

ADVANCED CYBER-THREAT INTELLIGENCE, DETECTION AND MITIGATION PLATFORM FOR A TRUSTED INTERNET OF THINGS

MEETING THE NEEDS OF INFORMATION AMONG LEAS AND ISPS

D. KAVALLIEROS – KEMEA



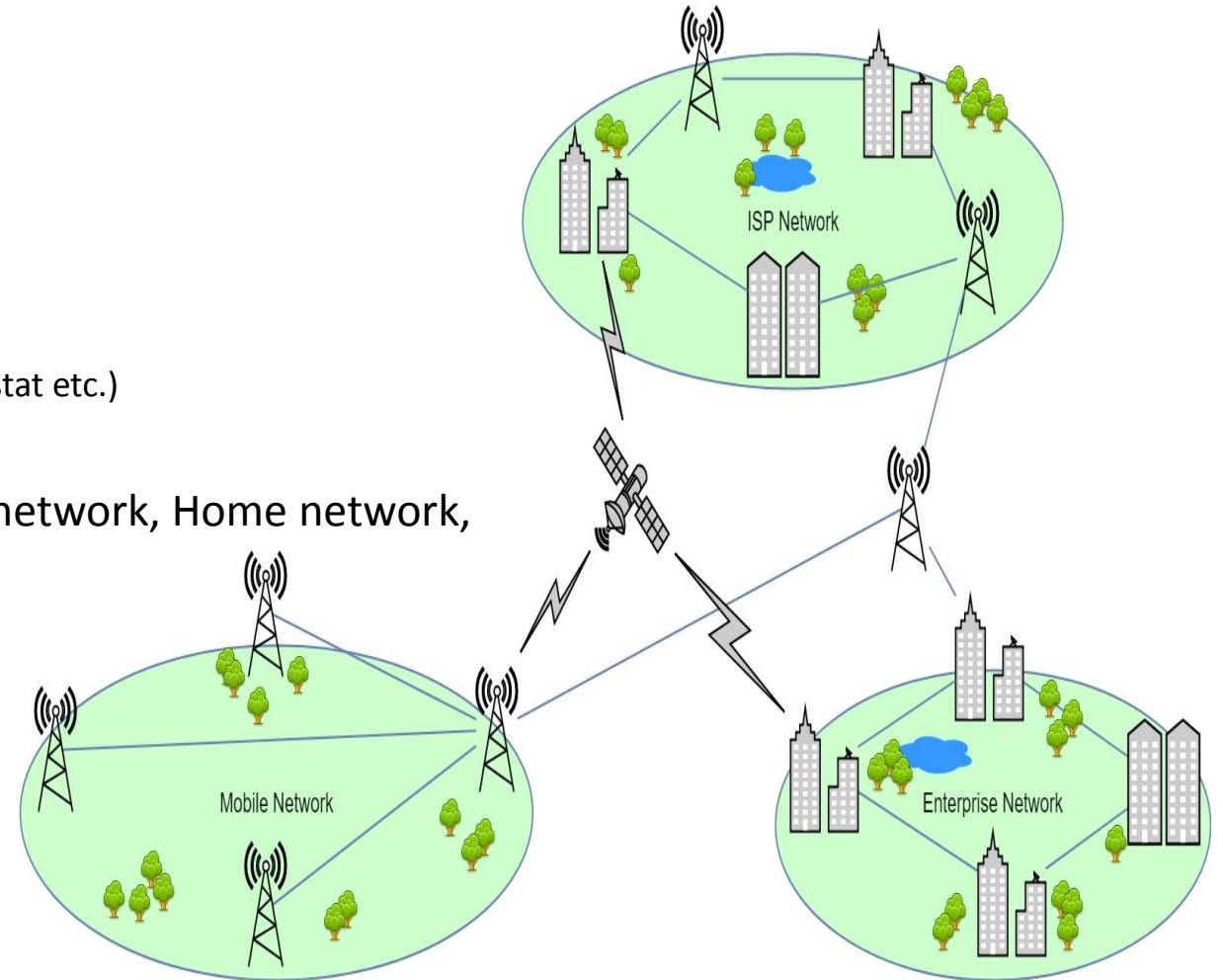
This work is performed within the **Cyber-Trust Project** (Advanced Cyber-Threat Intelligence, Detection and Mitigation Platform for a Trusted Internet of Things), with the support of the European Commission and the Horizon 2020 Program, under **Grant Agreement No 786698**



“The CYBER-TRUST project aims to develop an innovative cyber-threat intelligence gathering, detection, and mitigation platform to tackle the grand challenges towards securing the ecosystem of IoT devices”



- The increasing number of smart devices (IoT)
- The increasing areas of applications
 - ☐ Industry
 - ☐ Cars
 - ☐ Sensors (e.g. Cameras)
 - ☐ House (e.g. fridge, air conditioner, baby monitor, thermostat etc.)
 - ☐ Wearable devices (e.g. watches, glasses, etc.)
- The interconnectivity between networks (e.g. ISP network, Home network, Business network etc.)
- The massive transfer of important and personal data through multiple networks.
- The increasing number of attacks and the appearance of zero-day vulnerabilities in smart-devices.



SO1

- Create a new paradigm for the NG cyber-security defense systems

SO2

- Quickly detect and effectively respond to sophisticated cyber-attacks

SO3

- Deliver advanced solutions for collecting forensic information

SO4

- Minimize impact on sensitive data protection and user's privacy

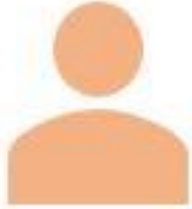


The Cyber-Trust “Cyber-Threat Intelligence, Detection and Mitigation Platform for a Trusted Internet of Things” software platform, is showcasing how Law Enforcement Agents will be assisted in viewing and receiving information from Telecom/Internet providers and Smart Homes that potentially holds digital evidences of specific cyber-crimes, in a timely manner.

1. Create an efficient communication between LEAs and ISPs through cyber-trust platform
2. Enhance the investigation methods and tools of Law Enforcement Agencies (LEAs)
3. Detect and respond to malicious cyber-threats towards Smart-Homes

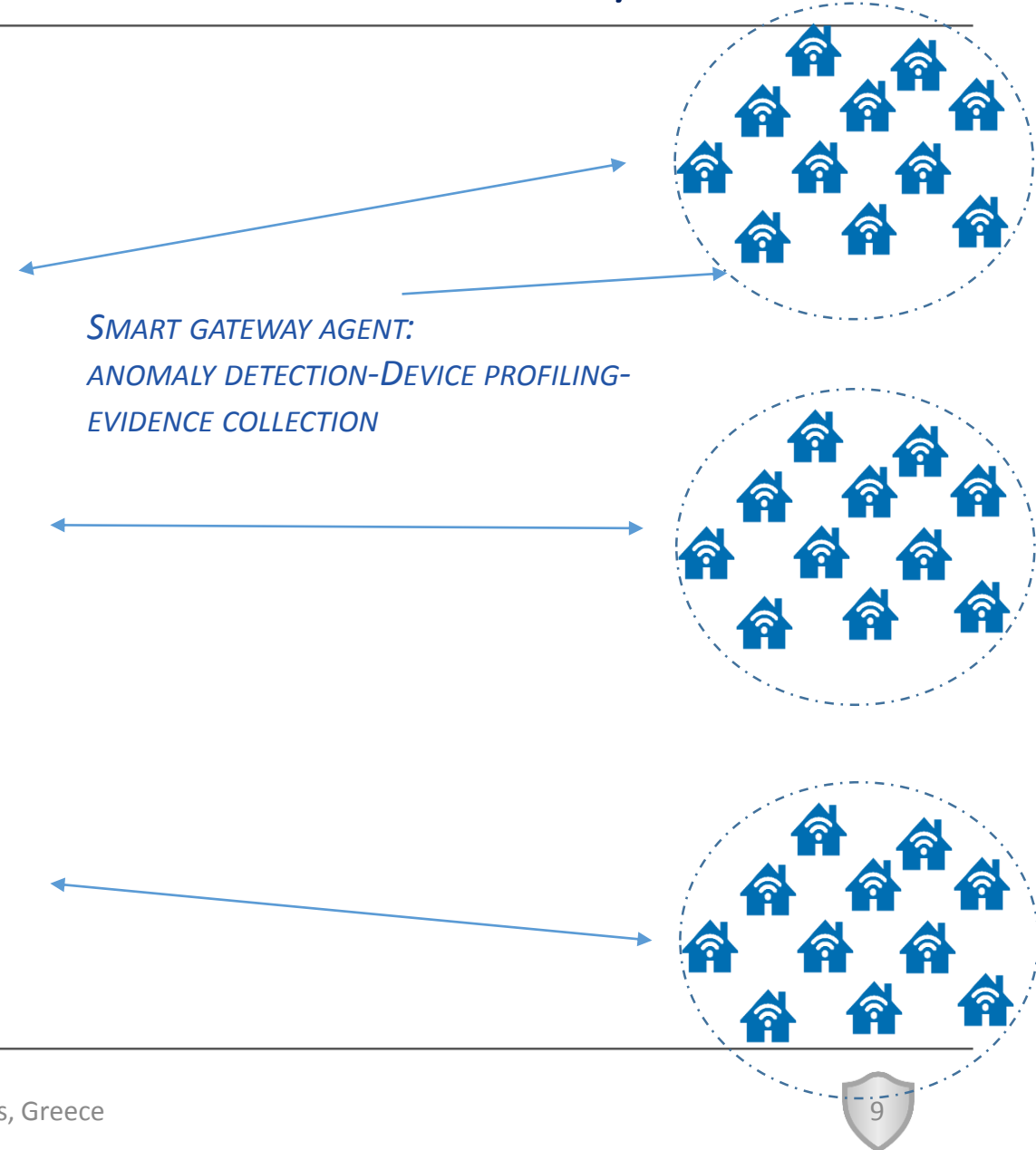
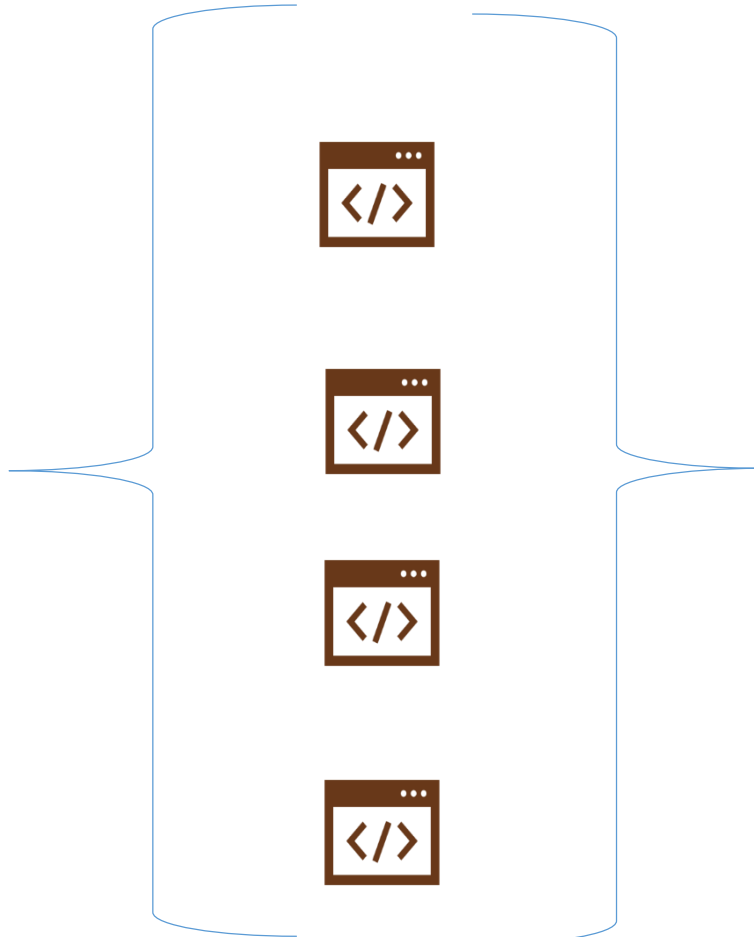


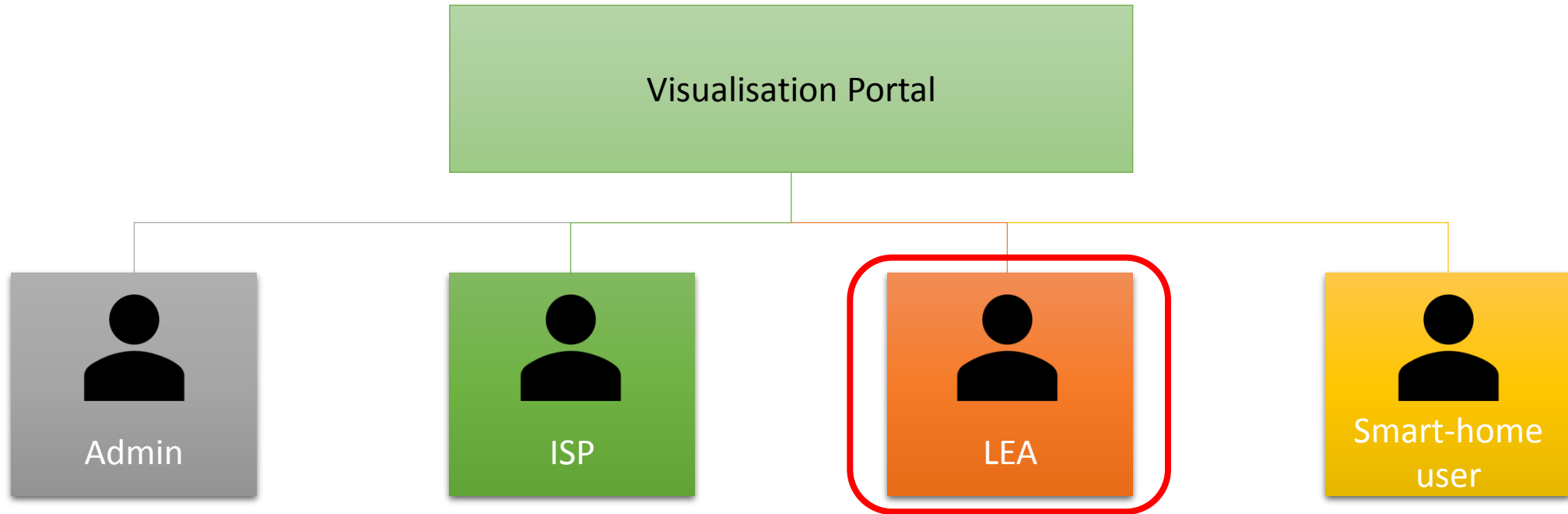
Map The leas needs

1. state-of-the art of industrial and research solutions
2. Creation of end-user Questionnaires
3. Development of use cases
4. Identification of end-user requirements
5. Prioritization of end-user Requirements through Moscow Analysis
6. Functional and Non-Functional Requirements of platform
7. Translation to system & technical requirements

	Industry and organization employers (e.g. Internet Service Provider): <ul style="list-style-type: none">• Information Security Operation Centre (ISOC/SOC) team member• Network Security/Cyber Security Expert• Risk assessment and management• Computer Security Incident Response Team (CSIRT) team member• Network/Data/System administrator
	Digital forensic and blockchain experts: <ul style="list-style-type: none">• LEA (Cyber-Crime investigator)• LEA (Digital evidence examiner)• Non-LEA Digital forensic expert• Blockchain experts
	Smart Home/Device Owner (SHO): <ul style="list-style-type: none">• Smart homeowners• Users possessing smart devices (e.g. smart-phone, smart-home appliances etc.)

Cyber-trust Goal







LEA

Logout

CASES

List

Cases

Cases list

Copy data

.CSV

.XLS

.PDF

Print

Add new case

Refresh

Search:

Case ID	Status	Reference	Date opening
1	Open	Test ref	2019-09-27 10:12:00
2	Open	Ref test2	2019-09-18 11:05:00
3	Open	Test 4	2019-09-27 11:24:00
4	Open		2020-01-01 22:39:00
5	Open	Test ref	2019-10-02 00:00:00

Showing 1 to 5 of 5 entries

Previous

1

Next



Cases

LEA

Logout

CASES

List

Case

Cases list

Internal case reference number

MSE 2019

Legal process

Trial

Nature of the case

Criminal case

Legal processed signed data

2019-10-29 00:00:00

Request due date

2019-11-08 00:00:00

Reference

MSE 2019 cyber-attack

Accounts

LAE 1

Back

Cases

LEA

Logout

CASES

List

Cases list

MSE 2019 | Trial

Case information

Internal case reference number

MSE 2019

Legal process

Trial

Nature of the case

Criminal case

Legal processed signed data

2019-10-29 00:00:00

Request due date

2019-11-08 00:00:00

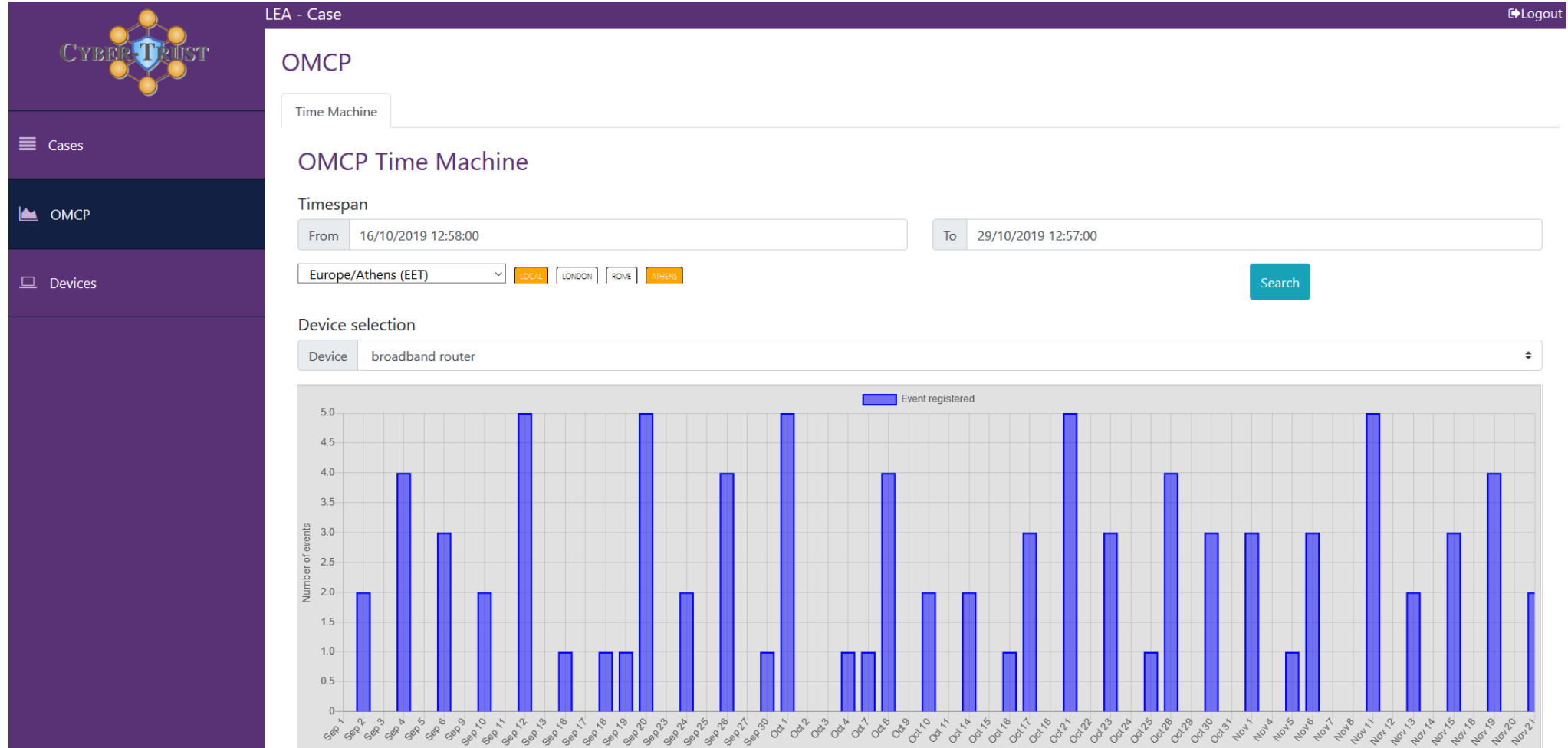
Reference

MSE 2019 cyber-attack

Accounts

LAE 1

Back





Cases

OMCP

Devices

LEA - Case

Logout

Case Components

Devices

Devices list

Add new deviceRefresh

Search:

Copy dataCSVXLSPDFPrint

Description	Type	Owner	OS	Manufacturer	Model
		5cdd5aca6ec17ba4a7ceb05a	null	null	SM-A510F
		5cdd5aca6ec17ba4a7ceb05a	null	null	SM-A510F
44	1111	5cdd5aca6ec17ba4a7ceb05a	UNIX	CISCO	4
44	1111	5cdd5aca6ec17ba4a7ceb05a	UNIX	CISCO	4
44	1111	5cdd5aca6ec17ba4a7ceb05a	UNIX	CISCO	4
44	1111	5cdd5aca6ec17ba4a7ceb05a	UNIX	CISCO	4
decri	type	5cdd81de6ec17ba4a7ceb9dc	android	samsung	SM-A510F
decri	type	5cdd81de6ec17ba4a7ceb9dc	android	samsung	SM-A510F
descr	Kind	5cdd5aca6ec17ba4a7ceb05a	OS2	Samsung	SM-A510F
My Nexus	smartphone	5cde72bf6ec17b07a2aeab9	Android	Samsung	SM-A510F

Showing 1 to 10 of 41 entries

Previous12345Next

1. Secure chain of custody
2. Access in timely manner
3. State-of-the art research solutions
4. Easier to control and share information between ISPs and LEAs



www.cyber-trust.eu



twitter.com/CyberTrustEU



www.linkedin.com/groups/13627755



www.facebook.com/cybertrust/



Thank you for your attention!

Dimitrios Kavallieros

Project Coordinator

Tel.: +30 2107710805 (ext. 399)

e-mail: d.Kavallieros@kemea-research.gr



www.cyber-trust.eu



www.kemea.en