REPORT TECNICO

INFO GATHERING

Redatto da: *Nicolò Calì Cybersecurity Student*

Data: 05/01/2026

1. Introduzione

1.1 Obiettivo dell'Attività

Effettuare una simulazione della fase di raccolta informazioni (Info Gathering) utilizzando dati pubblici su un target a scelta, nel nostro caso prenderemo in esame il famoso regista Quentin Tarantino.

1.2 Scopo

Lo scopo di questa simulazione è quello di capire al meglio la fase di raccolta di informazioni. Utilizzeremo essenzialmente due strumenti: ***Google*** *e* ***Maltego***

2. Ambiente di Lavoro e Strumenti

2.1 Configurazione del Laboratorio

Per la nostra simulazione basterà avere semplicemente una connessione ad internet ed il software “Maltego” installato nel nostro sistema operativo.

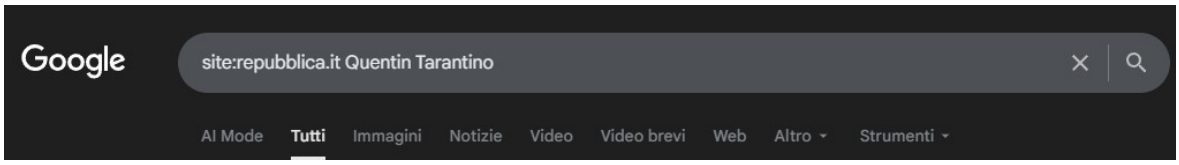
2.2 Strumenti Utilizzati

- Un motore di ricerca, **Google** nel nostro caso;
- **Maltego**.

3. Attività Tecnica e Metodologia

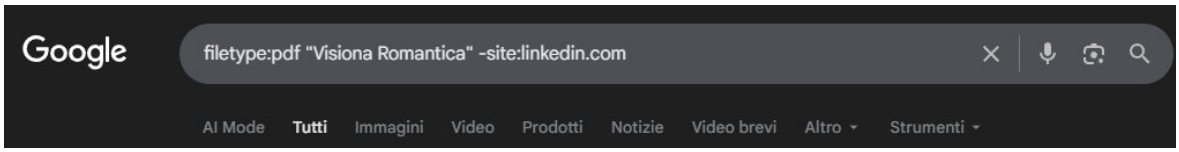
3.1 Fase di Ricognizione (Information Gathering)

Effettuiamo un’iniziale attività di Google Dorking tramite motore di ricerca provando ad utilizzare solo siti di divulgazione ufficiali per mezzo dell’operatore “site:”.



- ***Prompt utilizzato****:* site:repubblica.it Quentin Tarantino
- ***Osservazione****: L'analisi delle fonti aperte ha permesso di ricostruire il profilo professionale del target. È emerso che il soggetto è stato co-fondatore insieme a Lawrence Bender della società "A Band Apart" (operativa fino allo scioglimento avvenuto nel 2006). Attualmente, risulta essere il fondatore e proprietario della casa di produzione attiva denominata "Visiona Romantica".*

In assenza di un portale web diretto, è stata effettuata una ricerca mirata di documenti pubblici, escludendo i risultati provenienti da social network professionali (in particolare Linkedin).

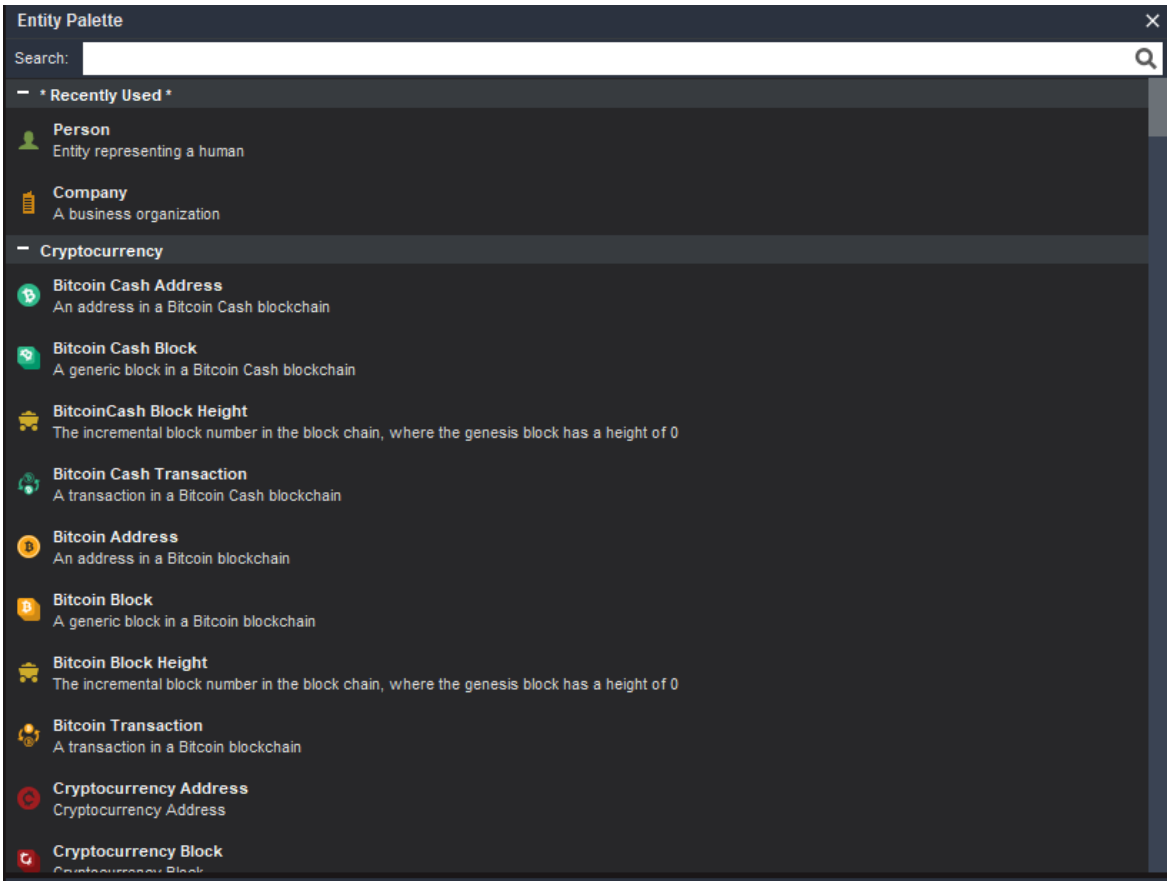


- ***Prompt utilizzato**:* filetype:pdf “Visiona Romantica” -site:linkedin.com
- ***Osservazione**:* L'analisi documentale ha permesso di stabilire che la società target si appoggia, per la distribuzione, alla partner "Columbia Pictures". Di conseguenza, l'infrastruttura digitale di riferimento è stata identificata nel dominio della casa madre "sonypictures.com".

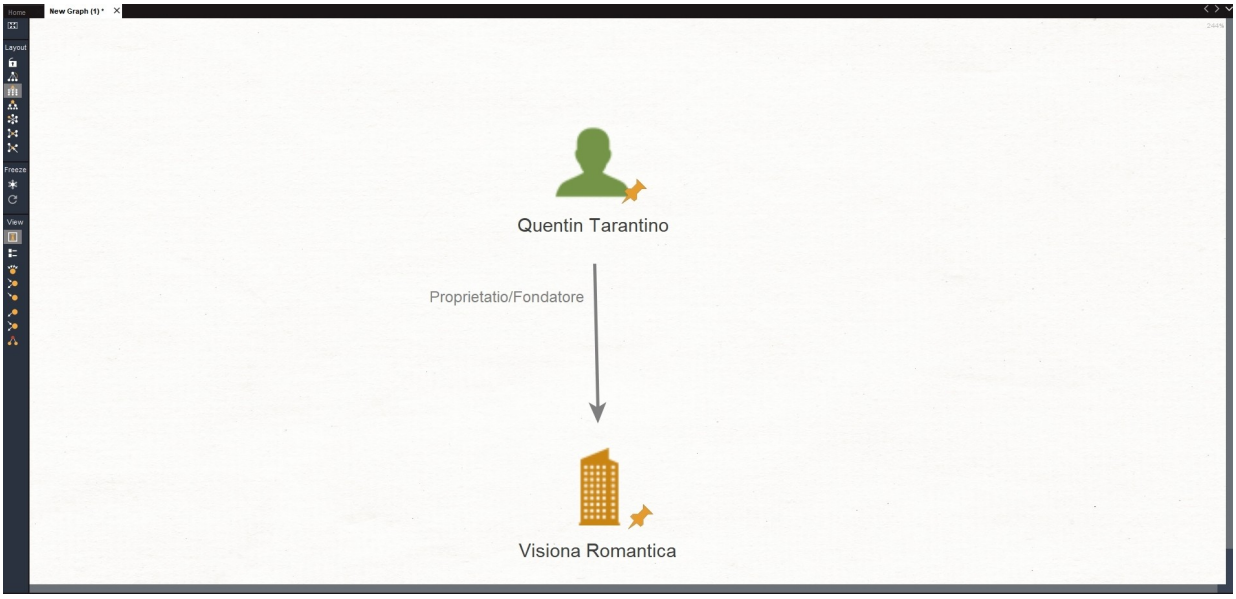
3.2 Esecuzione del Test / Attività su Maltego

Mappatura relazionale delle entità e analisi dell'infrastruttura DNS tramite trasformazioni Maltego.

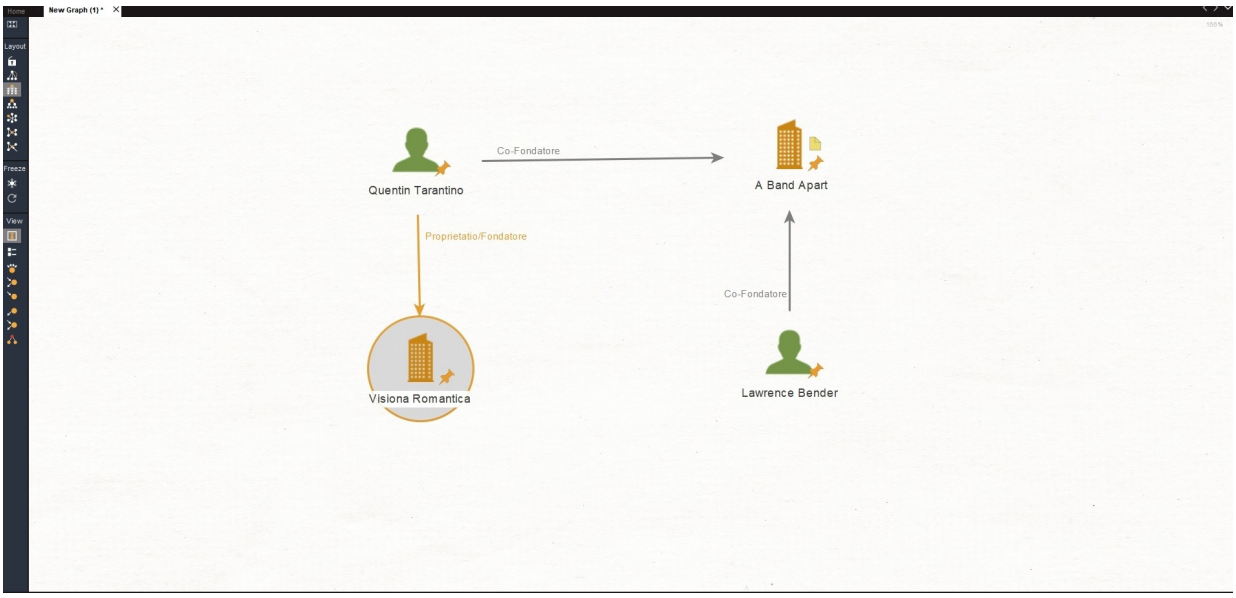
Per creare un grafico dettagliato selezioniamo l’entità che vogliamo inserire dalla nostra “Entity Palette”:



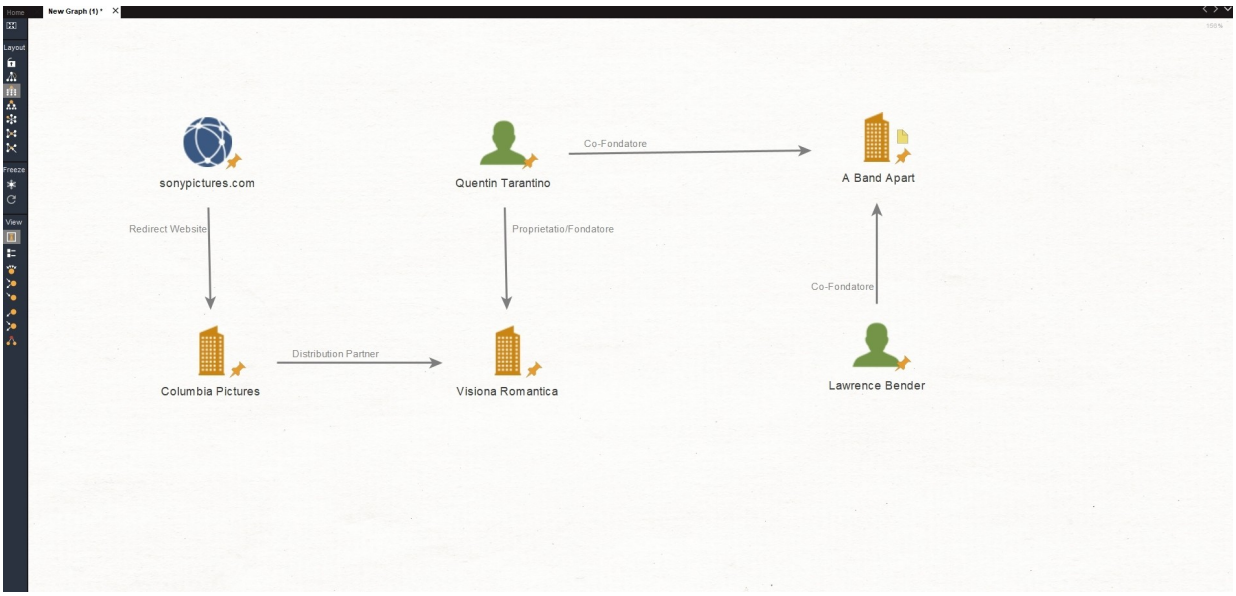
Successivamente importo nel grafico il nostro Target (Person → Quentin Tarantino) e la Società attualmente esistente (Company → Visiona Romantica):



Farò la stessa cosa con la vecchia Società (Company → A Band Apart) ed il suo vecchio socio (Person → Lawrence Bender):

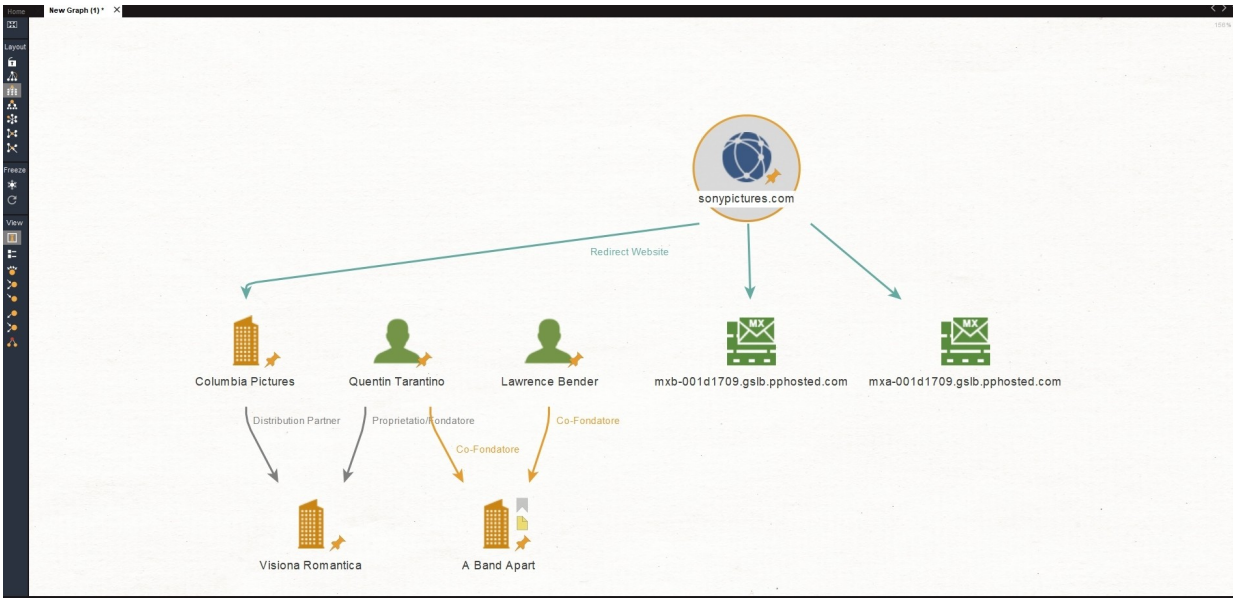


Inserirò per finire la compagnia partner Columbia Pictures ed il Domain a cui si appoggia (sonypictures.com):



Adesso che il nostro grafico è pronto possiamo provare ad effettuare un test sul sito sonypictures.com utilizzando La trasformazione “To DNS Name – MX” che individua il server fisico che si occupa della ricezione di email.

- ***Comando lanciato***: To DNS Name – MX
- ***Analisi dell'output***:



L'interrogazione dei record **DNS (MX)** su tale dominio ha rivelato l'utilizzo di server esterni gestiti da **Proofpoint** (`pphosted`), indicando la presenza di un servizio avanzato di filtraggio e sicurezza della posta elettronica.

4. Conclusione

Dall'attività di **Information Gathering** non sono emerse vulnerabilità critiche esposte (es. server non aggiornati o dati trapelati). Al contrario, la scelta di non gestire un'infrastruttura proprietaria ma di affidarsi a un partner Enterprise (Sony) ha drasticamente ridotto il rischio di potenziali minacce (superficie di attacco).