

Service and tool developed and operated by :



# AVCaesar

Type: Meta antivirus tool

Security Management Platform

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

disruptive traffic

Architecture principle

pcap file retr

Threat information

Identification of

AVCaesar Server

sharing



Public, Corporate

or Private CSIRT

xpert Team perform deep analysis with

automatic or manual tools

Passive RJ45 TAF

Packaging: Web service solution

Private server solution

## System requirements

- Internet Browser
- For the private server: 2.6 GHz, 12 Cores, 32 Go RAM, 6To HDD (high transfer rate), Intel VTx or AMD V, LAN 100Gb/s or more
- For the private solution : 10 licenses for antivirus

#### **Main Functionalities**

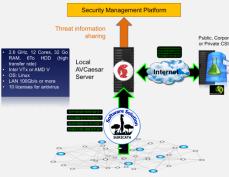
- In real-time 10 antivirus simultaneously
- Web-service (reachable as request)
- Dedicated components of a network to treat sample of traffic
- Possible connection with Security Management Platform to centralise alert.
- Connected either on-line or off-line with updated database of malware (open database malware.lu).
- Part of CSIRT service which allows sharing cyber-alert and receiving cyber detection notification.

## Deployment



#### Web Service solution

- Registration on the CERT Malware.lu
  - Service options: Limited files checked by month or year
  - Unlimited files option. Service operated by malware.lu branded by itrust



Passive Optic TAP 🚺

#### Private server solution

- Server hosted by user but deployed and maintained by malware.lu.
- Communication with security platform enabled
   Communication with
  - Communication
    CERT enabled

# For more information contact info@itrust.lu or click on this link Info