



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

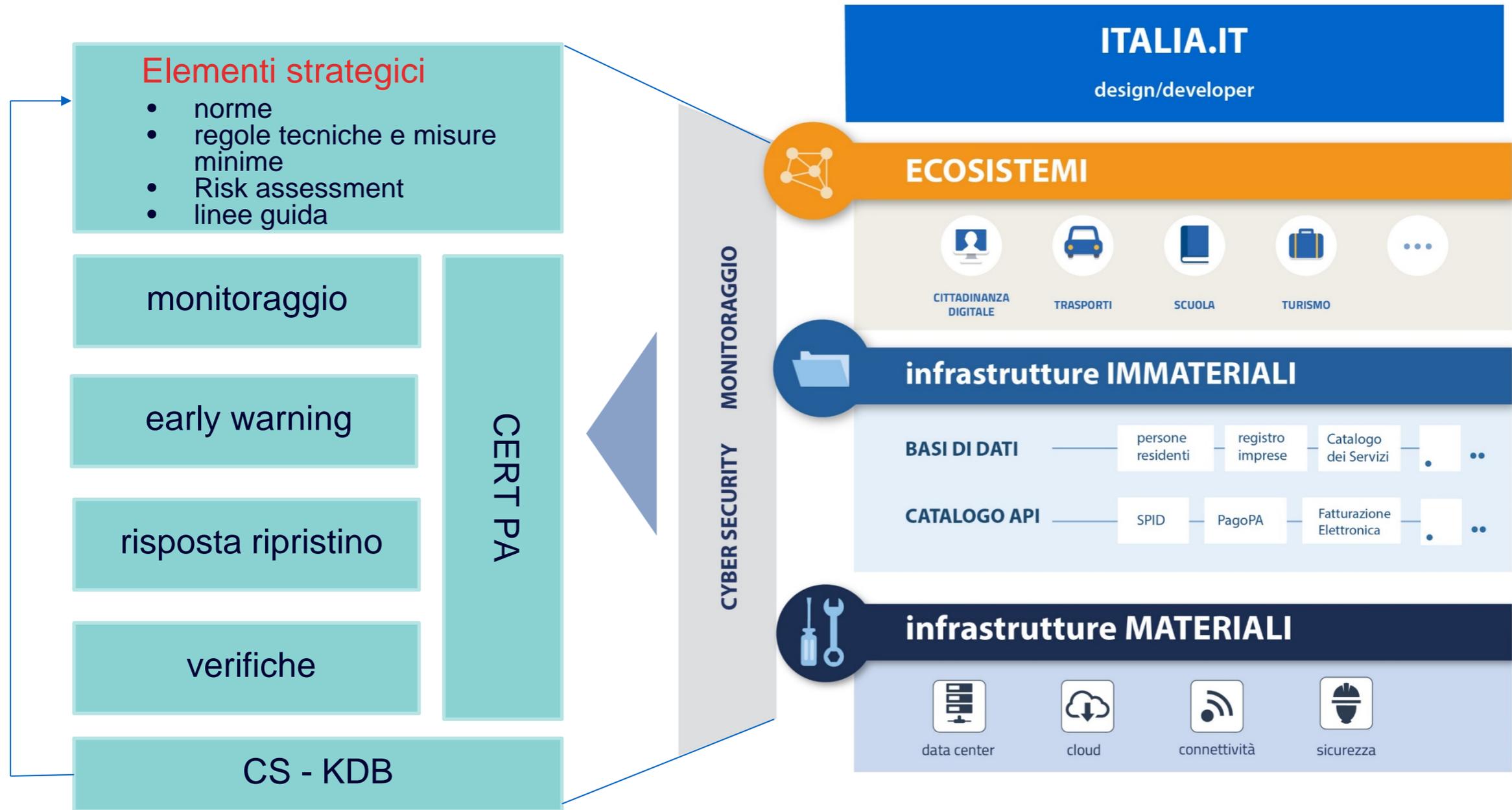


Sommario

1. Il CERT-PA di AgID nel sistema nazionale di sicurezza cibernetica.
2. Struttura e servizi del CERT-PA.
3. Strumenti per la sicurezza cibernetica nazionale (e non solo).



Ruolo di AgID e del CERT-PA



Sistema nazionale di sicurezza cibernetica

Strategia e
coordinamento

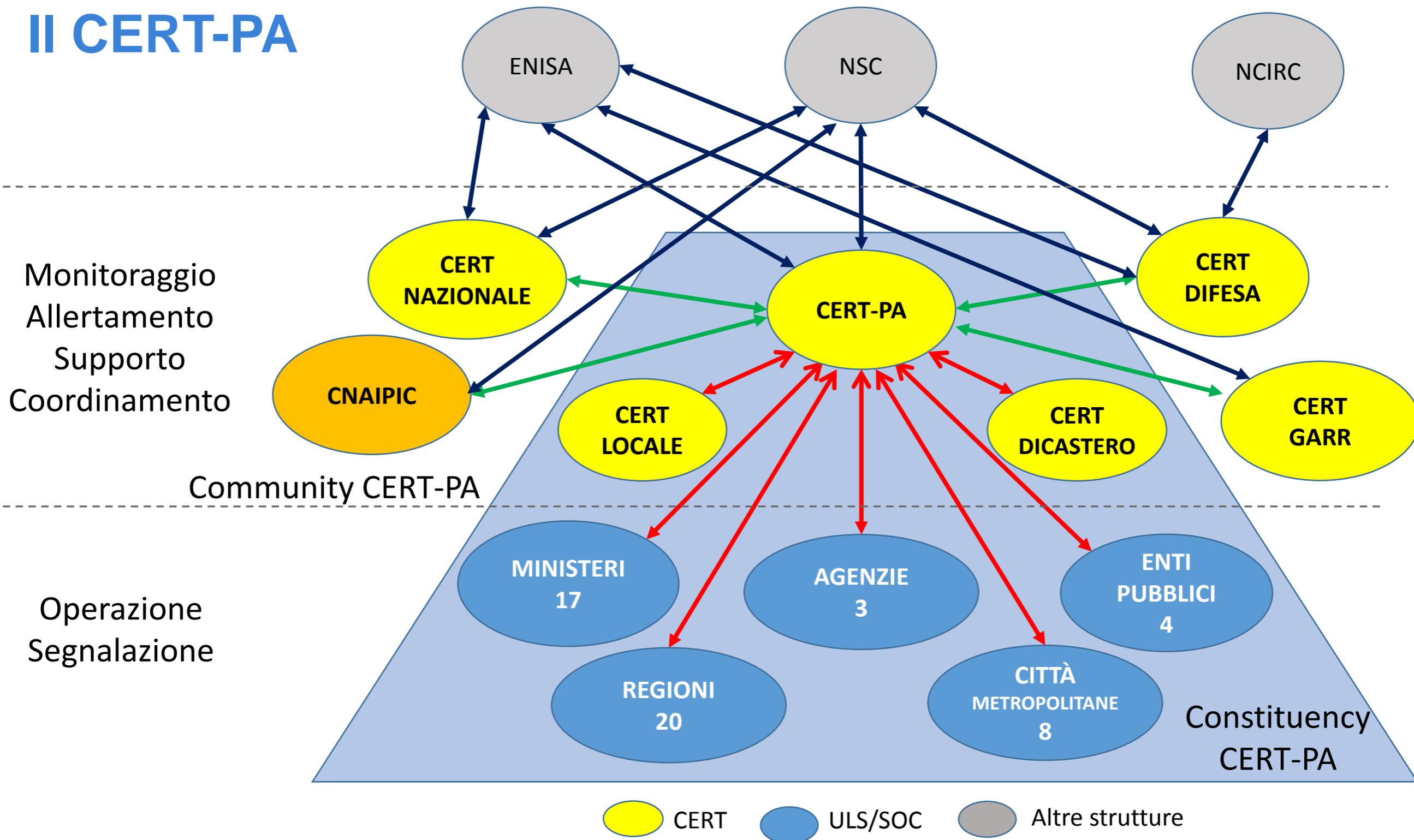
Prevenzione e
risposta

Monitoraggio e
indagine



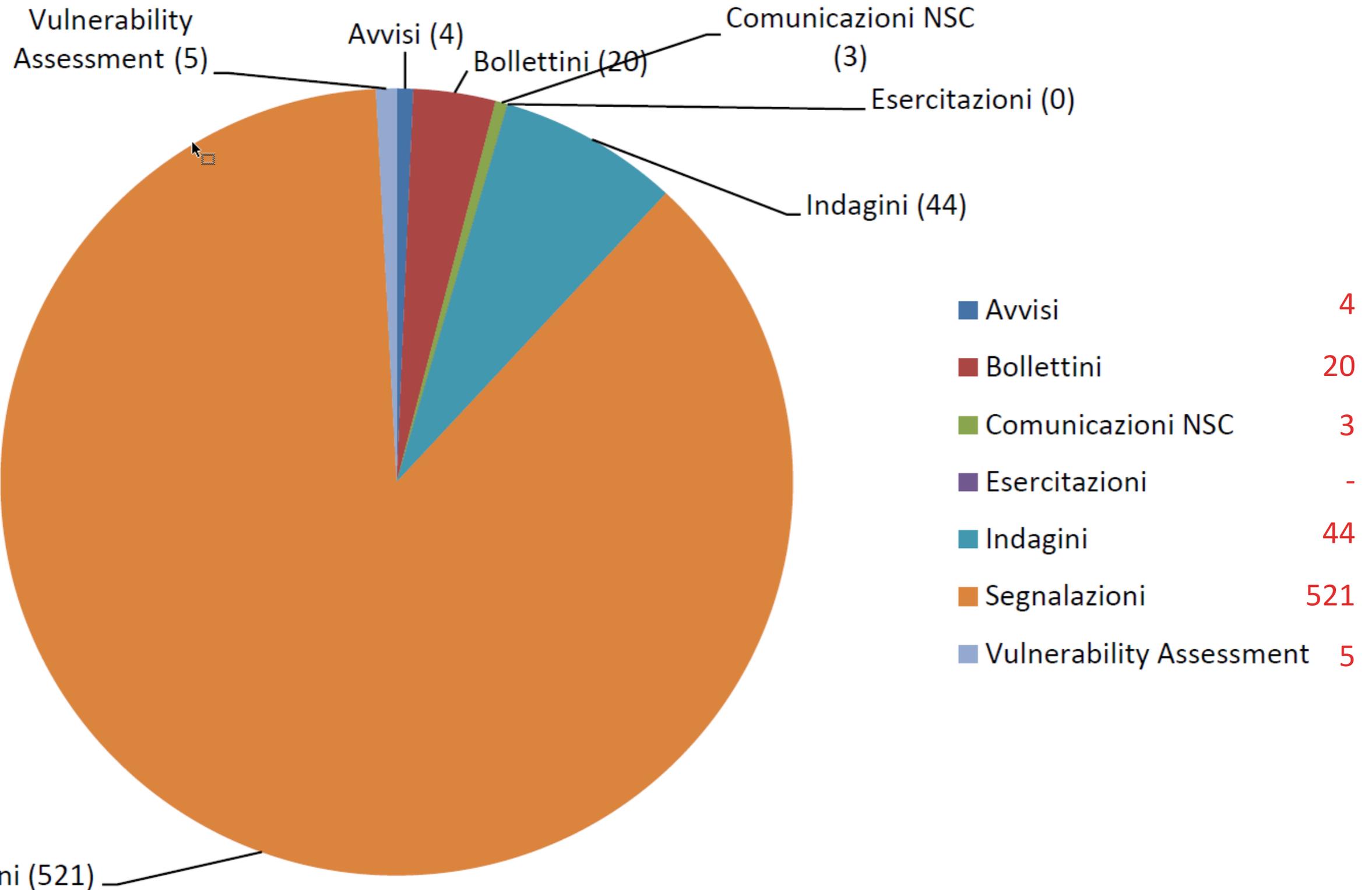


II CERT-PA

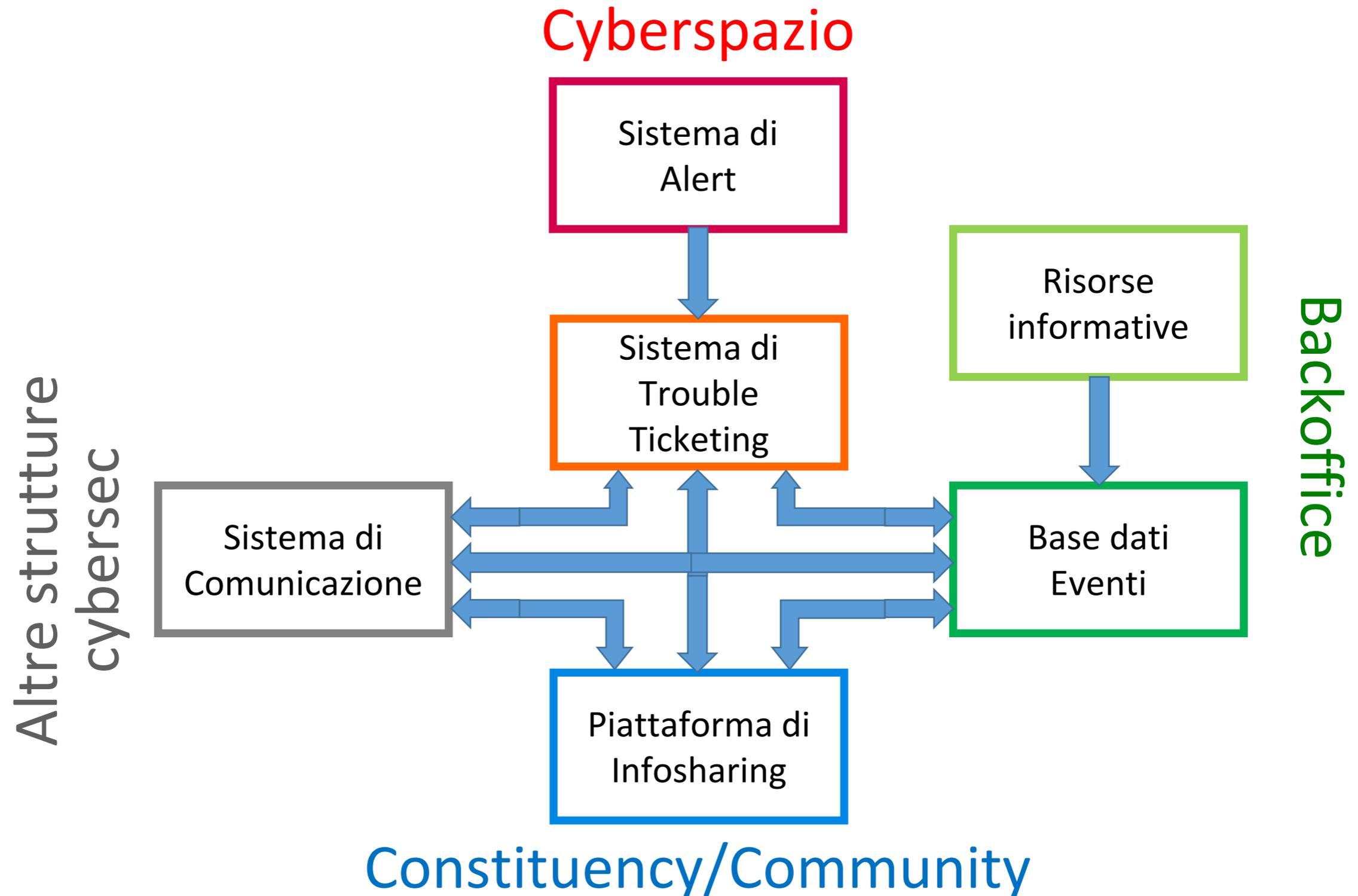




Attività del CERT-PA (2017)

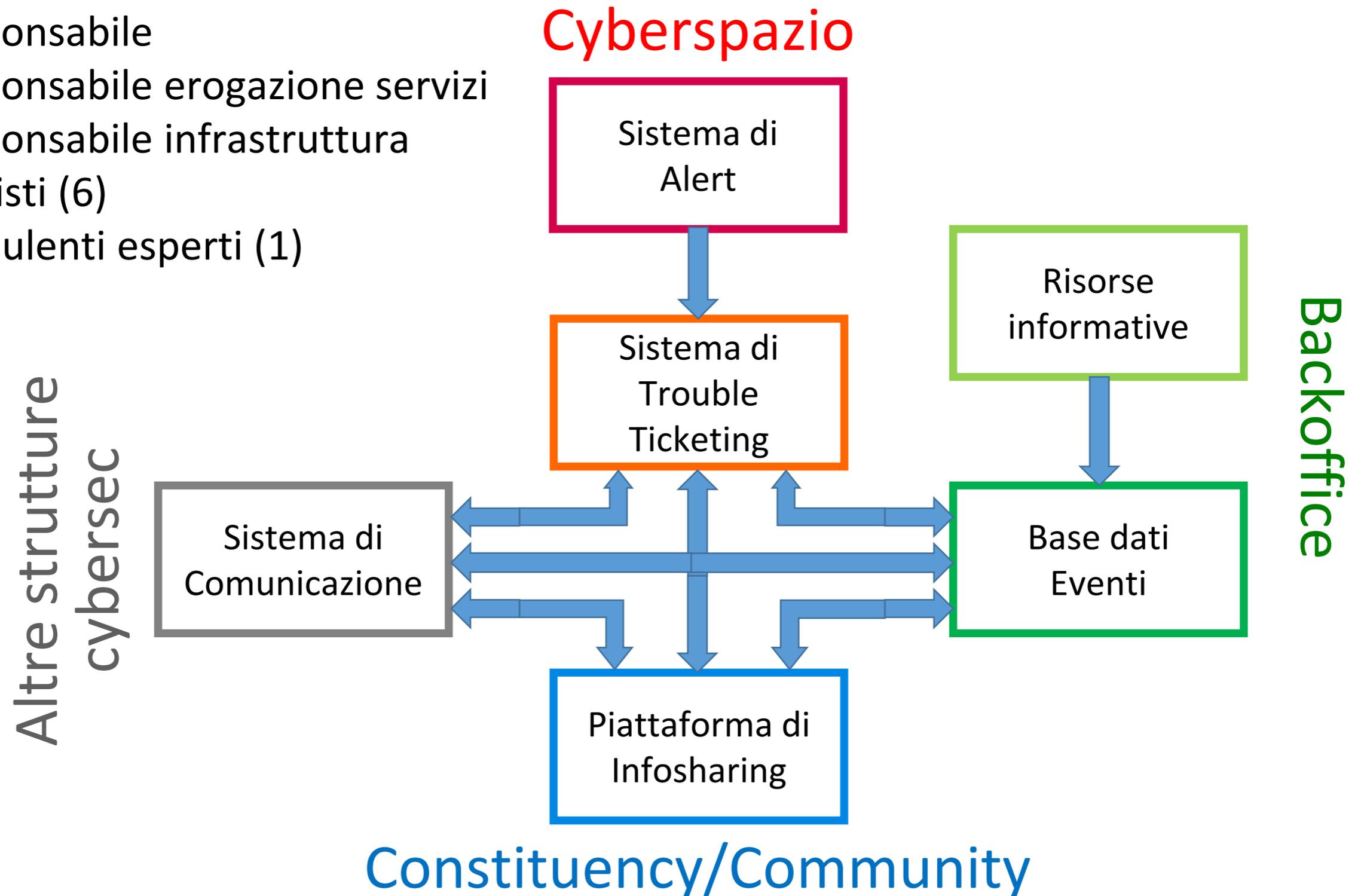


Struttura operativa del CERT-PA



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

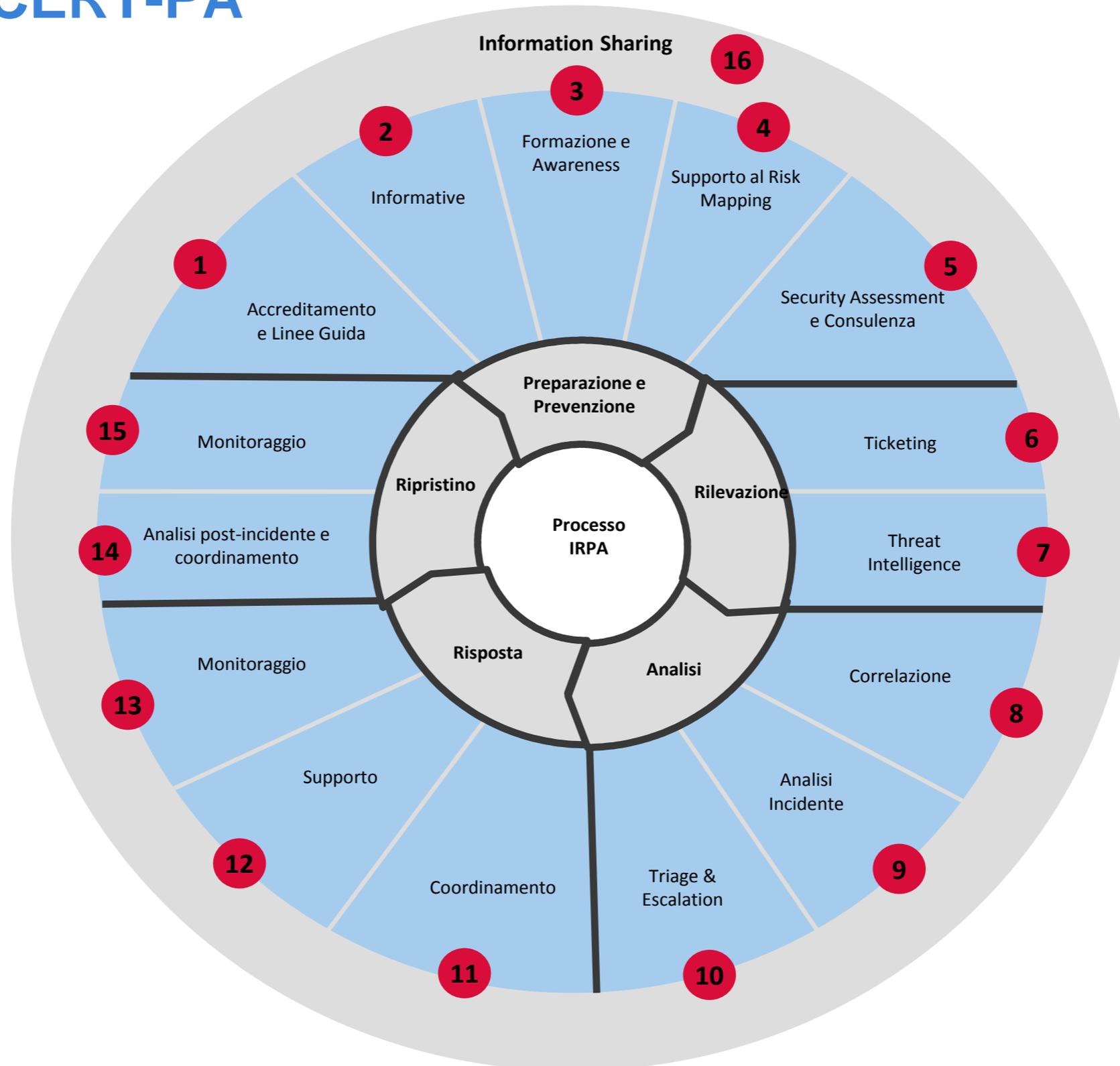
hashr is a tool able to compute hash of the files and compare them with a hashlist file. using hashr you can verify if IoC malware hashes (like APT) are present in your system.

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

The screenshot shows the homepage of the CERT-PA website. At the top, there is a navigation bar with the following links: Home, Chi Siamo, Contatti, Link Utili, and Utenti Registrati. The main content area is divided into two columns. The left column features a 'News' section with several articles, each with a title, date, and a 'Maggiori dettagli' link. The right column features an 'In evidenza' section with a featured article about Ransomware (es. Cryptolocker) and a 'Ultimi Bollettini' section with a list of recent bulletins.

Home

News

WPAD Name Collision Vulnerability
24/05/2016
Il 23 Maggio 2016 US-CERT ha pubblicato l'alert TA16-144A in cui notifica una vulnerabilità di contesto che può coinvolgere il protocollo WPAD.
[Maggiori dettagli](#)

Worm infetta router Ubiquity tramite una vecchia vulnerabilità
20/05/2016
Ubiquiti Networks ha rilasciato un avviso attraverso il quale informa i propri clienti della presenza di un worm che prende di mira i prodotti della società sfruttando una vulnerabilità vecchia critica risolta nel mese di luglio 2015.
[Maggiori dettagli](#)

Rilascio aggiornamenti per Adobe flash player
13/05/2016
In data 12 Maggio 2016, con la pubblicazione APSB16-15, Adobe annuncia il rilascio di aggiornamenti per flash player.
[Maggiori dettagli](#)

Rilascio di Google Chrome
12/05/2016
In data 11 Maggio 2016 Google ha rilasciato la nuova versione del browser Chrome
[Maggiori dettagli](#)

WordPress 4.5.2 - Security Release
10/05/2016
È stata rilasciata la versione 4.5.2 del popolare CMS WordPress. Il vendor invita gli utenti ad aggiornare quanto prima le proprie installazioni in quanto il rilascio in oggetto è stato classificato come "Security Release".

In evidenza

Ransomware (es. Cryptolocker)
Consigli utili per difendersi dalla minaccia e proteggere i propri dati.

Ultimi Bollettini

Per accedere al contenuto dei bollettini occorre la registrazione al sito

CERT-PA-B015-160601
Campagna Spear Phishing – "Procuratore della Repubblica"
01/06/2016

CERT-PA-B014-160511
Microsoft e Adobe: bollettini sulla sicurezza Maggio 2016
11/05/2016

CERT-PA-B013-160414
Spear Phishing Equitalia per diffusione Ransomware - Nuova variante CTB-Locker

Piattaforma di Infosharing

portal.cert-pa.it

The screenshot shows a web browser window displaying the 'Chiave GPG - Agid CERT-PA' page on portal.cert-pa.it. The page features a navigation menu with 'Chiave GPG' highlighted. The main content area is divided into three sections: 'Chiave GPG CERT-PA', 'Download Chiave GPG CERT-PA', and 'Upload Chiave GPG Utente'. The 'Chiave GPG CERT-PA' section contains a public key block. The 'Download' section provides GPG fingerprints for both the key and a compressed version. The 'Upload' section includes a text area for the key ID and fingerprint, a file upload button, and buttons for 'Imposta chiave' and 'Revoca chiave'.

-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: GnuPG v1.4.14 (GNU/Linux)

mQINBFMsF7kBEAC9jO/NyAePmeYa22xEFhy/qYxemGQv2Z1TTrQzv2XZHEhd+
JoA
kmpiSFzLSCUXWpVu4Vd3sZa0aDuSbpICtASCpCcwEsfkMcRQb09wY64nItH4R
63V
xzvkv02ccpHJsRiw1E7PTRzfzyU63tNqD22zLkQgt9VqKXmYrH/BT/snvHKi2
r+M
hnI2/bV8o5wykb18LURjWkwrn/4UTuqRWUEF9zT4dh+QUpokfzJtcGhWUuG8
by5
a5LsLuPdp3fzjsBf+Pk2gppT/x7X/KPVqVYJ0LAC0z0LrHuXMTYVQhXZQfg5o
yCQ
2od6V0Gs6LRjhrI12/6MN+Ga28KAMEqQ0118T6mIw9YIs02TgVvZMYmPLWA-
djss
I7ZHhbEK27tYACP7MzdE3K4feKQdDCUn/BYPVGz+dC350G3NX1/n1Cx8daL13
FdZ
ZWMESd6ooH3Mbk/pCfBpomzR2EU9rVDPNc+Pg4ByB2v2XDUMR614vKIRZ1Kqp
c0v
YdtohF24iEBo8U+7+KQup/xvsFSdLKRkc6k0yZXXoZgZTMyVRTykSshAX2tCZ

GPG Fingerprint:
8C09265A32C5B3CA8BD890E7269C2736E02C4B14

GPG Fingerprint (formato compresso):
8C09265A32C5B3CA8BD890E7269C2736E02C4B14.zip

Key ID 09C359A5
Fingerprint 24A9A9893D8B605AA7A2F067C83EA61D09C359A5
File MarioTerranova.09C359A5.PGP_Pub.asc

+ Carica il file (.pgp, .gpg, .asc)

Imposta chiave Revoca chiave



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

The screenshot shows a web browser window with the URL <https://infosec.cert-pa.it>. The browser's address bar and navigation buttons are visible. The website's header is dark with a white navigation menu containing the following items: Home, Dashboard, CVE(s), Search, CWE(s), CAPEC(s), Statistics, Analyzer, Blocklist, and About. The main content area is a light gray box with the following text:

Benvenuto su infosec.cert-pa.it

Il sito ha lo scopo di fornire uno strumento per una corretta valutazione delle minacce cibernetiche portate verso le infrastrutture informatiche.

Il sito è un aggregatore di dati e informazioni relativi a tecniche d'attacco, vulnerabilità hardware e software, pubblicate originariamente dal [MITRE](#) e rilasciate con specifiche di dettaglio da parte del "National Vulnerability Database" (NVD).

Accedi [alla Dashboard](#) per avere un quadro di sintesi delle ultime informazioni disponibili. Utilizza il menu in alto per accedere alle altre sezioni, fra le quali la [lista completa dei CVE](#), delle debolezze software (CWE) e delle tecniche di attacco (CAPEC).

Sono disponibili anche informazioni su file binari sospetti ([Analyzer](#)) e indicatori di compromissione network ([Blocklist](#)).

Specifiche dettagliate sull'utilizzo del sito sono [disponibili nel manuale operativo](#).

At the bottom of the page, there is a footer that reads "Developed by" followed by the logo of the CERT-PA (Computer Emergency Response Team - Public Administration).



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

The screenshot shows the INFOSEC Dashboard interface. At the top, there is a navigation bar with links: Home, Dashboard, CVE(s), Search, CWE(s), CAPEC(s), Statistics, Analyzer, Blocklist, and About. The main content area is divided into two columns.

Latest 20 CVEs published by NIST

CVE	Published	Updated	CVSS	CWE	Vendor(s)	Famil(y)ies	Product(s)
CVE-2017-6469	2017-03-04	2017-03-04	N/A	N/A	N/A	N/A	N/A
CVE-2017-6471	2017-03-04	2017-03-04	N/A	N/A	N/A	N/A	N/A
CVE-2017-6474	2017-03-04	2017-03-04	N/A	N/A	N/A	N/A	N/A
CVE-2017-6467	2017-03-04	2017-03-04	N/A	N/A	N/A	N/A	N/A
CVE-2017-6473	2017-03-04	2017-03-04	N/A	N/A	N/A	N/A	N/A
CVE-2017-6472	2017-03-04	2017-03-04	N/A	N/A	N/A	N/A	N/A
CVE-2017-6468	2017-03-04	2017-03-04	N/A	N/A	N/A	N/A	N/A
CVE-2017-6470	2017-03-04	2017-03-04	N/A	N/A	N/A	N/A	N/A
CVE-2016-10070	2017-03-03	2017-03-03	N/A	N/A	N/A	N/A	N/A
CVE-2016-8236	2017-03-03	2017-03-03	N/A	N/A	N/A	N/A	N/A
CVE-2016-3127	2017-03-03	2017-03-03	N/A	N/A	N/A	N/A	N/A
CVE-2016-10066	2017-03-03	2017-03-03	N/A	N/A	N/A	N/A	N/A
CVE-2016-10065	2017-03-03	2017-03-03	N/A	N/A	N/A	N/A	N/A
CVE-2016-10061	2017-03-03	2017-03-03	N/A	N/A	N/A	N/A	N/A
CVE-2016-7969	2017-03-03	2017-03-03	N/A	N/A	N/A	N/A	N/A
CVE-2015-8814	2017-03-03	2017-03-03	N/A	N/A	N/A	N/A	N/A
CVE-2016-7400	2017-03-03	2017-03-03	N/A	N/A	N/A	N/A	N/A

Statistics

- 83120 Vulnerabilities
- 971 CWE(s)
- 463 CAPEC(s)
- 1277 MS Patches
- 6756 Malwares
- 137154 IoC in 28 Blocklists

Latest analyses

#	Filename	AV
#1	62809-74220-...	1/58
#2	rpc420_setup...	1/58
#3	nethost.exe	28/59
#4	81532-674473...	28/58
#5	nethost.exe	25/59
#6	FASTRARExtra...	9/59
#7	mininews-2.exe	28/58
#8	mininewsrepa...	5/58

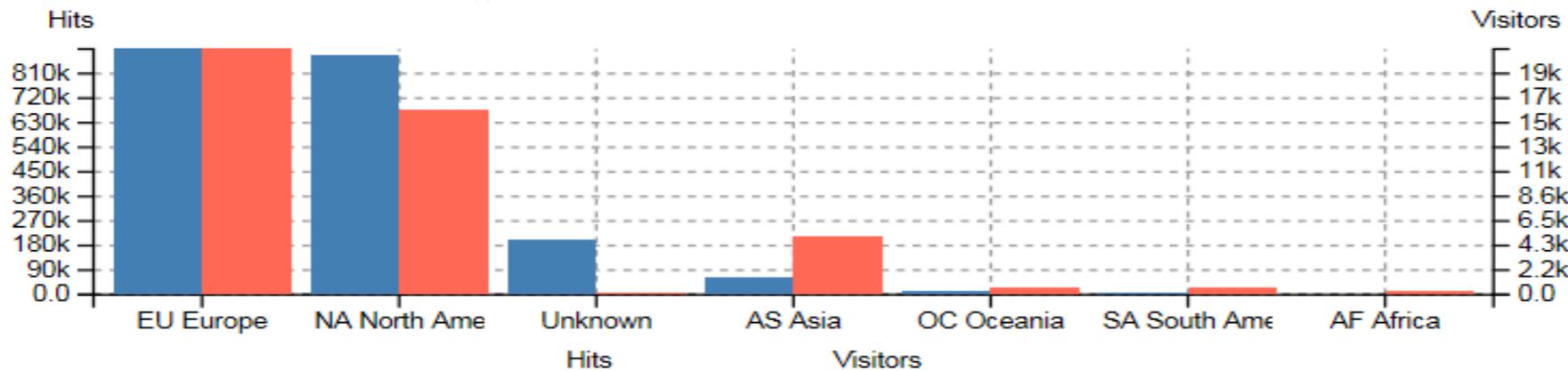


Accessi ad Infosec - Gennaio 2018

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