Computer security nei grandi esperimenti: l'approccio (e l'esperienza) di CMS. (E anche un po'oltre)

Gian Piero Siroli

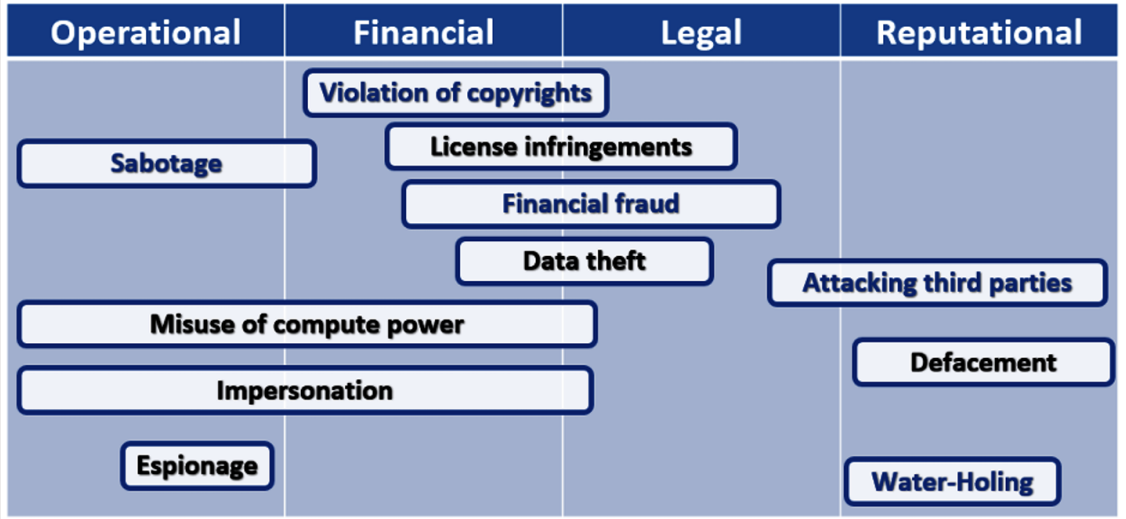
CMS Computer Security Officer

Workshop sul Calcolo nell'INFN (Paestum, maggio 2022)

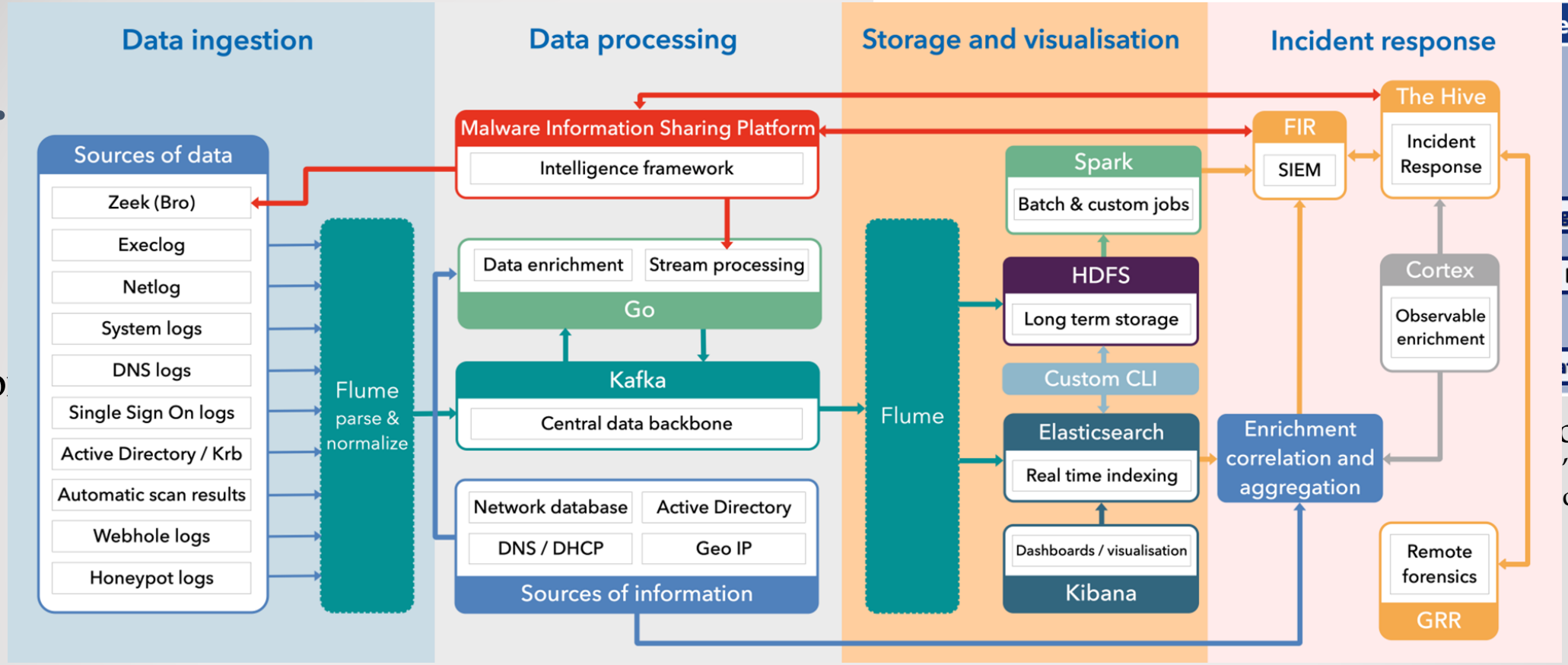
Dall'inizio:
Nel mezzo del cammin di nostra vita…

- Nuovo ruolo ad inizio 2018. Single contact point di CMS per questioni di sicurezza (richiesto da CERN Security Team)
- CMS Cyber ecosystem (cifre *molto approssimate*): ~350-400k CPU cores, vasta infrastruttura di rete intercontinentale & tecnologie Grid, ~15-20GB/s data transfer throughput, ~170PB dataset storage, ~~5MLOC(?) + online world
- Livello procedurale:
  - (ri)organizzazione mailing list CMS relativa a security
  - istituzione del CMS Computer Security Board/Team (4 membri a livello di coordinamento, incluso contatto WLCG). Possibile revisione
  - review e formalizzazione di una incident response procedure («discussa» con CERN ST). Suddivisione di CMS in diversi sottodomini di calcolo con relativi contatti per alert, incidenti ecc
  - raccolta di informazioni/docs
- Contatti piu' stretti con CERN ST (molto disponibili. scelta strategica) perche'…monitoring, network scanning, alerting…incident handling (*necessariamente* condiviso), WLCG etc. Contatti saltuari con US CMS security @ FNAL
  - Queste relazioni (cercate o trovate) sono primordiali. La Security e' una attivita' collettiva
- Breve attivita' iniziale su EU GDPR (General Data Protection Regulation) poi scorporata da Security con nomina di un CMS DPO (in stretto contatto)
  - Data Protection/Privacy e Security sono contesti vicini (e con intersezioni) ma concettualmente diversi
- Manpower ☹

…mi inoltrai in una selva oscura…



- Considerato il manpower ☹…
  - awareness raising a vari livelli (management per risorse e coders per s/w), security talks periodici
    - non e' facile, si deve fare cambiare mentalita', ancora molto lavoro da fare. Tecnica standard: "terrorismo psicologico" sul management, prospettando eventuali conseguenze operative, finanziarie, legali o di immagine in caso di attacchi, potenzialmente molto costosi e distruttivi anche a livello internazionale. Ransomware: rischio medio-alto
  - ricerca esterna (non CMS: CERN(*))
  - …e ancora piu' esterna… (non CERN: comp.science depts. etc)
    - qualche risultato (anche buono) e' arrivato. La ricerca di manpower continua (anche in questa audience?!)
- Una delle prime iniziative (*)
  - injection nel CERN Security Operation Center (SOC) di security log di una infrastruttura CMS particolarmente esposta alle reti esterne
  - vantaggi: il CERN mantiene, sviluppa ed analizza i dati del suo SOC, manpower di CMS quasi nullo (solo in configurazione). In caso di incidente il SOC ha gia' i dati necessari all'analisi (si guadagna tempo nel traceback). Di fatto, una collaborazione win-win. Ancora in fase di sviluppo pushing K8S logs. Su richiesta di M.Livni si e' cercato di estendere questo approccio ai log di Condor ma il CERN era meno interessato: dipende dal tipo di log, dimensioni etc



- Co
  - ci
    - ➢ ' sul
      cchi,
  -
  -
  - ➢

- Una delle prime iniziative (*)
  - injection nel CERN Security Operation Center (SOC) di security log di una infrastruttura CMS particolarmente esposta alle reti esterne
  - vantaggi: il CERN mantiene, sviluppa ed analizza i dati del suo SOC, manpower di CMS quasi nullo (solo in configurazione). In caso di incidente il SOC ha gia' i dati necessari all'analisi (si guadagna tempo nel traceback). Di fatto, una collaborazione win-win. Ancora in fase di sviluppo pushing K8S logs. Su richiesta di M.Livni si e' cercato di estendere questo approccio ai log di Condor ma il CERN era meno interessato: dipende dal tipo di log, dimensioni etc

Altre attivita' (passate, presenti)

- Frequente distribuzione di alert/warning (ricevuti spesso da CERN ma anche altri canali) su vulnerabilita' di vario tipo, verso sottodomini di calcolo CMS pertinenti al warning
- Un paio di comunicazioni di attivita' di cryptomining ricevute ed indagate (@ CC-IN2P3 e DESY). Esercitazione di tracking e disabilitazione di utenze
  - Cryptominer detection(?): CPU usage metrics(?), IoC, IP address (ci fidiamo del FW CERN!?)
- Open source code external dependencies (security vulnerabilities): qualche tipo di analisi @ build time, proposta verifica. CERN central software library gateway to secure open source packages: progetto IT (draft of CNIC & JCOP WGs) per un repository verificato e disponibile all'interno del CERN non decollato apparentemente per mancanza di interesse degli esperimenti (e forse anche manpower IT). Suggeriti static code checkers ed uso di software repository centralizzati (Sonatype Nexus or Apache Maven). Uso di watchlist (X-Force Exchange).
  - Opinione personale: SE fossimo in un contesto privato, questo approccio cosi' superficiale e lasciato ai coders sarebbe semplicemente impraticabile
- Penetration test da ANSSI (F) (online infrastructure) e CERN (eseguiti) o WLCG (pianificato e poi rinviato in attesa di tempi migliori)

Altre attivita' (presenti, future)

- Ransomware: verifica backup e procedura periodica di reload. Anche in online
  - Assessment di quali dati sono critici per il funzionamento di CMS (calibrazioni etc) e dove sono. Verifica dell'esistenza di backup di dati e sistemi critici come misura preventiva anti ransomware, con periodici recovery di test
  - ➢ Non SE, ma QUANDO. Attacco esteso potenzialmente disastroso (Maastricht Univ. 23.12.19, 30฿ ~2-300k€)
- Verifica/aggiornamento di canali e strumenti di comunicazione
- Cyber Security Risk Assessment interno (anche limitato?!)
- CERN IT sta sviluppando un framework per threat modelling…
- Continuare/incrementare awareness raising (anche per coders)
- Pushing di altri security logs nel CERN SOC??
- Aggiornamento costante attivita' WLCG
- Long term: monitorare GPU/FPGA security vulnerabilities
- VERY long term (t➔∞): posizionamento Security in organigramma CMS
  - ➢ Importante a tutti i livelli, ma e' *indispensabile* la *consapevolezza* del management

WLCG: SOC W/G, MISP

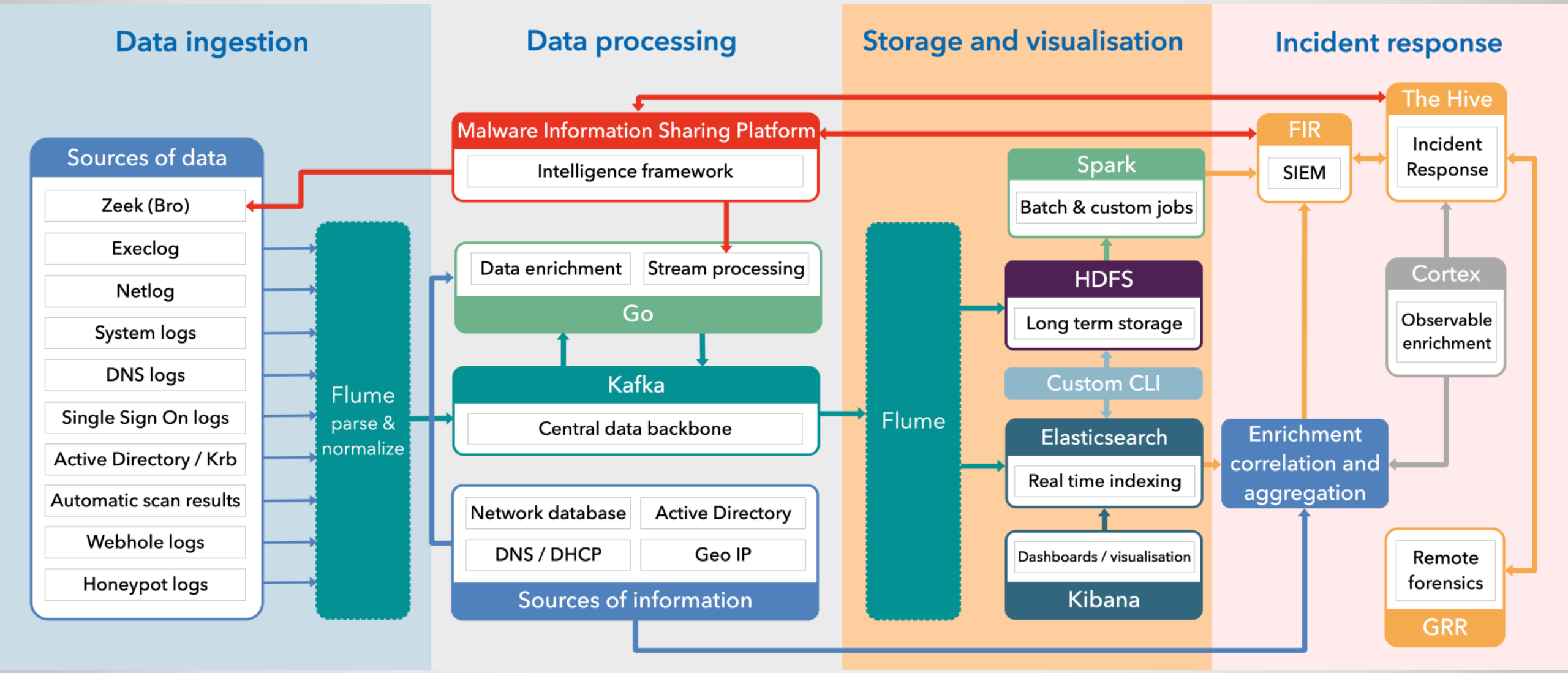
- Il gruppo Security INFN potrebbe trarre vantaggio da alcuni dei concetti/tools sviluppati da questo W/G di WLCG, in particolare lo CSIRT per quanto riguarda la condivisione di informazioni a livello internazionale (threat intelligence). Lavoro su MISP (Malware Information and Threat Sharing Platform) gia' iniziato nel recente passato da R.Veraldi in contatto con Liviu Valsan (CERN). Disponibilita' a collaborare lato CERN

References:

- Security Operations Centers Working Group (WLCG SOC W/G) and documentation (*)
  Goal: most Research/Education orgs lacking resources, time, efforts, skills
  Community vision, sharing with trusted partners
- Introduction (*) to MISP (additional permissions needed): deploy, config, set up, share

(*) CERN certif

WLCG: SOC W/G, MISP



WLCG security

WLCG operational security strategy

1. Place *threat intelligence sharing at the core of security operations*

- Share specific threat intelligence (bad IP addresses, file hashes, etc.) in real time within community
- Produce relevant/target threat intelligence for WLCG
- Enable sites to leverage and make use of the threat intelligence

2. Improve WLCG's incident response capabilities. Attacks are global, so must be the response

- Bridge cooperation gaps:
  - Lack of cooperation between "campus" and "grid" or "scientific" security teams
  - Lack of global coordination on global attacks within the research & education community
- Consolidate traceability and incident response policies for clouds/federated identities

Iniziative internazionali(*)

- Necessario un approccio complessivo all'ecosistema di Security. Varie iniziative internazionali in evoluzione.
- L'INFN dovrebbe *almeno* monitorarne lo sviluppo (per il momento…GPS) ed eventualmente integrarsi su alcuni aspetti, se le condizioni (e le risorse) lo permettono. Il mondo HEP (R&E) sta andando in quella direzione
- A livello nazionale: GARR, Agenzia per la cybersicurezza Nazionale (ACN), report non pubblici su vulnerabilita' e IoC …

- Source of threat intelligence available to entire sector
  Central R&E MISP instance (hosted at CERN)
- Technical collaboration
  SOC WG
- High level coordination
  WISE IR-TI
- Global operational security
  EGI CSIRT, OSG Security, SAFER (global trust group protecting Research & Education infrastructures with incident response and threat intelligence sharing capabilities)

(*) EGI CSIRT, WISE COMMUNITY, WLCG

In sintesi

Dettagli tecnici a parte…

- Fare network: e' *fondamentale* collaborare con altre organizzazioni, nazionali (GARR, ACN) ed internazionali (CERN, WLCG, SAFER) per ricevere alerts, IoCs, threat intelligence (MISP) etc. Approccio collaborativo alla security → non puo' essere a macchia di leopardo internamente
  - Possibile riuscirci?
- Monitor: raccolta di log (logins, network connections, commands…) ed una analisi centralizzata e coordinata (SOC/CSIRT/SIEM) per rivelare incidenti e lo stato globale della infrastruttura
- Risorse: cosa si puo' fare "in house" e/o in outsource?

Giusto per info, dove sta andando il CERN (con un po' di fatica):

- Controllo/verifica di security sulla importanzione di librerie, packages, VMs/containers (coders)
- 2FA (in particolare per utenze critiche)
- Partecipazione a SAFER

- NON sottovalutare la security (come nel recente passato)

Computer security

Social engineering: phishing
(do it yourself)

Can you tell the difference between a legitimate website and one that's a phishing attempt?

Open-Source Phishing Framework to test your organization's exposure to phishing:
Launch a Campaign

https://www.opendns.com/phishing-quiz/

https://phishingquiz.withgoogle.com/

Privacy & surveillance
(do it yourself demo)

Just to get an idea of what kind of behaviours any website can monitor:

https://clickclickclick.click (speakers on)

How trackers see your browser

How does tracking technology follow your trail around the web

I don't care if my powerpoint presentation has 300 slides…You are staying until it's over.

It's over