Istituto Nazionale di Fisica Nucleare
NUcleo CyberSecurity

NUCS

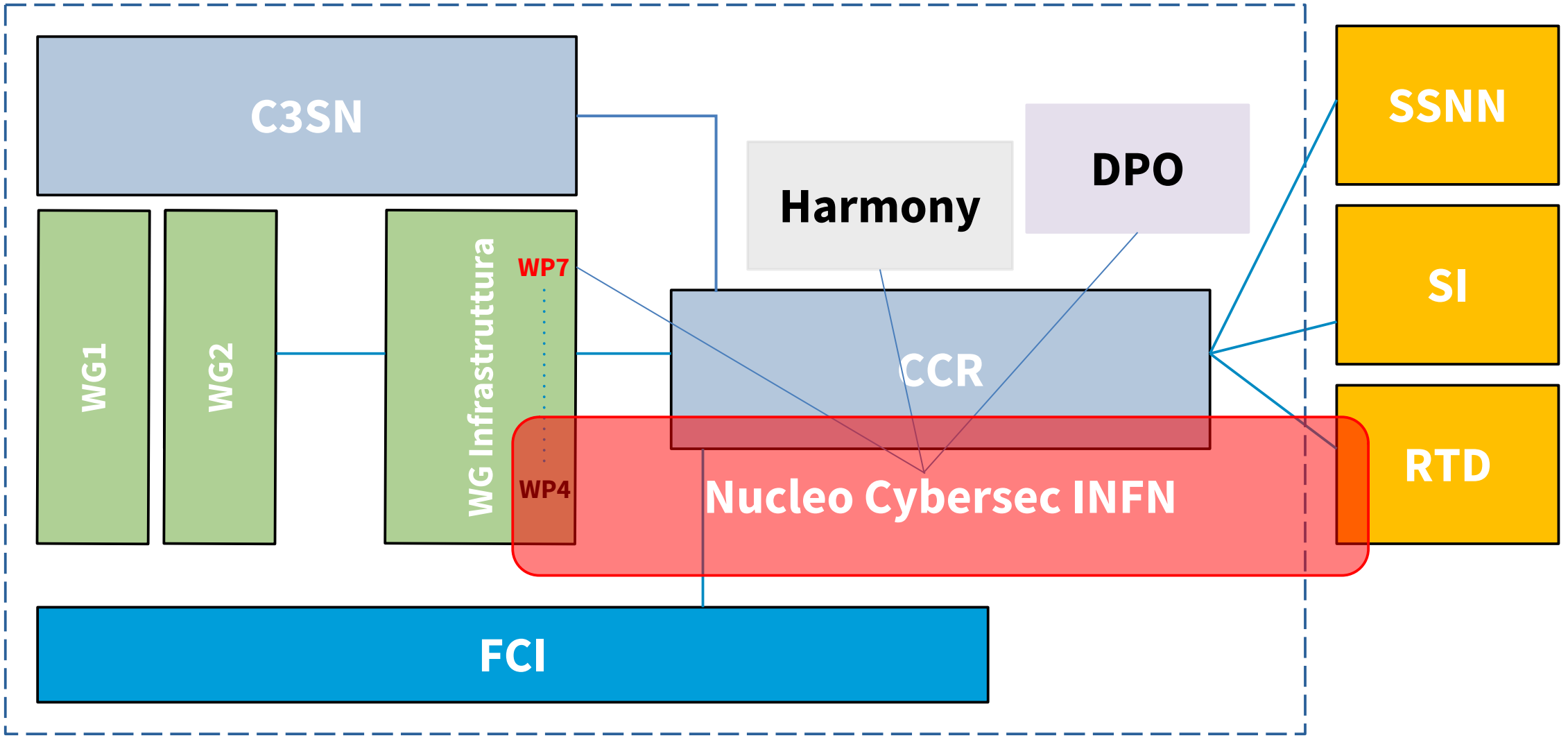
Great expectations

Jack Tamigi

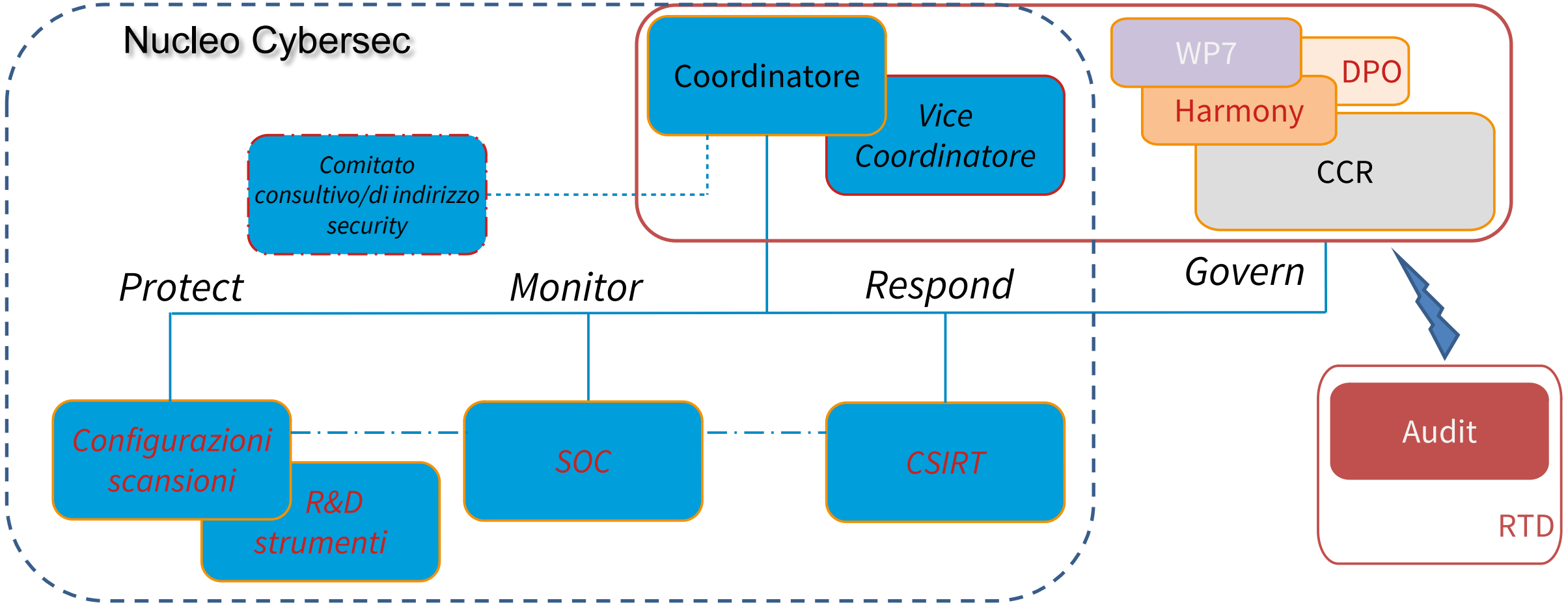
Mini WS CCR sulla Sicurezza Informatica

13-15/2/2023 - Padova

The Big Picture



Organigramma bis



Piano triennale TD → 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.

Manpower revisited

CSIRT
2 FTE ≅ 2 x 0.4 + 4 x 0.3

SCANSIONI
1.6 FTE ≅ 1 x 0.4 + 4 x 0.3

SOC & MISP (mainly R&D)
2.5 FTE ≅ 1 x 0.4 + 7 x 0.3

CCR/Datacloud
5.1 FTE distribuite su 19 persone

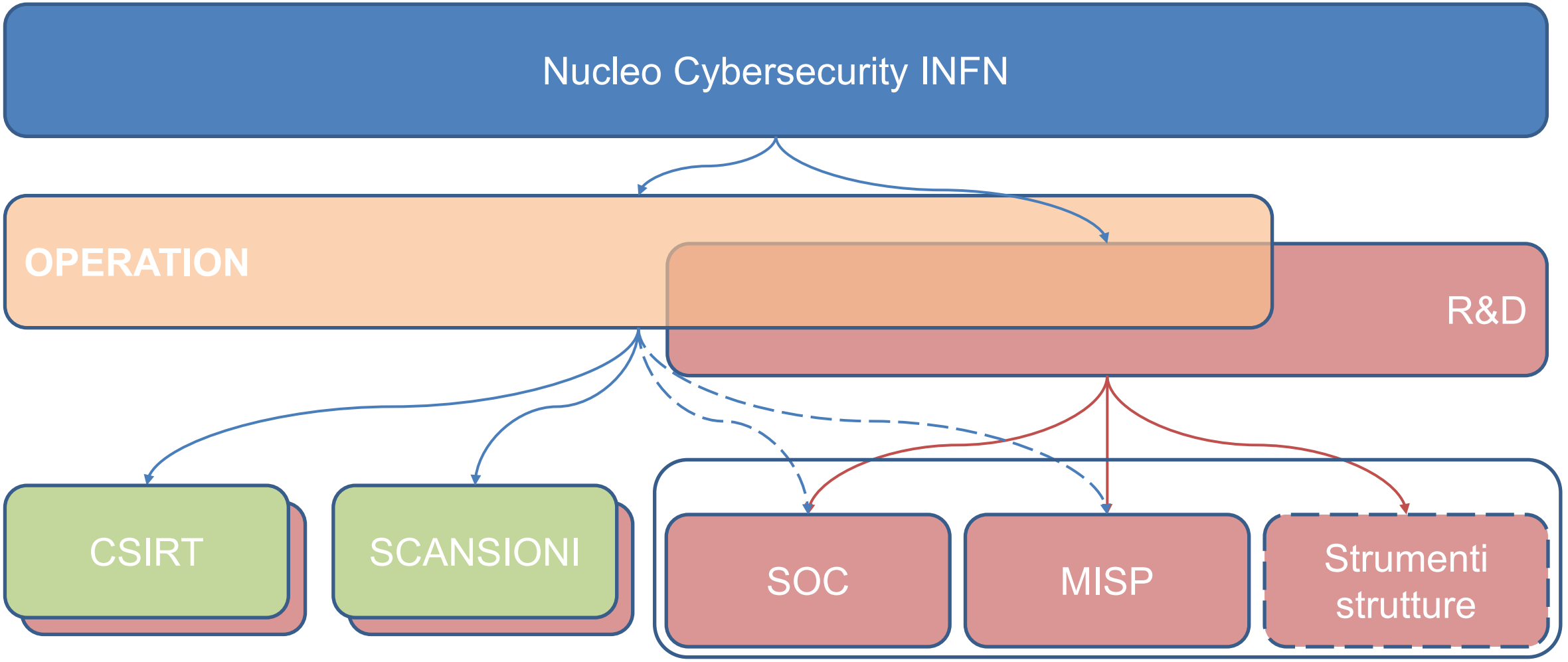
PNRR
4 FTE *dedicate*

9.1 FTE
ragionevole considerando WP7

Ipotesi di lavoro

- **0.4 FTE coordinatori**
- **0.3 FTE partecipazione *minima***

Wrap up attività cybersecurity

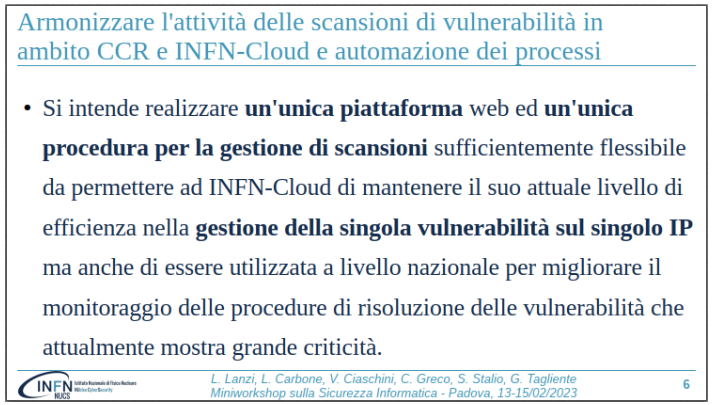


Proposta tempi

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

Scansioni

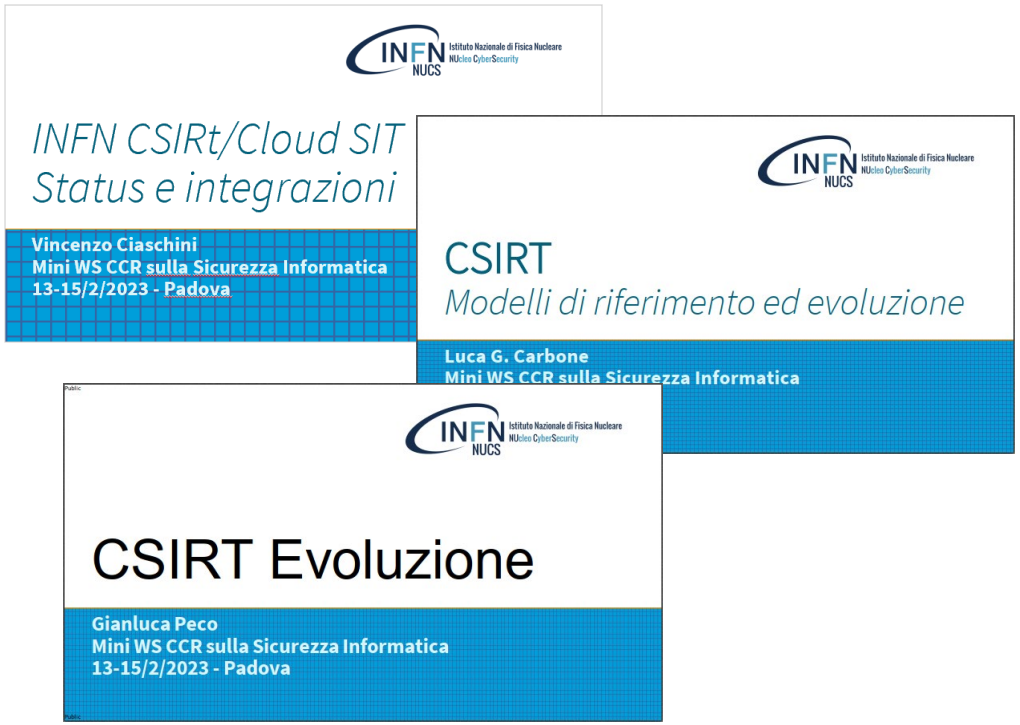
L. Lanzi, *L. Carbone*, V. Ciaschini, C. Greco, S. Stalio G. Tagliente

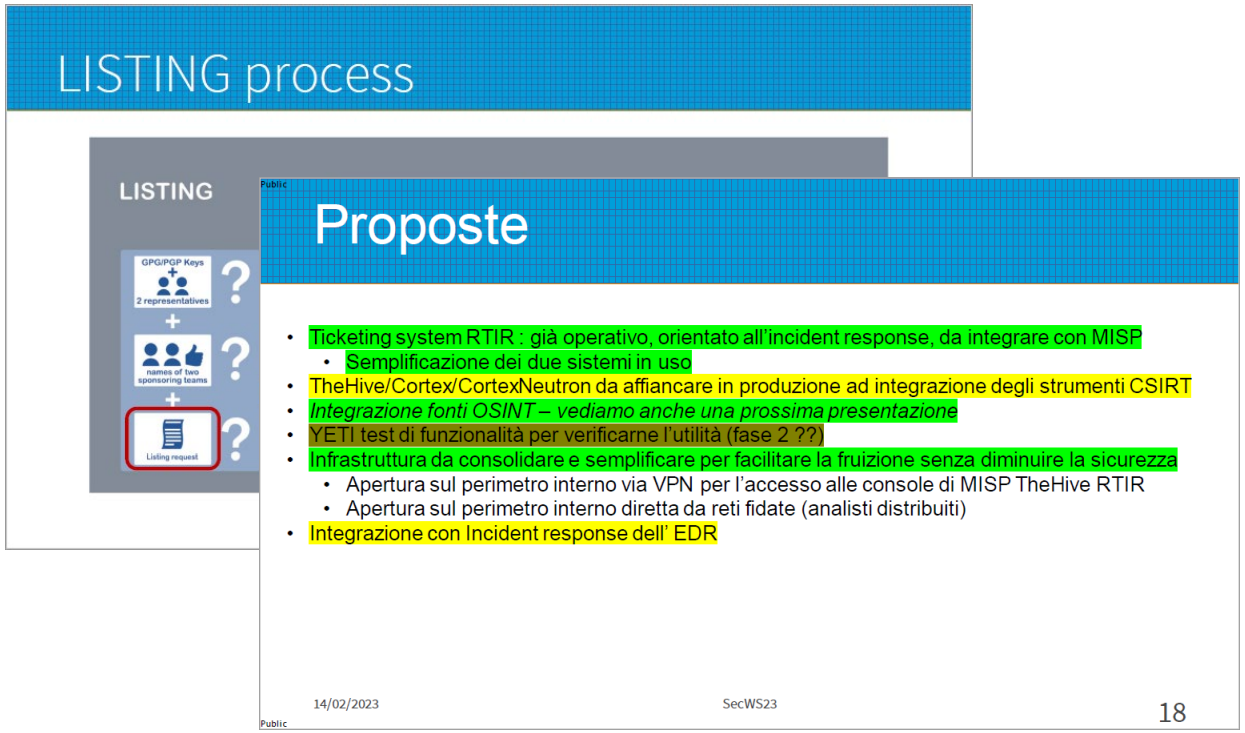


Realizzazione strumenti, scrittura policy, armonizzazione

CSIRT

L. Carbone, **V. Ciaschini**, S. Dal Pra, *[R&D: L. Lanzi],* G. Peco, V. Rega ,V. Spinoso, *S. Stalio*





Manpower sotto soglia critica

Evoluzione strumenti, scrittura documentazione (processi, policy), entro l'anno **TI listed member**

R&D: SOC

G. Peco, F. Amori, S. Barberis, L. Carbone, V. Ciaschini, S. Dal Pra, A. De Salvo, L. Lanzi, V. Spinoso, P. Veronesi, F. Zani

R&D: SOC

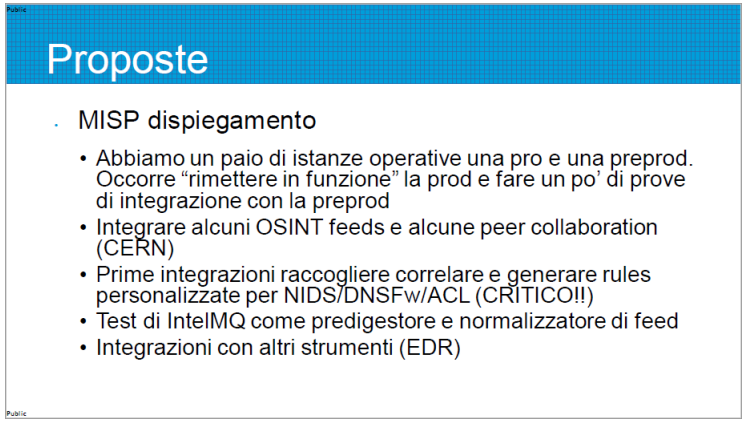
G. Peco, F. Amori, S. Barberis, L. Carbone, V. Ciaschini, S. Dal Pra, A. De Salvo, L. Lanzi, V. Spinoso, P. Veronesi, F. Zani

Gruppo molto nutrito

Possibile impostare da subito attività produttiva su wazuh: realizzazione infrastruttura, studio/disegno struttura logica nazionale, analisi altri tool, … - da sfruttare senz'altro contatti al CERN con WLCG SOC group collaborazione con giovani R. Alfieri;

R&D: MISP

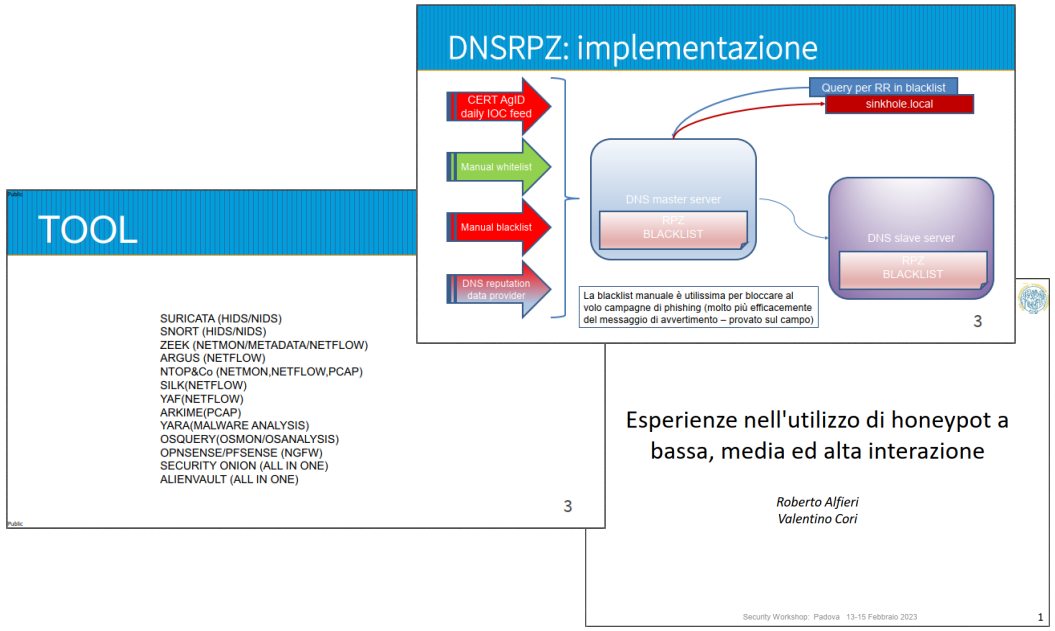
MISP: S. Barberis, L. Carbone, V. Ciaschini, S. Dal Pra, G. Peco, G. Siroli, F. Zani



Le due istanze MISP attualmente in funzione (o quasi) vanno rese operative, e (ri)attivato il feed sharing con il CERN; vanno esplorati altri strumenti di OSINT - TI

R&D: Strumenti

Gruppo non definito – alcune attività in collaborazione con netgroup



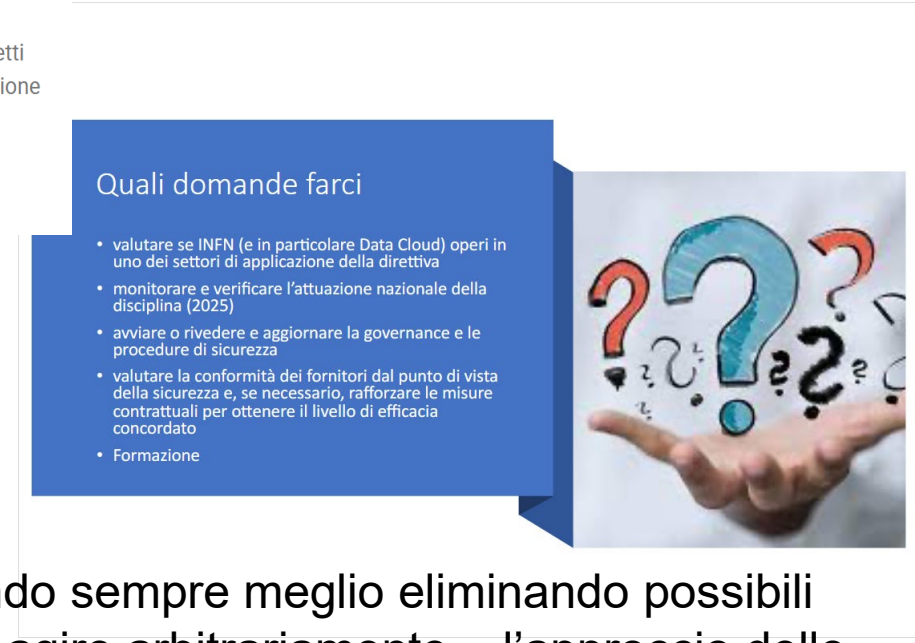
Tool da implementare (DNS RPZ) o da studiare/provare per attività necessarie di raccolta/analisi dati, prevenzione/protezione attacchi.

Quadro Normativo

La nuova disciplina europea sulla cyber security: aspetti tecnico-giuridici a confronto. 45m

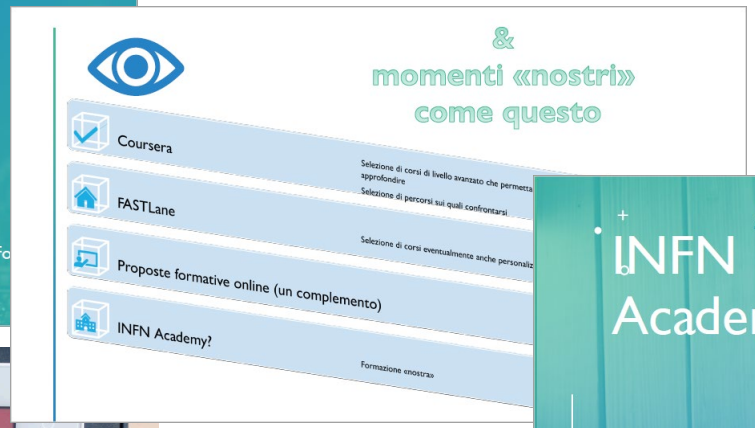
L'intervento mira ad analizzare i principi e la disciplina introdotta dal nuovo quadro giuridico europeo in materia di cyber security, ed in particolare la Direttiva NIS 2 relativa a misure per un livello comune ed elevato di cibersicurezza nell'Unione, la direttiva 2022/2557 relativa alla resilienza dei soggetti critici, nonché il Regolamento (UE) 2019/881 del 17 Aprile 2019 relativo all'ENISA, l'Agenzia dell'Unione europea per la cibersicurezza e alla certificazione della cibersicurezza per le tecnologie dell'informazione e della comunicazione.
L'analisi delle innovazioni normative sarà affrontata anche in virtù delle ricadute pratiche nei contesti dei servizi informatici di interesse dell'INFN.

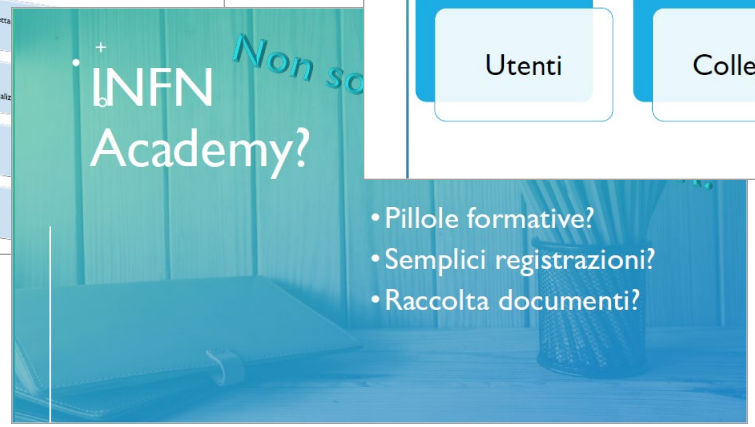
Speakers: Barbara Martelli (Istituto Nazionale di Fisica Nucleare) , Nadina Foggetti (Istituto Nazionale di Fisica Nucleare)

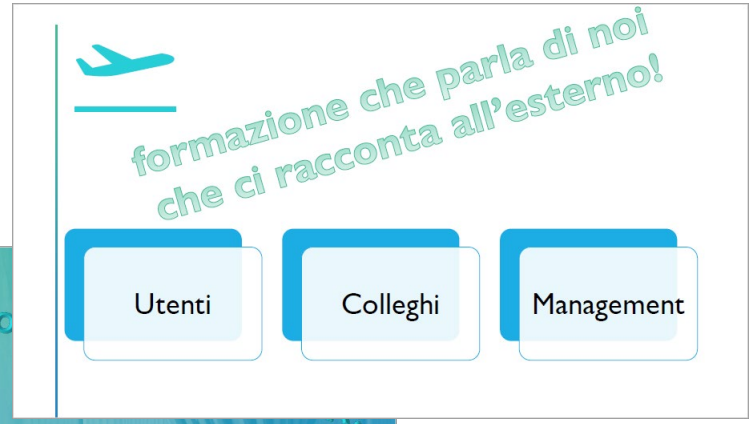


Sintesi velocissima: con NIS2 il quadro normativo si sta precisando sempre meglio eliminando possibili equivoci e sottraendo in qualche misura agli stati la possibilità di agire arbitrariamente – l'approccio delle certificazioni va lentamente (ma stabilmente) riverberandosi su tutte le attività di cybersecurity. NIS2 probabilmente imporrà di rivedere il nostro approccio alla classificazione delle macchine (GA vs TS), di ragionare sulle infrastrutture critiche e sull'utilizzo del S/W open, di adottare alcune pratiche obbligatorie in ambiti certificati anche in ambiti che non lo sono (vedi BC).

Formazione







Formazione continua come pilastro fondamentale della cybersecurity: il fattore umano continua a essere l'anello debole della catena.

Conclusioni

Grazie a:

- organizzazione: **Rossana Chiaratti**, Patrizia Belluomo, Vincenzo Ciaschini, Leandro Lanzi, Michele Michelotto, Gianluca Peco
- oratori
- **partecipanti: tanti e molto coinvolti**