CERT-PA

Computer Emergency Response (Readiness) Team della Pubblica Amministrazione

Mario Terranova
Responsabile Area CERT-PA

Webinar

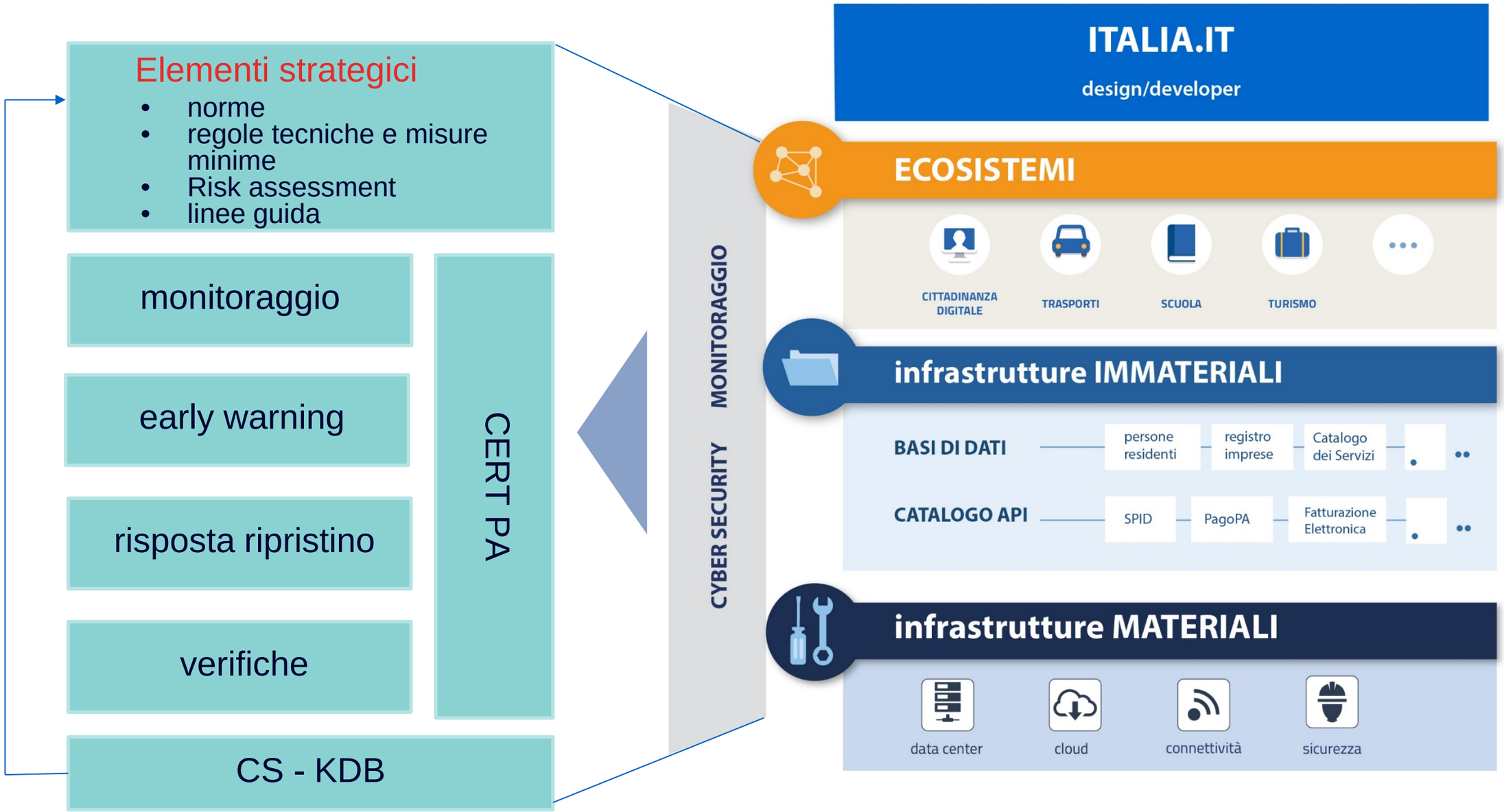
Cybersecurity: iniziative e azioni per una PA più sicura

6 febbraio 2018

COMPUTER EMERGENCY RESPONSE TEAM
PUBBLICA AMMINISTRAZIONE
CERT - PA

Sommario

Ruolo di AgID e del CERT-PA



Sistema nazionale di sicurezza cibernetica

Strategia e coordinamento

Prevenzione e risposta

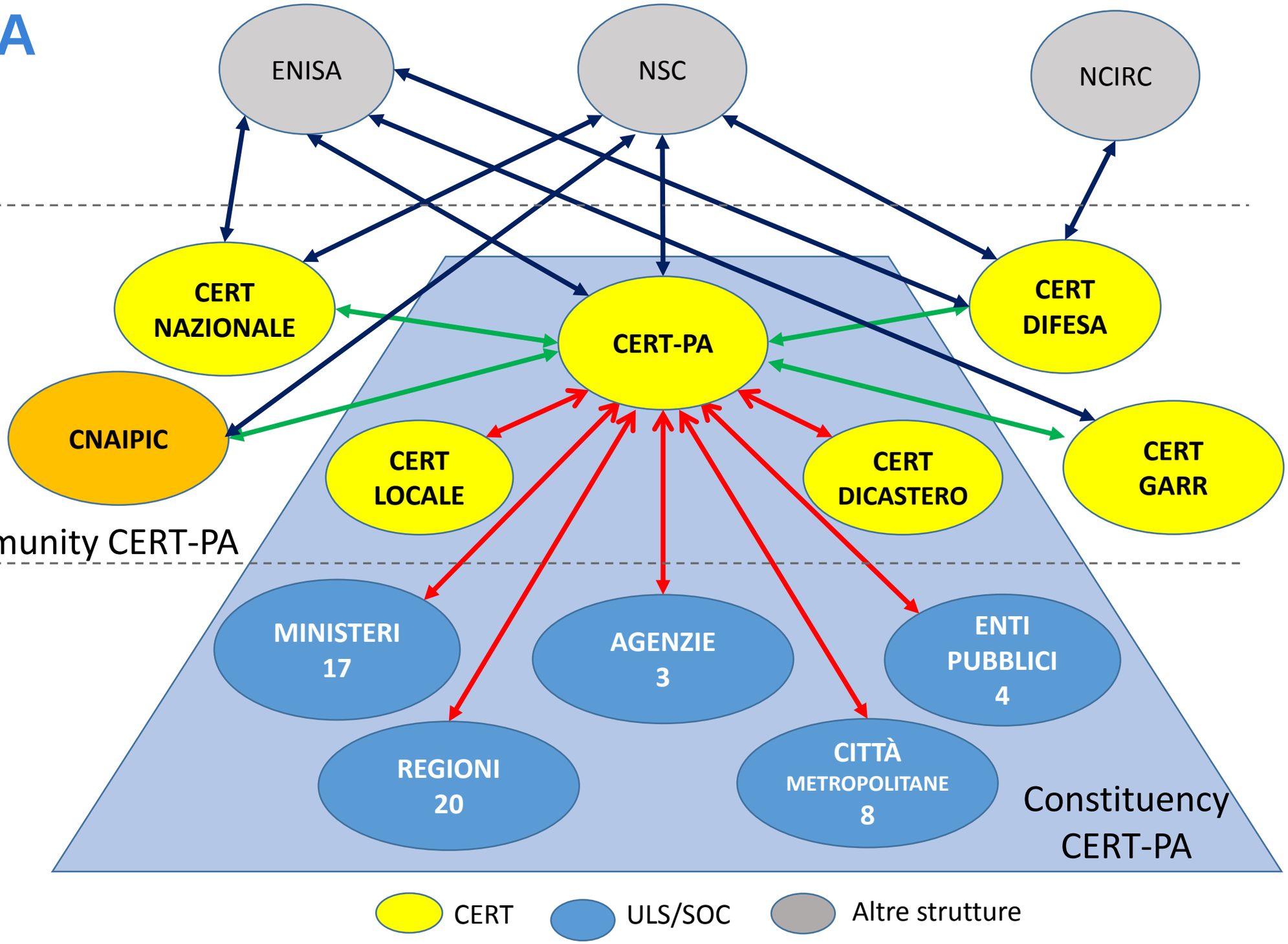
Monitoraggio e indagine

Il CERT-PA

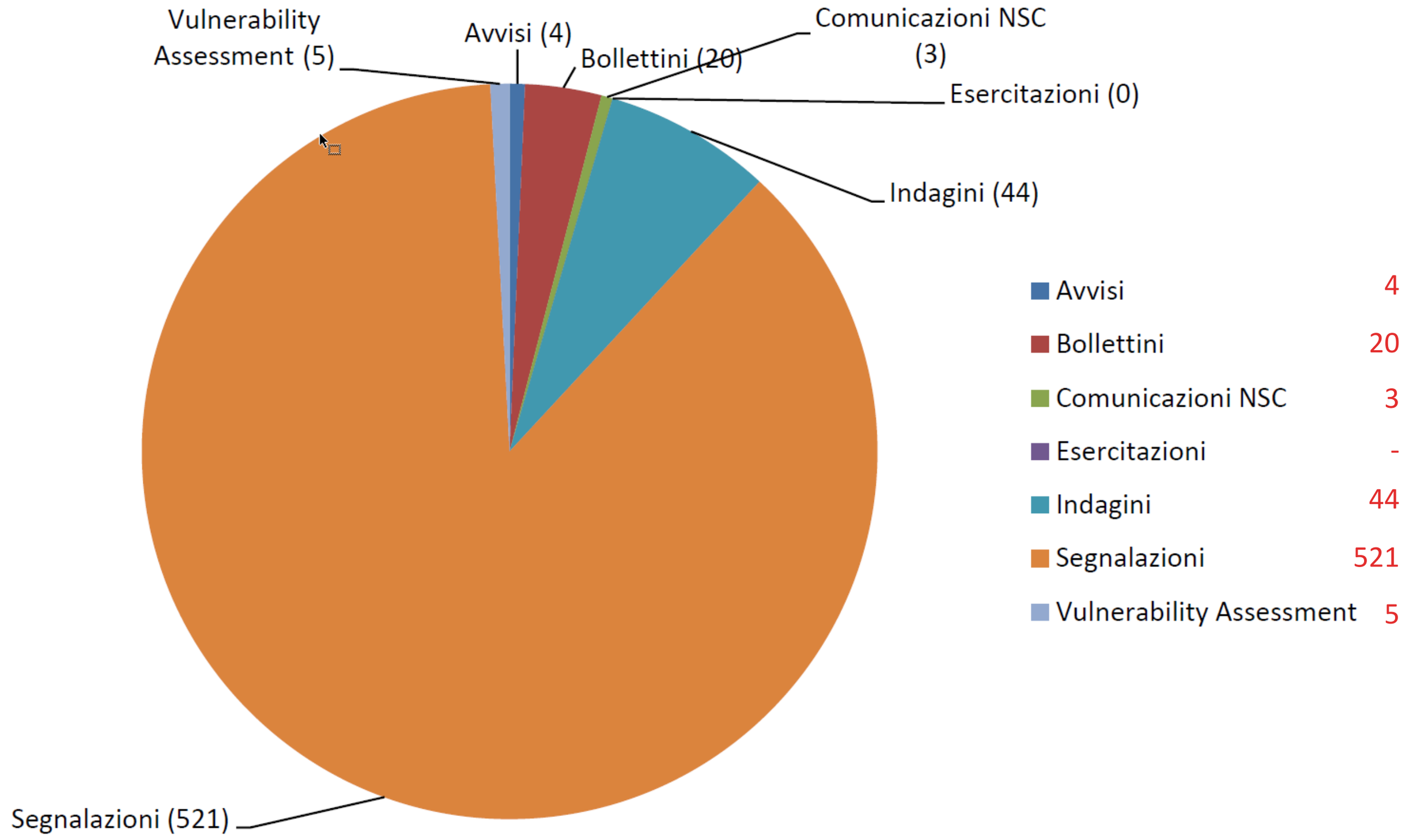
Monitoraggio
Allertamento
Supporto
Coordinamento

Community CERT-PA

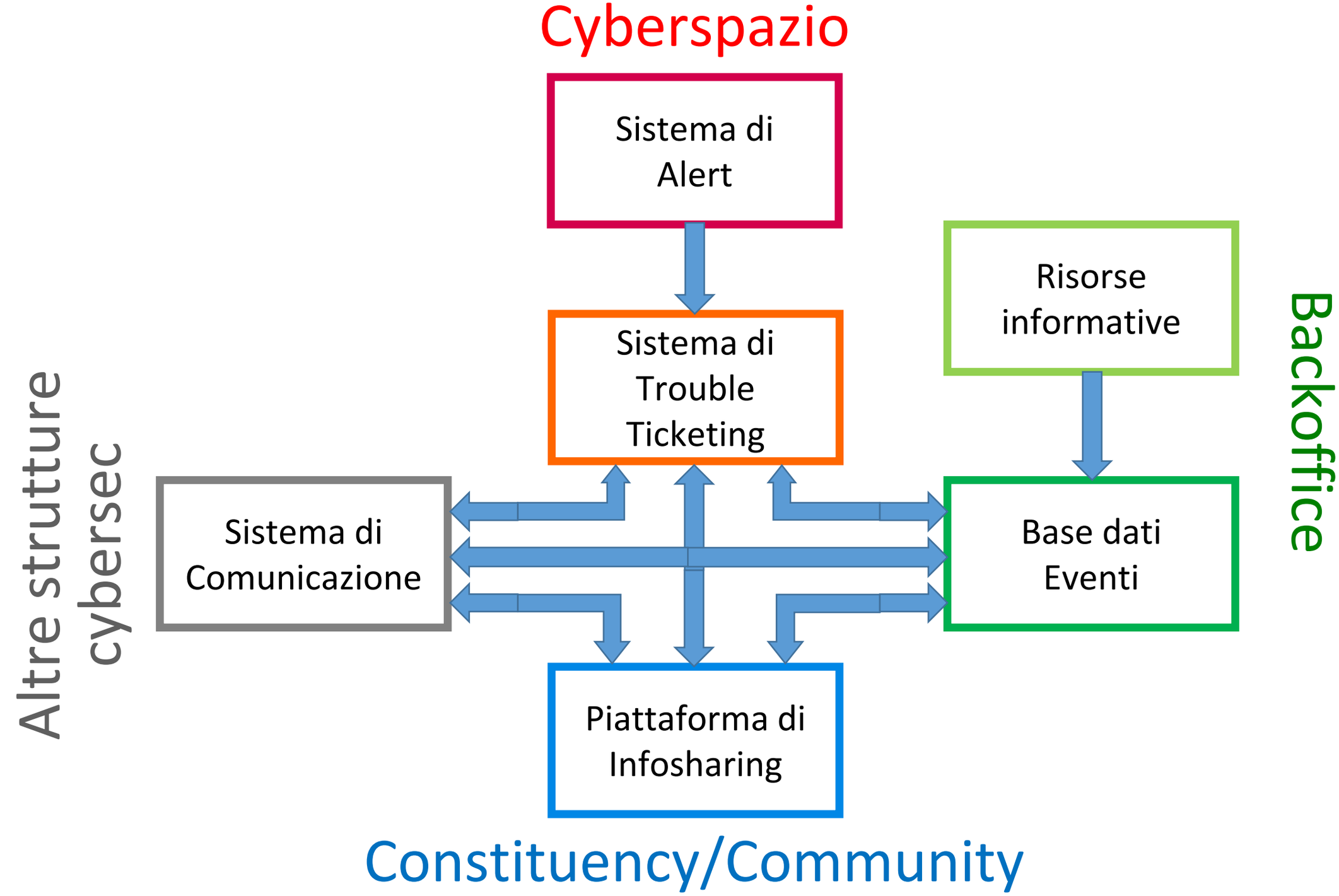
Operazione
Segnalazione



Attività del CERT-PA (2017)

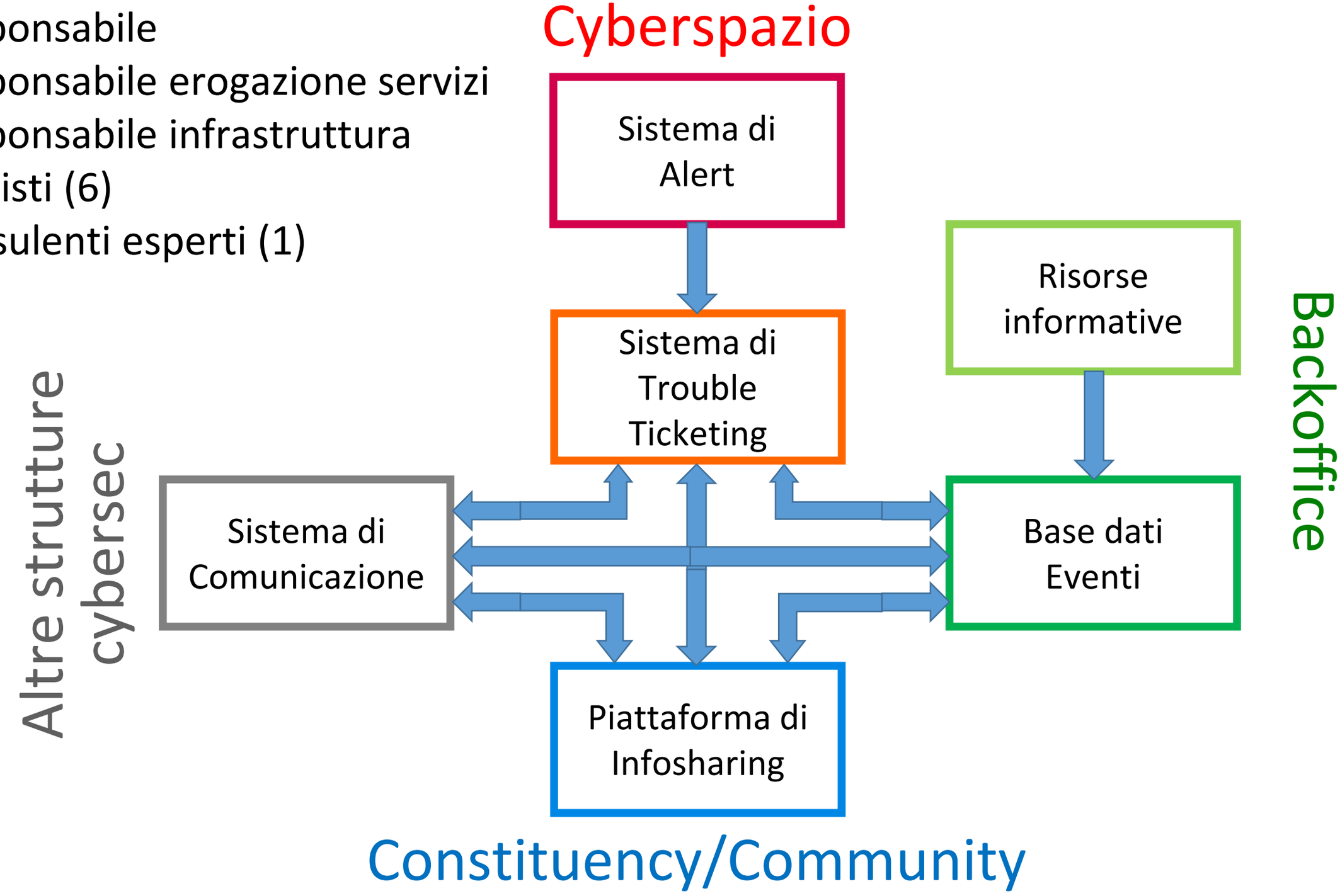


Struttura operativa del CERT-PA



Struttura operativa del CERT-PA

- Responsabile
- Responsabile erogazione servizi
- Responsabile infrastruttura
- Analisti (6)
- Consulenti esperti (1)



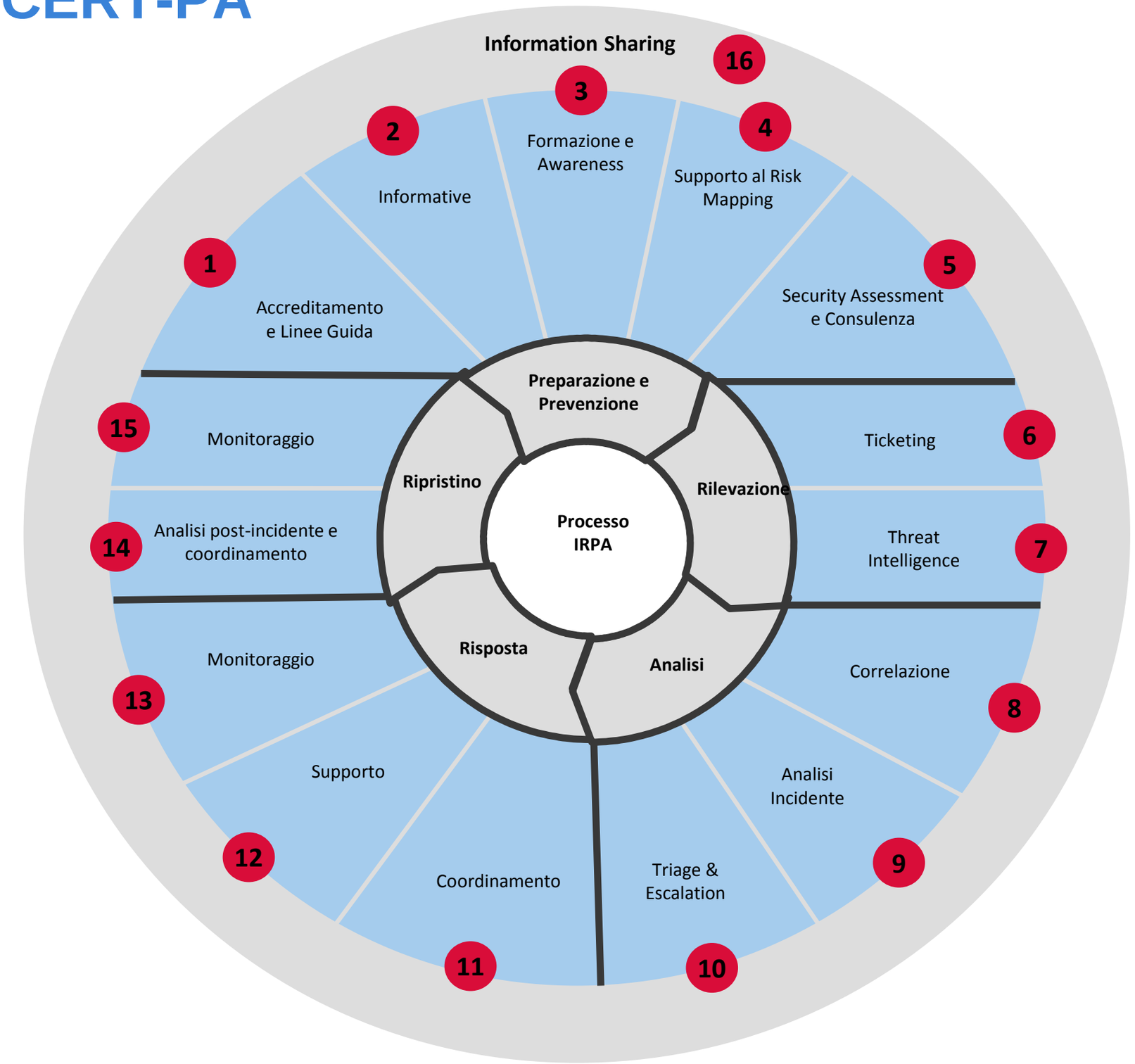
HASHR

HOWTO-HASHR.txt - Blocco note

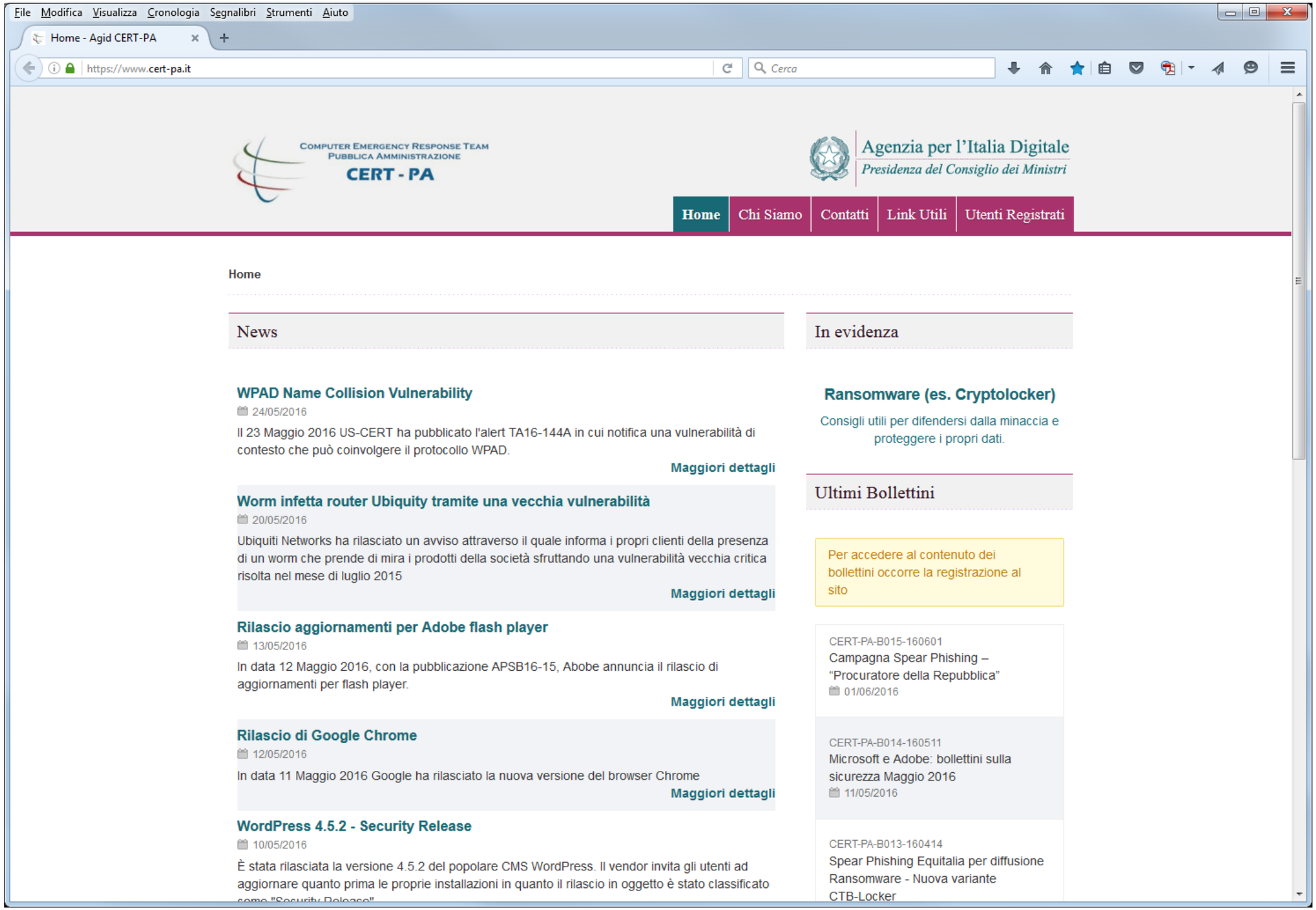
File Modifica Formato Visualizza ?

```
COSA È HASHR
============
Hashr è un tool scritto dagli analisti del CERT-PA che consente di computare hash dei file ed eventualmente cercare la
corrispondenza su una lista di hash predefinita (es. IoC di hash).
Hashr supporta i seguenti algoritmi di hash: md5, sha1, sha256, imphash (sui file di tipo PE).
Il tool è stato compilato per piattaforma Microsoft Windows, su richiesta è possibile pacchettizzare hashr anche per
le piattaforme Linux e OSX.

Per consultare l'help in linea usare l'opzione -h
================================================================================
C:\hashr>hashr.exe -h

  www.cert-pa.it | cert-pa@cert-pa.it
  hashr v.0.2
________________________________________________________________________________

usage: hashr [-h] [-v] [-r] [-d] [--filetype FILETYPE] [-e] [--hashlist FILE]
             [--encrypted] [-o OUTPUT]
             HASH TARGET

hashr is a tool able to compute hash of the files and compare them with a hashlist file. Using hashr you can verify if
IoC malware hashes (like APT) are present in your system.

positional arguments:
  HASH                  algorithm supported: md5, sha1, sha256, imphash
  TARGET                file or directory name from which to obtain the hash

optional arguments:
  -h, --help            show this help message and exit
  -v, --version         show program's version number and exit
  -r, --recursive       recursive directory
  -d, --duplicate       show duplicate hashes found
  --filetype FILETYPE   filter for extension (use comma separator)
  -e, --exclude         exclude filetype
  --hashlist FILE       load file with homogeneous hashes list
  --encrypted           only for encrypted hashlist
  -o OUTPUT             write output file

================================================================================
```

I servizi del CERT-PA

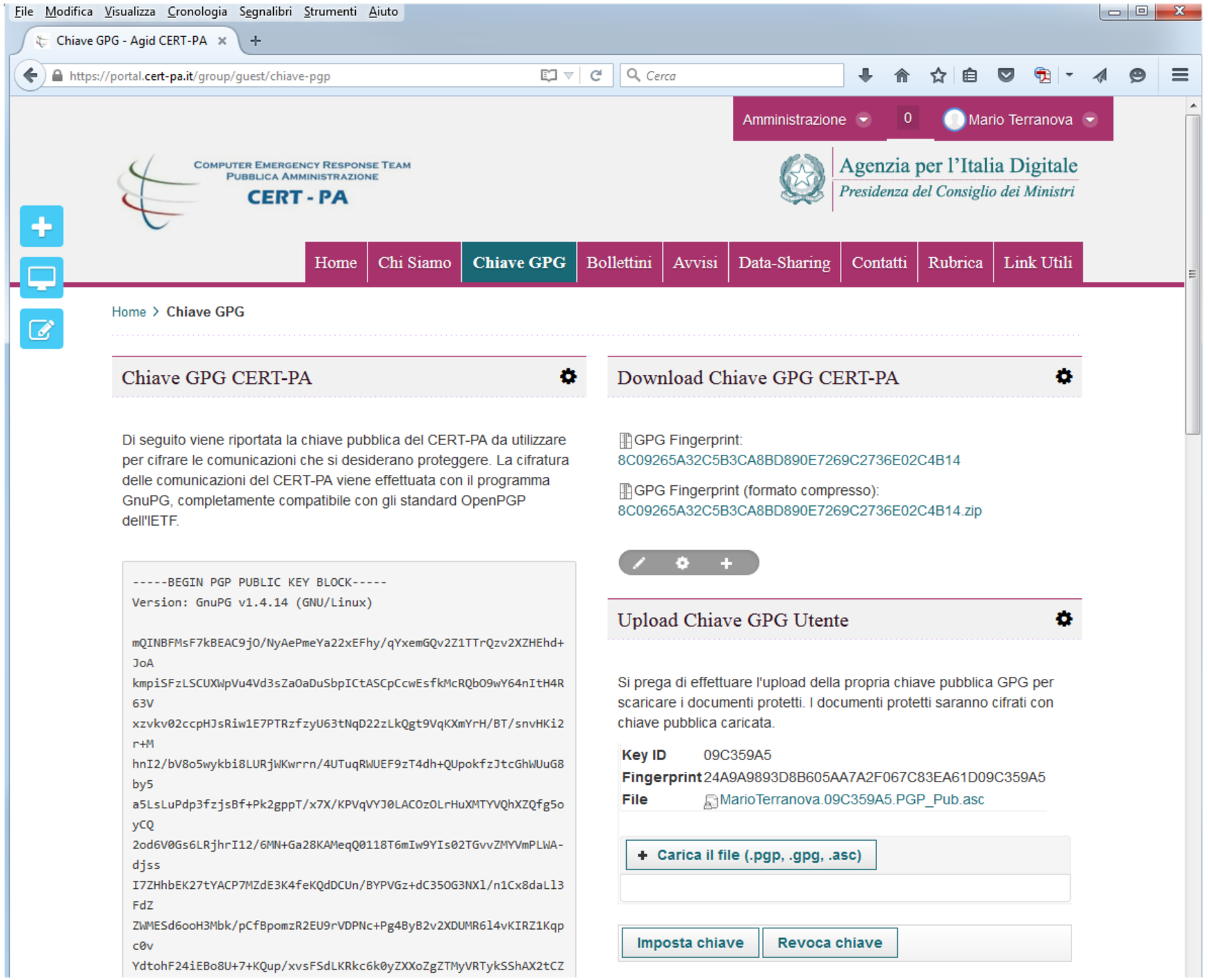


WEB site
www.cert-pa.it

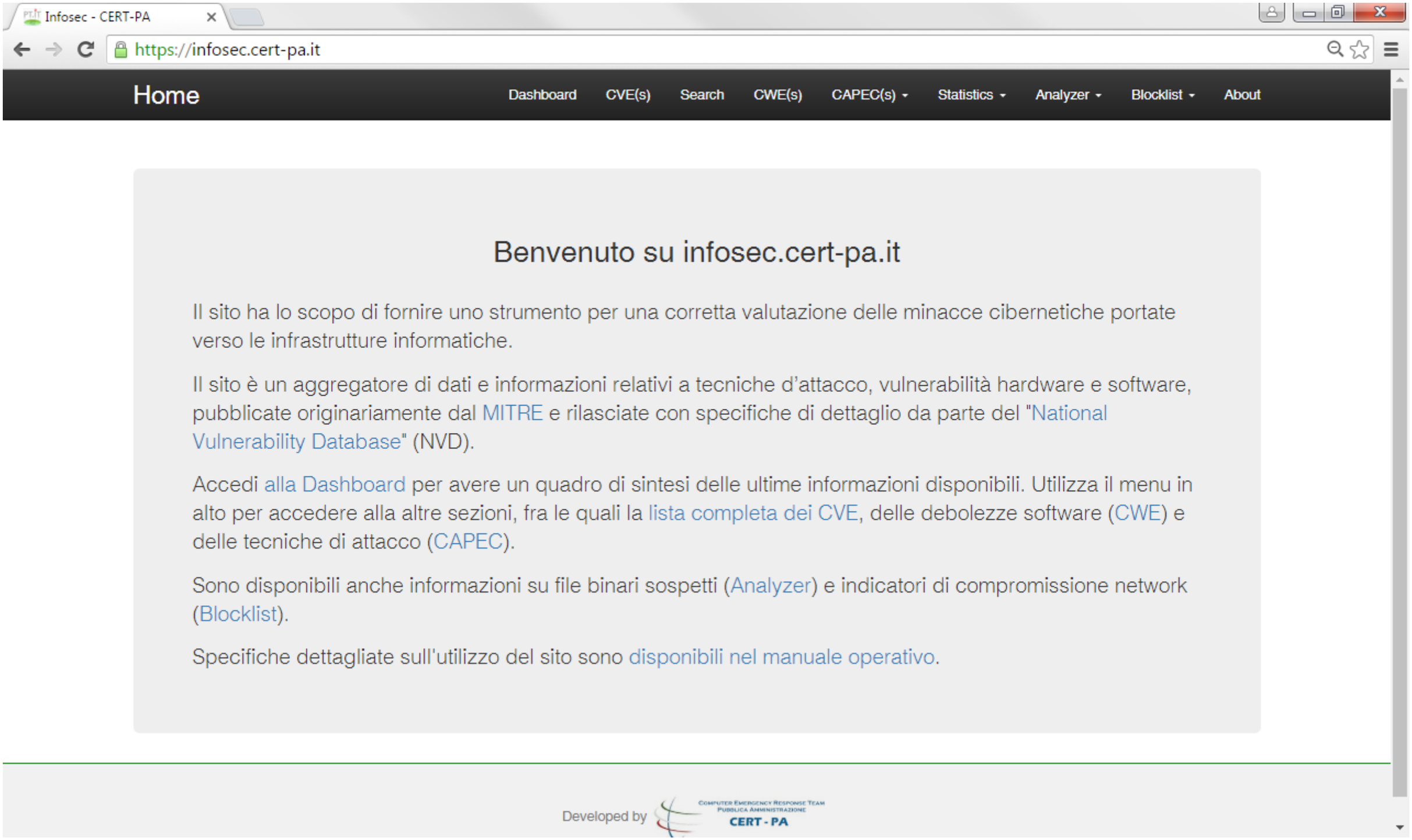


Piattaforma di Infosharing

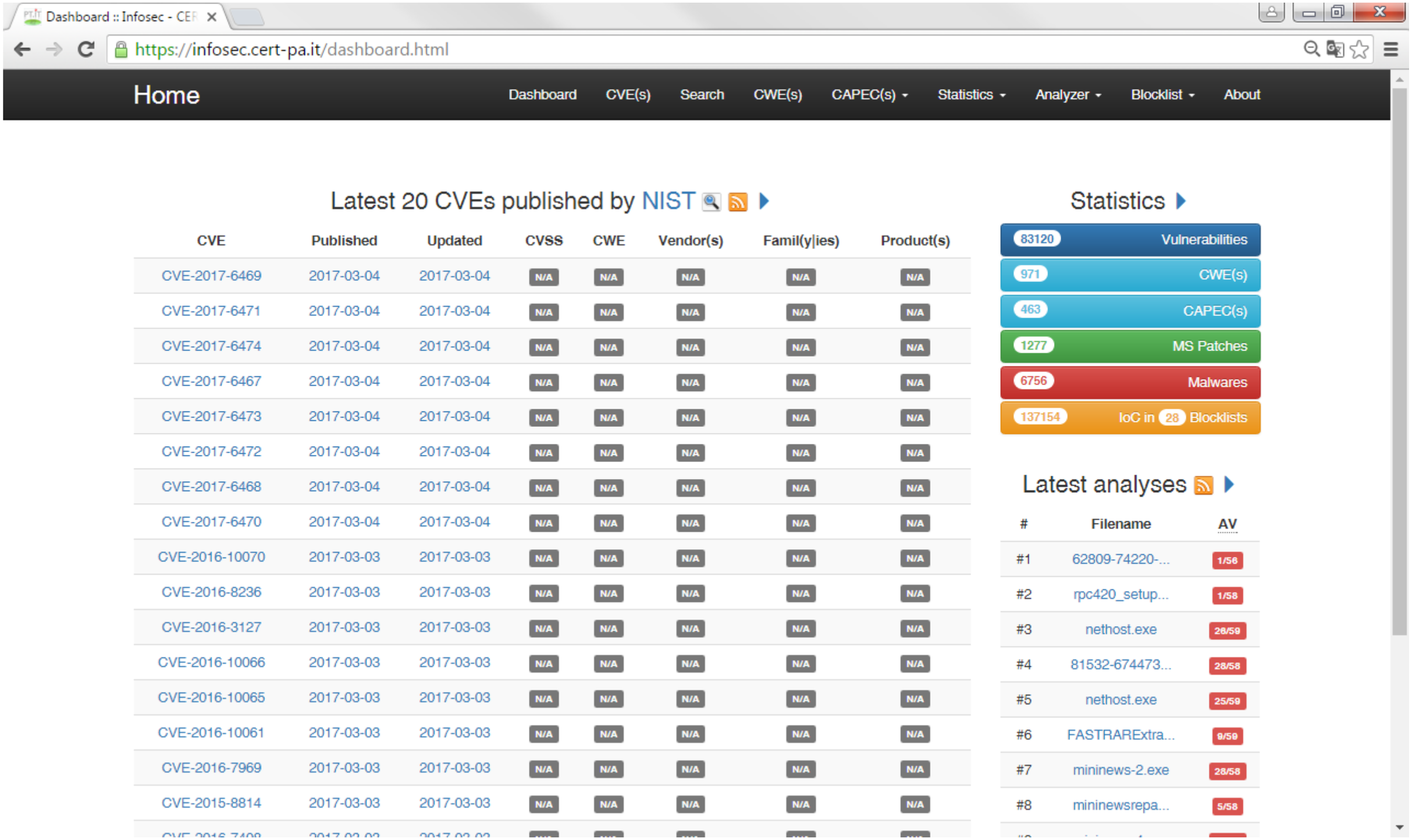
portal.cert-pa.it



INFOSEC (https://infosec.cert-pa.it)



INFOSEC Dashboard (https://infosec.cert-pa.it/dashboard.html)

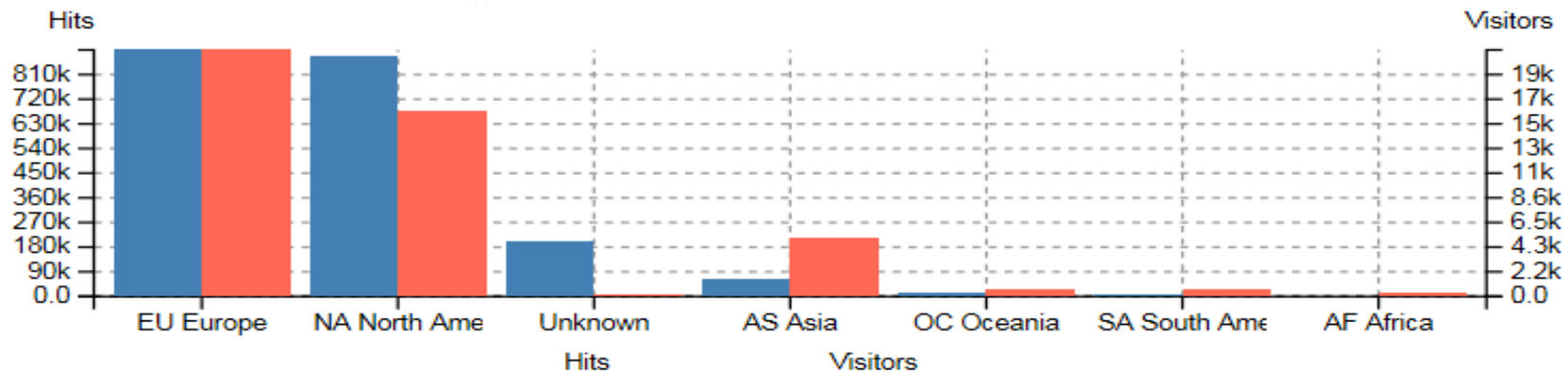


Accessi ad Infosec - Gennaio 2018

GEO LOCATION

CONTINENT > COUNTRY SORTED BY UNIQUE HITS [, AVGTS, CUMTS, MAXTS]

Panel Options



#	Hits	Visitors	Bandwidth	Data
	2.075.945 Max: 870.108 Min: 1	44.787 Max: 15.776 Min: 1	32.95 GiB Max: 19.94 GiB Min: 950 B	151 Total
1	904.822 (43.59%)	21.568 (48.16%)	23.32 GiB (70.78%)	EU Europe
2	884.155 (42.59%)	16.269 (36.33%)	7.77 GiB (23.60%)	NA North America
3	202.497 (9.75%)	243 (0.54%)	279.85 MiB (0.83%)	Unknown
4	61.657 (2.97%)	5.106 (11.40%)	1.3 GiB (3.95%)	AS Asia
5	13.171 (0.63%)	617 (1.38%)	79.81 MiB (0.24%)	OC Oceania
6	6.545 (0.32%)	613 (1.37%)	132.4 MiB (0.39%)	SA South America
7	3.098 (0.15%)	371 (0.83%)	70.86 MiB (0.21%)	AF Africa

IT	570.761	(27,5%)
FR	154.195	
DE	93.145	
RU	25.029	
ES	13.238	
GB	8.708	

Il Paese che cambia passa da qui.

Agenzia per l'Italia Digitale

Presidenza del Consiglio dei Ministri

www.agid.gov.it

https://www.cert-pa.it https://infosec.cert-pa.it

COMPUTER EMERGENCY RESPONSE TEAM
PUBBLICA AMMINISTRAZIONE
CERT - PA