About Open-Source and CSIRT

Prof Nabil SAHLI (nabilsahli@gmail.com / n.sahli@ansi.tn)

FIRST
Improving Security Together

الوكالة الوطنية للسلامة المعلوماتية
Agence Nationale de la Sécurité Informatique
tunCERT
Tunisian Computer Emergency Response Team

Cost of Implementation of a CSIRT **Infrastructure**

- Equipments (PCs+ Servers + forensics tools)
- Software tools :
  - **License fees**

  --> Recurent **Big annual Maintenance fees**

How to decrease this big « cost center »
+ avoid delays (+…) in CSIRT iservices mplementation, (escape from « our » painful and long administrative acquisition procedures)

Be able to More Invest in **Capacity Building** (**training**, …) & the funding of CSIRT activities (awareness compaigns, …)

CSIRT's Software Needs

Need for a « Strong »
CSIRT Security Architecture
➔ Cardinal and qualitative Completness of deployed Solutions

Need for Tools for implementing the CSIRT process

Need for various and multi-platform investigation and forensics tools

Bigs Budgets (Expensive licenses, Recurent cost of maintenance fees,..)

SOLUTION =Use of OPEN-SOURCE tools

~ 0 Licences

Open-Source

"Beautiful world"

- Free Licences
- Sources Codes availables

+ Respect of standards
+ GUIs and Good Community assistance
+ Perinity (better than some commercial solutions)

+ NOW: available optional «Contractual Support» & Training, for "must" solutions (OpenCore)

FALSE Myths

Open source is "insecure" myth

"it's insecure because everyone can see how it works."

--> **No software relies on the obscurity of source code for security**. If there was any truth in that, Microsoft Windows would be the most secure OS ever created,

Commercial tools have better "support" myth

--> The "Must" open source tools have "contractual cheap support" (training, assistance, …)
+ Very Rich and Friendly assistance from the (philantropic) Community of open-source

OTHER IMPACTS

Free access to Source codes

Open Source Tools Can be Customized/Extended

An enabler for R&D activities

(Other potential Return On Investment)

You are a "Legal provider" of Open source Security solutions

Open Source Tools Can be installed by the CSIRT on the constituency's infrastructures

Once you have handled an incident

--> Need to IMMEDIATELY strength the constituency Security

--> Install Open source security Tools

Available on FIRST youtube channel of the symposium

Training "Open Source Tools for CSIRT" session

PLAN

I- About Open-Source and CSIRT

CSIRT Infrastructure

II- Network Security Architecture

III- Cyber-space Monitoring and Honeynet systems

CSIRT Activities

IV- CSIRT Process Management systems

- Alert and Warning Process
- Incident Handling Process

V- Forensics and investigation tools

Take OUT

- ***Connection credentials to Live Platform and/or Download of Live-DVD***
- ***Additional Trainings on demand***