

NUCS

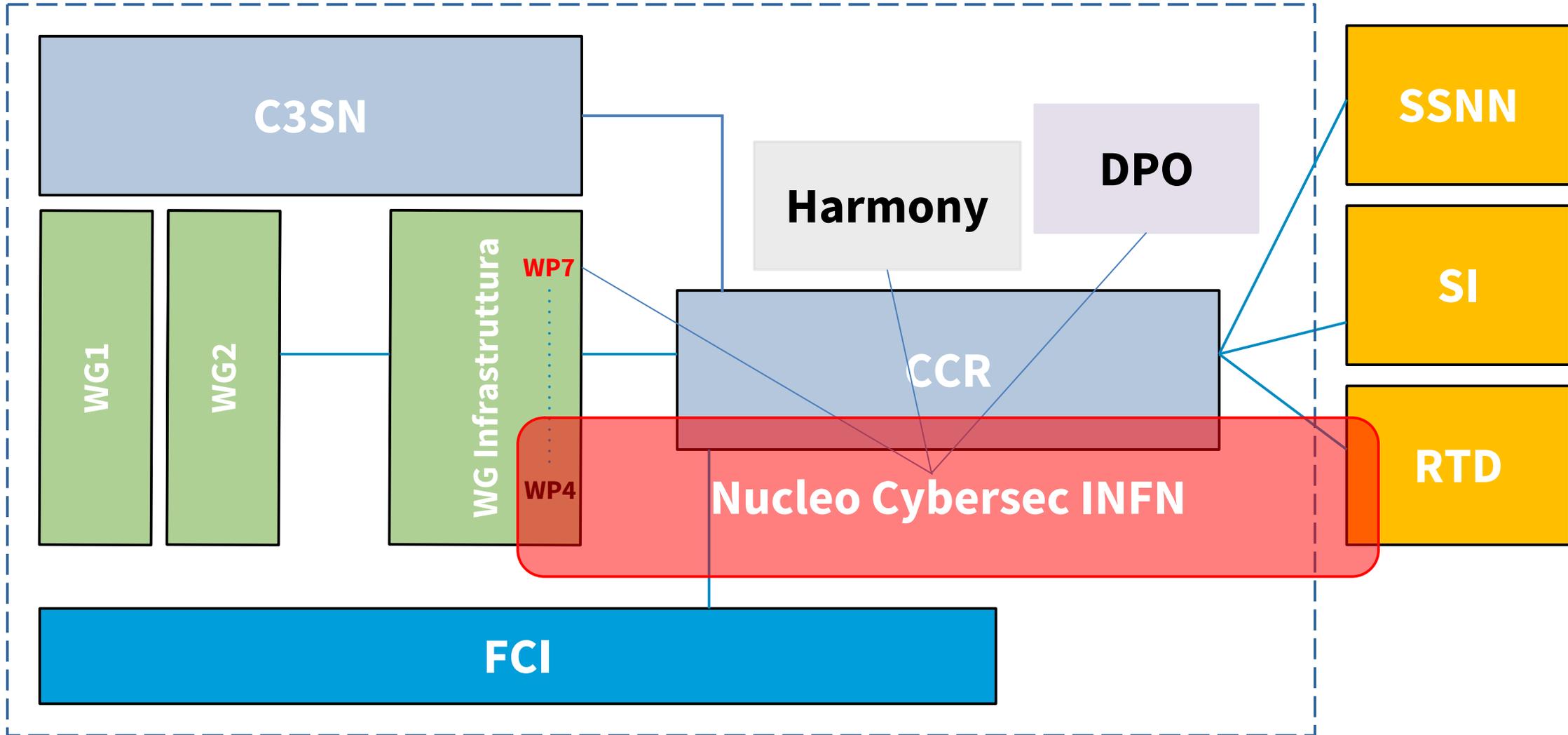
Great expectations

Jack Tamigi

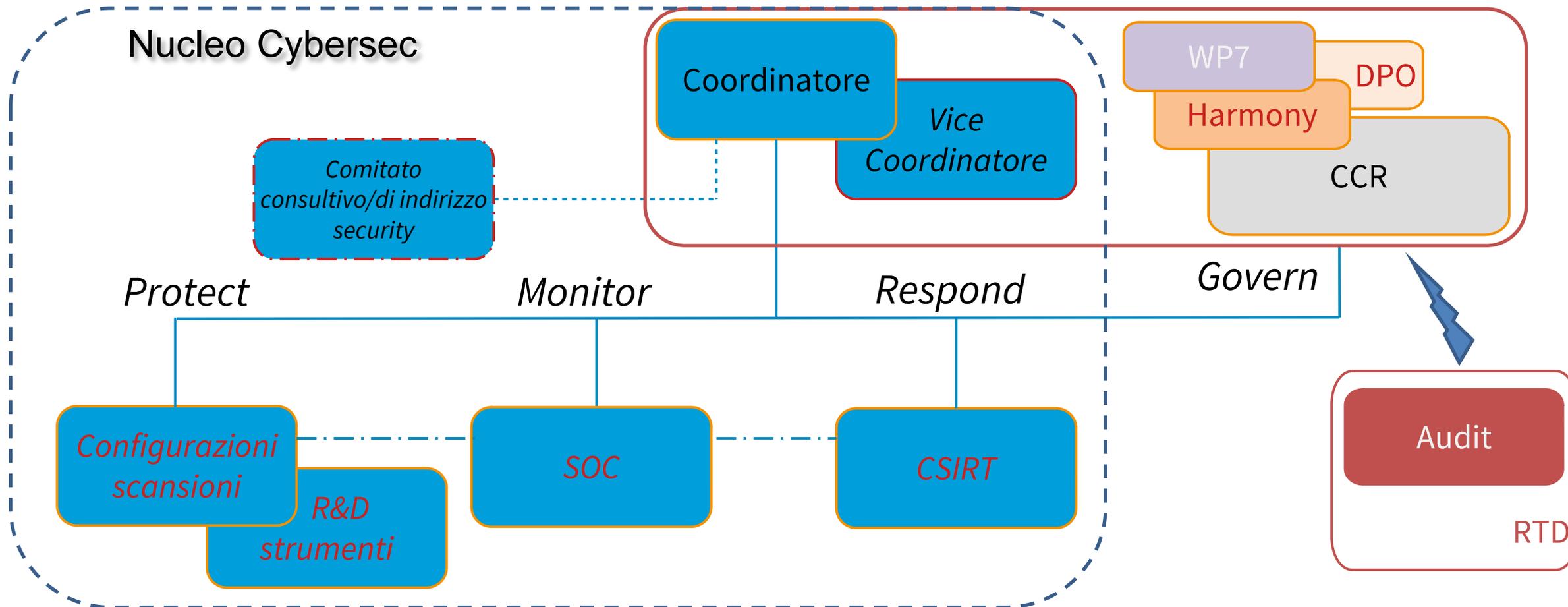
Mini WS CCR sulla Sicurezza Informatica

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 $\cong 2 \times 0.4 + 4 \times 0.3$

SCANSIONI

1.6 FTE $\cong 1 \times 0.4 + 4 \times 0.3$

SOC & MISP (mainly R&D)

2.5 FTE $\cong 1 \times 0.4 + 7 \times 0.3$

CCR/Datacloud

5.1 FTE distribuite su 19 persone

PNRR

4 FTE *dedicate*

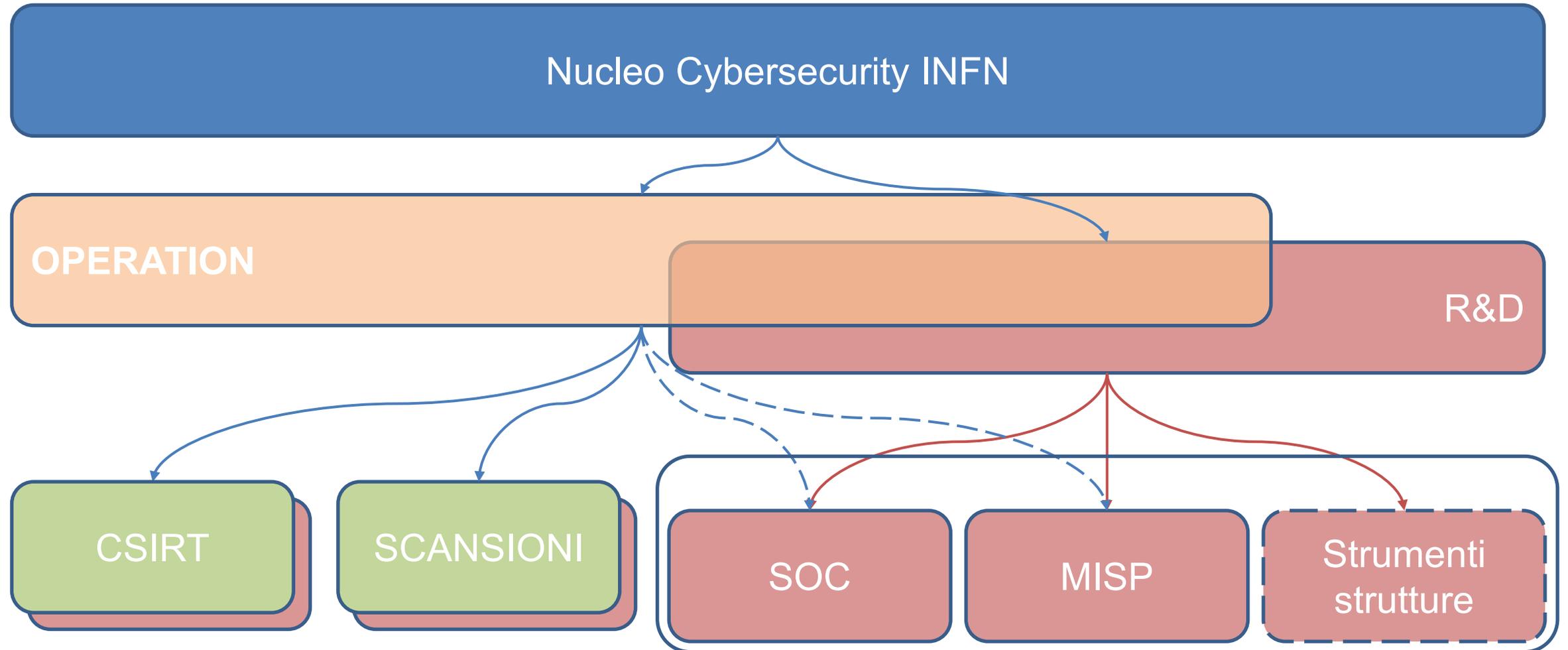
9.1 FTE

*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

INFN Istituto Nazionale di Fisica Nucleare
NUCS NUCleo CyberSecurity

Scansioni di vulnerabilità in ambito CCR

Leandro Lanzi

Miniworkshop sulla Sicurezza Informatica
(Padova, 13-15 febbraio 2023)

INFN Istituto Nazionale di Fisica Nucleare
NUCS NUCleo CyberSecurity

Scansioni di vulnerabilità

Gruppo scansioni del NUCleo di CyberSecurity dell'INFN
L. Lanzi, L. Carbone, V. Ciaschini, C. Greco, S. Stalio, G. Tagliente

Miniworkshop sulla Sicurezza Informatica
(Padova, 13-15 febbraio 2023)

INFN
CLOUD

Scansioni di sicurezza
in INFN Cloud

Stefano Stalio

Miniworkshop sulla Sicurezza Informatica - Padova, 13-15 Febbraio 2023

Armonizzare l'attività delle scansioni di vulnerabilità in ambito CCR e INFN-Cloud e automazione dei processi

- Si intende realizzare **un'unica piattaforma** web ed **un'unica procedura per la gestione di scansioni** sufficientemente flessibile da permettere ad INFN-Cloud di mantenere il suo attuale livello di efficienza nella **gestione della singola vulnerabilità sul singolo IP** ma anche di essere utilizzata a livello nazionale per migliorare il monitoraggio delle procedure di risoluzione delle vulnerabilità che attualmente mostra grande criticità.

INFN NUCS
L. Lanzi, L. Carbone, V. Ciaschini, C. Greco, S. Stalio, G. Tagliente
Miniworkshop sulla Sicurezza Informatica - Padova, 13-15/02/2023

6

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

INFN NUCS Istituto Nazionale di Fisica Nucleare
NUCS CyberSecurity

*INFN CSIRT/Cloud SIT
Status e integrazioni*

Vincenzo Ciaschini
Mini WS CCR sulla Sicurezza Informatica
13-15/2/2023 - Padova

INFN NUCS Istituto Nazionale di Fisica Nucleare
NUCS CyberSecurity

CSIRT
Modelli di riferimento ed evoluzione

Luca G. Carbone
Mini WS CCR sulla Sicurezza Informatica

INFN NUCS Istituto Nazionale di Fisica Nucleare
NUCS CyberSecurity

CSIRT Evoluzione

Gianluca Peco
Mini WS CCR sulla Sicurezza Informatica
13-15/2/2023 - Padova

LISTING process

Proposte

- Ticketing system RTIR : già operativo, orientato all'incident response, da integrare con MISP
 - Semplificazione dei due sistemi in uso
- TheHive/Cortex/CortexNeutron da affiancare in produzione ad integrazione degli strumenti CSIRT
- Integrazione fonti OSINT – vediamo anche una prossima presentazione
- YETI test di funzionalità per verificarne l'utilità (fase 2 ??)
- Infrastruttura da consolidare e semplificare per facilitare la fruizione senza diminuire la sicurezza
 - Apertura sul perimetro interno via VPN per l'accesso alle console di MISP TheHive RTIR
 - Apertura sul perimetro interno diretta da reti fidate (analisti distribuiti)
- Integrazione con Incident response dell' EDR

14/02/2023 SecWS23

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



INFN Istituto Nazionale di Fisica Nucleare
NUCS Nuclear CyberSecurity

SOC Foundation

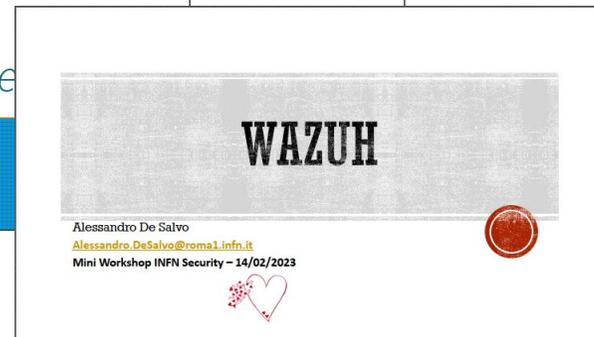
Gianluca Peco
Mini WS CCR sulla Sicurezza Informatica
13-15/2/2023 - Padova



INFN Istituto Nazionale di Fisica Nucleare
NUCS Nuclear CyberSecurity

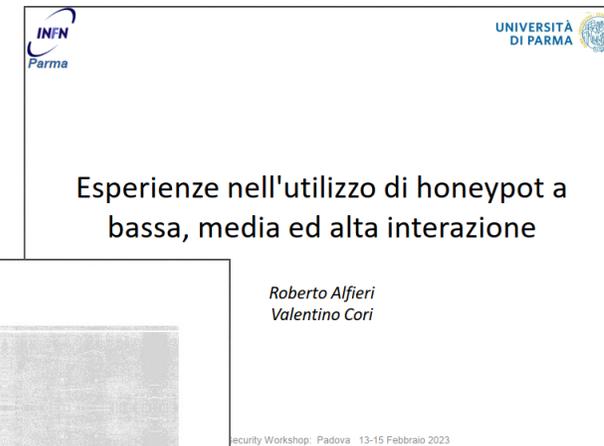
wazuh - prime esperienze

Luca G. Carbone
Mini WS CCR sulla Sicurezza Informatica
13-15/2/2023 - Padova



WAZUH

Alessandro De Salvo
Alessandro.DeSalvo@roma1.infn.it
Mini Workshop INFN Security - 14/02/2023



INFN Parma

UNIVERSITÀ DI PARMA

Esperienze nell'utilizzo di honeypot a bassa, media ed alta interazione

Roberto Alfieri
Valentino Cori

Security Workshop - Padova - 13-15 Febbraio 2023

1

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: infrastruttura, piano attività

- Scelta del modello (distribuito, centralizzato, federato)
- Scelta delle sonde (Log, Host, Rete, FW, App)
- Scelta degli strumenti (SIEM, SOAR)
- Implementazione prototipo piattaforma (😊)

14/02/2023

SecWS23

8

R&D: infrastruttura, piano attività EDR

- Dispiegamento piattaforma EDR (Microsoft Security)
- Configurazioni console multisito
- Onboarding endpoint
- Integrazione con MISP
- Integrazione con CSIRT Tool
- Policy e Formazione

14/02/2023

SecWS23

84

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



Public

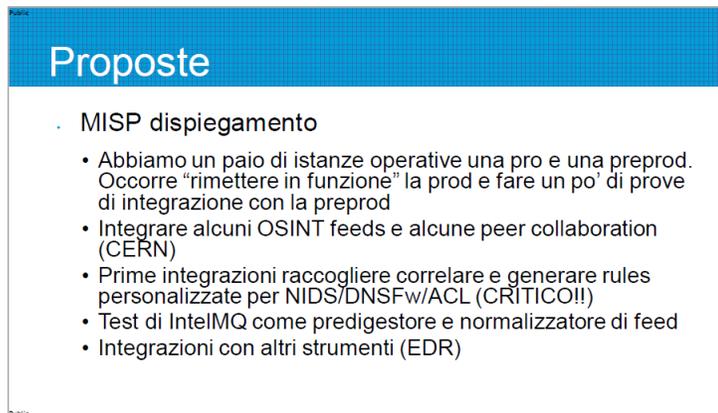
INFN Istituto Nazionale di Fisica Nucleare
NUCS Nuclear CyberSecurity

CTI & OSINT

Cyber Threat Intelligence & Open Source Intelligence

Gianluca Peco
Mini WS CCR sulla Sicurezza Informatica
13-15/2/2023 - Padova

Public



Proposte

- MISP dispiegamento
 - Abbiamo un paio di istanze operative una pro e una preprod. Occorre "rimettere in funzione" la prod e fare un po' di prove di integrazione con la preprod
 - Integrare alcuni OSINT feeds e alcune peer collaboration (CERN)
 - Prime integrazioni raccogliere correlare e generare rules personalizzate per NIDS/DNSFw/ACL (CRITICO!!)
 - Test di IntelMQ come predigestore e normalizzatore di feed
 - Integrazioni con altri strumenti (EDR)

Public

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

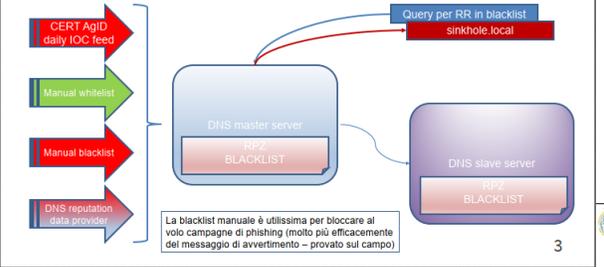

Strumenti per le strutture
Gianluca Peco
Mini WS CCR sulla Sicurezza Informatica
13-15/2/2023 - Padova


Strumenti per le strutture
Luca G. Carbone
Mini WS CCR sulla Sicurezza Informatica
13-15/2/2023 - Padova

TOOL

- SURICATA (HIDS/NIDS)
- SNORT (HIDS/NIDS)
- ZEEK (NETMON/METADATA/NETFLOW)
- ARGUS (NETFLOW)
- NTOP&Co (NETMON,NETFLOW,PCAP)
- SILK(NETFLOW)
- YAF(NETFLOW)
- ARKIME(PCAP)
- YARA(MALWARE ANALYSIS)
- OSQUERY(OSMON/OSANALYSIS)
- OPENSENSE/PFSENSE (NGFW)
- SECURITY ONION (ALL IN ONE)
- ALIENVAULT (ALL IN ONE)

DNSRPZ: implementazione



Query per RR in blacklist
sinkhole local

La blacklist manuale è utilissima per bloccare al volo campagne di phishing (molto più efficacemente del messaggio di avvertimento – provato sul campo)

Esperienze nell'utilizzo di honeypot a bassa, media ed alta interazione

Roberto Alfieri
Valentino Cori

Security Workshop: Padova 13-15 Febbraio 2023

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 cibersecurity 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 cibersecurity e alla certificazione della cibersecurity 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)

Quali domande farci

- valutare se INFN (e in particolare Data Cloud) operi in uno dei settori di applicazione della direttiva
- monitorare e verificare l'attuazione nazionale della disciplina (2025)
- avviare o rivedere e aggiornare la governance e le procedure di sicurezza
- valutare la conformità dei fornitori dal punto di vista della sicurezza e, se necessario, rafforzare le misure contrattuali per ottenere il livello di efficacia concordato
- Formazione



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

PROPOSTA DI PIANO FORMATIVO CYBERSECURITY

Silvia Arezzini

- Gruppo CCR_ formazione
- Gruppo e-learning Ufficio F...

MINWORKSHOP security
Padova, 15 febbraio 2023

&
momenti «nostri»
come questo

- ✓ Coursera
Selezione di corsi di livello avanzato che permetta approfondire
- FASTLane
Selezione di percorsi sui quali confrontarsi
- Proposte formative online (un complemento)
Selezione di corsi eventualmente anche personalizzati
- INFN Academy?
Formazione «nostra»

formazione che parla di noi
che ci racconta all'esterno!

Utenti Colleghi Management

Non so
+ INFN Academy?

- Pillole formative?
- Semplici registrazioni?
- Raccolta documenti?



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**