NuCS

il Nucleo CyberSecurity dell'INFN

Qui e nuce nucleum esse vult, frangit nucem

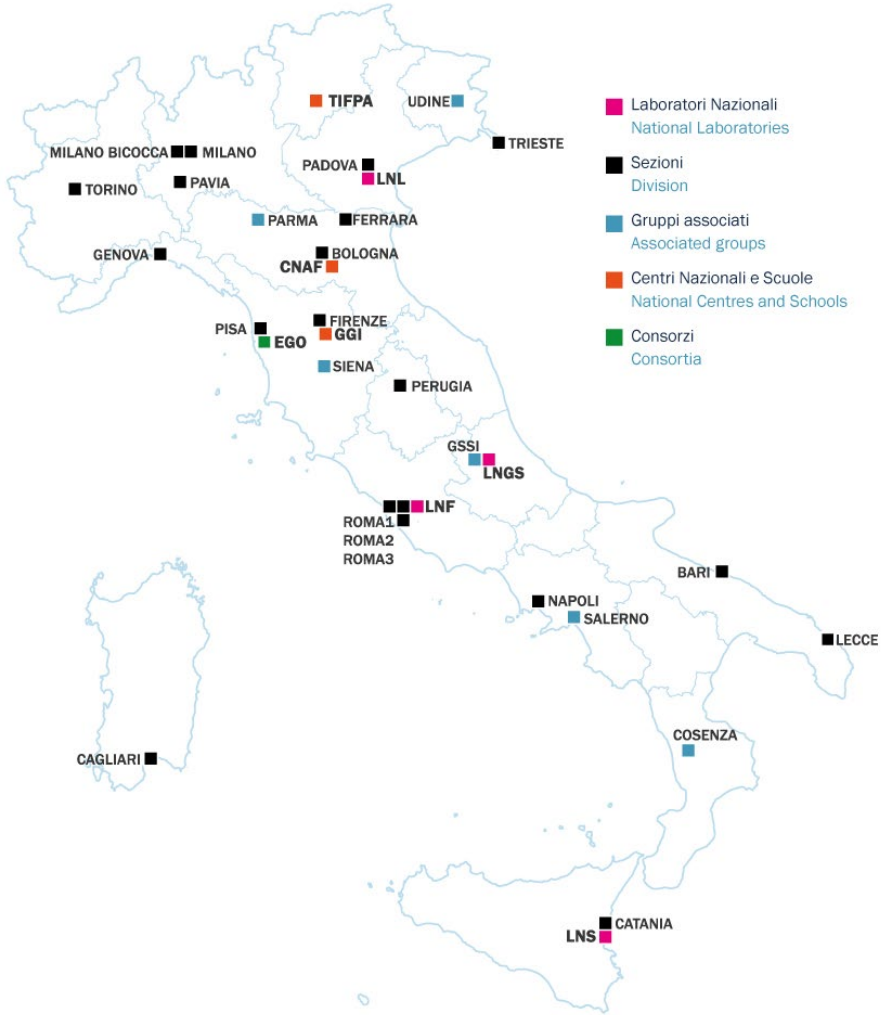
Luca Giovanni Carbone

INFN

ConfGARR23

SAPERI INTERCONNESSI

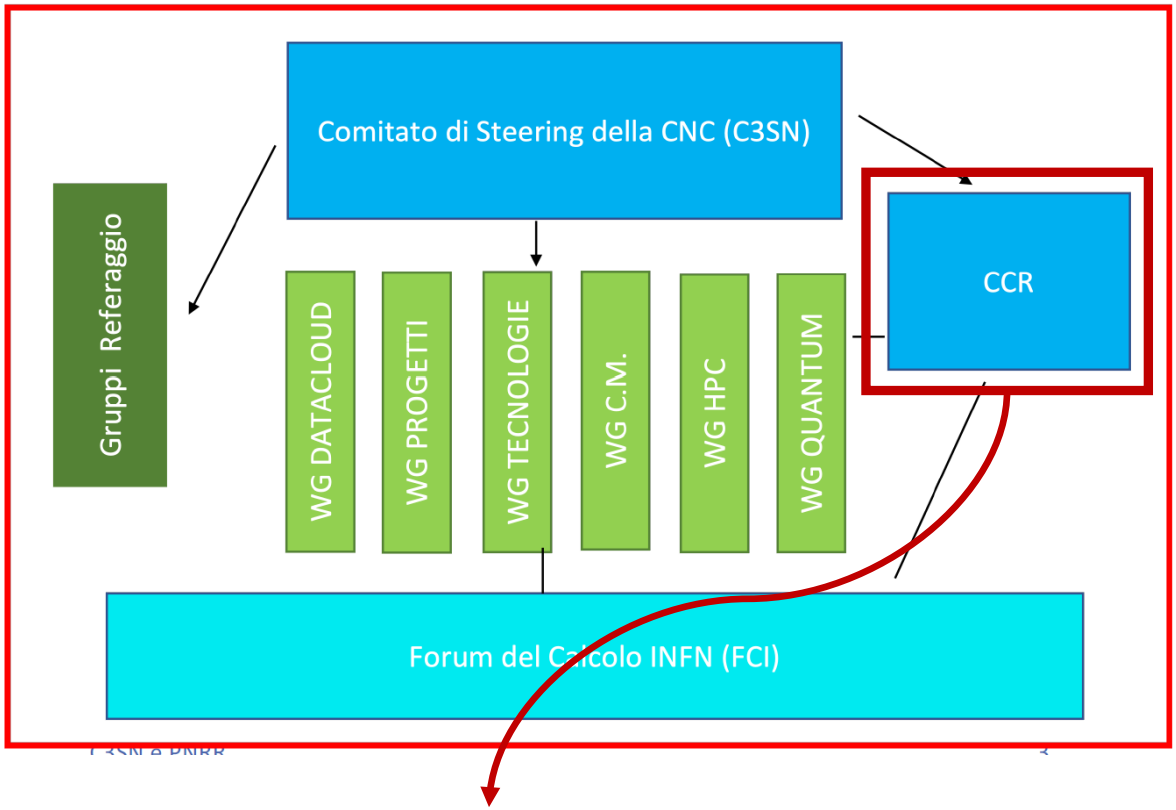
INFN: ecosistema e qualche numero



Utenti: ~10k
IPv4 address space: ~60k
IPv6 address space: n x /48
thput aggregato: ~ 0.5 Tb/sec

- cluster calcolo scientifico
  - T1, 9 T2, n T3/...
- Datacloud (con isole ISO)
- SSNN, SI (CNAF, LNL, LNF)
- servizi infrastrutturali locali (DNS, mail, ...)
- server esperimento locali
- amministrazione centrale + locali
- desktop/laptop personali
- (switch, stampanti, ...)

Il calcolo: la Commissione Nazionale Calcolo



Mandato CCR:

- (...)
- **gestire la sicurezza informatica dell'Istituto, di concerto col Responsabile per la Transizione Digitale** (nasce il ruolo del *responsabile nazionale cybersecurity*);
- (...)

La cybersecurity *storica*

Le strutture si sono di norma occupate *autonomamente* di security; storicamente CCR ha sempre promosso attività sulla security attraverso gruppi di lavoro (*WG Security*, *Harmony*) che si sono occupati di R&D, coordinamento di alcune attività, formazione, normativa e, negli anni, hanno prodotto (in ordine sparso):

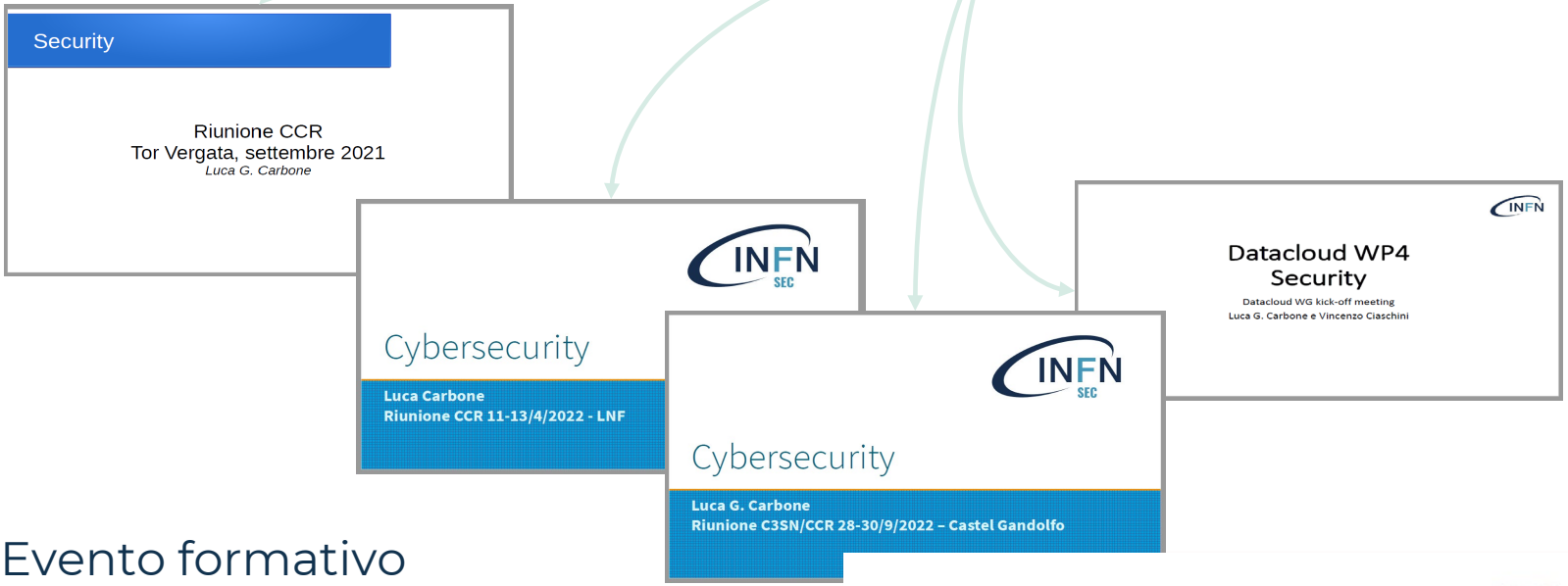
- infrastruttura wireless condivisa
- disciplinare sull'utilizzo delle risorse
- applicazione MM AgID e procedura valutazione rischio informatico
- audit interni
- scansioni vulnerabilità
- policy condivisa su password e filtri perimetrali
- CSIRT INFN

- firewall trasparenti
- argus (sniffer di rete)
- storage RO per log
- IPv6 monitoring tools
- comparativa tra vulnerability scan
- Linux *hardening*
- ...

Cosa è mancato?
- **coordinamento organico tra strutture**
- **visibilità globale eventi di sicurezza**
- **condivisione**
- **procedure e ruoli definiti**

La traversata del deserto

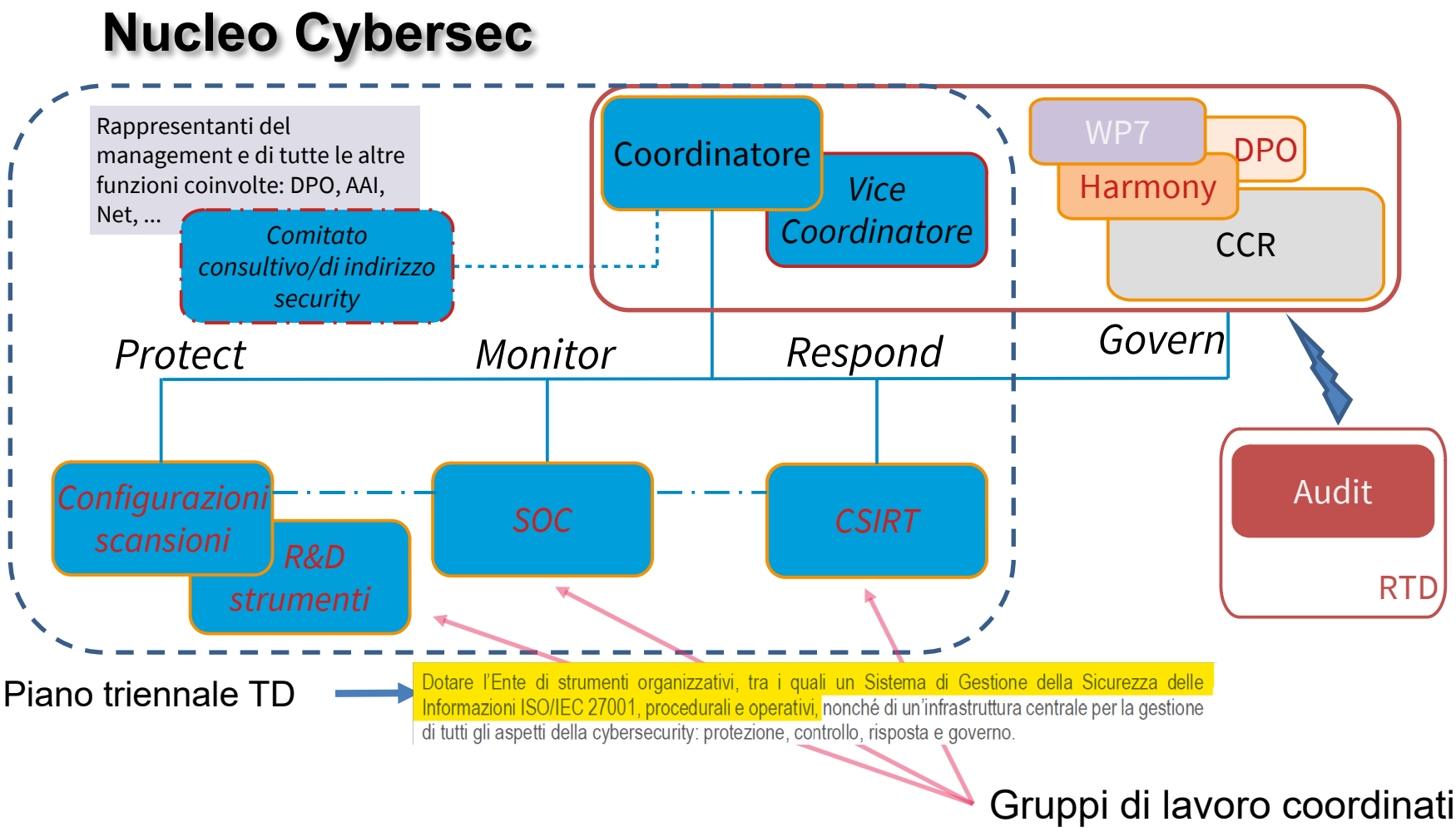
Proposte organizzative



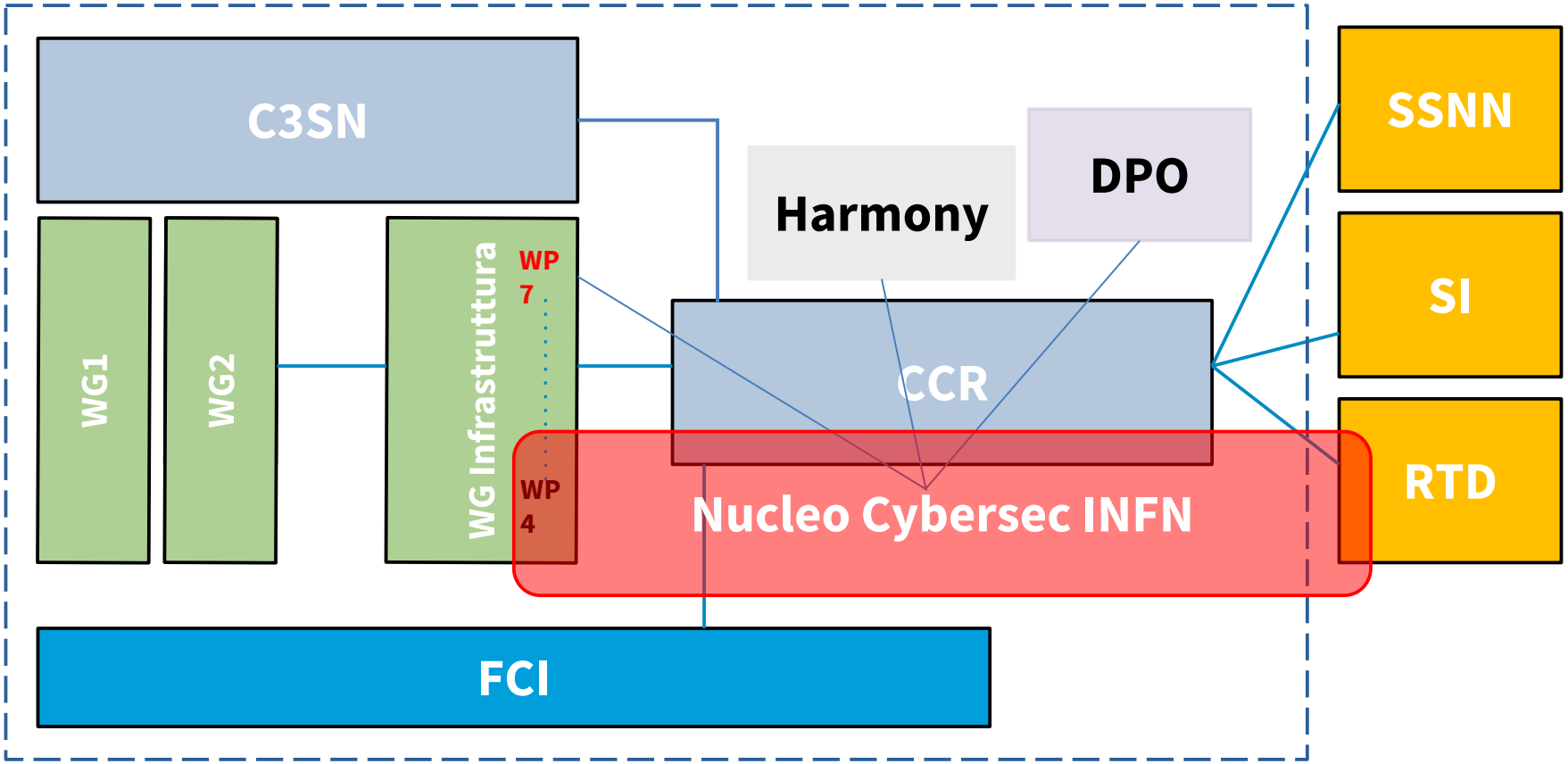
Evento formativo

Workshop fondativo

La cybersecurity oggi (quasi...)



The Big Picture



Piano triennale per la Transizione Digitale (Dicembre 2022)

Area Sicurezza Informatica

Dotare l'Ente di strumenti organizzativi, tra i quali un Sistema di Gestione della Sicurezza delle Informazioni ISO/IEC 27001, procedurali e operativi, nonché di un'infrastruttura centrale per la gestione di tutti gli aspetti della cybersecurity: protezione, controllo, risposta e governo.
Migliorare la postura di sicurezza dell'Ente attraverso attività specifiche e mirate:

- aumento della consapevolezza dell'utenza;
- adozione di policy di sicurezza comuni/coordinate e strumenti/infrastrutture centralizzati;
- definizione di una baseline per la configurazione sicura dei servizi informatici esposti.

Il piano si articolerà sulle seguenti linee d'azione generali:

- formazione del personale e miglioramento della consapevolezza in materia di sicurezza informatica e, in particolare, in riferimento alle pratiche di gestione della posta elettronica (riconoscimento del *phishing*), delle credenziali di accesso (introduzione all'utilizzo di password manager) e – in generale – di approccio all'utilizzo delle risorse informatiche;
- diminuzione del perimetro d'attacco e miglioramento della postura di sicurezza delle strutture mediante l'adozione di politiche coordinate e comuni per quanto riguarda la configurazione dei servizi esposti e degli strumenti di controllo e prevenzione;
- creazione di una struttura operativa centrale in grado di assolvere e coordinare le funzioni fondamentali di protezione, controllo, risposta e governo per tutto l'Ente;
- creazione di un'infrastruttura centralizzata per la raccolta dei dati di sicurezza dalle varie strutture, l'analisi degli stessi e la *threat intelligence*, al fine di implementare le opportune e necessarie attività preventive/proattive e reattive e il coordinamento con CERT/CSIRT nazionali e internazionali;
- promozione dell'utilizzo di un cybersecurity framework e di tool di risk assessment e monitoring;
- gestione del Rischio: Individuazione di un sistema di Valutazione del Rischio standardizzato da adottare in tutte le strutture come quello messo a disposizione dell'Agid "Tool di Risk Management", che permetta di valutare tutti gli aspetti inerenti alla sicurezza dell'informazione e permetta ai Titolari dei dati una visione complessiva efficace ed efficiente.

Configurazioni

NuCS

SOC

Cybersecurity framework

Relazioni con il Framework Nazionale per la CyberSecurity

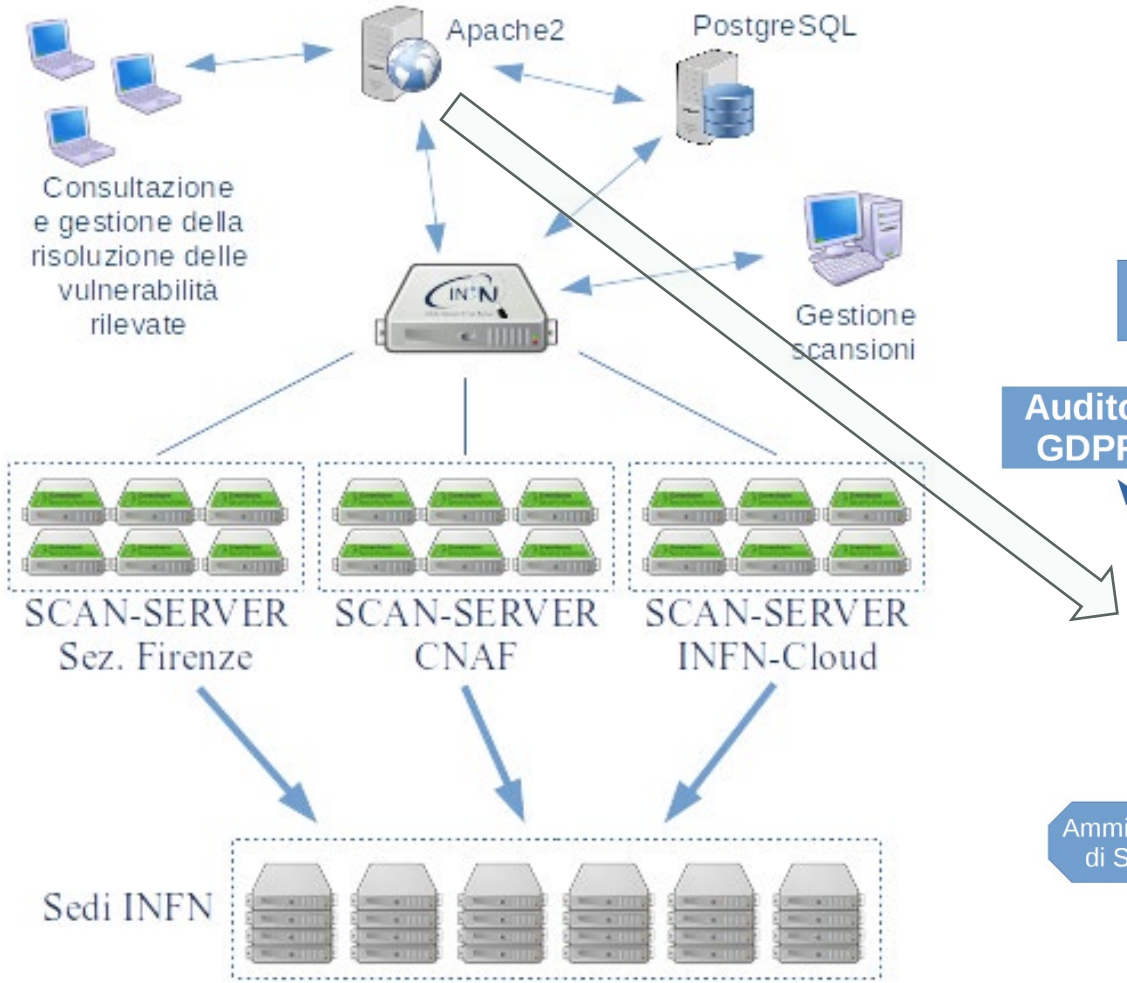
- **IDENTIFY**: *definizione asset, dati e processi strategici*
- **PROTECT**: ***implementazione di strumenti, attività e controlli volti alle protezione degli asset***
- **DETECT**: ***rilevazione anomalie e incidenti***
- **RESPOND**: ***mitigazione impatto incidenti***
- **RECOVER**: *ripristino rapido ed efficiente di risorse e processi compromessi*

CIS Sapienza: *Framework Nazionale* per la Cybersecurity e la Data Protection

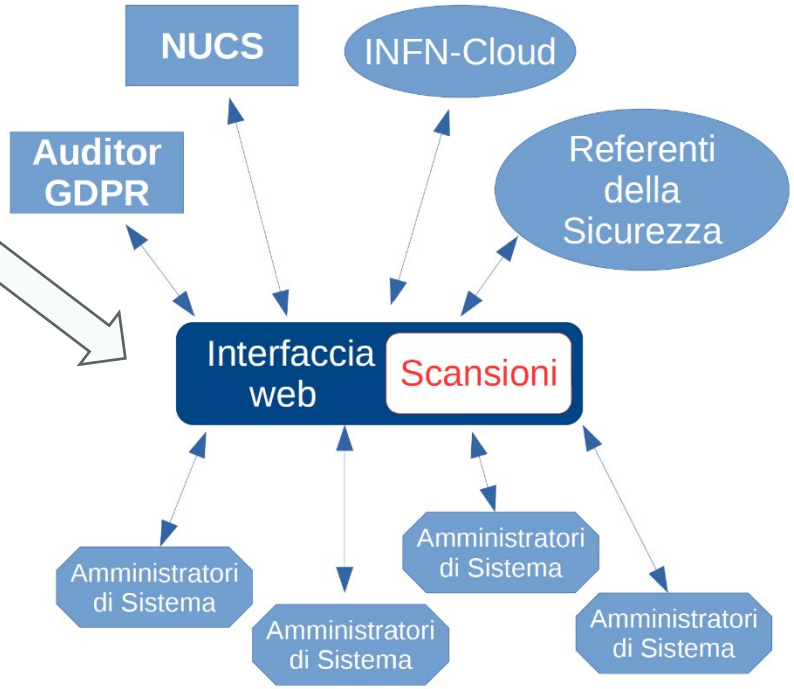
CSIRT *(L.G. Carbone, V. Ciaschini)*

- **6 persone/2 FTE** – 1 turno da 7 gg ogni 6 settimane (1/6 < 0.3)
  - *routine (garantita)*:
    - prima interfaccia con CERT/CSIRT terzi (CERT AgID, CSIRT Italia, GARR CERT, EGI-CSIRT, ...), gestione contatti istituzionali;
    - gestione segnalazioni da fonti aperte/istituzionali (Shadowserver, CERT AgID, CSIRT Italia, US-CERT/CISA ...): raccolta informazioni, valutazione pertinenza e rischio, eventuale trasmissione segnalazioni ai responsabili locali;
    - gestione vulnerabilità Datacloud;
    - consulenza;
  - *emergenza*: gestione incidenti (il team al completo) in collaborazione/coordinamento con il servizio calcolo coinvolto/responsabile locale (personale CSIRT non agisce direttamente su sistemi compromessi)
  - **Evoluzione: *trusted introducer* entro 2023; aggiornamento strumenti (rt => theHive, Cortex)**

Scansioni *(L. Lanzi)*

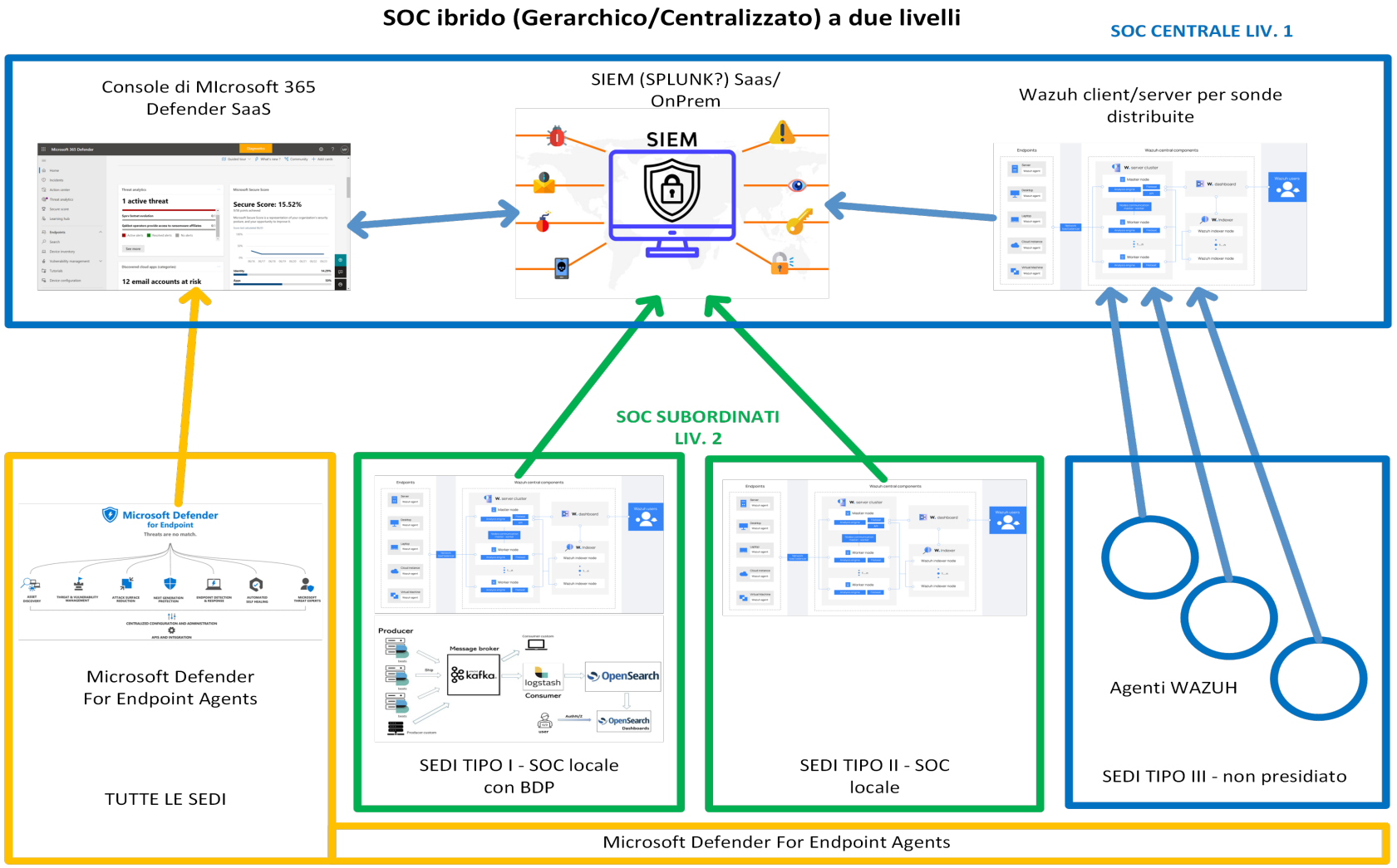


Prevista anche integrazione con *Shadowserver*

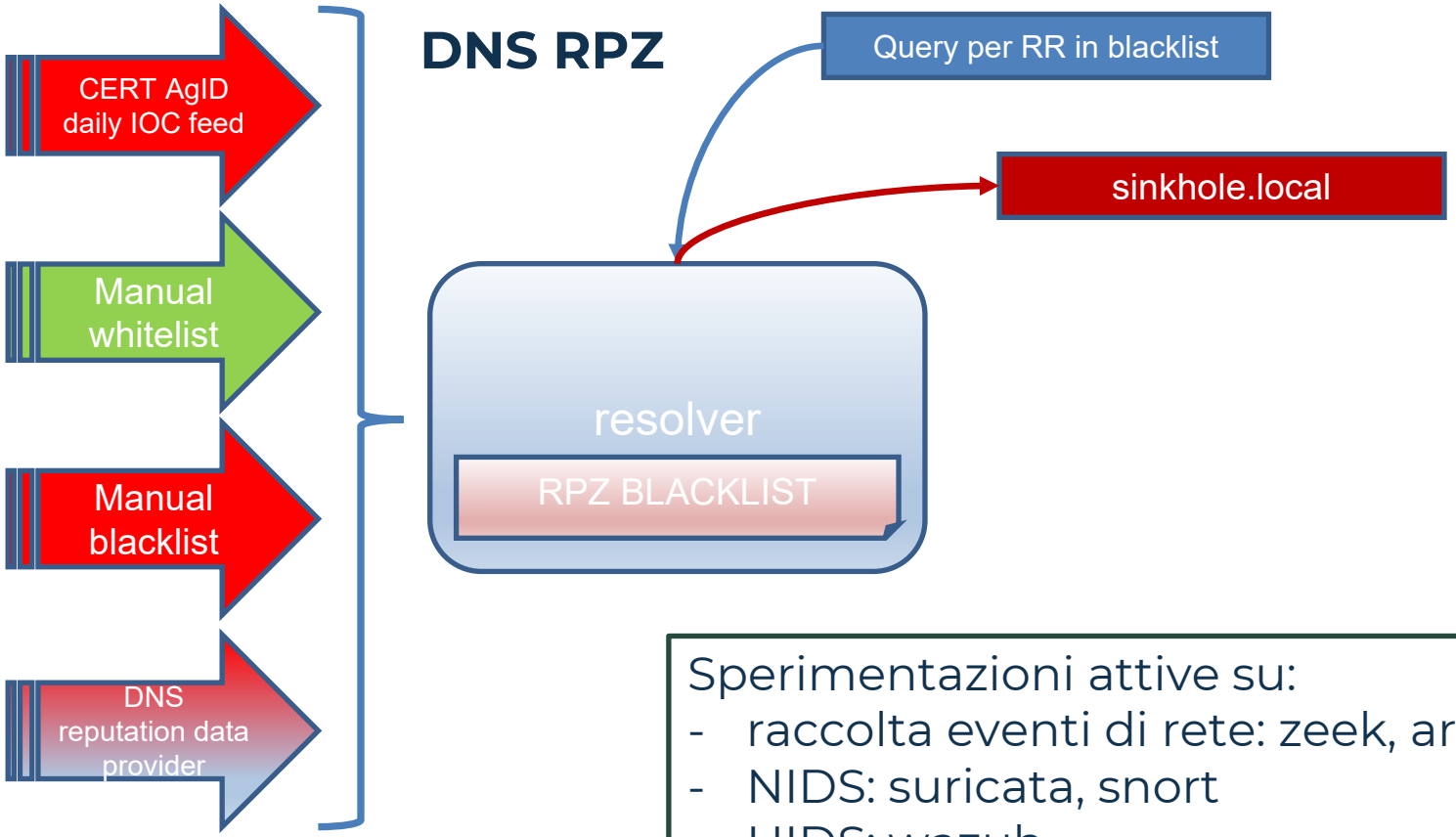


SOC *(G. Peco)*

SOC ibrido (Gerarchico/Centralizzato) a due livelli



Strumenti, configurazioni



Sperimentazioni attive su:
- raccolta eventi di rete: zeek, argus, ntop
- NIDS: suricata, snort
- HIDS: wazuh
- MISP
- condivisione IOC

roadmap

Data	Milestone
marzo	**Definizione gruppi Operation/R&D e coordinatori**
giugno	Istanza MISP in produzione
agosto	**CSIRT e SCANSIONI a regime**
ottobre	infrastruttura di test SOC up'n'running strumenti per strutture definiti
…	fase di test
dicembre	prototipo SOC in produzione, *CSIRT TI listed*

NUCS INFN: chi vuol mangiare la noce deve romperne il guscio

carbone@infn.it

ConfGARR23

SAPERI INTERCONNESSI