Security INFN
Der Stand der Dinge

Luca G. Carbone

Mini WS CCR sulla Sicurezza Informatica

13-15/2/2023 – Padova

Le puntate precedenti

Proposte organizzative

Security

Riunione CCR
Tor Vergata, settembre 2021
Luca G. Carbone

INFN SEC

Cybersecurity

Luca Carbone
Riunione CCR 11-13/4/2022 - LNF

INFN SEC

Cybersecurity

Luca G. Carbone
Riunione C3SN/CCR 28-30/9/2022 – Castel Gandolfo

INFN

Datacloud WP4
Security

Datacloud WG kick-off meeting
Luca G. Carbone e Vincenzo Ciaschini

INFN SEC

Cybersecurity Framework

Luca G. Carbone
Tutorial Days CCR 10-12/10/2022 – LNF

Proposta INFN CSIRT

Proposta di istituzione del
INFN-CERT

Vincenzo Ciaschini
Riccardo Veraldi

Jun/Sep 2019

Evento formativo

Il punto di partenza

INFN-CERT: servizi erogati ?

- **Alerts e warning**
- Gestione incidenti
  - Analisi incidenti
  - **Risposta agli incidenti, supporto e coordinamento**
  - Risposta agli incidenti con supporto on-site
  - **E' auspicabile una stretta collaborazione con il gruppo Harmony INFN e soprattutto con l'ufficio Legale INFN possibile rilevanza penale**
- Gestione Vulnerabilità
- Security audit/assestment (su richiesta)
- Configurazioni, mantenimento della sicurezza informatica
- Sviluppo di security tools
- Servizi di intrusion detection
- Analisi forense dei dati relativi a incidenti informatici (chiavi di registro,
- Analisi del rischio
- Business continuity-disaster recovery
- **Security consulting**
- **Awareness building**
- **Corsi di formazione**
- Valutazione dei prodotti

manpower

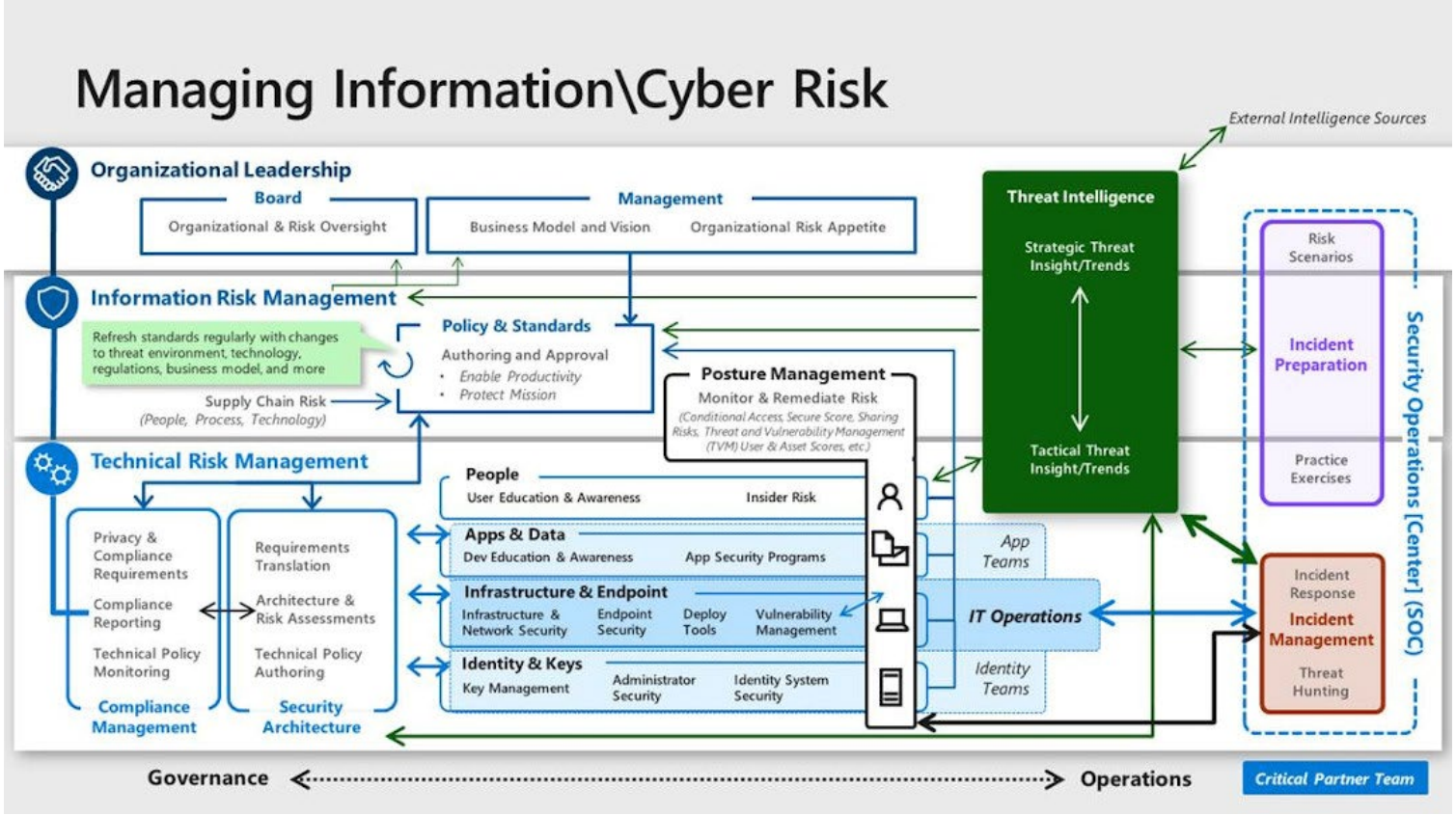
Staff: linee guida

- Per fornire 2 servizi principali (fra quelli elencati) almeno 4 persone ad es:
  - Distribuzione delle security advisory
  - Gestione incidenti
- Per organizzare uno CSIRT FULL SERVICE che risponde in orari di ufficio: da 6 a 8 FTE
- CSIRT FULL SERVICE 24/7: 12 FTE

Ciaschini, Veraldi: Proposta di istituzione del INFN CERT, 2019

Bonus: Microsoft - how to organise your security team

The following functions represent a **fully populated enterprise security team**, which may be ***aspirational*** for some organizations. Organizations often need to ***prioritize*** where to invest first based on their risk profile, ***available resources***, and needs.



PRIORITIZE: from Key Sixteen…

The *Key Sixteen* (DayBlink, 2019)

… 16 key functions that the most successful and established organizations had in common

- **Blue team**
- **Cyber Crime**
- **IAM**
- **Incident Response**
- **Legal**
- **Log management**
- **Network Security**
- **Project Management**
- **Red team**
- **Risk Management**
- **Security & Compliance**
- **Security Architecture**
- **Software Development**
- **System Administration**
- **Threat Intelligence**
- **Vulnerability Management & Remediation**

CSIRT/CERT

A priori nessuna delle attività evidenziate in rosso è trascurabile (alcune sono obbligatorie) – il modello di supporto volontario minaccia di non garantire attività sistematica e prevedibile, e va aggiornato/integrato; la proposta deve essere sostenibile.

. . . to The Key Four

(*distillato* delle K16 abbastanza generale da poter essere mappato su qualsiasi cybersecurity framework)

- **PROTECT**: shield, defend, prevent
  - scansioni, configurazioni sistemi e apparecchiature di rete, controlli d'accesso, coordinamento, requisiti applicazioni e servizi, EDR/XDR, …
- **MONITOR**: detect, hunt
  - **SOC**: selezione/raccolta/analisi dati, realizzazione e gestione infrastruttura, threat intelligence/management, vulnerability management, ...
- **RESPOND**: recover, sustain
  - **CSIRT**: incident response ; BC, DR (backup sezioni: infrastruttura e strategia), …
- **GOVERN**: manage, comply, educate, manage risk
  - organizzazione, interazione con il management, policy, framework, allocazione risorse, valutazione obbiettivi e risultati, cybersecurity awareness, formazione, risk assessment, compliance, ...

Dove *eravamo*

- **PROTECT**
  - WG Security [~2.5 FTE] (in collaborazione non sempre coordinate ed efficiente con AAI, DSI, SSNN, NetGroup, ...): scansioni, elaborazione policy e configurazioni, R&D
- **MONITOR**
  - CSIRT
  - WG Security
- **RESPOND**
  - CSIRT
- **GOVERN**
  - CCR discute e ratifica proposte ed elaborazioni da WG Security, Audit, Harmony, DPO, … (intrecciati più o meno inestricabilmente)

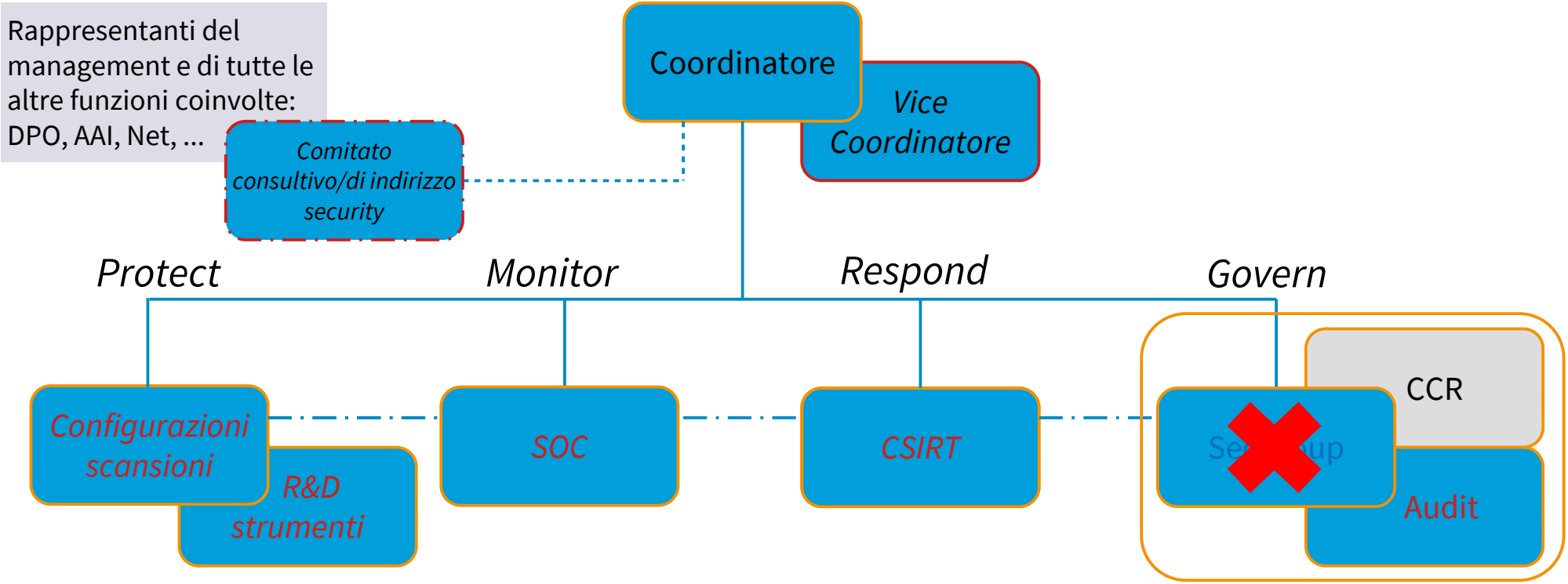
La proposta: WG funzionali

- **PROTECT**
  - **Configurazioni e scansioni**
  - **R&D e strumenti**
- **MONITOR**
  - **SOC** (infrastruttura e operazioni – semidistribuito per natura)
- **RESPOND**
  - **CSIRT** (distribuito)
- **GOVERN** (allocazione di un budget ed eventuale istituzione di un gruppo di referee?)
  - ***SecGroup*, CCR, ...**
  - **Audit**

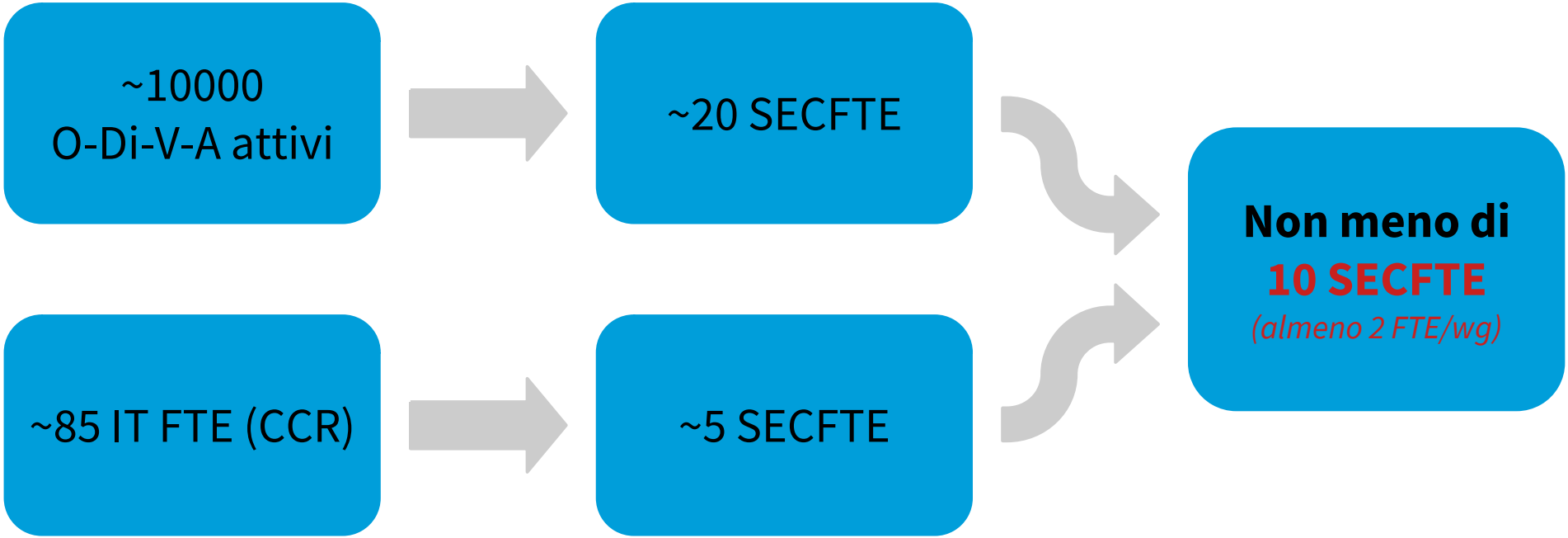
Funzioni che richiedono un coordinatore

(e, sperabilmente, personale da coordinare)

Organigramma



Stime per INFN



Dettaglio FTE per funzione

Configurazioni Scansioni 2

R&D Strumenti 2

Protect: 4-2 (accorpando le funzioni)

Processi critici che necessitano di continuità operativa (idealmente 24/7) o ***automazione estrema***

SOC 2

Monitor: 2-3

CSIRT 2

Respond: 2-3

Audit 2

Govern: 2

Aggregated View		
Information Security Function	**Prevalence**	
Security Operations	25-30%	**45-55%**
Threat Investigation / Intelligence	20-25%	
Security Risk Management (incl. Compliance)	15-20%	**15-20%**
Network Security	6-12%	**15-30%**
Security Architecture	4-5%	
Vulnerability Management	2-6%	
Software Development / Engineering	1-5%	
Enterprise Security	1-3%	
Project Management Office	0-5%	
Offensive Engineering	0-1%	

Roadmap

Settembre: definita troppo conservativa, ma ovviamente tutto dipende da manpower

- **2022**
  - *definizione cybersecurity framework (CSFW)*
  - definizione struttura, personale, responsabilità/armonizzazione con il CSFW scelto
  - definizione strumenti SOC & CSIRT
- **2023**
  - dispiegamento struttura gestione, coordinamento e intervento
  - adozione CSFW in strutture pilota;
  - realizzazione nucleo pilota SOC (infrastruttura raccolta/analisi dati)
- **2024**
  - SOC in produzione per tutte le strutture, adozione strumenti di threat intelligence
  - CSFW in tutte le strutture

Da definire: metriche o indicatori risultati raggiunti/obbiettivi realizzati

Piano triennale per la Transizione Digitale (delibera 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

Sec Group

SOC

Cybersecurity framework

Come si fa cybersecurity oggi?
NIST CSF – CyberSecurity Framework

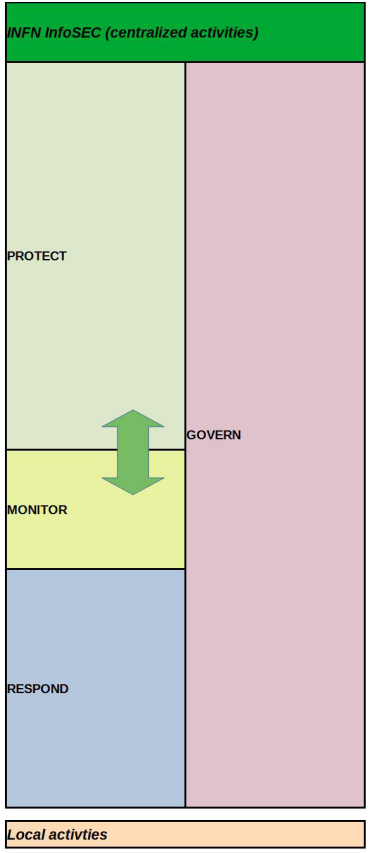
Le 5 funzioni/attività fondamentali da implementare:

- **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

I vantaggi della centralizzazione

Framework	
Function	**Category**
IDENTIFY	Asset Management
	Business Environment
	Governance
	Risk Assessment
	Risk Management Strategy
	Supply Chain Risk Management
	Data Management
PROTECT	Identity Management, Auth. and Access Control
	Awareness and Training
	Data Security
	Information Protection Processes and Procedures
	Maintenance
	Protective Technology
DETECT	Anomalies and Events
	Security Continuous Monitoring
	Detection Processes
RESPOND	Response Planning
	Communications
	Analysis
	Mitigation
	Improvements
RECOVER	Recovery Planning
	Improvements
	Communications



- Replicare struttura e processi di analisi e gestione in > 25 strutture comporterebbe robuste inefficienze, costi alti e problemi di coordinamento;
- Visibilità globale su eventi di sicurezza: tempi di risposta inferiori, diminuita probabilità effetto domino;
- Sfruttamento e trasmissione competenze più efficienti

- Alcune attività puntuali andrebbero comunque svolte localmente nelle sezioni, ma secondo processi definiti e coordinati a livello centrale (asset management, risk assessment, data protection/backup, ...)

Questionario sulla CyberSecurity – un campione (Tutorial Days CCR, ottobre 2022)

Oct 2022

- **Utilizzate uno strumento per la rilevazione in tempo reale di attacchi informatici, intrusioni o - più semplicemente - per l'analisi sommaria del traffico di rete?**
  - *7/20 NO; le rimanenti sezioni usano F/W, **solo 2 usano strumenti specifici***
- **Utilizzate uno strumento (o una suite di strumenti) per la collezione centralizzata, la memorizzazione, l'analisi dei log di sistema e la correlazione di eventi security related?**
  - *Tutte le sezioni fanno log-collection, **nessuna fa analisi in real-time***
- **Vi servite di aggregatori di informazioni OSINT/indicatori di compromissione o di strumenti per la raccolta e l'analisi di informazioni OSINT sul vostro dominio? In caso affermativo siete in grado di utilizzare tempestivamente ed efficacememte gli IOC?**
  - ***18/20 NO, 2 in maniera non strutturata***

driving by the rear view mirror

- Facciamo molto, ma non tutto e in maniera disomogenea e poco organica;
- Le informazioni rilevanti rimangono confinate nelle strutture in cui gli eventi si verificano, e questa è una strategia sicuramente perdente;
- **Dispieghiamo praticamente solo strumenti reattivi** – alla luce del punto precedente è una scelta (probabilmente obbligata) particolarmente pericolosa;
- La proverbiale autonomia delle strutture in macanza di manpower adeguato rende assai problematico gestire produttivamente ed efficacemente, ciò che più importa, la sicurezza informatica dell'ente.

Datacloud kickoff: WP4 - Security

Oct 2022

- **Datacloud** ha bisogno di una infrastruttura/organizzazione di gestione della sicurezza informatica:
  - definizione politiche e regole, gestione attività operative, risposta agli incidenti, ripristino, rapporti con utenti ed enti esterni, etc…
- **INFN**, nelle cui sezioni e laboratori gran parte dell'infrastruttura sarà immersa, ha la medesima necessità.

Realizziamo un'infrastruttura di gestione (logica/fisica) unica che permetta di razionalizzare le attività e l'utilizzo delle risorse nel rispetto dei differenti contesti

- *Non abbiamo le risorse per gestire due infrastrutture distinte*
- *La segregazione (di attività e informazioni) non paga*

Gestione Cybersecurity

- Verranno implementate le 4 attività fondamentali (*distillate* dai framework standard) mediante:
  - realizzazione di un SOC/CSIRT;
  - definizione di politiche e procedure;
- Servirà:
  - adeguato manpower per R&D, realizzazione infrastruttura e gestione attività (almeno 8/5);
  - risorse per H/W, eventualmente S/W (licenze)

WP4 - operation

PROTECT
MONITOR

- Il SOC si farà carico di entrambe le funzioni
- Alcune attività operative tipiche di un SOC (gestione delle vulnerabilità, scansioni, definizione di configurazione standard, …) sono già svolte indipendentemente da INFN-Cloud e WG Security CCR: ***non ha senso avere implementazioni distinte (e scarsamente comunicanti)***
- C'è ancora tanto (*quasi tutto!*) da realizzare, in particolare per quanto riguarda:
  - **monitoring**
  - **automazione dell'analisi** *(fondamentale in caso di scarso manpower)*
  - **collegamento con fonti di intelligence**

RESPOND

Esistono lo CSIRT INFN e il SIT di INFN-Cloud:

- Compiti molto simili
- Infrastruttura per la gran parte duplicate: hanno sistemi di mailing cifrati praticamente identici e identici sistemi di ticketing

Target perfetto per la razionalizzazione

- Probabili aggiornamento e revisione degli strumenti
- Necessario almeno uno tra:
  - Partecipazione attiva di un rappresentante per ogni T2 (preferibile…);
  - Accesso ai nodi del T2

WP4 – governance & policy

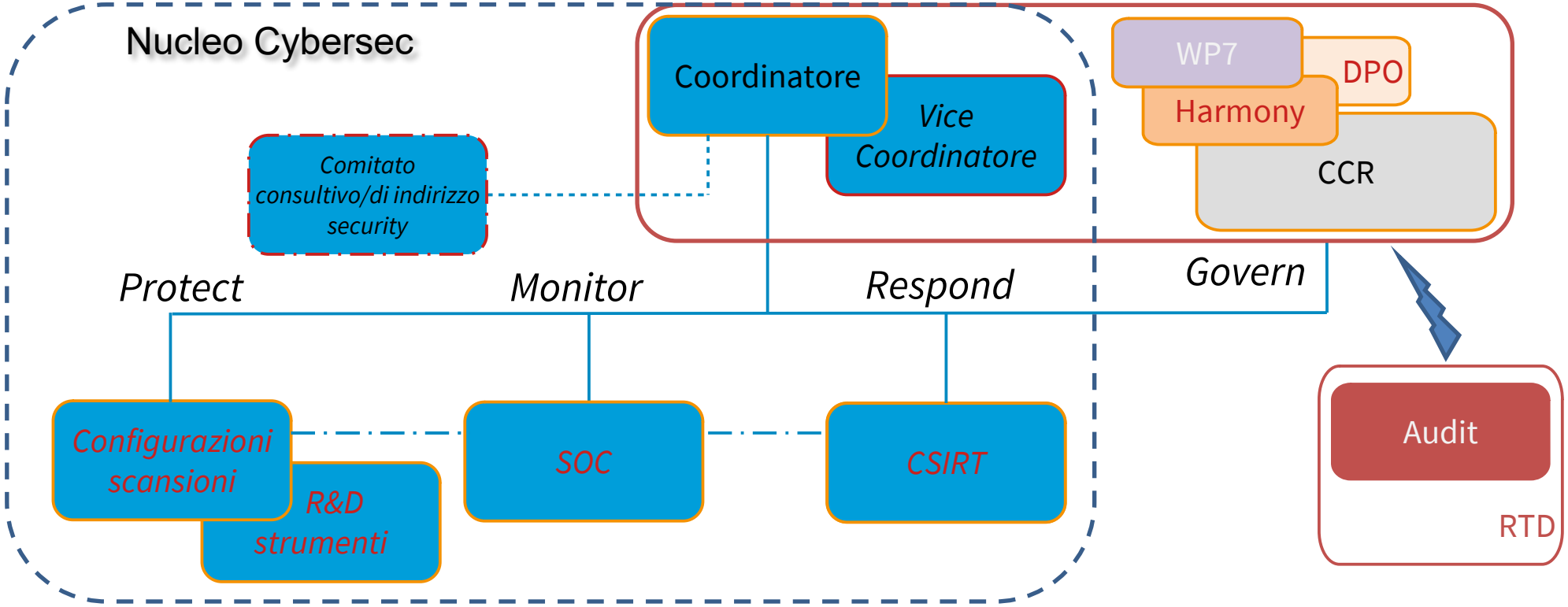
GOVERN

- Il punto di partenza saranno le policy elaborate da WP4 di INFN CLOUD
- L'attività verrà svolta:
  - in collaborazione - molto stretta, per evidenti motivi, per quanto riguarda l'attività di elaborazione delle policy e dell'architettura normativa - con il WP7 (Sistemi integrati di gestione, legal compliance), con il DPO e il Gruppo Harmony di CCR (con cui andranno istituiti canali di comunicazione e coordinamento efficienti);
  - In coordinamento con il WP1 per ciò che attiene alle attività più strettamente operative e in generale con tutti gli altri WP per le aree di loro competenza
- Andranno isituzionalizzati canali di comunicazione con EGI CSIRT

WP4 – tempi e manpower

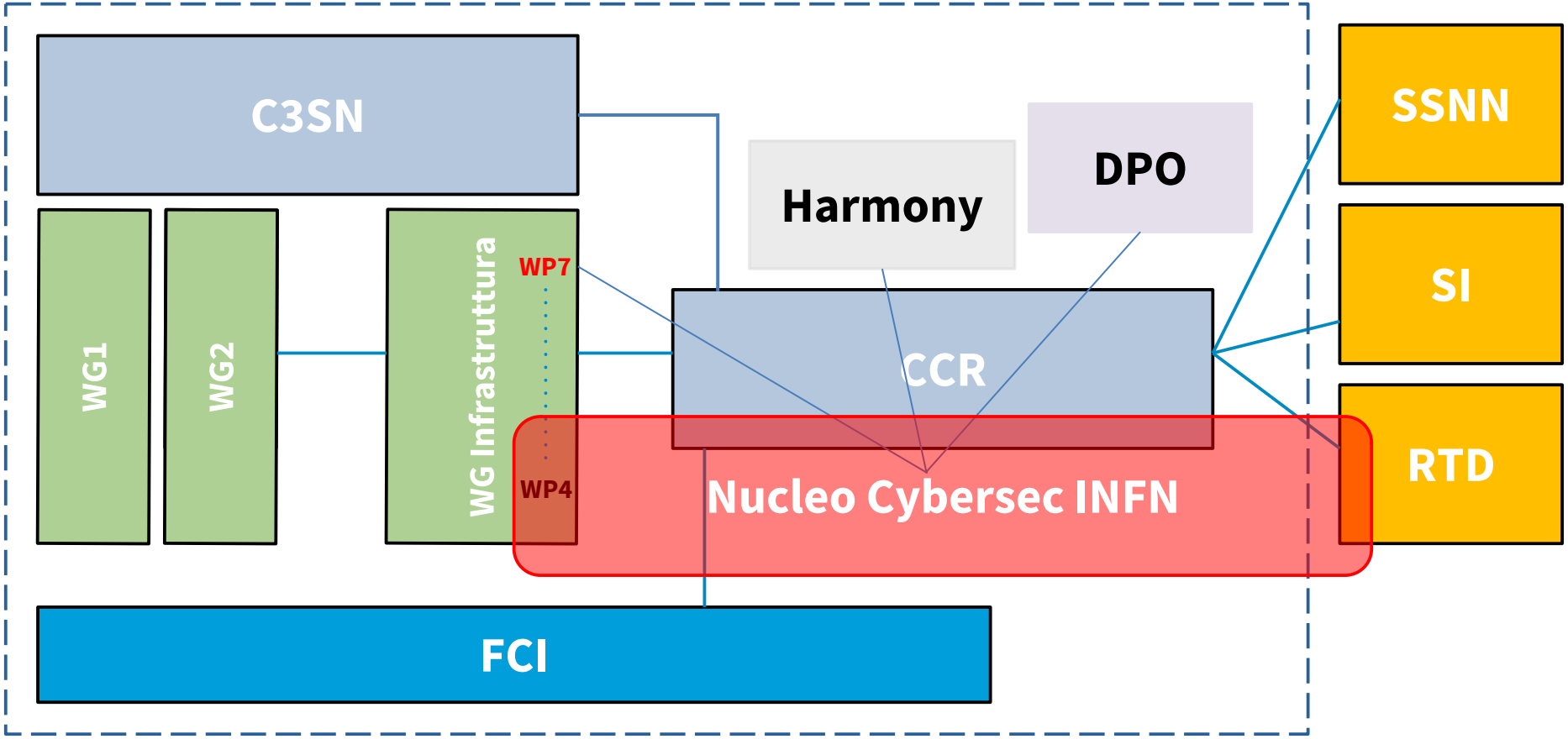
- Con *almeno* 10 persone sarebbe possibile realizzare un prototipo funzionante di SOC entro la fine del 2023:
  - Alcune persone già impegnate nel WG Security di CCR hanno dato la loro disponibilità di massima a partecipare all'attività del WP
  - *Possiamo ragionevolmente attenderne ~4 da assunzioni PNRR?*
  - Con meno persone (rispetto alle 10) o si taglieranno parti importanti del piano o si allungheranno i tempi; in generale non sarà semplice erogare servizi adeguati alle necessità

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.

The Big Picture



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***

SOC – MONITOR (NIST: PROTECT DETECT)
CSIRT – RESPOND (NIST: RESPOND)

- **SOC** (by SANS): A combination of **people**, **processes** and **technology** protecting the information systems of an organization through proactive design and configuration, ongoing monitoring of system state, detection of unintended actions of undesiderable state, and minimizing damage from unwanted effects. CSIRT is a reactive approach to security, responding to incidents after they have occurred. *SOC is a **proactive approach** to security, monitoring for potential events and responding before they can have an impact.*
- **CSIRT** (by ENISA, FIRST.org): a generic term for a team that provides a set fo services: information and cybersecurity incident handling (code service), security monitoring, vulnerability management, situational awareness and cybersecurity knowledge management. *CSIRT is a **reactive approach** to security, responding to incidents after they have occurred.*
- *(…) SOC is the first line, they receive all alerts, where CSIRT would only receive escalated alerts*

CSIRT

- **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;
    - gestione segnalazioni da fonti aperte/istituzionali (shadowserver, CERT AgID, CSIRT Italia, US-CERT/CISA …): raccolta informazioni, valutazione pertinenza e rischio, eventuale inoltro segnalazioni ai responsabili locali;
    - gestione ticket aperti;
    - consulenza;
  - *emergenza*:
    - gestione incidenti (insieme a tutto il team) in collaborazione/coordinamento con il servizio calcolo coinvolto (personale CSIRT non agisce direttamente su sistemi compromessi)

CSIRT evoluzione

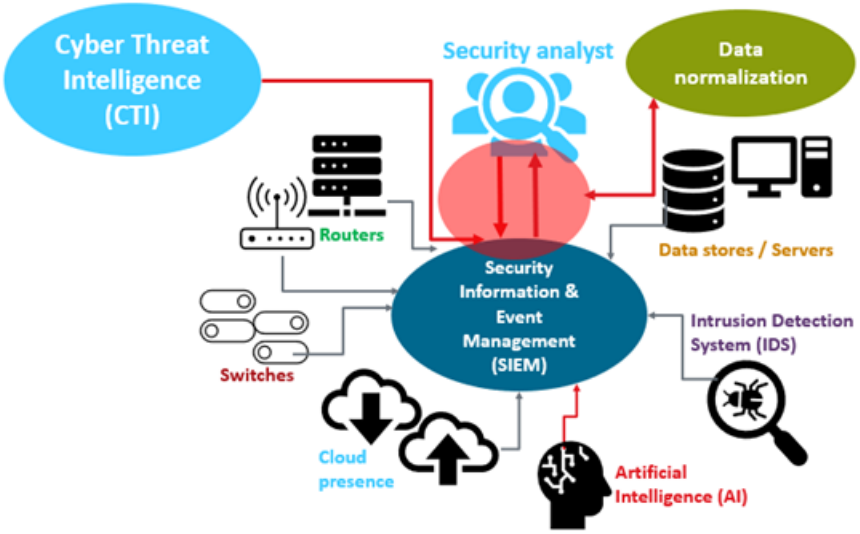
- **infrastruttura**
  - basata su infrastruttura di virtualizzazione ridondata dei SSNN, richiede aggiornamento:
    - sistema di ticket tracking (da agganciare a strumenti OSINT – open source intelligence);
    - server di posta sicuro (ora basato su BSD, di difficile gestione – collaborazione in corso con Gruppo Mailing);
- **processi**
  - gestione automatizzata segnalazioni servizi esposti da shadowserver (creazione db consultabile, …);
  - adozione ulteriori strumenti/fonti OSINT (shodan, spiderfoot, …);

SOC

people X technology (automation) ~ K

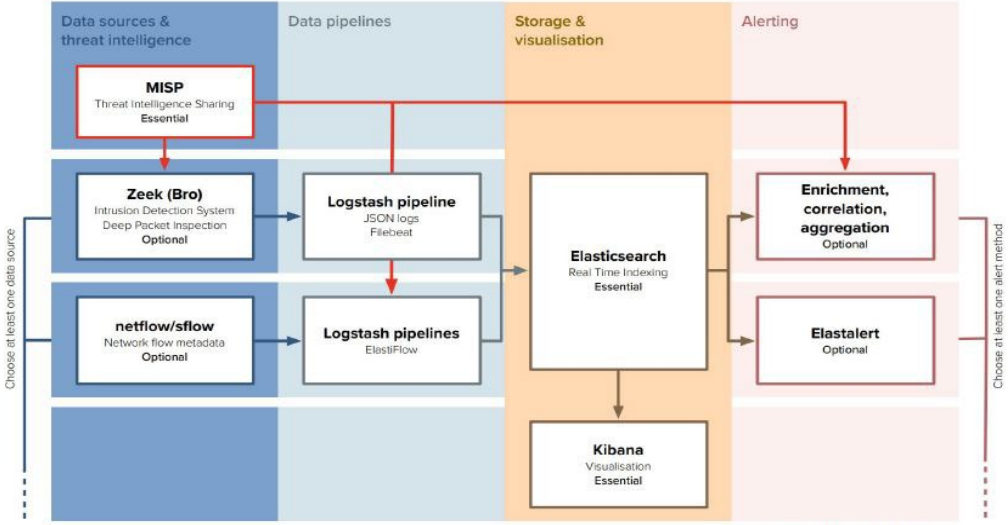
- Ente di media grandezza (10k utenti) 16x5 SOC (8x5x2 turni):
  - No automation: 8 FTE (analisti) + 2 FTE (coordinatori)
  - SIEM (Security Information and Event Management) powered: (4 + 0.5) FTE
- Tecnologie da implementare:
  - Centralizzazione log ed eventi di sicurezza
  - Integrazione con threat intelligence, vulnerabilità, OSINT, EDR, …
  - Prioritizzazione eventi
  - Connessione con asset management, vulnerability management, intrusion prevention, firewall, trouble ticketing, ...
  - Automatizzazione risposte a eventi predefiniti

SOC models



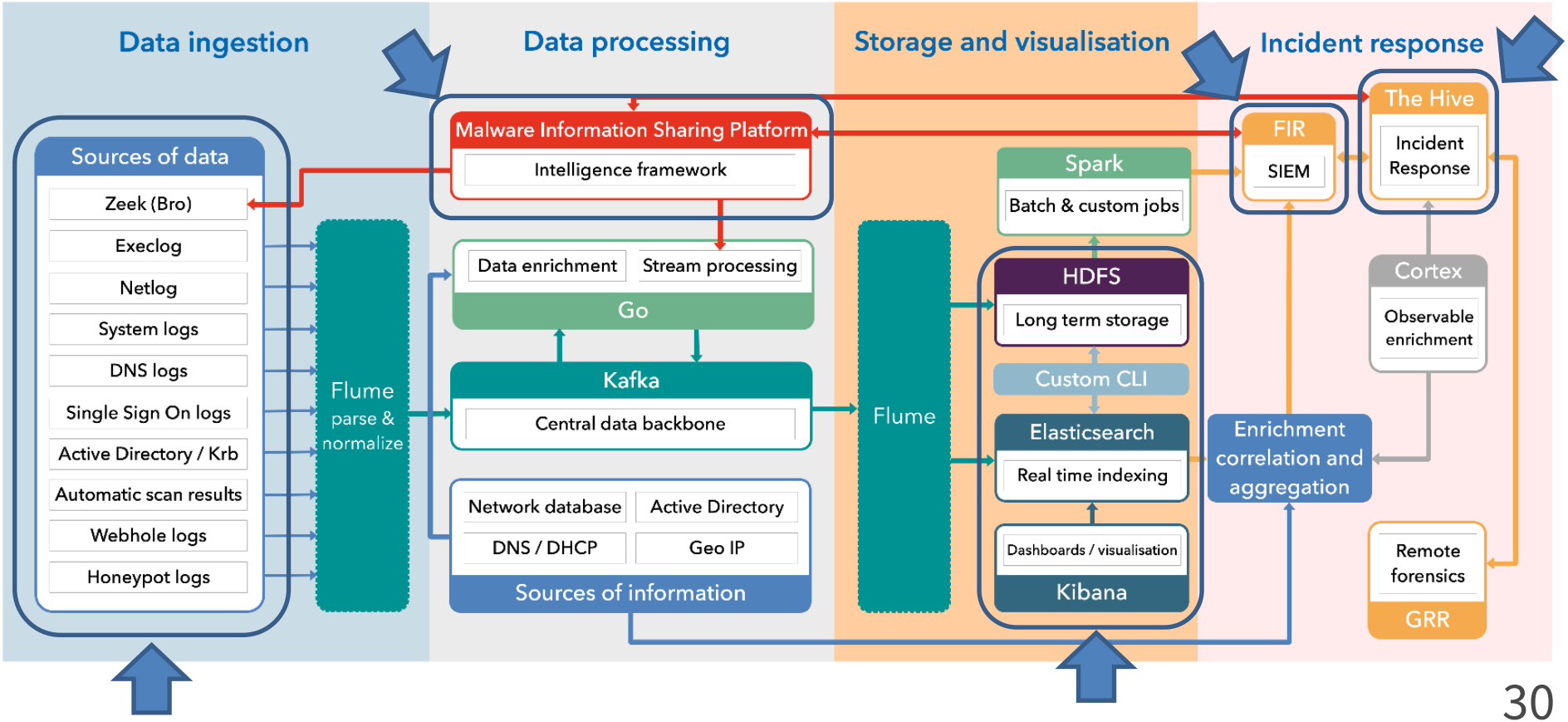
SOC data flow

WLCG SOC WG Reference Model



D Crooks, et al. DOI 10.22323/1.351.0010

WLCG SOC in dettaglio…



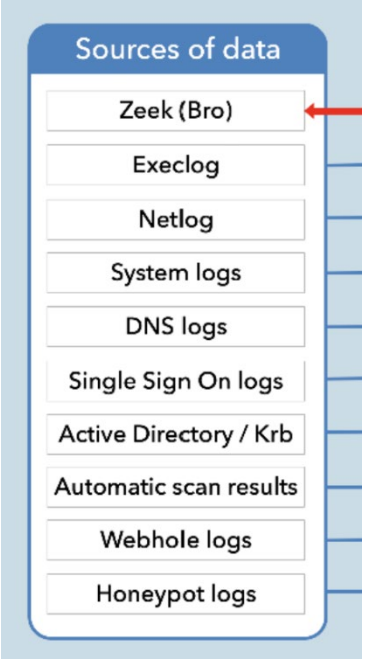
SCANSIONI
(coordinartore per acclamazione: **Leandro Lanzi**)

- integrazione/armonizzazione modalità scansioni in strutture/cloud;
- perfezionamento del ciclo di gestione scansioni e vulnerabilità:
  - coinvolgimento diretto responsabili locali security strutture/Tier per mitigazione/risoluzione vulnerabilità gravi in modalità kiosk-like (segnalazioni tramite apertura automatica ticket, gestione a cura dei responsabili locali; solo consulenza e controllo da parte del gruppo);
  - applicazione automatica/non assistita patch/aggiornamenti in ambiente controllato (Datacloud);

MISP

- **MISP** (*Malware Information Sharing Platform*) is a platform for exchanging, sharing, and analyzing malicious activity. It allows organizations and individuals to share, store, and analyze threat data and indicators, as well as collaborate and respond to incidents in real time. (…)
- Esistono sia feed pubblici sia feed di vendor, ma la vera opportunità messa a disposizione dallo strumento risiede nella possibilità di instaurare relazioni di trust con enti affidabili e dal *profilo di rischio compatibile con il nostro* per condividere informazioni di qualità (CERN, per esempio, con il quale è stato già stipulato il *Threat Intelligence Sharing Agreement*);
- Istanza già installata (ma mai entrata seriamente in produzione) va resuscitata e integrata nella nostra infrastruttura (con strumenti opportuni per CSIRT e SOC).

Strumenti per le strutture



- *(in un mondo perfetto)* va indagata e definita dotazione *standard* (sulla quale sviluppare know-how per facilitarne installazione e manutenzione) per:
  - protezione rete/macchine (non potremo permetterci NGFW - e le relative signature aggiornate annualmemte - per tutte le strutture):
    - EDR, HIDS, NIDS, firewall, …
    - **DNS firewall** (prototipo in funzione);
  - generazione dati da elaborare centralmente:
    - network sniffer (argus), EDR, HIDS, NIDS (zeek), firewall, strumento per raccolta, selezione, normalizzazione log, …

Spigolature – things to do

- **DNS firewall**: prototipo a MIB in produzione su DNS server di sezione da poco più di 1 anno:
  - RPZ: a Response Policy Zone is **a mechanism to introduce a customized policy in DNS servers, so that recursive resolvers return possibly modified results**. *By modifying a result, access to the corresponding host can be blocked.*
  - Blacklist contenente la lista dei domini/degli indirizzi responsabili di attività malevole (phishing etc.) quotidianamente diffusa da CERT AgID (e anche altre liste pubbliche di tracker, siti pubblicitari, malware spreader, …).
- **Creazione canali di comunicazione alternativi** (telegram? signal?)
  - per gestire eventuali emergenze per il gruppo in assenza di strumenti ufficiali
  - per veicolare comunicazioni importanti e asincrone verso responsabili sicurezza locali.

CSIRT, SOC, dati: un caso di studio (1)

canale Telegram di CSIRT Italia

Rilevato lo sfruttamento massivo della CVE-2021–21974 in VMWare ESXi (AL01/230204/CSIRT-ITA)

ALERT 04/02/2023 22:23

VMWare | Exploit | ESXi | CVE-2021–21974

Sintesi

Rilevato il massiccio sfruttamento attivo in rete della vulnerabilità CVE-2021–21974 – già sanata dal vendor nel febbraio 2021 – presente nei prodotti VMware ESXi.

Rischio

Stima d'impatto della vulnerabilità sulla comunità di riferimento: ALTO/ARANCIONE (70,25/100)[1].

In sintesi: vulnerabilità
- datata, corretta da due anni
- per la quale esistono mitigazioni (spegnere servizio, chiudere porta su F/W)

NON particolarmente preoccupante

Tutto a posto? (Un caso di studio, 2)

HOME > CRONACA

Attacco hacker in corso nel mondo. Migliaia di server compromessi

La Francia è il paese più colpito, con Finlandia e Italia, ma i ransomware attivati hanno preso di mira anche le reti di Canada e Stati Uniti. Lo rileva l'Agenzia per la Cybersicurezza Nazionale. Tim: "Il servizio si è stabilizzato"

tempo di lettura: 5 min

di Gian Franco Coppola

ATTACCO HACKER

aggiornato alle **20:17** 05 febbraio 2023

AGI AGENZIA ITALIA

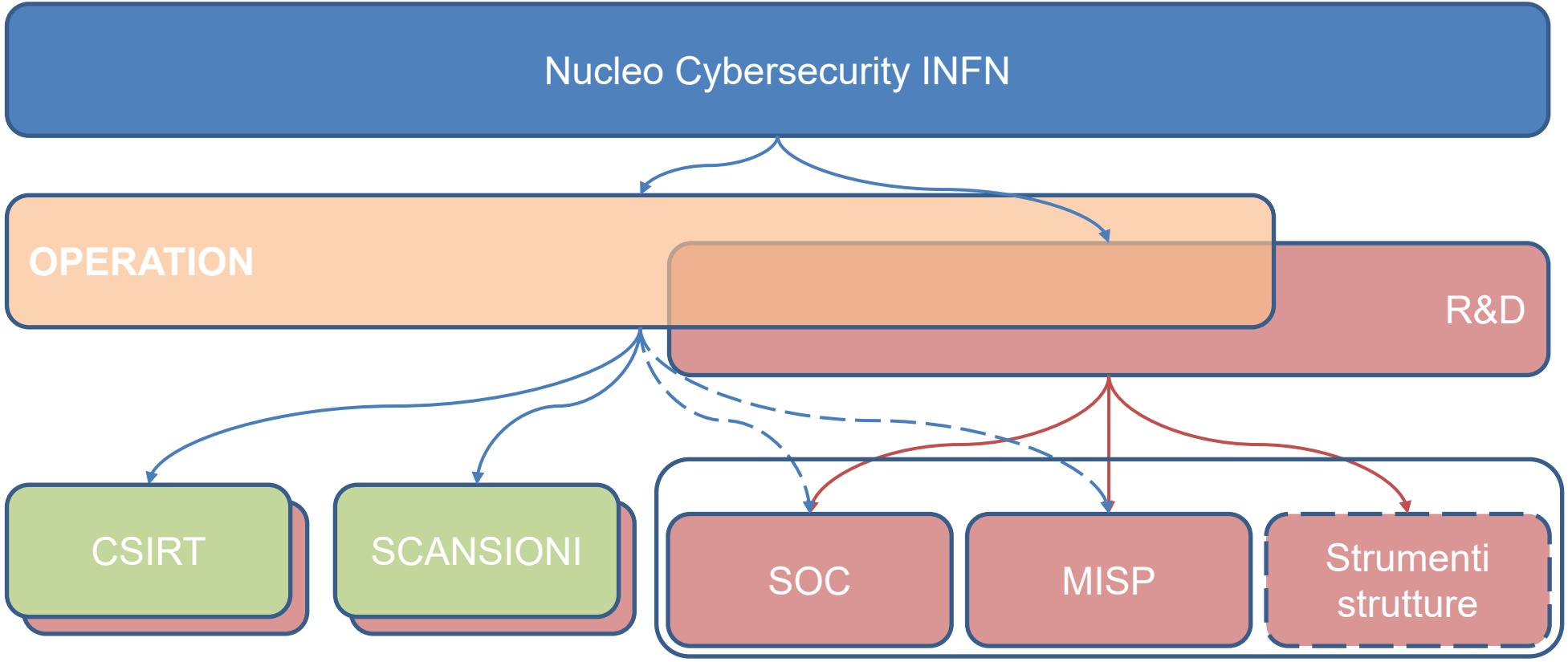
E non solo: titolo d'apertura di Corsera, Repubblica, Stampa, telegiornali vari, …: *è plausibile (e lecito) che il management si agiti.*

Controlli (Un caso di studio, 3)

- Cosa serve?
  - DB con risultati scansioni su tutte le reti INFN;
  - dati di traffico da tutte le strutture (quelli che servono per rilevare eventuali anomalie: scansioni su reti/porte, picchi di traffico, …);
  - dashboard statistiche traffico per tutte le linee INFN (GARR GINS);
  - threat intelligence (condivisione eventuali IOC);
  - altre fonti OSINT (tra cui stampa estera);

- trovate 12 macchine con porta 427/tcp accessibile da rete geografica
  - contattati singolarmente i responsabili locali della security: entro 12 ore (era domenica sera) 10/12 macchine controllate: aggiornate e quindi non vulnerabili, o spente; porta incriminata chiusa su router perimetrale;
  - diramato avviso a tutti per precauzione;
- management tranquillizzato (se non sul momento il giorno dopo);
- morale: 1) i dati sono *indispensabili* e 2) *può capitare di doverli usare anche di sera.*

Wrap up attività cybersecurity



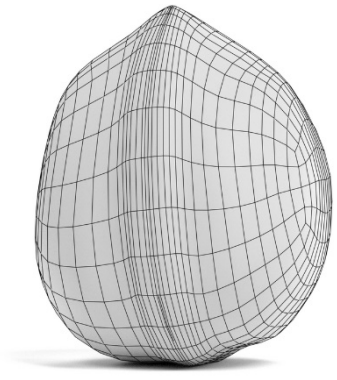
Proposta tempi

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

Last but not least: il nome…

NUcleo **C**yber**S**ecurity INFN

NUCS INFN o **NUX** INFN



Semplice, non cacofonico, richiama l'idea della protezione, abbastanza facilmente integrabile con logo grafico stilizzabile (wireframe like): opinioni?

… e il logo

INFN Istituto Nazionale di Fisica Nucleare
NUcleo CyberSecurity

INFN Istituto Nazionale di Fisica Nucleare
Nucleo CyberSecurity

INFN Istituto Nazionale di Fisica Nucleare
NUcleo CyberSecurity - NUCS

INFN Istituto Nazionale di Fisica Nucleare
NUcleo CyberSecurity

INFN Istituto Nazionale di Fisica Nucleare
NUcleo CyberSecurity - NUCS

INFN Istituto Nazionale di Fisica Nucleare
NUcleo CyberSecurity

INFN NUCS Istituto Nazionale di Fisica Nucleare
NUcleo CyberSecurity

Buon lavoro!

Designed by studiogstock / Freepik