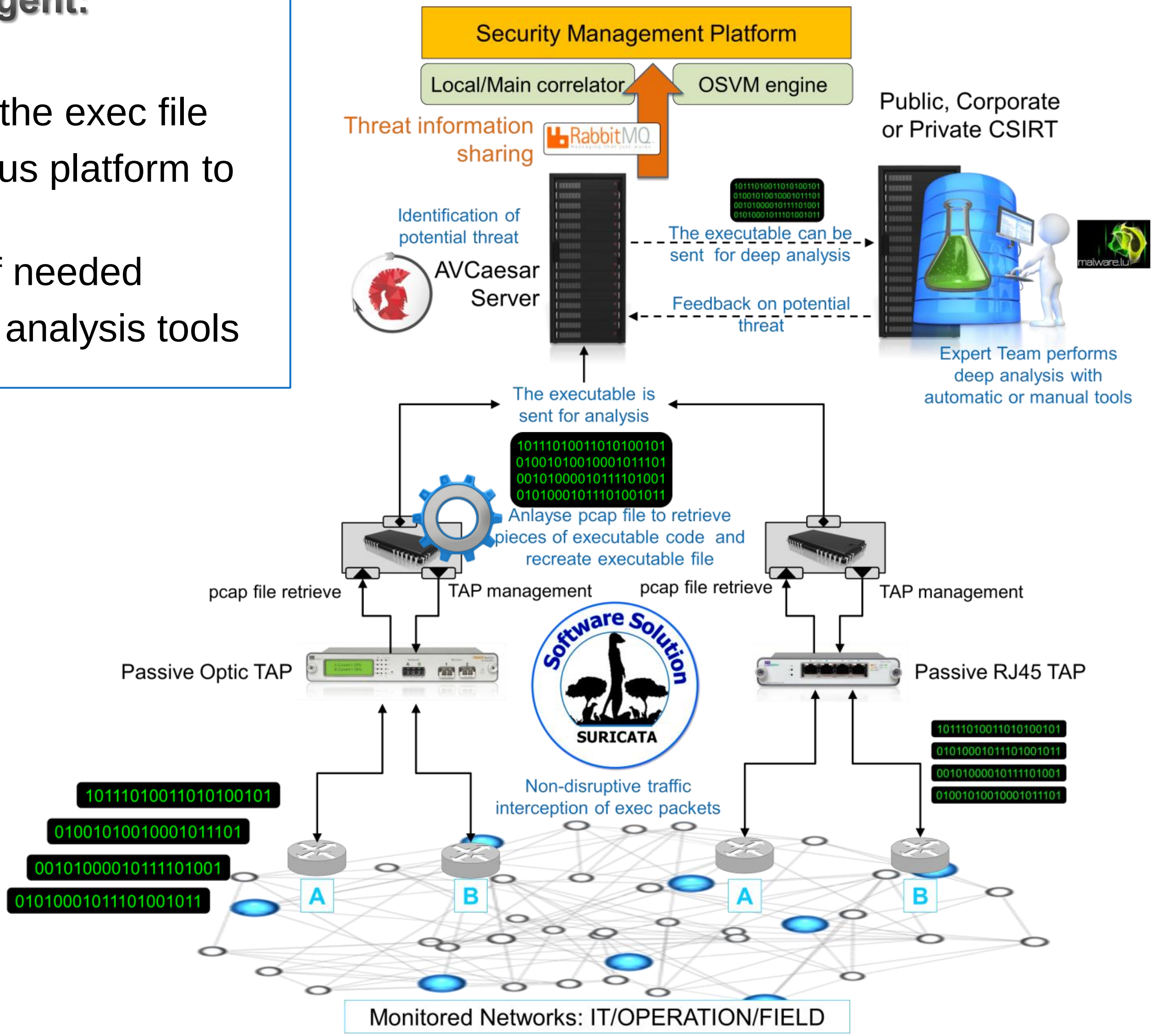
- Develop client for Linux OS, OS X, embedded OS.
- Develop a non-client supported version to test system as SCADA systems without being invasive.

AVCaesar: a global antivirus solution

Overview

Aim of the detection agent:

- Capture exec packets
- Analyse and recreate the exec file
- Send to a multi-antivirus platform to analyse criticality
- Send to expert team if needed
- Send to SMP or other analysis tools



Security Management Platform

Local/Main correlator

OSVM engine

Threat information sharing

RabbitMQ

Public, Corporate or Private CSIRT

Identification of potential threat

AVCaesar Server

The executable can be sent for deep analysis

Feedback on potential threat

malware.lu

Expert Team performs deep analysis with automatic or manual tools

The executable is sent for analysis

10111010011010100101
01001010010001011101
00101000010111101001
01010001011101001011

Anlayse pcap file to retrieve pieces of executable code and recreate executable file

pcap file retrieve

TAP management

pcap file retrieve

TAP management

Passive Optic TAP

Software Solution

SURICATA

Passive RJ45 TAP

10111010011010100101
01010001011101001011
00101000010111101001
01001010010001011101

Non-disruptive traffic interception of exec packets

10111010011010100101
01001010010001011101
00101000010111101001
01010001011101001011

A

B

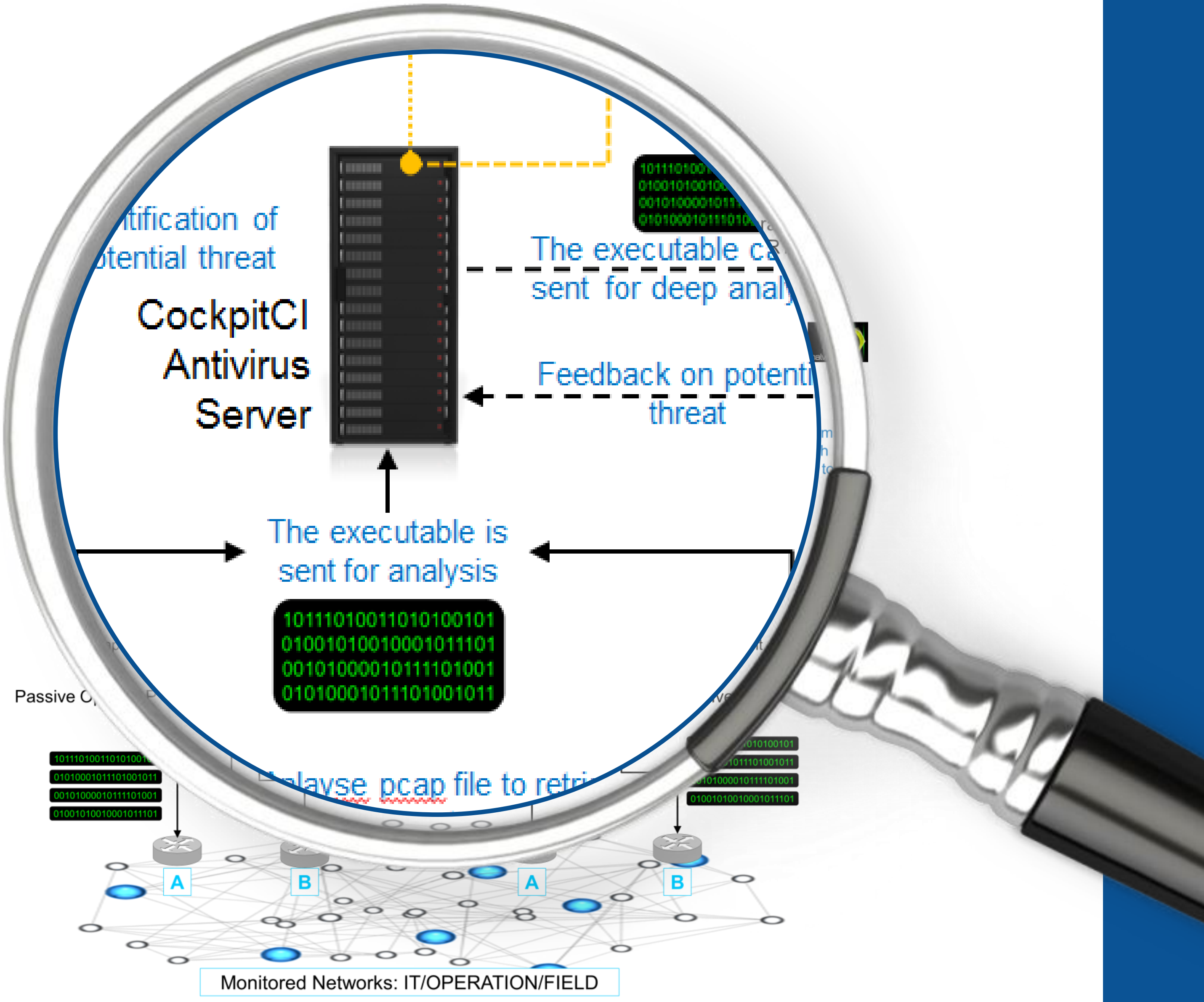
A

B

Monitored Networks: IT/OPERATION/FIELD

Scope of the demonstration of AVCaesar

AVCaesar service



tification of otential threat

CockpitCI Antivirus Server

The executable ca sent for deep analy

Feedback on potenti threat

The executable is sent for analysis

nlayse pcap file to retri

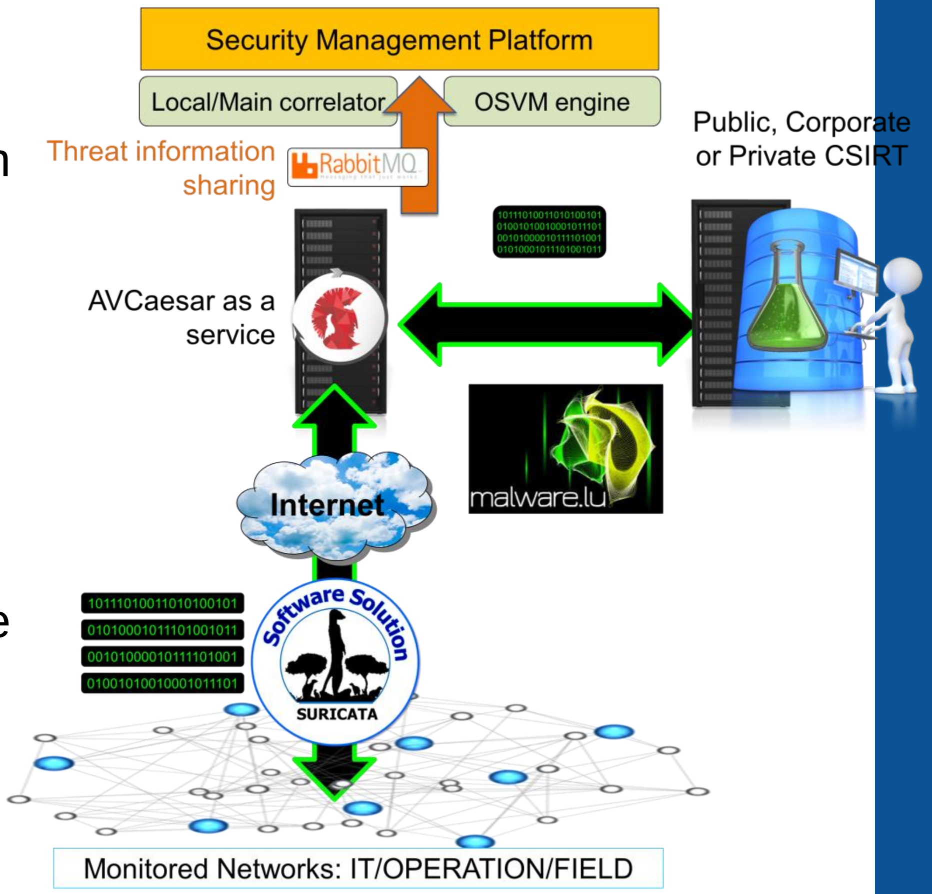
Passive O

Monitored Networks: IT/OPERATION/FIELD

Deployment Design: AVCaesar as a service

AVCaesar as a service of CERT Malware.lu operated by itrust

- Customer registered on the CERT Malware.lu and choose an option of service to use AVCaesar service:
  1. Limited files checked by month or year
  2. Unlimited files option.
- Operation of the server is managed by itrust.
- The tap management used software option.
- The connection with Security Management Platform will be enable but limited due to the bandwidth.



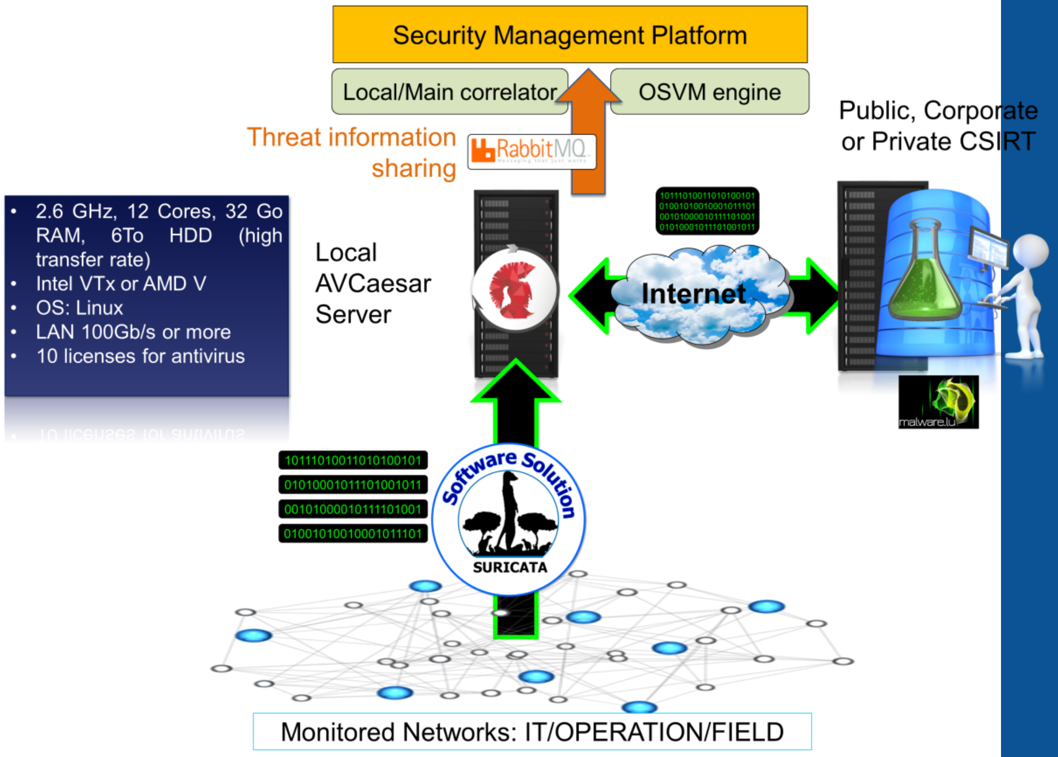
Security Management Platform
Local/Main correlator
OSVM engine
Threat information sharing
RabbitMQ
Public, Corporate or Private CSIRT
AVCaesar as a service
malware.lu
Internet
Software Solution
SURICATA
Monitored Networks: IT/OPERATION/FIELD

Deployment Design: AVCaesar as an appliance

Local AVCaesar server

- Server is located in the customer premises (need of 10 antivirus licenses)
- The server is deployed and maintained by itrust and operated by the owner (NB: the owner is in charge of server security)

- The owner can choose hardware tap option to increase the solution (the deployment and adaptation of these devices belongs to end-users).
- Possibility to communicate threat information with SMP, LocalMain Correlator and OSVM engine.
- The files can also be send to Malware.lu for deep analysis.



- 2.6 GHz, 12 Cores, 32 Go RAM, 6To HDD (high transfer rate)
- Intel VTx or AMD V
- OS: Linux
- LAN 100Gb/s or more
- 10 licenses for antivirus

Security Management Platform
Local/Main correlator
OSVM engine
Threat information sharing
RabbitMQ
Public, Corporate or Private CSIRT
Local AVCaesar Server
Internet
Software Solution
SURICATA
malware.lu
Monitored Networks: IT/OPERATION/FIELD

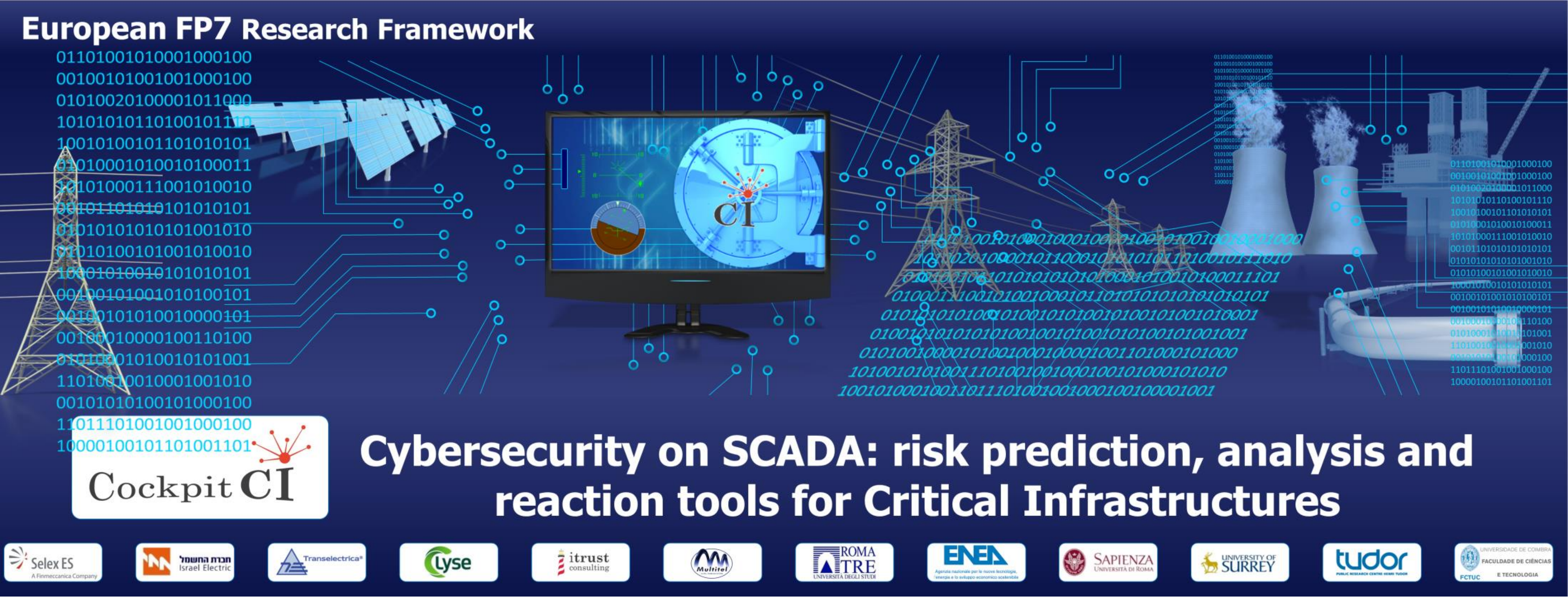
Major outcomes and future works

Major outcomes

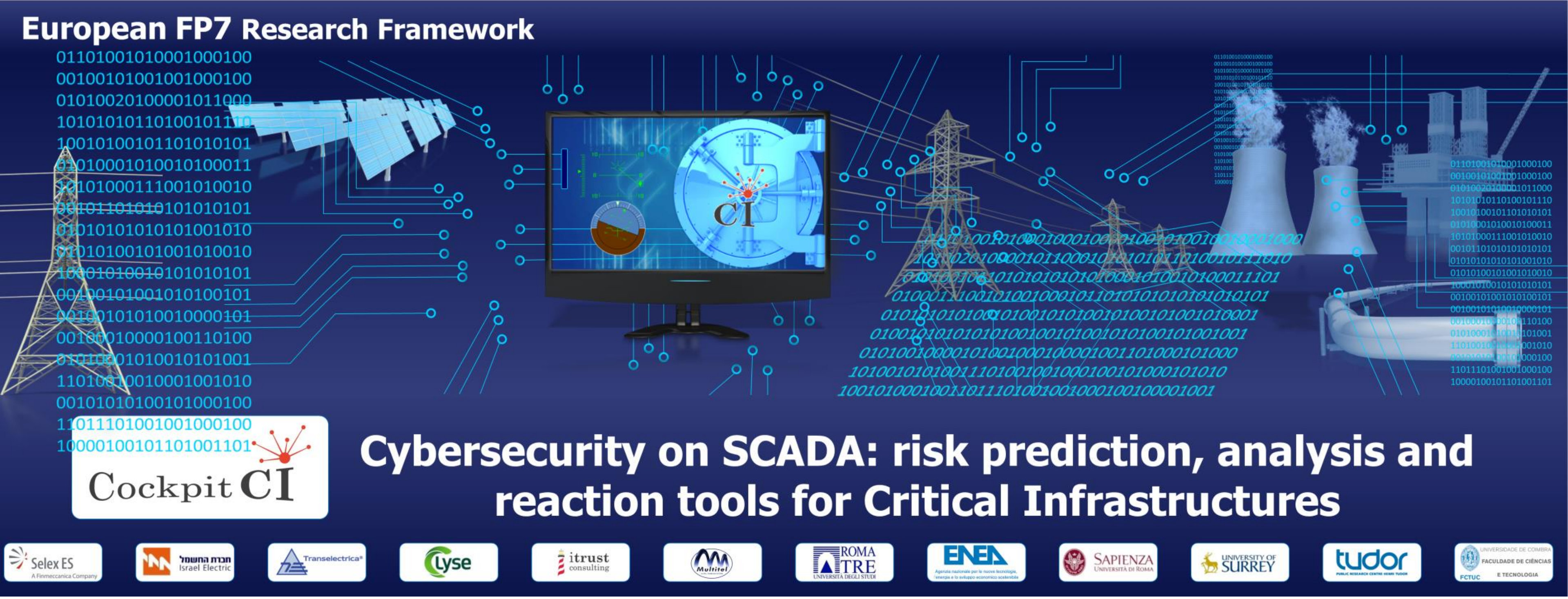
- This antivirus enables in real-time 10 antivirus simultaneously
- The antivirus could be deployed as a web-service (reachable as request) or a dedicated components of the CIs network to treat sample of traffic
- The antivirus engine is connected either on-line or off-line with updated database of malware (open database *malware.lu*).
- The web-service is part of CSIRT service which allows sharing cyber-alert and receiving cyber detection notification.
- The system is deployed as service at 30th October and is intended to be proposed to our industrial partners to test it (IEC, Transelectrica and Lyse)
- The system will be tested by governmental and European organisation in the next months.

Future issues

- Enable the information sharing to the SMP
- Deploy the system on the Hybrid-test bed



Any question ?



European FP7 Research Framework

Cockpit CI

Cybersecurity on SCADA: risk prediction, analysis and reaction tools for Critical Infrastructures

Thank you for your attention