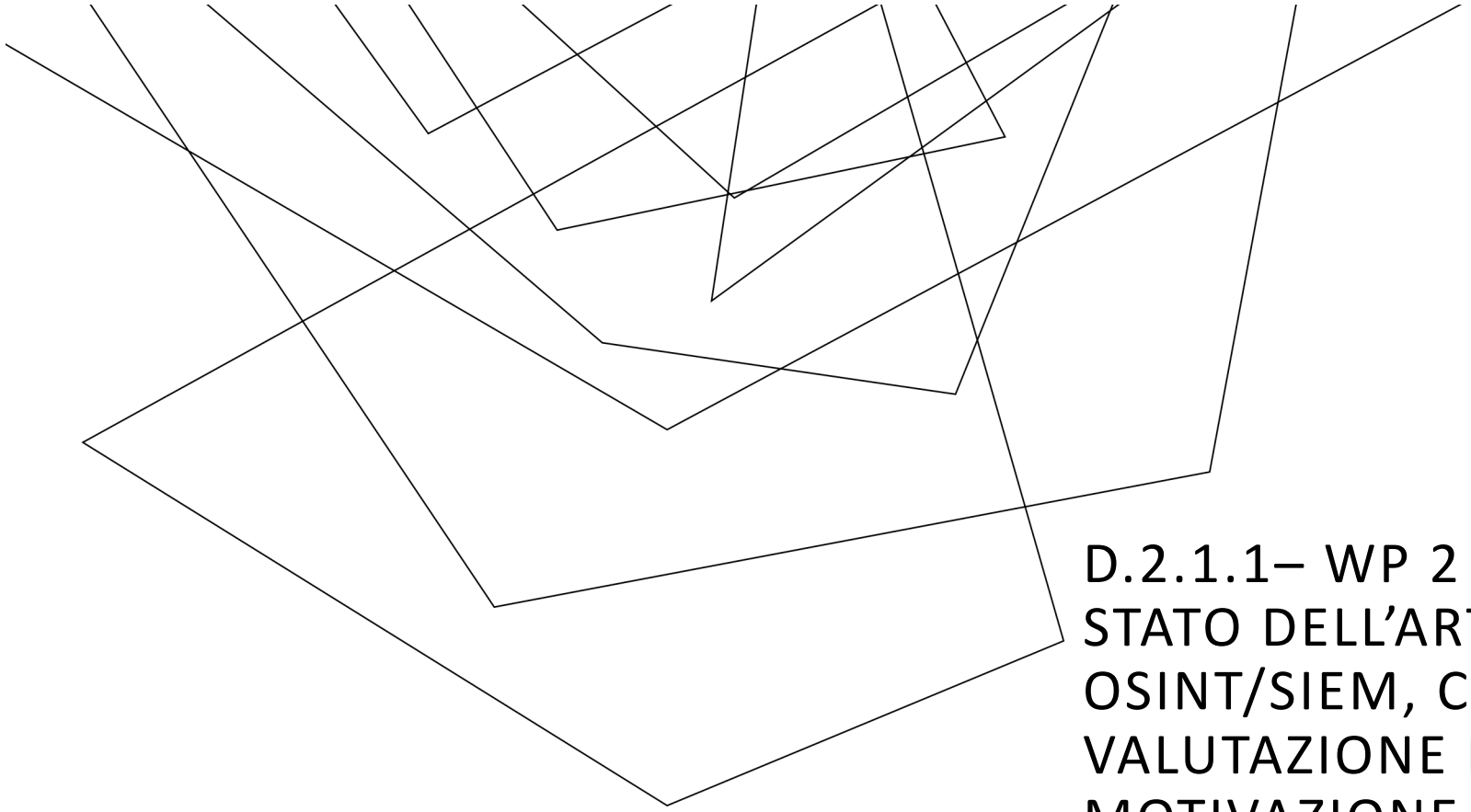


D.2.1.1– WP 2
STATO DELL'ARTE IN AMBITO OSINT/SIEM, CON VALUTAZIONE E MOTIVAZIONE PER PIATTAFORMA OSINT/SIEM SCELTA COME RIFERIMENTO

Francesco Santini

PARTECIPANTI

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

LINK

- https://fico.dmi.unipg.it/res/wp2/D211.pdf

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

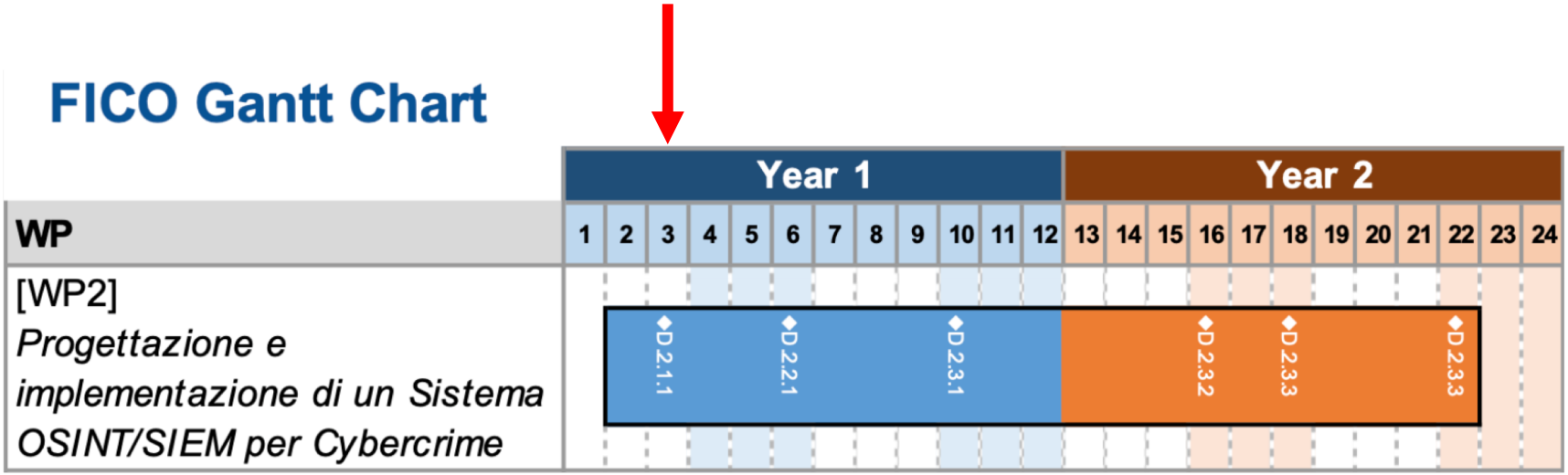
- Per l'analisi dei dati si implementeranno tecniche di Intelligenza Artificiale (e di Explainability), Algoritmiche, e statistiche.
- La validazione del sistema avverrà attraverso **l'applicazione su casi studio pratici**, per esempio iniettando dati sintetici al fine di ottenere la rilevazione di un 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.

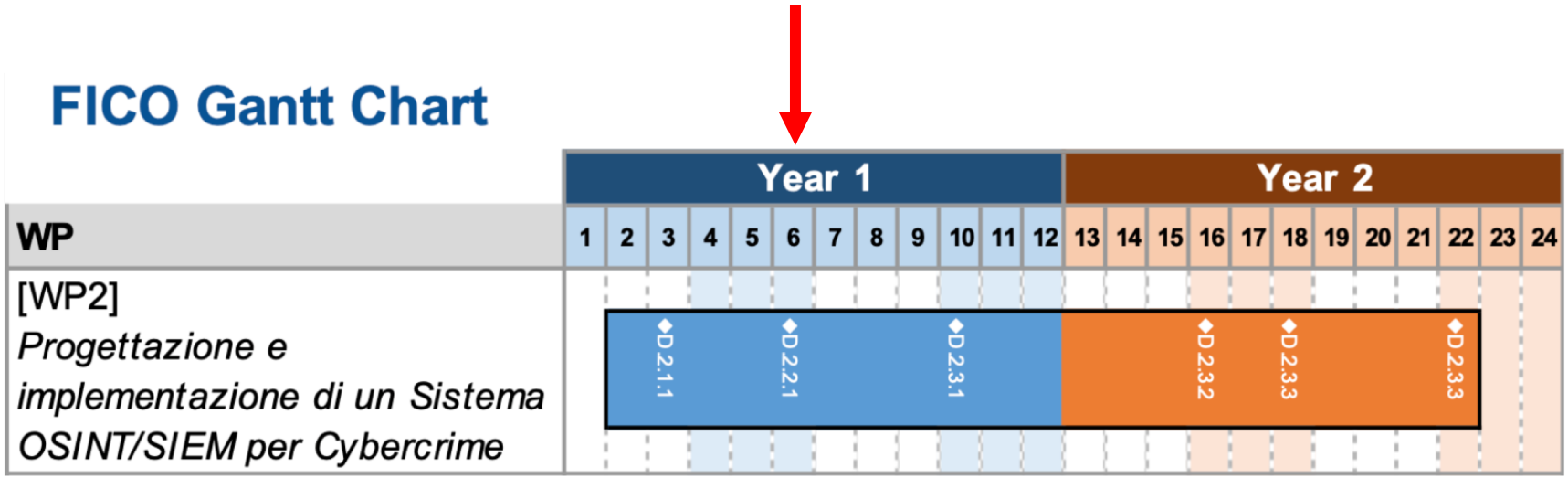
TASK 2.1 ANALISI DELLA LETTERATURA SCIENTIFICA E DEI PROGETTI IN CORSO IN TEMA OSINT/SIEM E SCELTA DEL SISTEMA SIEM DI RIFERIMENTO

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



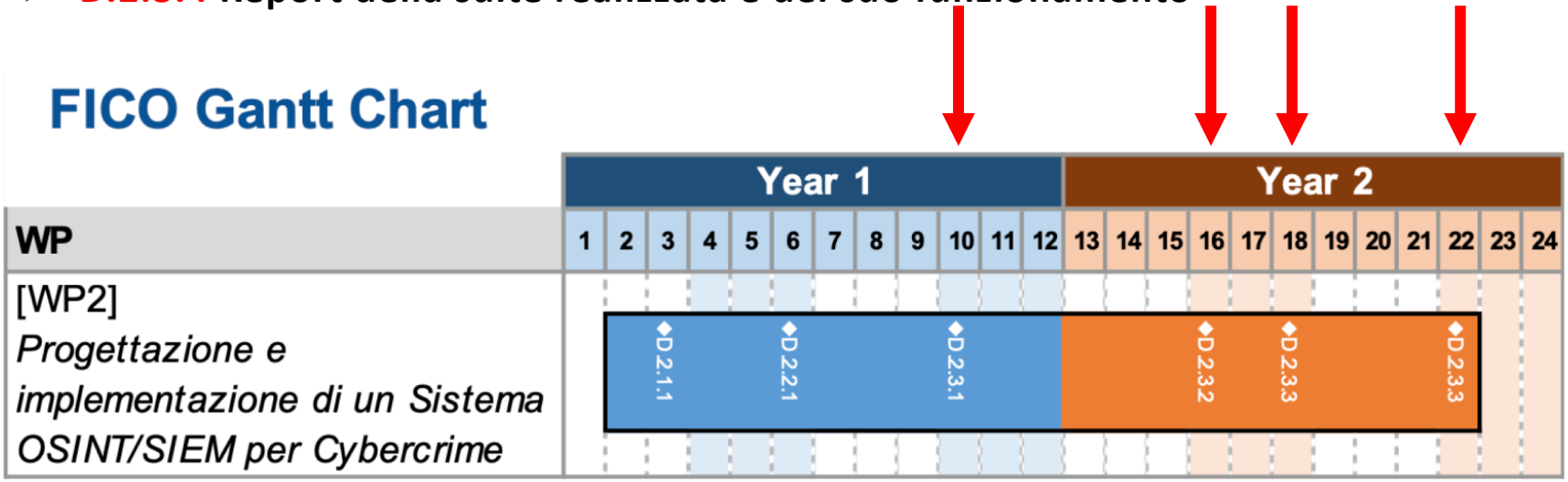
TASK 2.2 STUDIO FONTI OPEN SOURCE (OSINT)

- **D.2.2.1 Report delle modalità di acquisizione e del formato dati (collegato a D.3.3.1)**



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



D.2.2.1

- Santini
- Introduzione e terminologia riguardante le piattaforme SIEM
  - SIEM
  - Collezione di dati
  - Correlazione degli alert
- Letteratura su piattaforme SIEM
  - Una lista di sistemi SIEM

D.2.2.1

- Grilli
- Fonti OSINT
  - Abbreviazioni e acronimi
  - Definizioni e terminologia
  - Tipologie di fonti OSINT
- Metodologia e ciclo delle operazioni OSINT
  - Step 1: Raccolta (Collection)
  - Step 2: Elaborazione (Processing)
  - Step 3: Sfruttamento o analisi (Exploitation or analysis)
  - Step 4: Produzione (Production)
- Principali tecnologie utilizzate dall'OSINT

D.2.2.1

- Poggioni, Milani, Taticchi
- **Tecniche di analisi di dati proveniente da fonti aperte basate su AI**
  - Modelli basati su regole
  - Modelli semantici
  - Modelli grafici
  - Modelli di apprendimento automatico
  - Modelli ibridi

D.2.2.1

- Gnaldi
- **Tecniche e indicatori di misurazione del rischio di corruzione da fonti aperte**
  - La corruzione come variabile latente e multidimensionale
  - Indicatori red flags di rischio di corruzione: la selezione operata dall'Autorità Nazionale Anticorruzione (ANAC) per misurare il rischio di corruzione a livello territoriale
  - Verso un indicatore composito di rischio di corruzione negli appalti pubblici?
  - Scelta del sistema di normalizzazione
  - Scelta degli schemi di ponderazione
  - Scelta del sistema di aggregazione
  - Analisi delle relazioni tra indicatori elementari e della struttura di dimensionalità dei dati

D.2.2.1

- Navarra, Pinotti
- **Tecniche di analisi di dati proveniente da fonti aperte basate su altri algoritmi**
- Misure di centralità in reti (PageRank)

CARATTERISTICHE E OBIETTIVI DI UN SIEM

- La **centralizzazione degli alert**, che è la prima caratteristica centrale delle piattaforme SIEM:
  - Consente l'utilizzo di ulteriori algoritmi di detection che possono indicare anomalie e attacchi non sufficientemente segnalati dai singoli sensori.
  - L'anomalia può però diventare più significativa quando le informazioni vengono invece aggregate.

- I SIEM inoltre contribuiscono in modo sostanziale all'attività di **pianificazione**.
  - Le piattaforme SIEM hanno lo scopo di definire un insieme di azioni che possono essere intraprese per bloccare un attacco o mitigare i suoi effetti.

- Il primo obiettivo di una piattaforma SIEM è quello di **raccogliere e centralizzare** le informazioni provenienti da più sensori.

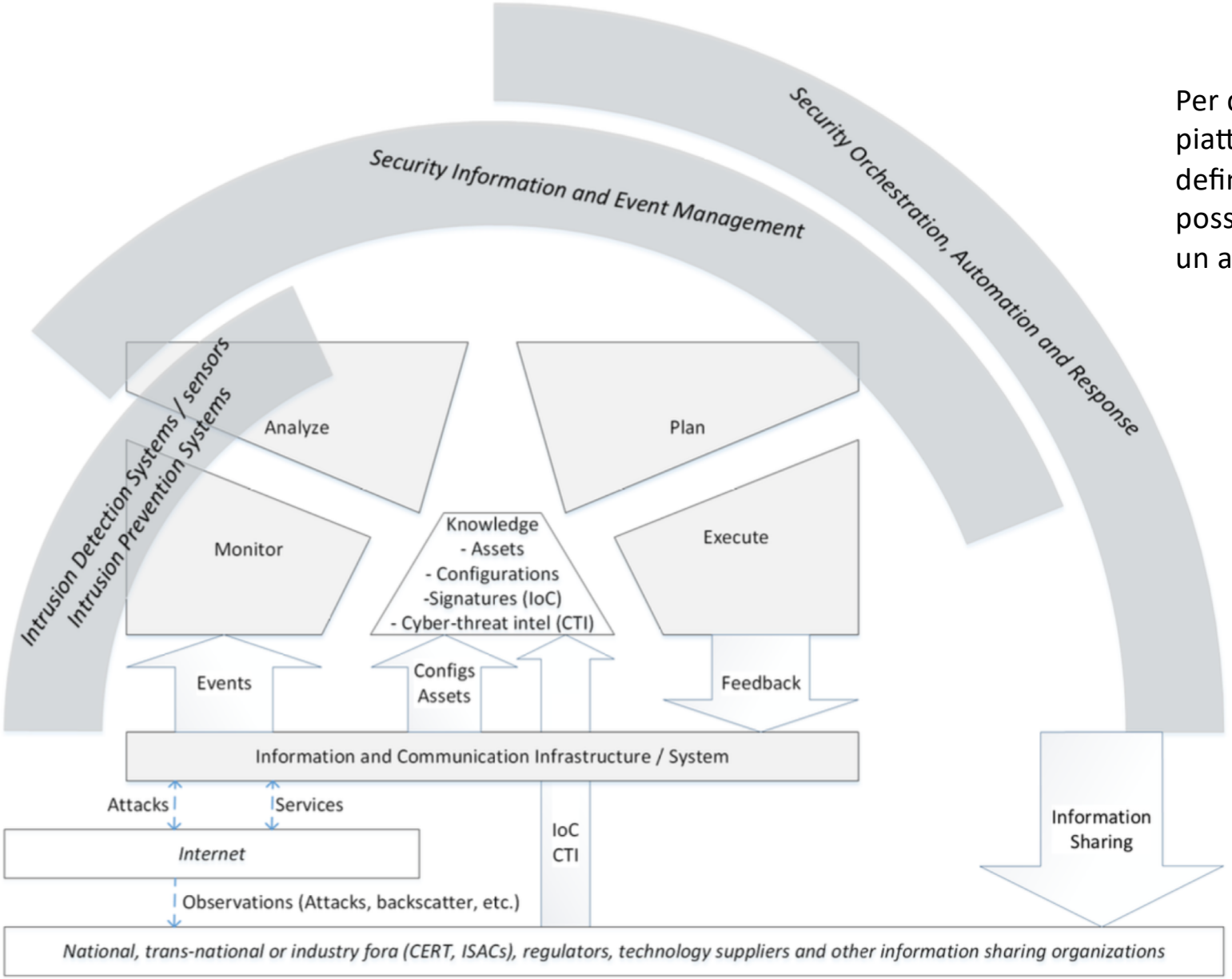
CARATTERISTICHE E OBIETTIVI DI UN SIEM

- La comunicazione di un messaggio di alert riguarda tre livelli differenti:
  1. lo **schema** definisce la struttura dei messaggi, il tipo e il significato degli attributi,
  2. la **codifica** definisce come tali messaggi e gli attutiscono codificati per formare stringhe di bit,
  3. i **protocolli** di trasporto descrivono come l'informazione codificata sia comunicata dal sensore al SIEM.

- La **correlazione** degli alert ha l'obiettivo di dare un senso al flusso di avvisi ricevuto dal SIEM. La correlazione ha diversi obiettivi:
  1. **ridurre il numero di alert** che l'analista deve elaborare raggruppando insieme gli avvisi;
  2. **aggiungere elementi contestuali** per consentire un'analisi più accurata e rapida di un gruppo di alert;
  3. **aggiungere alert** agli elementi di pianificazione e mitigazione **di livello superiore** in modo che vengano gestiti correttamente;
  4. **scartare gli alert considerati falsi positivi** e che non richiedono ulteriore elaborazione.

CARATTERISTICHE E OBIETTIVI DI UN SIEM

- L'approccio iniziale alla correlazione degli avvisi si è basato spesso su regole, descrivendo esplicitamente le relazioni logiche tra avvisi o regole per inferire tali relazioni.
- I database SQL comportano una significativa riduzione delle prestazioni per la procedura di indicizzazione. Mentre questa è utile per effettuare delle interrogazioni, le piattaforme SIEM sono caratterizzate da un'alta intensità di inserimento:
  - = Database NoSQL



Per quanto riguarda l'attività di plan, le piattaforme SIEM hanno lo scopo di definire un insieme di azioni che possono essere intraprese per bloccare un attacco o mitigare i suoi effetti.

29 SIEM proprietari (prodotti commerciali)

SIEM OPEN SOURCE

- ELK nel Gennaio 2021 è passato ad una nuova licenza non riconosciuta come OpenSource dalla comunità.
- **OpenSearch** è un progetto software open source lanciato nel 2021 come fork dei progetti Elasticsearch e Kibana, con lo sviluppo guidato da Amazon Web Services.
- **Logz.io Cloud SIEM** è basato su OpenSearch. Lo strumento offre tre opzioni di prezzo: quell «Community» è gratuita.
- **OSSIM**: consiste nella versione open source dell'offerta Unified Security Management (USM) di AlienVault. L'elenco dei progetti open source inclusi in OSSIM include: FProbe, Munin, Nagios, NFSen/NFDump, OpenVAS, OSSEC, PRADS, Snort, Suricata e TCPTrack.
- **Prelude**: Simile a OSSIM, Prelude è un framework SIEM che unifica vari altri strumenti open source. Ancora come OSSIM, esso consiste in una versione open source dell'omonimo strumento commerciale. Prelude accetta registri ed eventi da più fonti e li archivia tutti in un'unica posizione utilizzando l'Intrusion Detection Message Exchange Format.

SIEM OPEN SOURCE

- **Apache Metron**: evolvendosi dalla piattaforma OpenSOC di Cisco e rilasciato per la prima volta nel 2016. Metron si affida ad altri progetti Apache per la raccolta, lo streaming e l'elaborazione dei dati di sicurezza. Gli eventi vengono successivamente analizzati e normalizzati in JSON standard e quindi arricchiti e in alcuni casi etichettati. Per la visualizzazione, le distribuzioni Metron usano comunemente Kibana. ll progetto sembra però essere stato ritirato da Apache a Dicembre 2020.