CERT.LV
Informācijas tehnoloģiju drošības incidentu novēršanas institūcija

ENISA National Cyber Security Strategies workshop

Responsible Disclosure

May 13, 2015 RIGA LATVIA

Varis Teivans
CERT.LV

What is Responsible Disclosure?

CERT.LV
Informācijas tehnoloģiju drošības incidentu novēršanas institūcija

- **Responsible**
  - Coordinated disclosure
  - Rules of engagement & principle of doin the least possible harm just to provide POC
    - ISO/IEC 29147, ISO/IEC 30111
  - Intention
- **Full disclosure**
  - Good
  - Bad
  - Ugly

Responsible Disclosure leading actors

CERT.LV
Informācijas tehnoloģiju drošības incidentu novēršanas institūcija

- **Vulnerability**
- **Researcher / Hacker**
- **Target**
  - **System**
  - **Software**
  - **Hardware**
    - **Vendor**
    - **Owner**

- **TIME**

Responsible Disclosure leading actors

CERT.LV
Informācijas tehnoloģiju drošības incidentu novēršanas institūcija

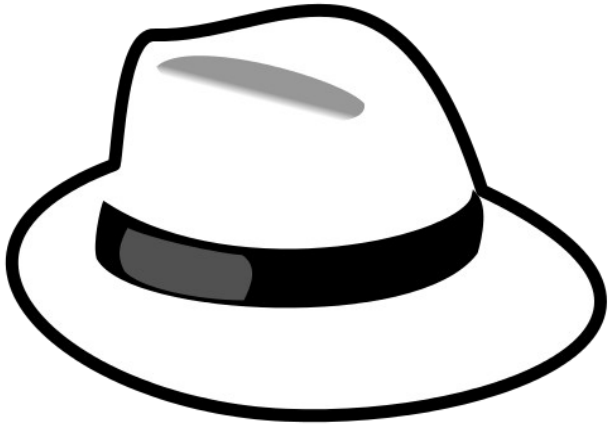
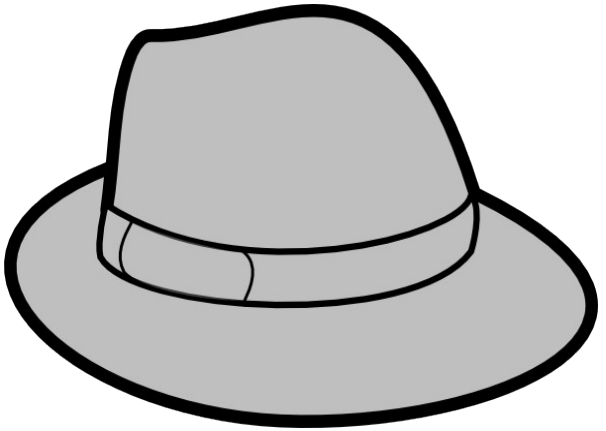
- **ENISA defines vulnerability as: The existence of a weakness, design, or implementation error that can lead to an unexpected, undesirable event compromising the security of the computer system, network, application, or protocol involved**

  Availability+Integrity+Confidentiality

Responsible Disclosure

CERT.LV
Informācijas tehnoloģiju drošības incidentu novēršanas institūcija

- **Black hat or White hat ?**


Responsible Disclosure implementation

CERT.LV
Informācijas tehnoloģiju drošības incidentu novēršanas institūcija

- **Responsible disclosure VS Bug Bounty**
- **Motivators**
- **CERT as coordinator**
- **Timeframe**

Responsible Disclosure Goals

CERT.LV
Informācijas tehnoloģiju drošības incidentu novēršanas institūcija

- **A common RD framework that can be applicable country / EU wide**
- **Protect the researcher ?**
- **Comply with existig legal framework?**

Responsible Disclosure Experience in Latvia

CERT.LV
Informācijas tehnoloģiju drošības incidentu novēršanas institūcija

- **Implemented: Swedbank**
- **Not implemented but has use cases**
  - **Valmiera municipality**
  - **Bank authentication**
  - **Several government web sites & information systems**
  - **Mobile apps**
  - **Public transport RFID**

Responsible Disclosure Things to consider

CERT.LV
Informācijas tehnoloģiju drošības incidentu novēršanas institūcija

- **Bug bounty / Bug hunting**
- **Defining a reaction time**
- **Responsible / Coordinated**
- **Reaward**
- **There are risks but benefits seem to be more**
- **Educated & security aware society**

Thank you!