Supporting operational communities

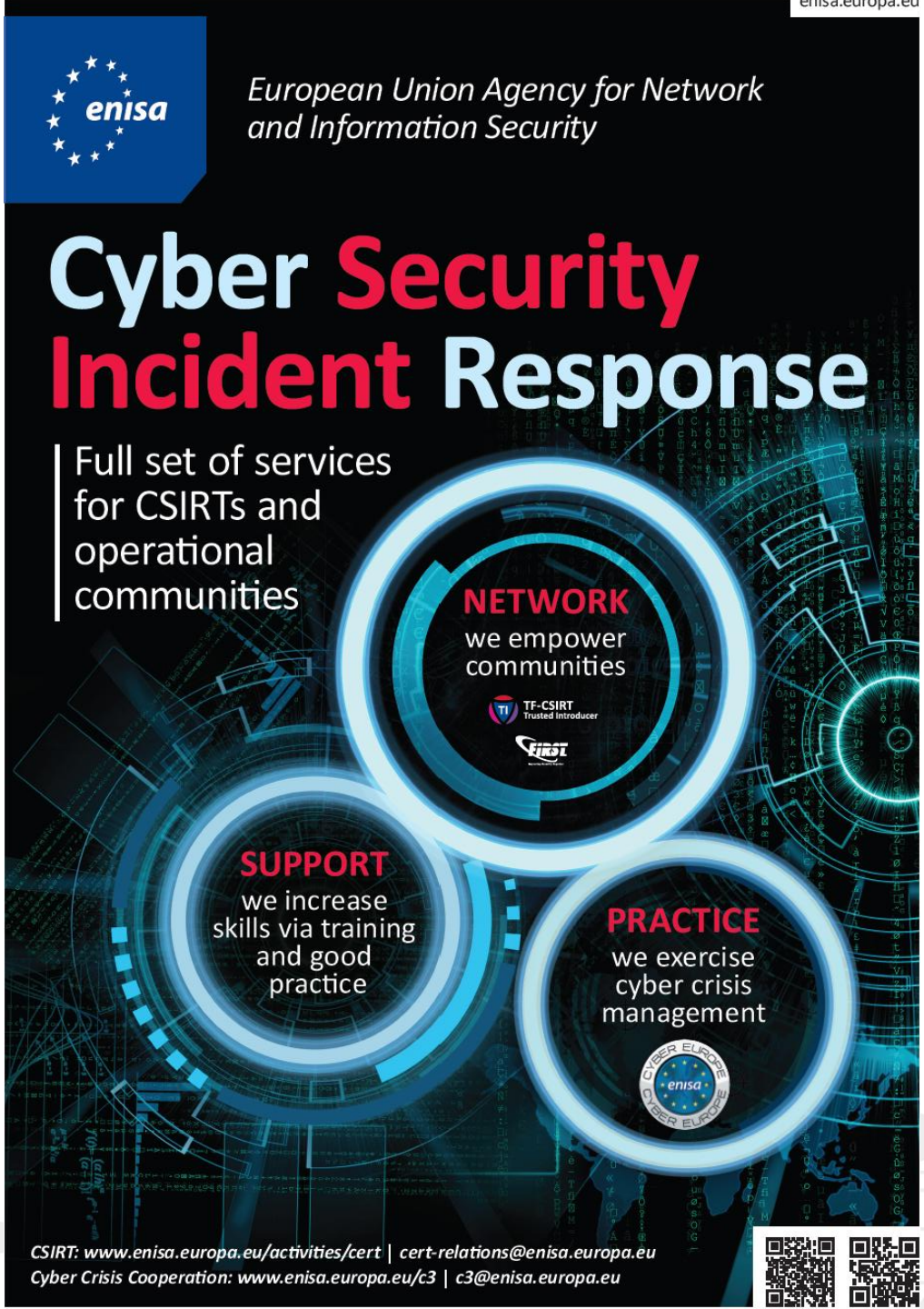
Lauri Palkmets, Yonas Leguesse

European Union Agency for Network and Information Security

Core Operational Department

Operational Security Unit

Operational Security Unit #COD3#



Initiatives since:

2005 Start up programme for CSIRTs (ENISA guidelines and support on how to set up and operate CSIRT)

2008 Focus on national and governmental CSIRTs – defining minimum requirements for operations

2010 Cyber Europe Exercise (EUROPE's first ever EU cyber security exercise; continued in 2012, 2014, 2016)

2011 CSIRT and Law Enforcement cooperation support (information sharing and fight against cybercrime)

2013 Operational training programme (for CSIRTs and other ICT security specialists)

2015 Train the trainer programme (to enlarge the CSIRT training capacity in Europe)

http://www.enisa.europa.eu/activities/cert

CSIRTs in Europe – Q1/2016

Currently in Europe 275 teams listed! Around 1/6 are n. or g. CSIRTs.

Austria
Belgium
Bulgaria
Croatia
Czech Republic
Denmark
Estonia
Finland
France
Germany
Greece
Hungary
Iceland
Ireland
Italy
Latvia
Lithuania
Luxembourg
Malta
Netherlands
Norway
Poland
Portugal
Romania
Slovakia
Slovenia
Spain
Sweden
Switzerland
United Kingdom
EU Institutions

We are building and actively supporting a growing network of national/governmental CSIRTs

CSIRT Interactive MAP: http://www.enisa.europa.eu/activities/cert/background/inv/certs-by-country-interactive-map

Cybersecurity Exercises by ENISA

Cyber Europe 2010

- Europe's first ever EU cyber security exercise

Joint EU-US Cybersecurity Exercise 2011

- First transatlantic cooperation exercise

Cyber Europe 2012

- Testing the EU Standard Operational Procedures (EU-SOPs)

EuroSOPEx 2012

- Large scale realistic cyber-crisis exercise

Cyber Europe 2014

- Involved MS, private sector and EU institutions.
- Testing the EU Standard Operational Procedures (EU-SOPs)

Cyber Europe 2016

- In planning phase

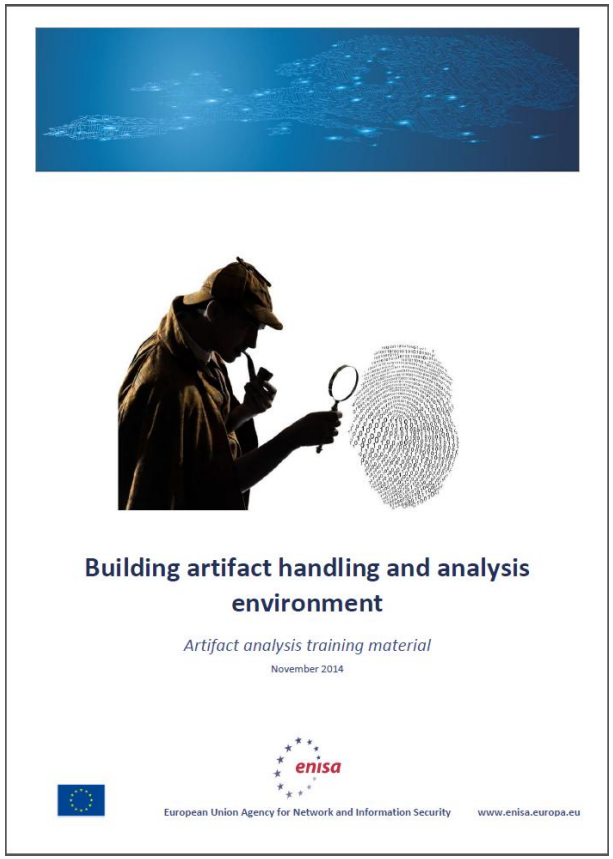
ENISA's library

- Good Practice Guide for Incident Management
- Proactive detection of incidents
- Fight against Cybercrime
- Alerts-Warnings-Announcements
- Incident Handling Automation
- Actionable Information

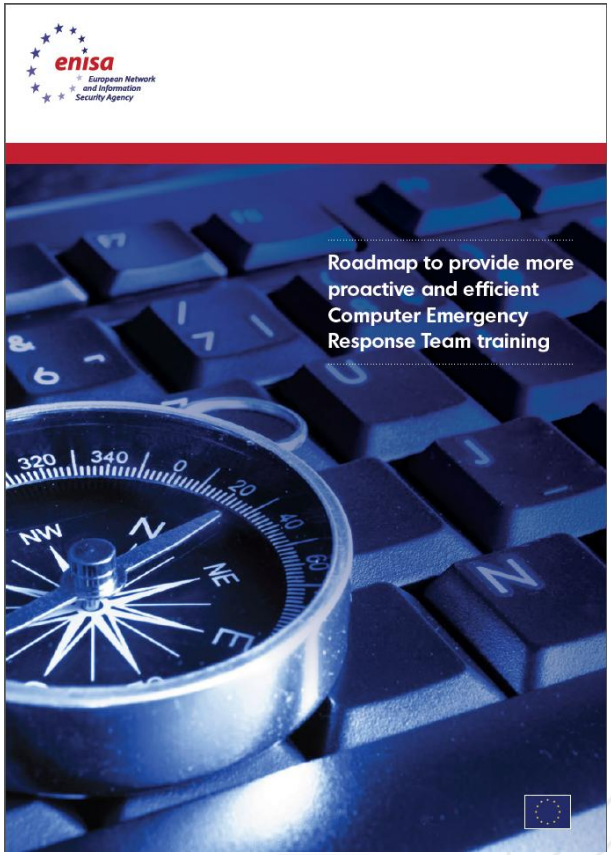
https://www.enisa.europa.eu/activities/cert/support

Material, Roadmap and Methodology

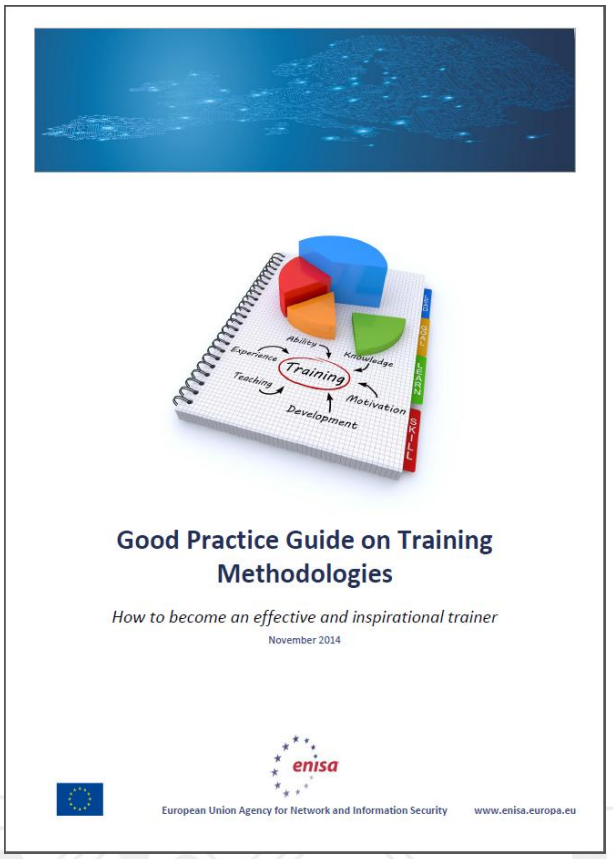
Material since 2008



Roadmap from 2012



Methodology from 2014



Delivered to the stakeholder

More than 35 different topics

Courses follow the needs of operational communities

ENISA trains trainers, multipliers and operational communities

Training Courses

Training Resources

https://www.enisa.europa.eu/activities/cert/training

Examples of training resources

Mobile threats incident handling

Digital forensics

Large scale incident handling

Network forensics

Triage & basic incident handling

Vulnerability handling

Artifact analysis fundamentals

Advanced artifact handling

Writing security advisories

Developing countermeasures

Identification and handling of electronic evidence

Automation in incident handling

Artifact analysis process chart

RTIR

Viper

MISP, CRITs

Virtualbox, Cuckoo, Volatility

MISP, CRITs

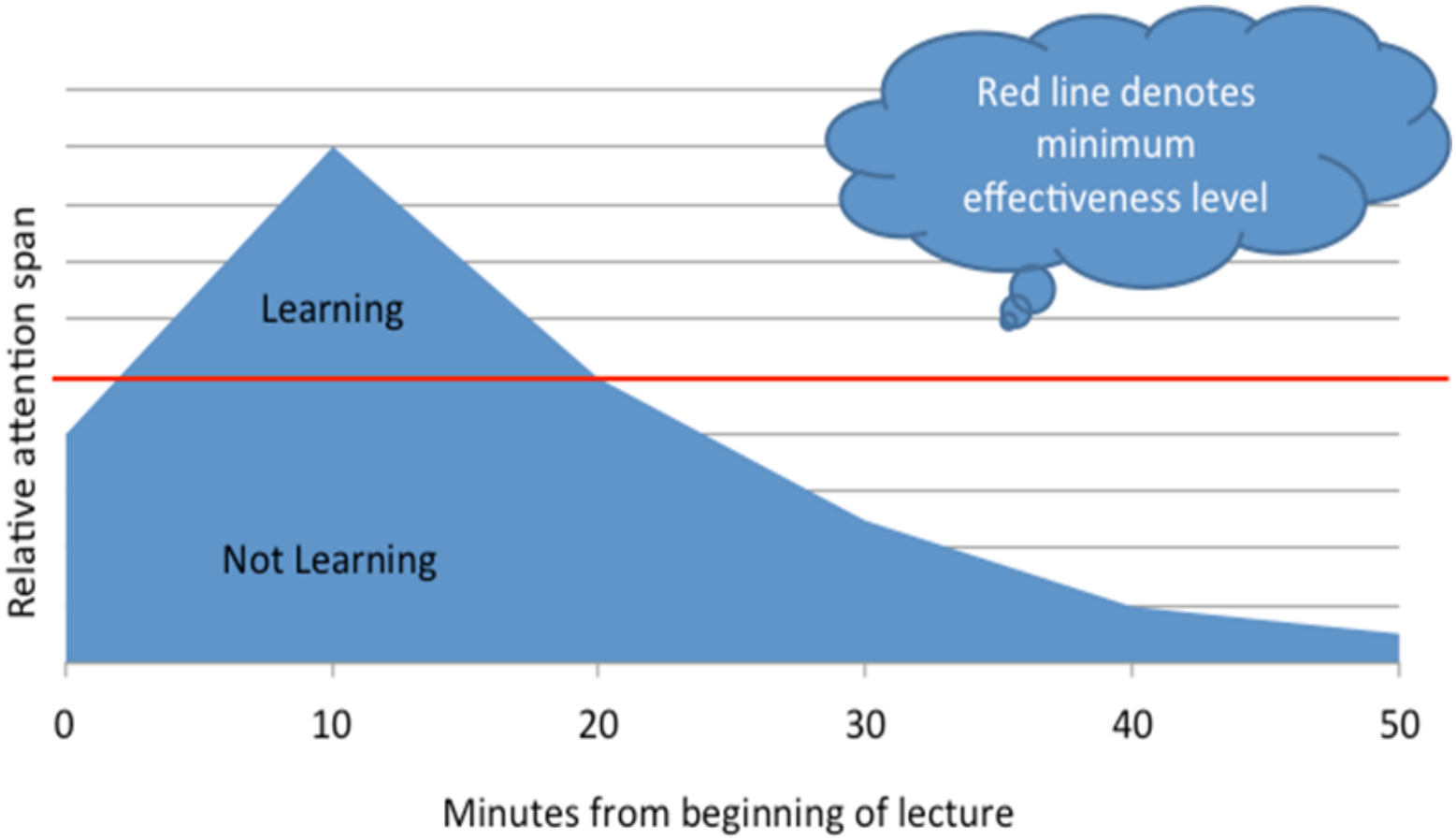
Debuggers: Ollydbg, Radare2, Immunity DBG , X64DBG, IDA Free
Memory Dumpers: LordPE, OllyDump
.Net deobfuscators: de4dot, ILSpy
Packer Detection: Detect It Easy, PeID, Exeinfo PE, PEView, PE Tools

MISP, CRITs

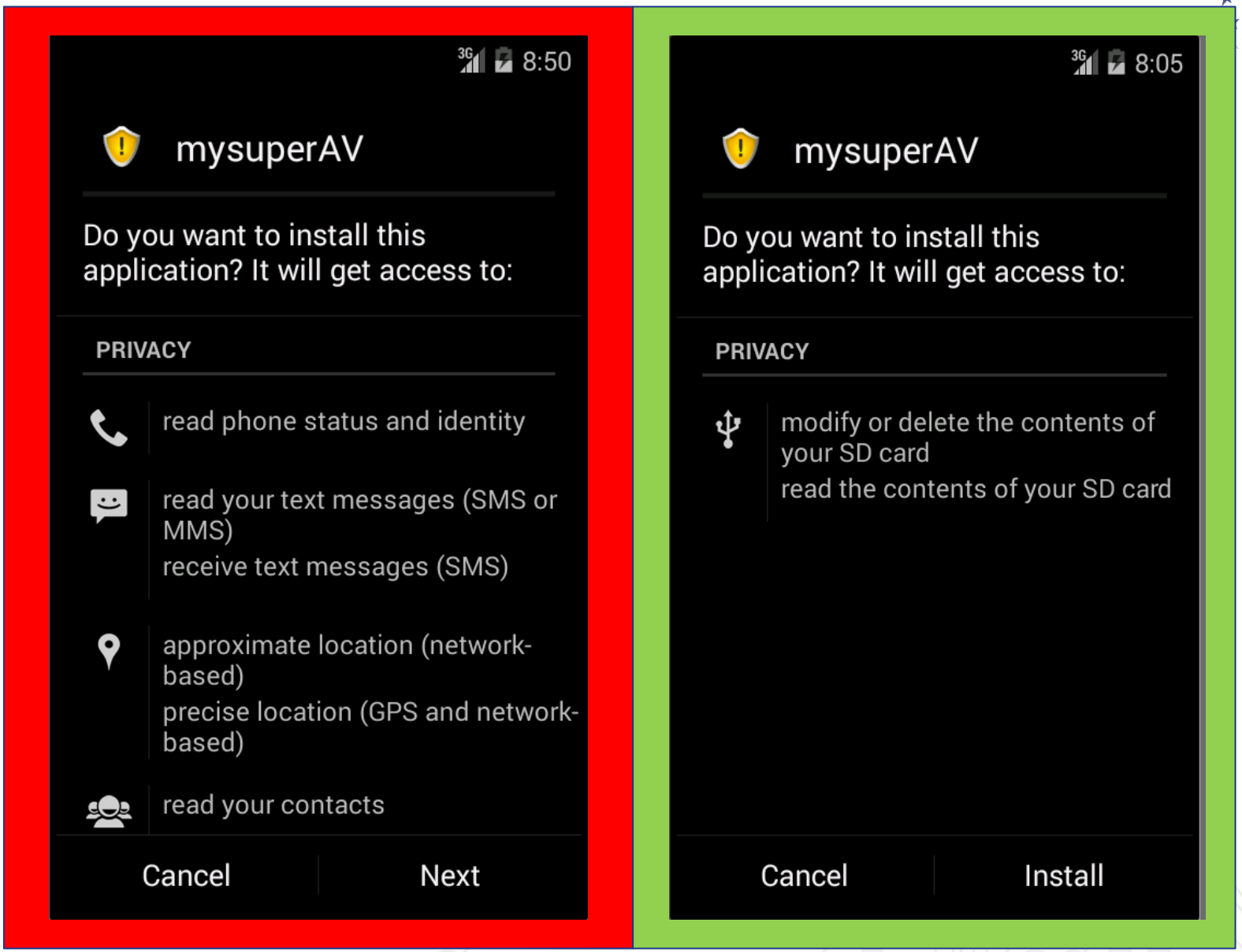
Train the trainers events

- Methodologies of conducting trainings
- Training needs and demands for trainers and teams
- Available trainings / cost models / efficiency

Good practice guide on training methodologies

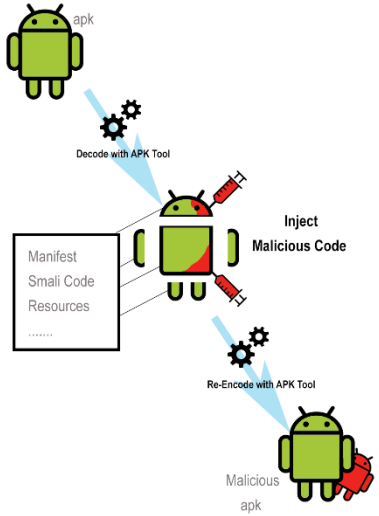


Mobile threats incident handling



What will we see?

App Cloning



Malware:

- SimpleLocker
- Pincer

OS Vulnerabilities: Webview

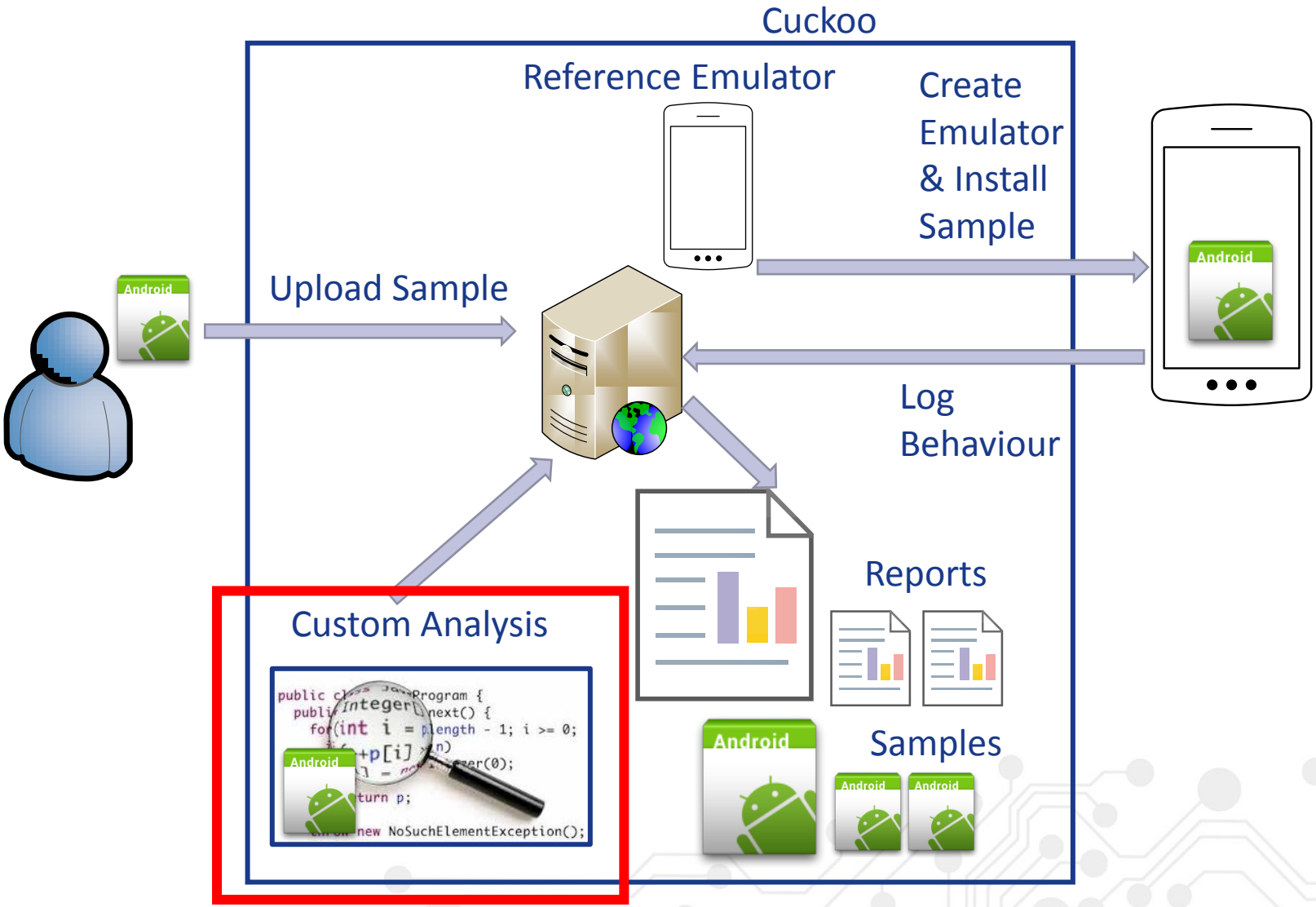
Mobile threats incident handling

VM – Toolset!

- Static analysis
- Dynamic analysis
- Network analysis
- ……

We provide tools, information, knowledge, and guidance that allows participants to set up their own analysis environments.

Cuckoo/Droid



Thank you

PO Box 1309, 710 01 Heraklion, Greece

Tel: +30 28 14 40 9710

info@enisa.europa.eu

www.enisa.europa.eu