



# GovCERT.it: prime esperienze

*SMAU - 20 ottobre 2005*

Sicurezza ICT: cosa sta succedendo nel nostro paese

*Matteo Cavallini GovCERT.it-CNIPA*

# Sommario

- I CERT-CSIRT
- Lo scenario di riferimento
- Il GovCERT.it

# I CERT-CSIRT

Diffusione e caratteristiche

# CSIRT e sinonimi

**C**OMPUTER

**S**ECURITY

**I**NCIDENT

**R**ESPONSE

**T**EAM

CERT

SERT

IRT

SIRT

IHT

CIRC

IMT

IRC

# Il primo CERT®

**2 Novembre 1988**

## Internet Worm

L'autore è Robert T. Morris jr., studente della Cornell University e figlio di R.M., uno degli autori di UNIX ed alto ufficiale della NSA.  
 Il worm blocca 6000-8000 computer (10%) della rete Internet (Arpanet) rendendola non operativa



**17 Novembre 1988**

## CERT

Viene creato presso la Carnegie Mellon University, con fondi governativi, il primo CERT con l'obiettivo di avere un team per la prevenzione di futuri incidenti (CERT/CC)



© 1988-2003 by Carnegie Mellon University

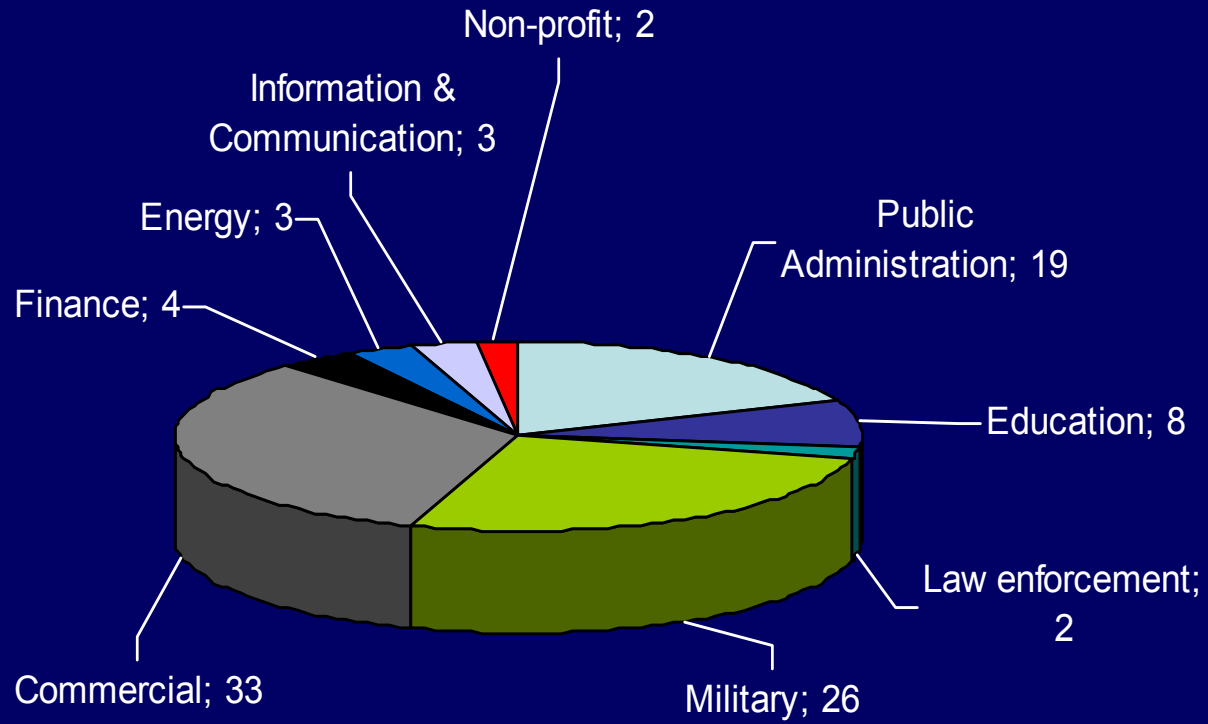
# CSIRT nel mondo

- 1989: viene creato il FIRST (Forum of Incident Response and Security Team) per facilitare la collaborazione fra i CSIRT USA
- 1992: primi CSIRT in Europa (Olanda, Germania) nell'ambito delle comunità di ricerca
- 1993: viene costituito il primo CSIRT australiano (AusCERT)
- 1997: prende vita l'APCERT (Asia e nazioni dell'area Pacifico)
- Fine anni '90: primi CSIRT in America Latina
- 2004: nasce il TF-CSIRT (CSIRT Task Force) in ambito TERENA (Trans-European Research and Networking Association)

# Dati attuali

**FIRST**  
**170 CSIRT**  
**affiliati**

**TF-CSIRT**  
**42 CSIRT**  
**affiliati**



**Settori di appartenenza (%)**

# Caratteristiche dei CSIRT

**Tipologia e missione**

**Constituency ed autorità**

**Modello organizzativo**

**Servizi erogati**

**Relazioni**

# Tipi e modelli organizzativi

## TIPI

**CSIRT interni**

**CSIRT nazionali**

**Centri di Analisi**

**Team di supporto di  
fornitori**

**MSSP**

## MODELLI

**CSIRT centralizzati**

**CSIRT distribuiti**

**CSIRT misti**

**CSIRT coordinamento**

**Security Team**

# Constituency ed autorità

- La constituency di un CSIRT, ossia la comunità di riferimento, è costituita dagli utenti, dagli enti e dalle organizzazioni cui il CSIRT eroga i suoi servizi
- Il livello di autorità attribuito ad un CSIRT determina conseguenze in merito all'efficacia della sua azione nei confronti della sua comunità di riferimento.

I possibili livelli di autorità sono i seguenti:

- **autorità piena** – quando il gruppo ha il potere di imporre azioni e comportamenti
- **autorità condivisa** – quando il gruppo è in grado di influenzare azioni e comportamenti partecipando anche ai processi decisionali
- **nessuna autorità** – quando il gruppo può solo dare raccomandazioni, consigli e suggerimenti, anche se autorevoli

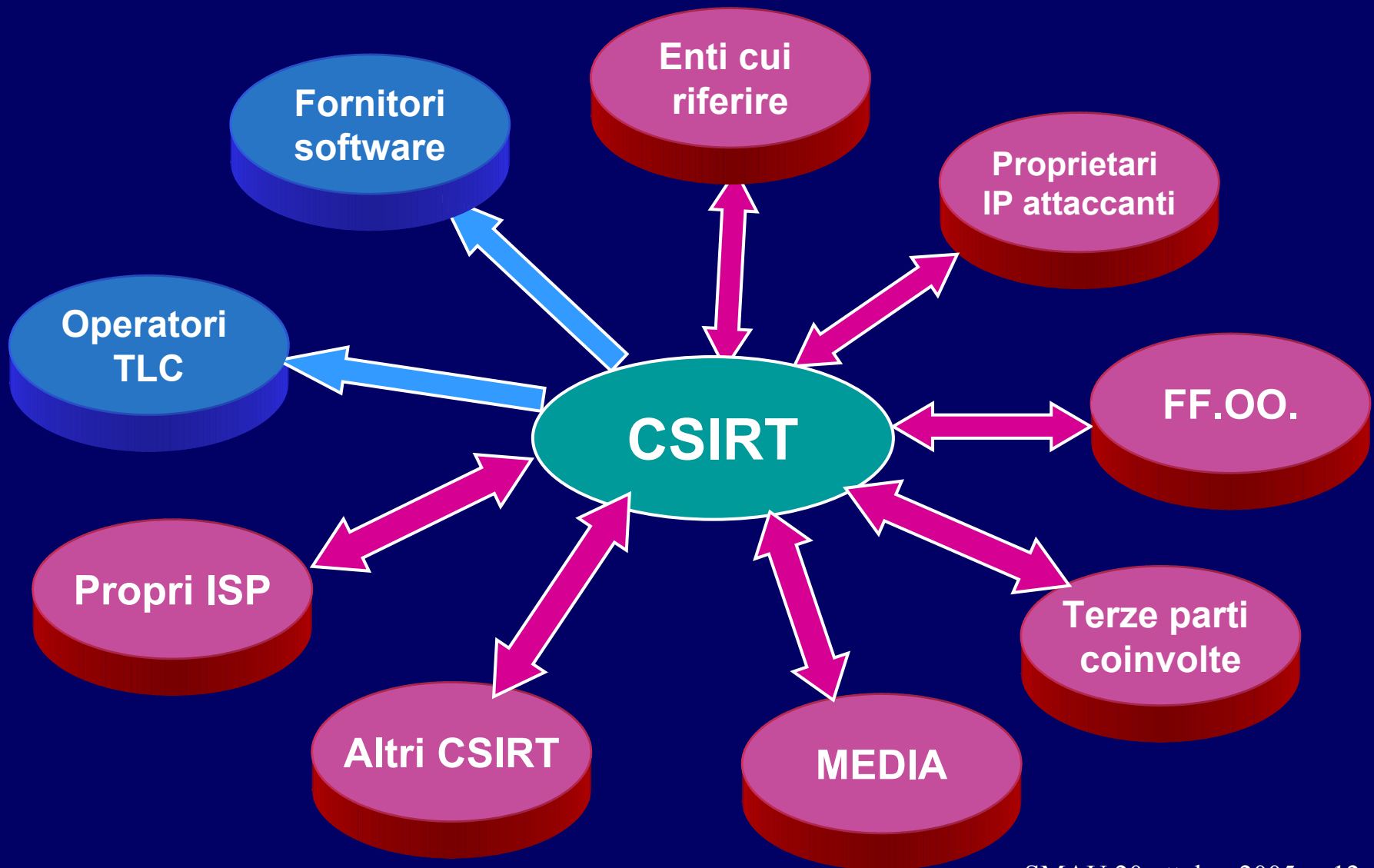
# Servizi dei CSIRT

<b><i>REATTIVI</i></b>
<b>Early warning</b>
<b>Gestione incidenti</b>
<b>Analisi</b>
<b>Intervento sul sito</b>
<b>Supporto alla risposta</b>
<b>Coordinamento della risposta</b>
<b>Gestione codici pericolosi</b>
<b>Analisi</b>
<b>Risposta</b>
<b>Coordinamento della risposta</b>

<b><i>PROATTIVI</i></b>
<b>Osservatorio tecnologico</b>
<b>Valutazioni/verifiche</b>
<b>Intrusion detection</b>
<b>Disseminazione informazioni</b>
<b>Raccolta e condivisione informazioni</b>

<b><i>QUALITÀ SICUREZZA</i></b>
<b>Analisi dei rischi</b>
<b>Pianificazione continuità di servizio</b>
<b>Consulenza</b>
<b>Sensibilizzazione</b>
<b>Formazione</b>
<b>Valutazione e certificazione prodotti</b>

# Relazioni di un CSIRT



# I CSIRT italiani più noti

- CERT-IT - Università di Milano
- GARR-CERT - Gruppo Armonizzato Reti Ricerca
- S<sup>2</sup>OC - Telecom Italia
- CERT-Difesa

# Lo scenario di riferimento

Normativa e progetto

# I CERT-AM

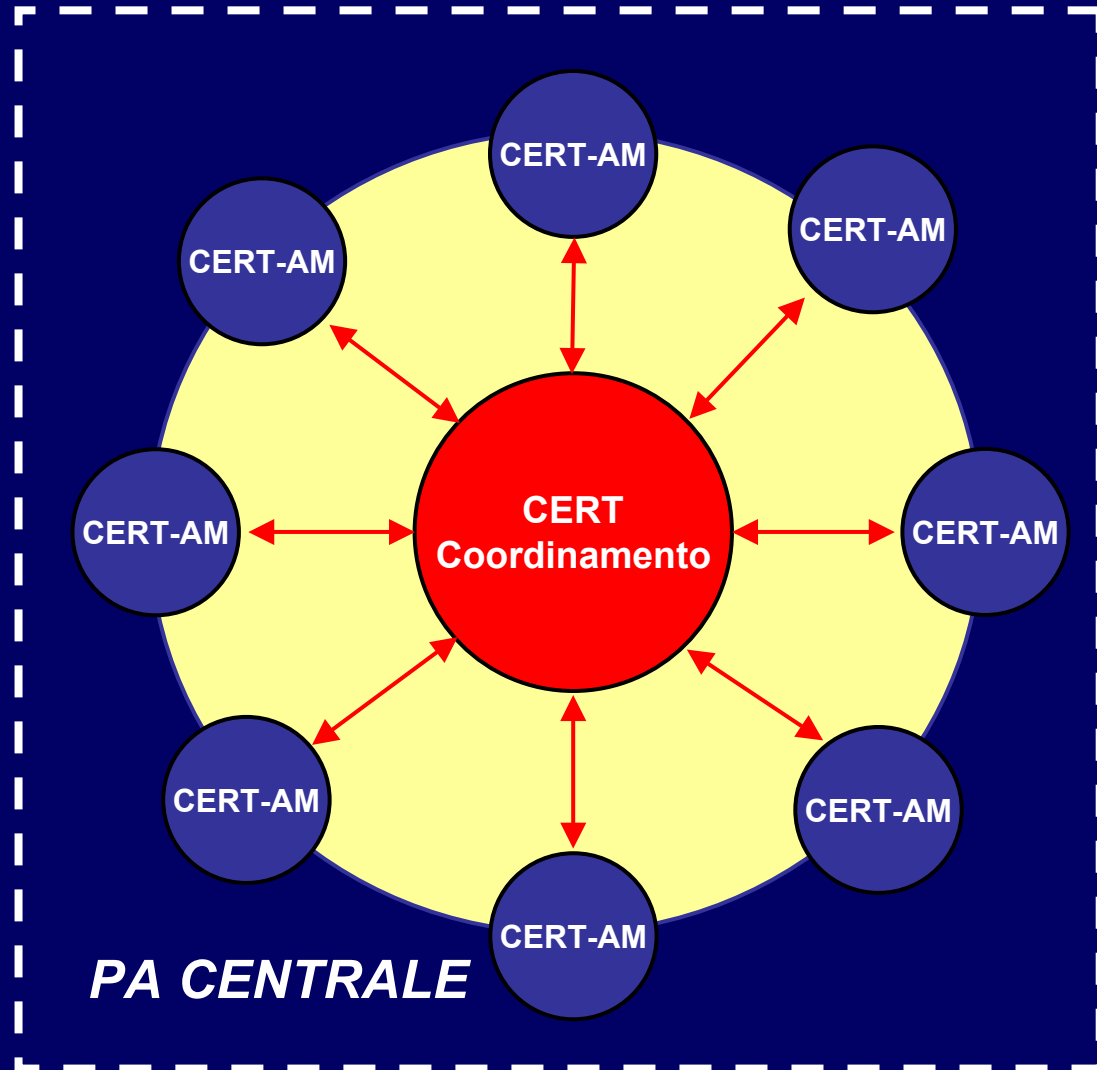
## Estratti della Direttiva 16/1/2002

- “Assume priorità la predisposizione di una procedura per la Gestione degli Incidenti e l’approntamento di uno specifico presidio organizzativo denominato CERT-AM: Computer Emergency Response Team dell’Amministrazione.”
- “Deve essere costituita una squadra di intervento per gli incidenti, in modo da poterli limitare e prevenire in maniera efficace ed economica.”
- “La squadra di intervento deve essere preparata a rilevare ed a reagire agli incidenti garantendo:
- Risposta efficace e preparata
  - Centralizzazione e non duplicazione degli sforzi
  - Incremento della consapevolezza degli utenti rispetto le minacce.”

# Il tassello mancante

DIRETTIVA 16/1/2002  
CERT-AM ED UNITÀ  
LOCALI NELLE PA  
CENTRALI

ISTITUZIONE DEL  
GovCERT.it  
CSIRT GOVERNATIVO DI  
COORDINAMENTO



# GovCERT.it

- Proposto dal “Comitato tecnico nazionale sulla sicurezza informatica e delle telecomunicazioni nelle pubbliche amministrazioni”
- Approvato dal Comitato dei ministri per la società dell’informazione
- Attuato dal CNIPA attraverso la creazione di una “Unità di gestione degli attacchi informatici” - maggio 2004
- Finanziamenti resi disponibili - settembre 2004
- Nucleo operativo attualmente costituito da 4 (+1) risorse

# GovCERT.it - obiettivi

- Assicurare un presidio informativo sugli eventi che possono colpire le infrastrutture, i servizi e gli utenti finali della PA, fornendo le informazioni idonee a prevenire e gestire le eventuali emergenze da parte del personale tecnico delle singole aziende della PA
- Emanare linee guida di tipo tecnico ed organizzativo per favorire ed uniformare la capacità di risposta agli incidenti e lo sviluppo e la cultura della sicurezza nelle PA
- Collaborare con altri Organi dello Stato che hanno competenza in materia e favorirne l'interazione
- Promuovere la formazione sulla sicurezza ICT ed in particolare sulla prevenzione e gestione degli incidenti di sicurezza informatica
- Costituire per la PA un punto di riferimento per la sicurezza informatica

# Il GovCERT.it

Unità gestione attacchi informatici - CNIPA

**Tipologia e missione**

**CSIRT interno**

**Constituency & autorità**

**PA Centrale  
Nessuna autorità**

**Modello organizzativo**

**CSIRT coordinamento**

# Linee di azione prioritarie

**Creazione e stabilizzazione delle relazioni con la  
Constituency**

**Progettazione, sviluppo ed erogazione alla  
Constituency dei servizi di maggiore utilità,  
efficacia ed economicità di sistema**

**Definizione di accordi di collaborazione con altri  
Organi dello Stato, con istituzioni analoghe anche  
internazionali, con fornitori di prodotti e servizi**

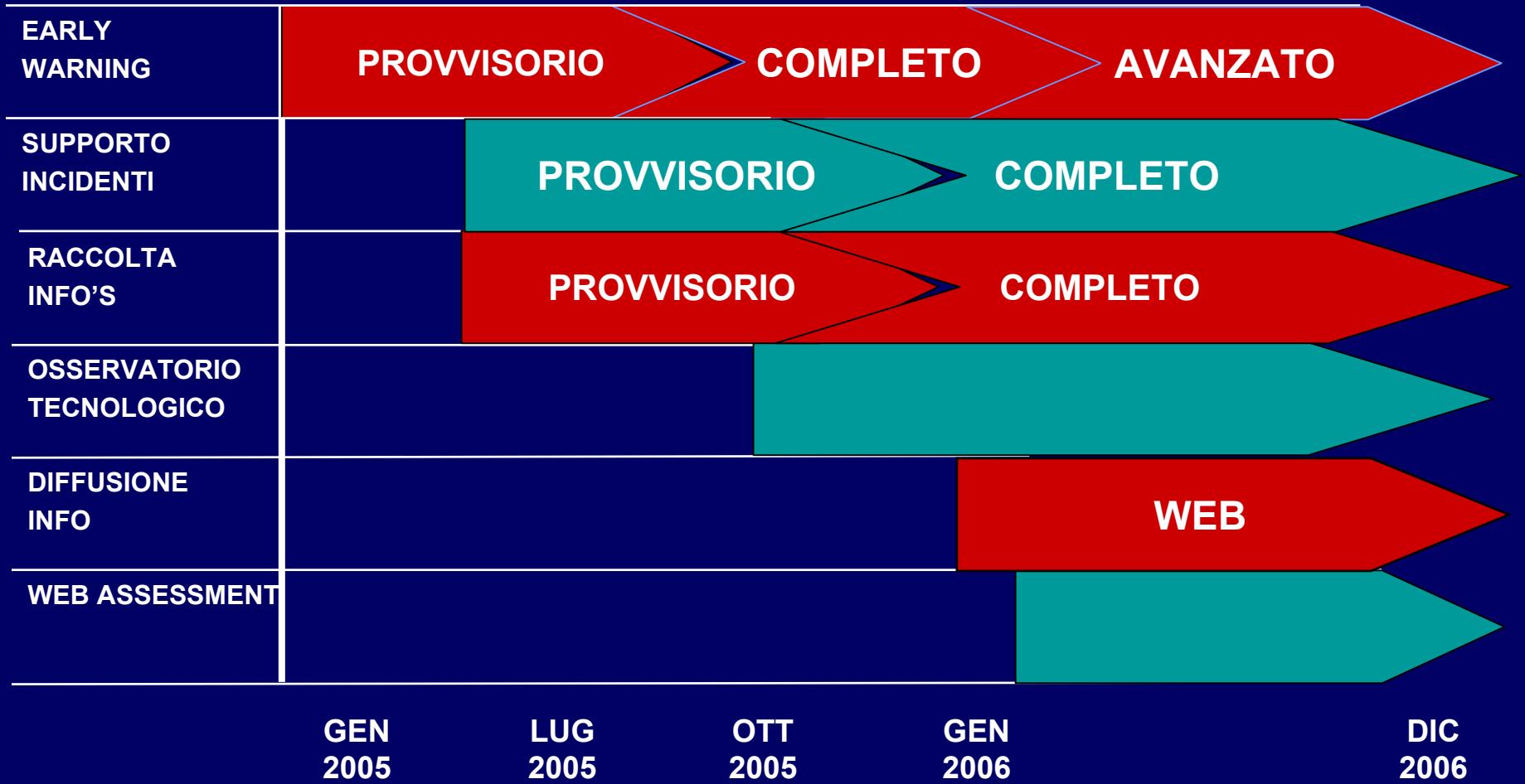
# GovCERT.it - Constituency

- Relazioni stabili e già operative con **29 Amministrazioni** (su 59) più alcune adesioni a titolo volontaristico
- Per ogni Amministrazione gli interlocutori del GovCERT.it sono stati classificati in:
  - ISTITUZIONALI
    - Consiglieri tecnici per la sicurezza ICT
    - Comitati Sicurezza ICT
    - Responsabili sistemi informativi
  - DI RIFERIMENTO
    - Responsabili sicurezza ICT
  - OPERATIVI
    - Gli appartenenti ai gruppi CSIRT/CERT-AM/unità locali o ai security team
- In corso la costituzione di un Gruppo di Lavoro ristretto per la definizione di linee guida per i CSIRT della PAC e della disciplina delle relazioni fra i CERT-AM ed il GovCERT.it; il gruppo fungerà da anche da gruppo di contatto con le Amministrazioni.

# GovCERT.it - servizi

<b><i>REATTIVI</i></b>	<b><i>PROATTIVI</i></b>	<b>QUALITÀ SICUREZZA</b>
<b>Early warning</b>	<b>Osservatorio tecnologico</b>	<b>Sensibilizzazione</b>
<b>Gestione incidenti</b>	<b>Valutazioni/verifiche</b>	<b>Formazione</b>
<b>Supporto alla risposta</b>	<b>Disseminazione informazioni</b>	
<b>Coordinamento della risposta</b>	<b>Raccolta e condivisione informazioni</b>	
<b>Gestione codici pericolosi</b>		
<b>Coordinamento della risposta</b>		

# Piano dei servizi



# Servizio Early Warning

I Bollettini prodotti sono:

- in **lingua italiana** e formati predefiniti;
- **firmati digitalmente**;
- creati sulla base di informazioni reperite da fonti private e pubbliche.

Da Gennaio 2005

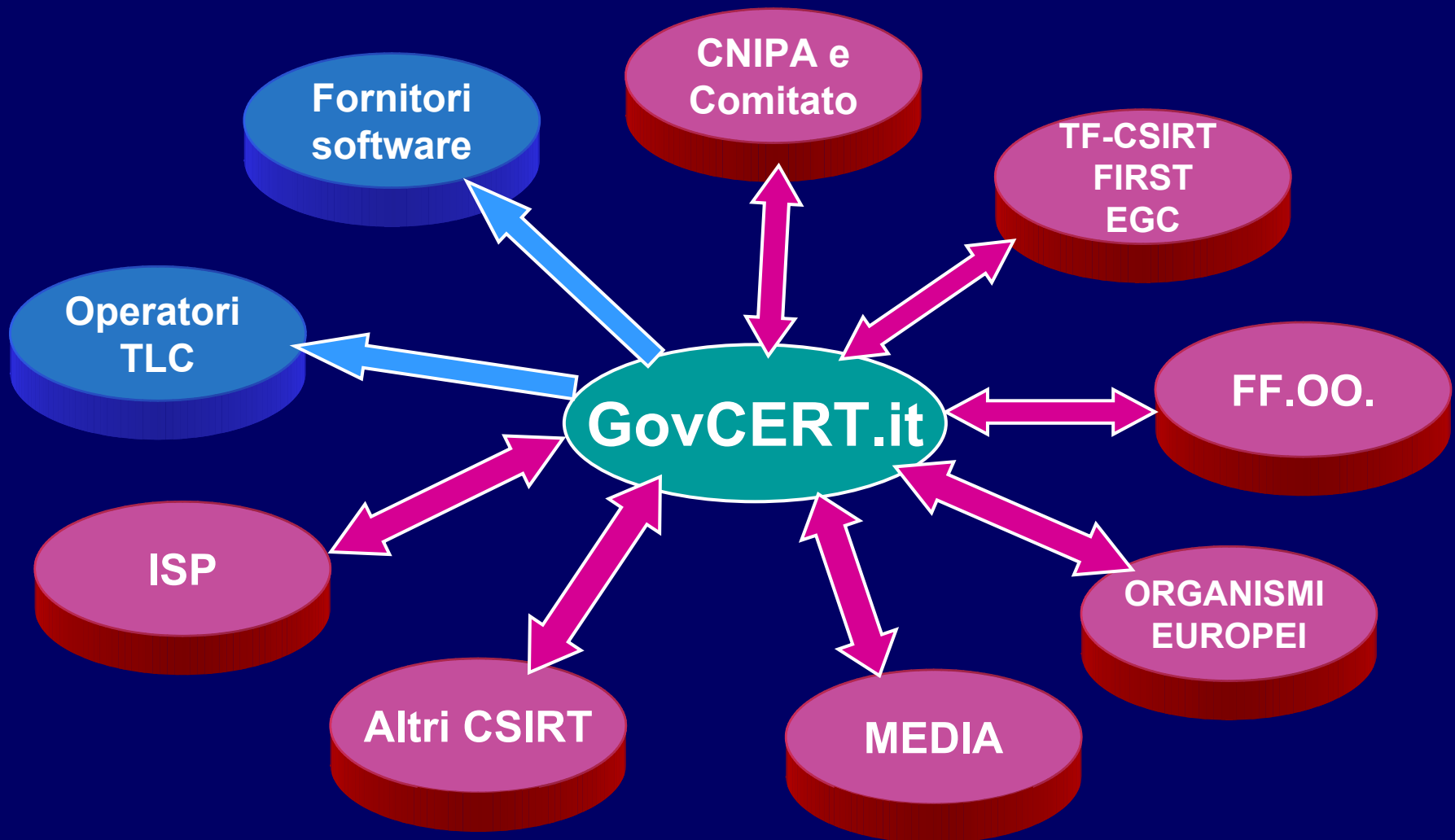
- **56** segnalazioni per nuove vulnerabilità gravi o importanti
- **11** avvisi di presenza in rete di malware a rischio medio o elevato
- Metriche e profilazione tecnologica delle Amministrazioni (in corso di definizione)
- Ampliamento del dominio tecnologico di osservazione

# Servizio gestione incidenti

Da gennaio 2005

- Rilevazione web defacement sui siti web della Constituency, delle Regioni, delle Province di maggiore importanza (Procedure di comunicazione con firma digitale e ove praticabile cifrate)
  - 16 web defacement rilevati e comunicati
- Ricevute alcune segnalazioni di incidenti
  - una di esse ha richiesto l'analisi del codice virale

# GovCERT.it - relazioni





**CSIRT**  
governativi  
in  
**EUROPA**

# WG ENISA

- Partecipazione al Gruppo di Lavoro ristretto su “CERT cooperation”, recente iniziativa di ENISA (European Network and Information Security Agency)
  - Prima attività: inventario dei CSIRT operanti nei paesi dell’Unione Europea

**Il giorno 11 ottobre si è svolto il primo incontro dei CSIRT Italiani che ha visto la partecipazione di 16 security-team italiani in rappresentanza di quasi tutti i settori della società. L’organizzazione è stata curata in collaborazione con il CERT-IT.**

“L'ottimista pensa che questo sia il  
migliore dei mondi possibili.  
Il pessimista sa che è vero.  
(Oscar Wilde) ”

Grazie dell'attenzione