

Relazione Tecnica : Report Info Ghatering

Il presente report documenta una **simulazione della fase di *Information Gathering***, condotta nell'ambito di un esercizio didattico finalizzato alla comprensione e all'applicazione pratica delle principali tecniche di raccolta di informazioni da fonti aperte.

L'obiettivo dell'attività è quello di **familiarizzare con strumenti e metodologie tipiche della fase iniziale di un assessment di sicurezza**, concentrandosi esclusivamente su dati pubblicamente accessibili. In particolare, l'esercizio mira a sviluppare la capacità di individuare, correlare e analizzare informazioni eterogenee, valutandone attendibilità, pertinenza e valore informativo.

Come *target* della simulazione è stato selezionato **Alessandro Del Piero**, figura pubblica di rilievo internazionale.

La fase di raccolta delle informazioni è stata condotta utilizzando principalmente:

- **Google**, come strumento di primo livello per l'individuazione di informazioni generali, contenuti testuali, profili social, riferimenti mediatici e documentazione pubblica;
- **Maltego**, per l'analisi strutturata delle relazioni tra entità (persone, organizzazioni, domini, piattaforme online), con l'obiettivo di visualizzare connessioni, pattern ricorrenti e possibili correlazioni non immediatamente evidenti

Raccolta di Informazioni con Google :

Come primo step dell'attività, al fine di costruire una base di conoscenza iniziale del target, è stato utilizzato **Google** come motore di ricerca. Grazie alle sue funzionalità, è stato possibile raccogliere e organizzare un insieme significativo di informazioni pubbliche utili a delineare il profilo di **Alessandro Del Piero**.

Per avere una ricerca più dettagliata e accurata è stata impiegata una funzione specifica di Google ovvero, **Google Dorking** (o **Google Hacking**) una tecnica avanzata di ricerca su Google che utilizza operatori speciali per trovare informazioni specifiche, file, directory o vulnerabilità di siti web, spesso non accessibili tramite le ricerche standard, sfruttando la sua capacità di indicizzare vasti contenuti.

Siamo partiti da una query semplice per delineare il suo profilo ovvero:

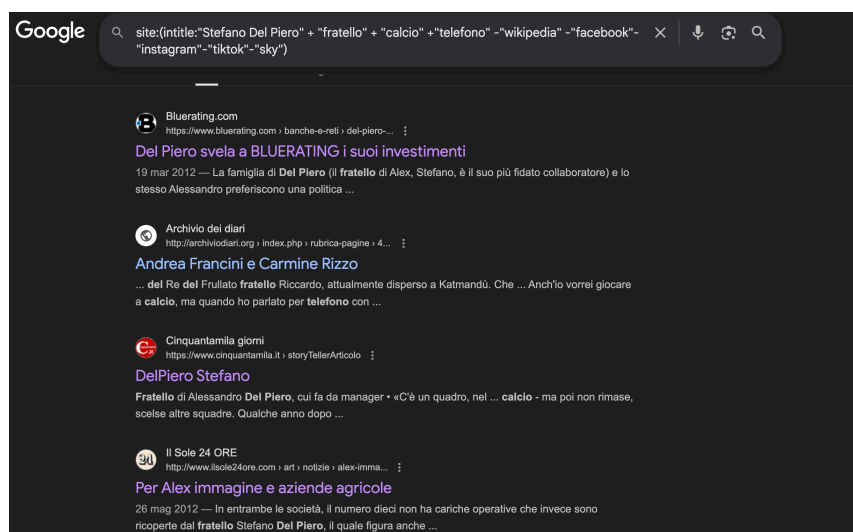
- **Query: "Del Piero" "profilo ufficiale" "famiglia"**

Dalle quali abbiamo ricavato i seguenti dati :

- **Nome completo:** Alessandro Del Piero
- **Data di nascita:** 9 novembre 1974
- **Luogo di nascita:** Conegliano (Treviso), Italia
- **Altezza:** circa 174 cm
- **Soprannome:** *Pinturicchio* (coniato da Gianni Agnelli)
- **Moglie:** Sonia Amoruso (sposati dal 2005)
- **Figli :** Tobias, Dorotea e Sasha.
- **Fratello :** Stefano Del Piero, che è stato anche il suo procuratore

Successivamente abbiamo affinato la ricerca in quanto un personaggio pubblico così famoso propone tutta una serie di articoli di gossip fuori dal nostro campo di ricerca con un'altra query :

- `site:(intitle:"Stefano Del Piero" + "fratello" + "calcio" + "telefono" -"wikipedia" -"facebook" -"instagram" -"tiktok" -"sky")`



Dalla ricerca effettuata emerge che, dal punto di vista imprenditoriale, **Alessandro Del Piero** è coinvolto in diverse realtà societarie. In particolare, detiene una partecipazione minoritaria pari al 3% del capitale sociale nella *Società Agricola Terraveneta*, costituita nel novembre precedente e con sede a Conegliano. Partecipa inoltre alla *Hera S.S.*, altra azienda agricola operante nella medesima area geografica.

Il restante portafoglio societario comprende la *Edge Srl*, società specializzata nella gestione dei diritti d'immagine, e la *Olympic Srl*, attiva nel settore immobiliare, nella quale Del Piero detiene la maggioranza delle quote. In entrambe le società non ricopre ruoli operativi, affidati al fratello **Stefano Del Piero**, presente anche come azionista di minoranza.

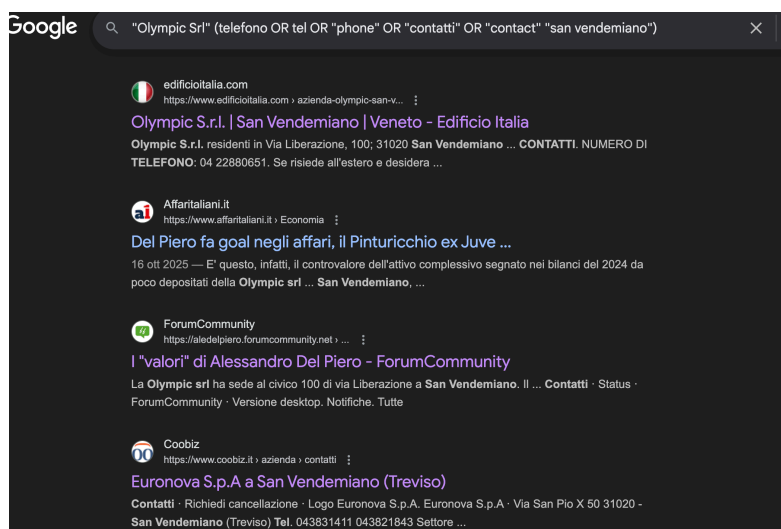
Tramite le query di ricerca sotto riportate è stato possibile individuare ulteriori informazioni di contatto e di contesto societario. In particolare, **Olympic S.r.l.**, con sede in **Via Liberazione 100, 31020 San Vendemiano (TV)**, risulta associata al seguente **numero di telefono pubblico: 0422 880651**.

È inoltre emerso che **Edge Srl**, (PEC: edgesrl@pec.it), anch'essa con sede in **Via Liberazione 100, San Vendemiano (TV)**, è coinvolta nella gestione dell'e-commerce "**Alessandro Del Piero Shop (ADP10)**", piattaforma ufficiale dedicata alla vendita di prodotti legati al brand di **Alessandro Del Piero**.

I dati individuati (sede legale, numero di telefono aziendale e collegamento tra le società) rientrano tra le informazioni pubbliche e non sensibili. Tuttavia, se correlati all'assetto societario e ai ruoli ricoperti, tali informazioni possono aumentare la superficie di attacco, in particolare in scenari di **Business Email Compromise (BEC)** e **social engineering**, rendendo più credibili tentativi di frode basati sull'impersonificazione di soggetti interni o partner aziendali.

QUERY DI RICERCA

- "Via Liberazione 100" "Edge Srl" "mail";
- "Olympic Srl" (telefono OR tel OR "phone" OR "contatti" OR "contact" "san vendemiano");
- "Olympic Srl" "Stefano Del Piero" ("amministratore" OR "legale rappresentante" OR "socio");

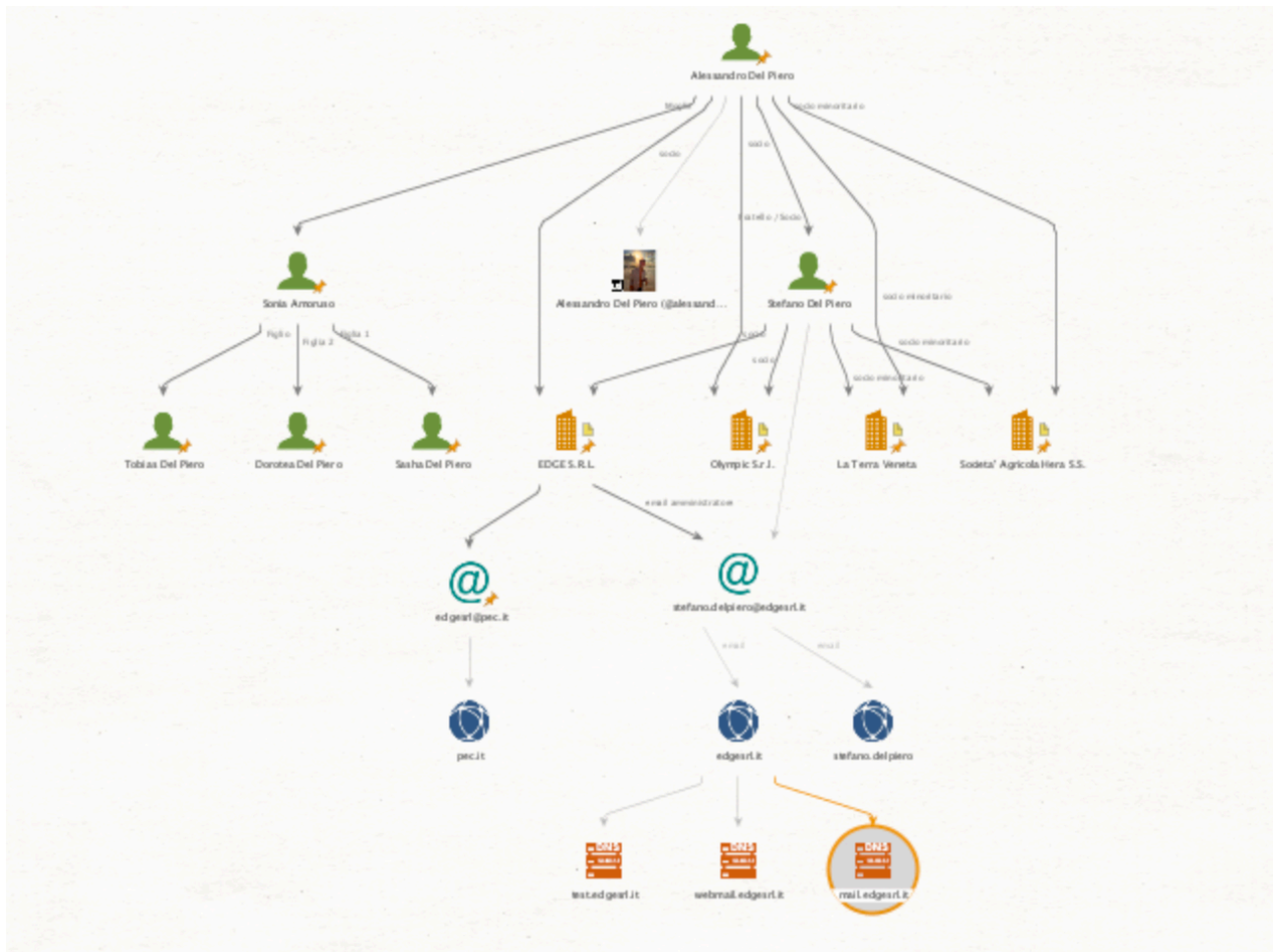


Anali Relazioni con Maltego :

Per approfondire le informazioni raccolte nella fase iniziale, è stato utilizzato **Maltego**, strumento OSINT che permette di analizzare e visualizzare le relazioni tra persone, aziende e altri elementi emersi durante la ricerca. L'utilizzo di Maltego consente di avere una visione più chiara e strutturata dei collegamenti tra le diverse entità.

Struttura della ricerca

La ricerca è stata avviata inserendo le entità principali identificate in precedenza (persone e società). A partire da queste, sono state applicate alcune migliorie per individuare ulteriori collegamenti e informazioni correlate. I risultati ottenuti sono stati infine organizzati in una rappresentazione grafica, utile per comprendere l'assetto societario e le relazioni tra i soggetti analizzati.



In particolare, l'attività si è concentrata sulla verifica dell'infrastruttura di posta elettronica tramite l'analisi dei record DNS principali (MX, sottodomini mail e webmail), al fine di validare la coerenza tra le aziende e gli indirizzi e-mail individuati.

I risultati ottenuti sono stati organizzati in una rappresentazione grafica che consente di distinguere tra dati direttamente osservabili e informazioni inferite, ciascuna accompagnata da un livello di confidenza.

Conclusioni

L'analisi ha permesso di ricostruire una visione d'insieme delle relazioni tra i soggetti analizzati, le società coinvolte e la relativa infrastruttura digitale, evidenziando come l'uso combinato di dati societari e tecnici consenta di ottenere informazioni rilevanti anche in assenza di accesso a fonti proprietarie.

L'utilizzo di Maltego si è dimostrato efficace non tanto per la scoperta automatica dei dati, quanto per la loro organizzazione, correlazione e valutazione critica.

Il progetto evidenzia inoltre l'importanza di distinguere tra informazioni verificate e inferenze basate su pattern tecnici, sottolineando il ruolo centrale della metodologia e della consapevolezza dei limiti degli strumenti OSINT.