

A light green background within a white rectangular frame, featuring a complex graphic of overlapping arrows and gears. The text is centered over this graphic.

**Sistema Intel·ligent de
Gestió de
Vulnerabilitats
Informàtiques**

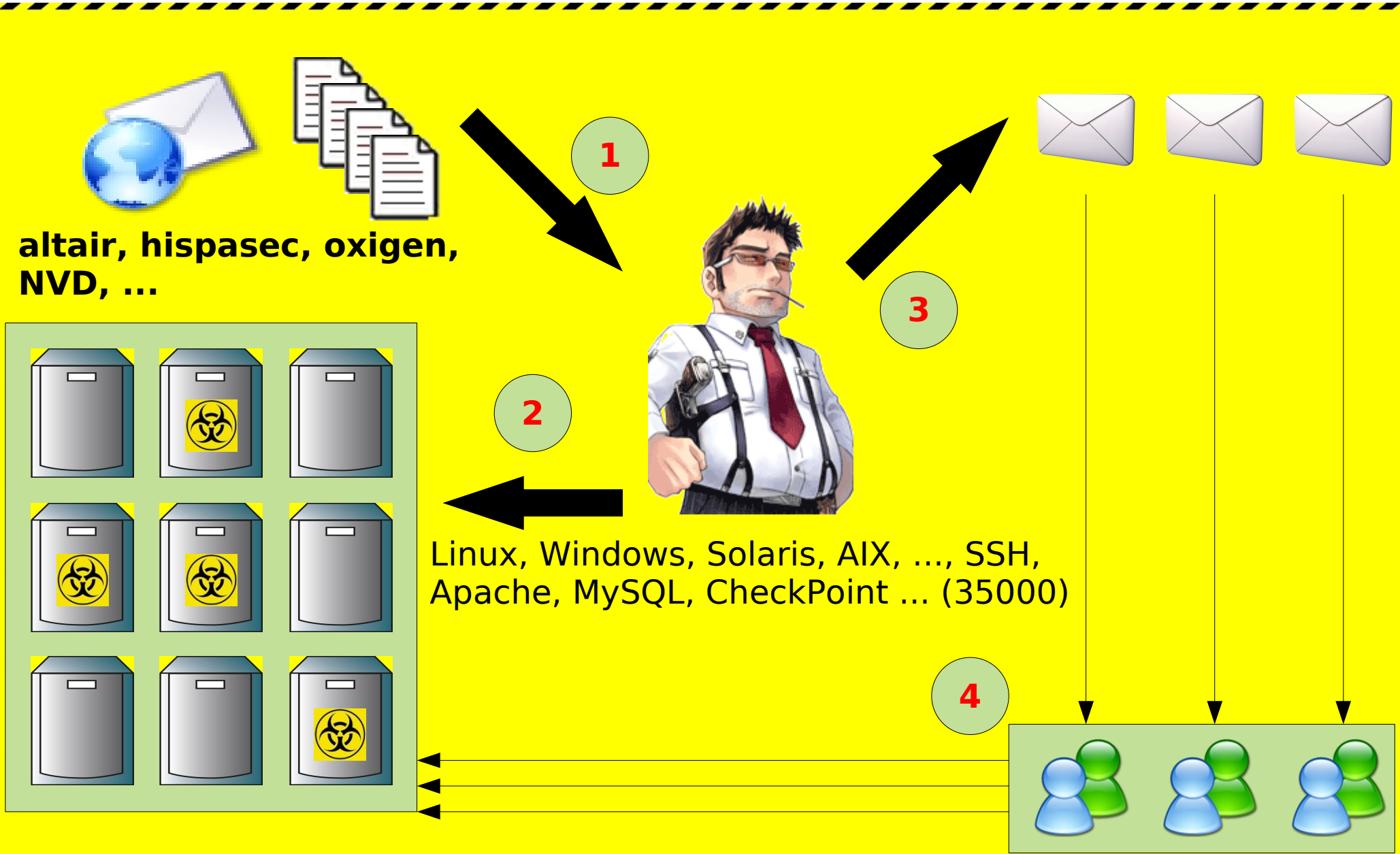


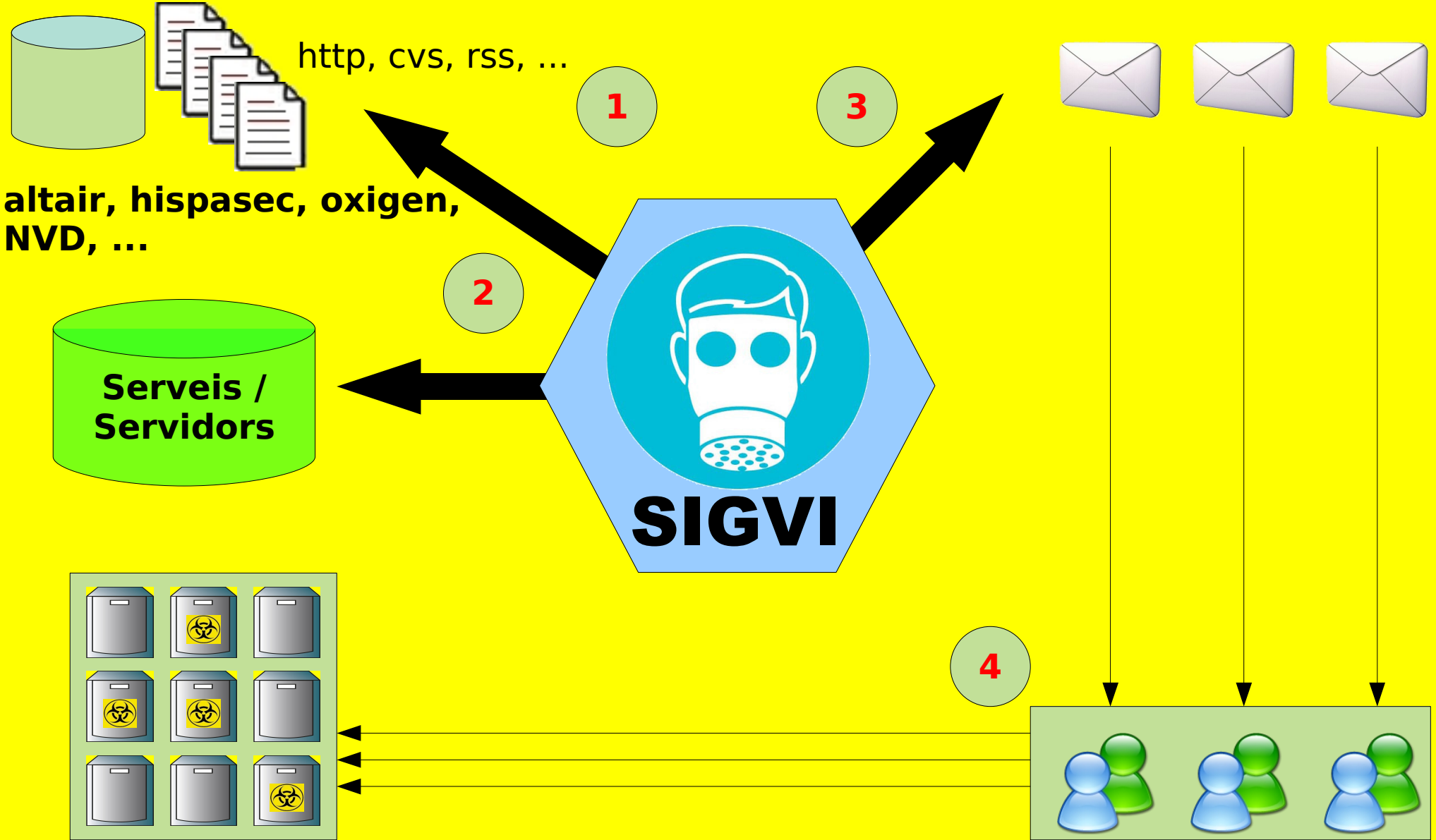
Augment constant de
Serveis i Servidors
als departaments
informàtics

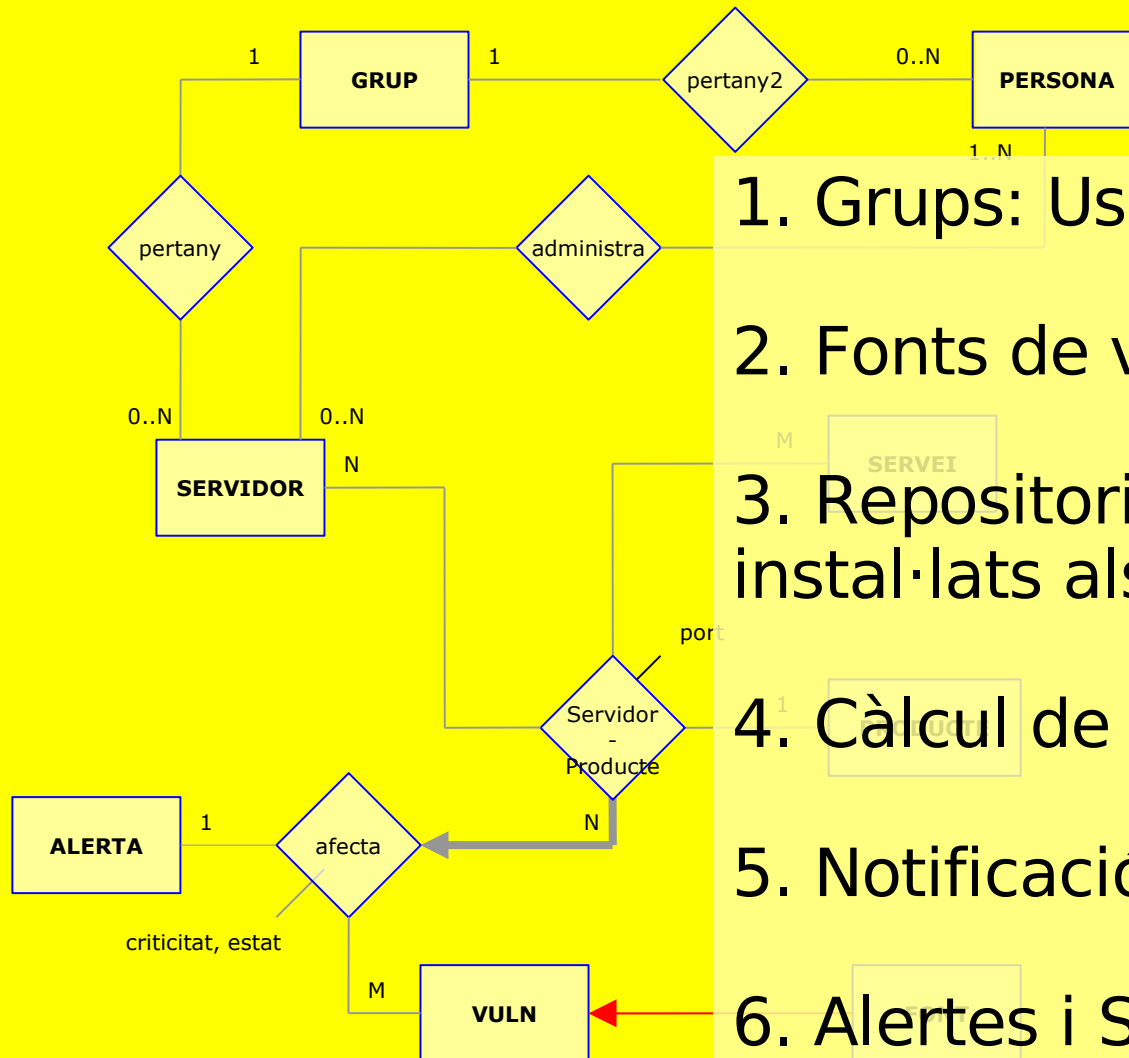
+

Aparició constant
de vulnerabilitats

Necessitat







1. Grups: Usuaris i Servidors

2. Fonts de vulnerabilitats

3. Repositori de productes i productes instal·lats als servidors (serveis)

4. Càlcul de l'**impacte**

5. Notificació

6. Alertes i Seguiment

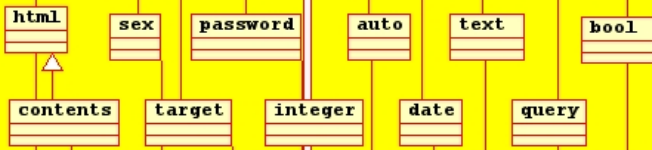


```

class field_type
# value_reference : char
# default_value : string
+ field_type()
+ show(field_name : string, readonly : bool)
+ show_simply(field_name : string)
+ check(value : any)
+ get_value(inout field_value : )
+ get_sql_value(field_value : any)
+ show_hidden()
+ get_value_from_post(field_name : string) : string
+ set_default_value(form_name : string, field_name : string)
+ set_value(form_name : string, field_name : string, value : any)
+ get_query_string(field_name : string, field_value : any)
+ field_insert(field_name : string, field_value : string)
+ field_udpate(field_name : string, old_value : any, new_value : any)
+ field_delete(field_name : string, value : any)

```

reference



foreign_key

foreign_key_tree

file

file_image

general

url

url_menu

+ id : string[]

list_dir

list_day

list_hour

list_mi

field_types

field

```

class field
# name : string
# alias : string
# type : string
# required : bool
# is_unique : bool
# visible : bool
# reference : field_types::field_type
# updatable : bool
# default_value : any
# is_detail : bool

```

- Implementat en plataforma LAMP

- Disseny orientat a objectes

- Característiques bàsiques:

- Modular
- Multi llenguatge
- Multi base de dades



SIGVI

Gestió de vulnerabilitats

TO-DO

Hi ha 145 alertes actives

Administració general

Usuaris

Servidors

Productes instal·lats als servidors

Alertes

Productes

Vulnerabilitats

Veure l'estat de vulnerabilitats als servidors

Eines

Evolució de les vulnerabilitats

Estat dels servidors

Servidor	Risc alt	Risc mig	Risc baix	Total
beyer	6	0	0	6
biber	7	0	0	7

- **Versió 100% funcional (v 1.0) per a petites implantacions.**

- **Estudi d'implantació a grans entitats**

- **Volum de dades:**

- **7076 vulnerabilitats (des de 2004)**

- **34961 productes vulnerables**



Gestió d'alertes

Mostrar totes les alertes (tancades i des

Canviar l'estat de les alertes seleccionades

Estat

Canviar

> Mostrant des de la fila 1 fins a la 50, de 158



Servidor	Producte afectat	Vulnerabilitat	Data creació	Estat	Criticitat	Observacions	Vuln actualitzada			
backus	Linux, Linux kernel, 2.6.11	CVE-2005-2457	2006-02-27 00:00:00							
backus	Linux, Linux kernel, 2.6.11	CVE-2005-2458	2006-02-27 00:00:00							
backus	Linux, Linux kernel, 2.6.11	CVE-2005-2459	2006-02-27 00:00:00				No	*	-	⌵
backus	Linux, Linux kernel, 2.6.11	CVE-2005-2872	2006-02-27 00:00:00	Oberta	8		No	*	-	⌵
backus	Linux, Linux kernel, 2.6.11	CVE-2005-3272	2006-02-27 00:00:00	Oberta	8		No	*	-	⌵
backus	Linux, Linux kernel, 2.6.11	CVE-2005-3273	2006-02-27 00:00:00	Oberta	8		No	*	-	⌵

Problemes en implementacions grans:

- Parametrització més flexible
- Integració amb Repositoris existents
- Problema de manteniment de les dades:

redundància (diferents repositoris)

modificacions cada cop que s'actualitza un producte



- Millora del motor de comparació per reduir els falsos positius: parametrització avançada.

- Necessitat d'alternatives al repositori de servidors i productes: agents externs (OCS Inventory).

- Comunicació amb el NVD: divulgació.

Gestió de fonts de vulnerabilitats

les fonts de dades | Càrrega de vulnerabilitats

Total: 5 registres.

Alias	Descripció	Parser	Paràmetres	Utilitzar?		
FULL 2005	nvd.nist.gov vulnerability database; EEUU: FULL 2005	nvd.nist.gov.php	http://nvd.nist.gov/download/nvdcve-2005.xml	No	*	-
NVD - FULL 2006	nvd.nist.gov vulnerability database; EEUU: FULL 2006	nvd.nist.gov.php	http://nvd.nist.gov/download/nvdcve-2006.xml	No	*	-
NVD - Local	Local file	nvd.nist.gov.php	/home/sigvi/www_sigvi/file_samples/nvdcve-modified.xml	No	*	-
NVD - Recent	nvd.nist.gov, recent file	nvd.nist.gov.php	http://nvd.nist.gov/download/nvdcve-recent.xml	Si	*	-

<http://sigvi.sourceforge.net/>

<https://lafarga.cpl.upc.edu/projects/sigvi/>

<http://nvd.nist.gov/>

e-mail: sebastian.gomez@upcnet.es



Evolució de les vulnerabilitats

