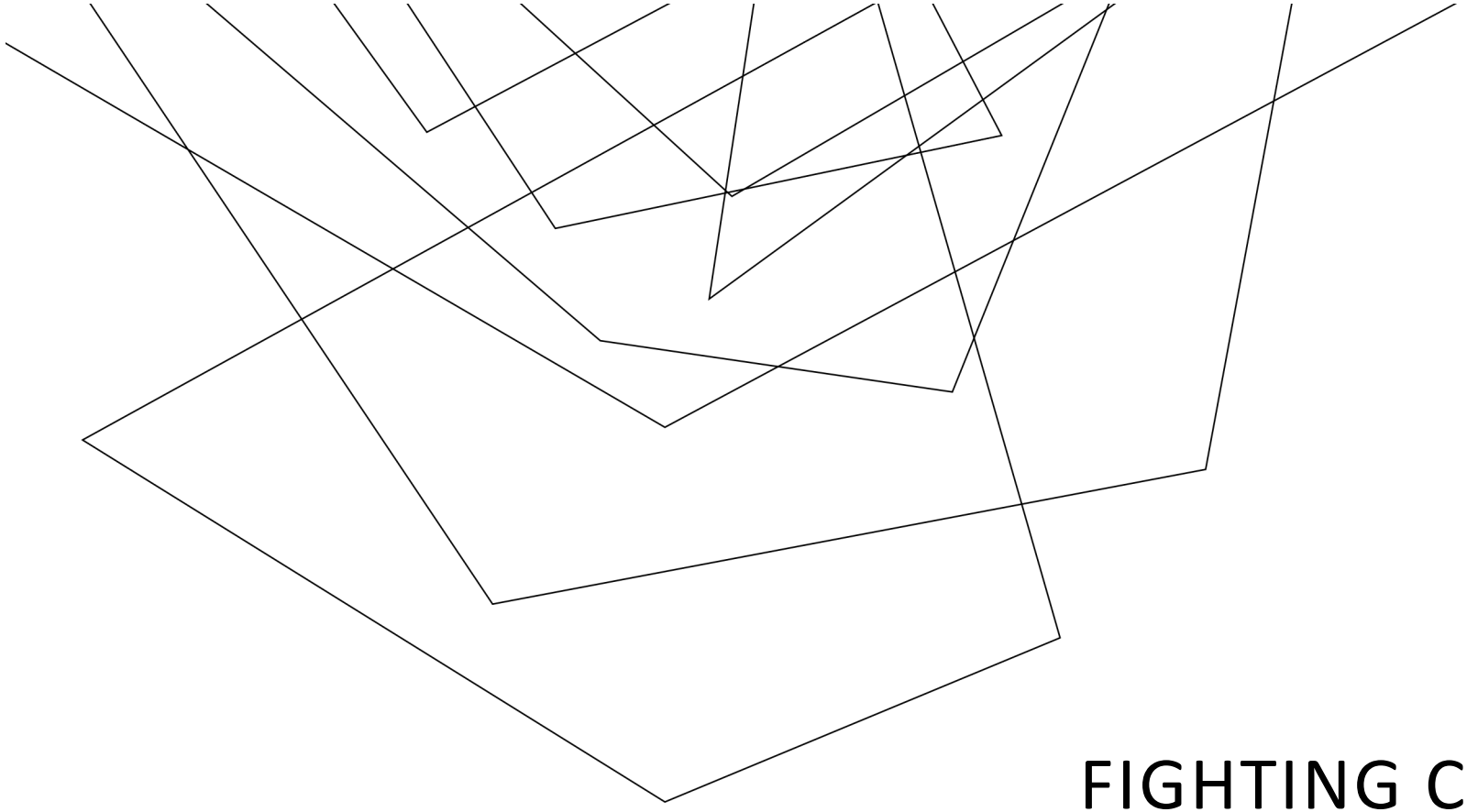


FIGHTING CYBERCRIME WITH OSINT – WP 2

Francesco Santini

PARTECIPANTI

- WP2: Santini, Milani, Poggioni, Grilli, Pinotti, Navarra, Taticchi, Gnaldi

WP 2 PROGETTAZIONE E IMPLEMENTAZIONE DI UN SISTEMA OSINT/SIEM PER CYBERCRIME

- *Vista rimodulazione budget non "implementazione" ma «progettazione e Proof of Concept»*

- Da documento progetto
  - **1: Il rischio che bando per risorsa assegnista di ricerca per sviluppo in WP1 e WP2 vada deserto: Si ridurranno i deliverable che prevedono implementazione alla sola progettazione e si utilizzeranno informazioni note per stimare risultati.**

OBIETTIVI

- Nel WP2, che ha come obiettivo primario la **creazione del sistema SIEM**,
- si individueranno quindi le fonti (aperte) dei dati da analizzare,
- come prelevarli dalla fonte,
- si riassumerà il loro formato,
- si descriverà inoltre le specifiche del sistema di gestione dei dati per la loro memorizzazione.
- Si procederà **all'utilizzo di database non-relazionali**, vista l'eterogeneità dei dati acquisiti da più fonti, contenenti testo, immagini, semplici valori, etc.

OBIETTIVI - ANALISI

- Per l'analisi dei dati si implementeranno tecniche di Intelligenza Artificiale (e di Explainability), Algoritmiche, e statistiche.
- La validazione del sistema avverrà attraverso **l'applicazione su casi studio pratici**, per esempio iniettando dati sintetici al fine di ottenere la rilevazione di un problema di sicurezza.
- Verranno inoltre utilizzate le metriche della letteratura per misurare le performance del SIEM (ad esempio FAR/FRR).

RISULTATI

- Il risultato più importante che ci aspettiamo nel WP2 è di declinare un sistema SIEM verso allarmi provenienti oltre che da traffico di rete, anche da fonti di informazioni OSINT (social, blog, dati economici, etc.), creando nuovi allarmi dedicati e integrandoli in un'analisi globale.

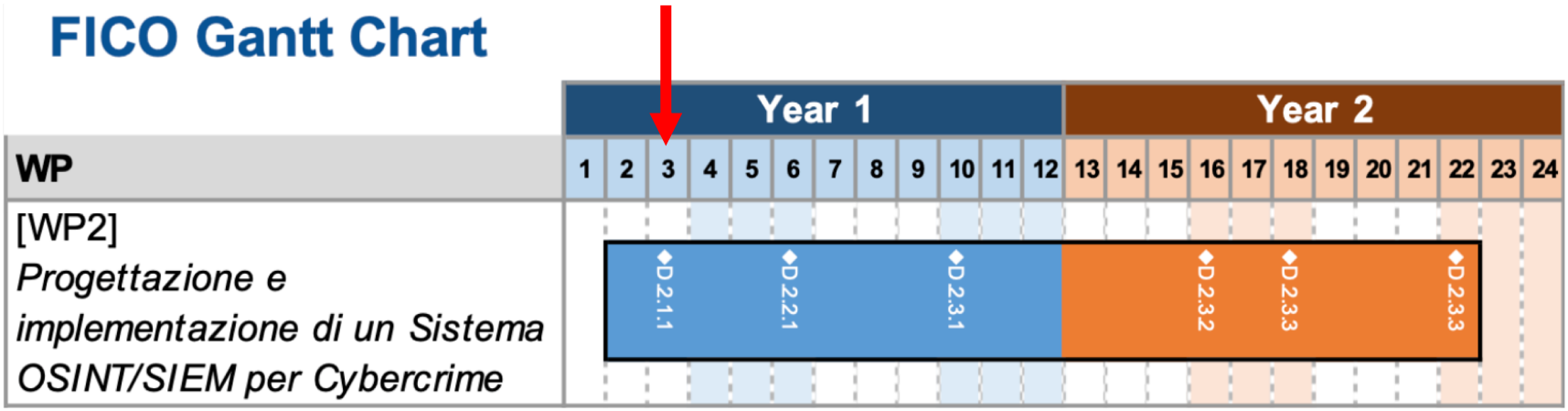
IMPATTO

- L'attività nel WP2 collegata all'avanzamento dei sistemi SIEM nell'uso di fonti OSINT permetterà di incrociare flussi di informazioni ben distanti ma correlati tra loro, ed abilitare quindi una piattaforma di intelligence, monitoraggio e sicurezza data-oriented altrimenti impossibile localmente su ciascuna fonte.

- Tale avanzata gestione dell'informazione migliorerà il processo decisionale di enti ed aziende pubbliche e private

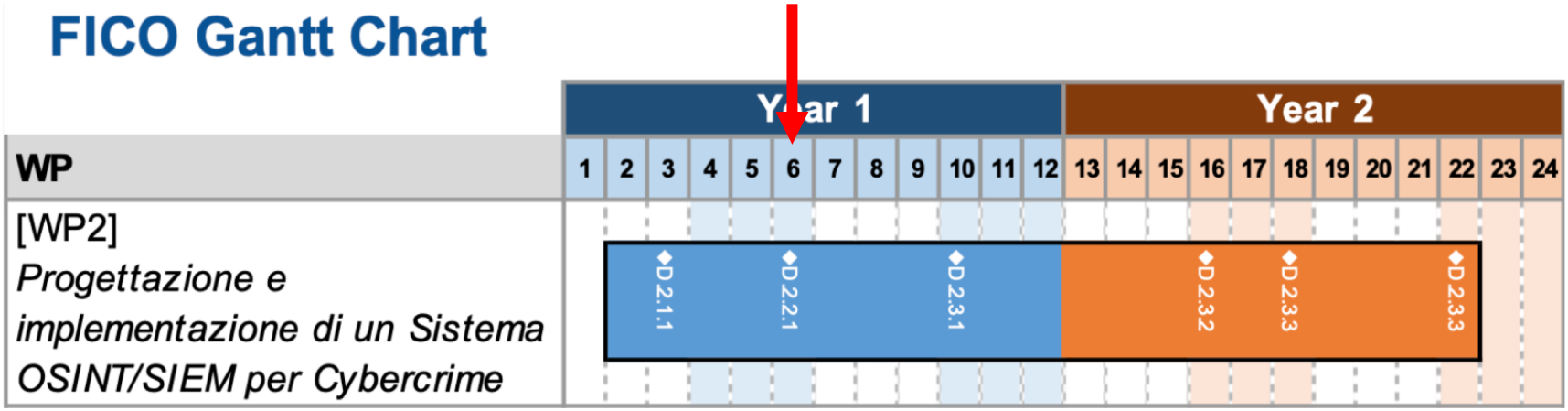
TASK 2.1 ANALISI DELLA LETTERATURA SCIENTIFICA E DEI PROGETTI IN CORSO IN TEMA OSINT/SIEM E SCELTA DEL SISTEMA SIEM DI RIFERIMENTO

- **D.2.1.1 Doc su stato dell'arte in ambito OSINT/SIEM, con valutazione e motivazione per piattaforme OSINT/SIEM scelto a riferimento**



TASK 2.2 STUDIO FONTI OPEN SOURCE (OSINT)

- **D.2.2.1 Report delle modalità di acquisizione e del formato dati (collegato a D.3.3.1)**
  - Qui tutto ok anche senza assegnista



TASK 2.3 PROGETTAZIONE ED IMPLEMENTAZIONE DELLA SUITE SIEM/OSINT

- Qui nel titolo appare implementazione, ma possiamo ritenerla un «progettazione e proof of concept»
- D.2.3.1 PoC del DB e del sistema SIEM/OSINT
- D.2.3.2 PoC Moduli SW (AI, Algoritmi su grafi, tool statistici)
- D.2.3.3 PoC Applicativo online per funzionalità di explanation
- D.2.3.4 Report della suite realizzata e del suo funzionamento