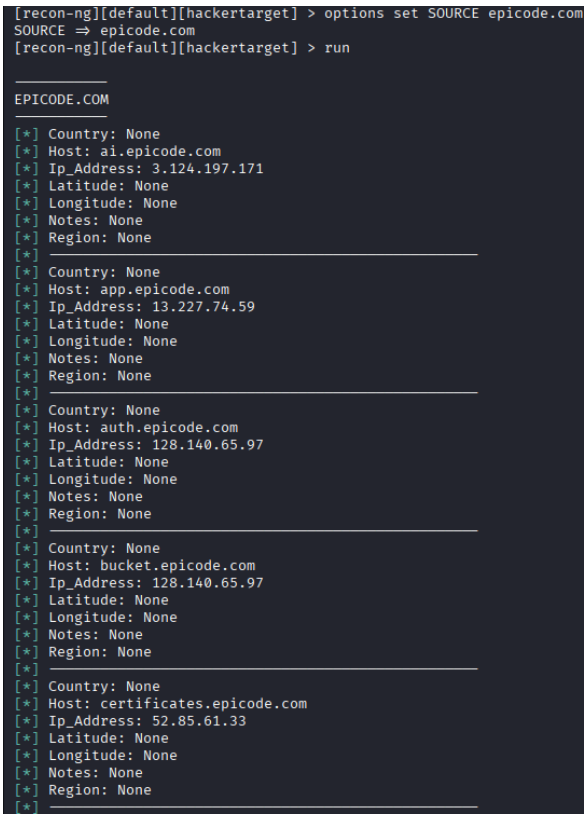
INDICE

INTRODUZIONE ED OBIETTIVO

INTRODUZIONE: l' attività svolta è stata orientata all'analisi OSINT di un dominio reale, con lo scopo di comprendere in modo pratico come individuare le risorse pubblicamente esposte da un'organizzazione e come correlarle a informazioni tecniche utili in un contesto di cybersecurity.
L'esercizio ha previsto l'utilizzo di strumenti per raccogliere dati su sottodomini, indirizzi IP, infrastrutture cloud, servizi accessibili e metadati DNS; l'intero processo ha permesso di osservare da vicino come viene strutturata la superficie d'attacco di un'azienda e quali informazioni possono essere ricavate senza effettuare alcuna interazione attiva o invasiva sui sistemi target.

OBIETTIVO: mappare la superficie esposta online del dominio tramite strumenti OSINT, identificando sottodomini, indirizzi IP, infrastrutture associate e informazioni tecniche utili alla valutazione iniziale di sicurezza.

RECORN-NG



Nella fase iniziale dell'attività è stata eseguita una ricognizione strutturata sul dominio principale per identificare eventuali servizi online collegati.
L'analisi ha permesso di individuare diversi sottodomini operativi, ciascuno associato al proprio indirizzo IP pubblico; questo tipo di mappatura consente di ottenere una visione completa dell'infrastruttura esposta su Internet, offrendo un quadro chiaro dei punti di accesso e delle componenti distribuite dell'organizzazione.
L'elenco dei sistemi rilevati comprende piattaforme applicative, ambienti di autenticazione, servizi di gestione documentale e altre risorse collegate, ognuna potenzialmente ospitata su provider differenti.

Per approfondire la comprensione dell'infrastruttura individuata nella fase precedente, sono stati analizzati gli indirizzi IP associati ai servizi rilevati; questa operazione ha permesso di ottenere informazioni sulla loro collocazione geografica e sui provider responsabili dell'hosting.

L'analisi ha evidenziato che i sistemi si appoggiano principalmente a infrastrutture distribuite in diverse aree geografiche, tra cui Stati Uniti ed Europa, con particolare concentrazione in Germania; i servizi risultano ospitati da provider internazionali di elevata affidabilità, come Amazon Web Services e CloudFront, il che indica l'utilizzo di piattaforme cloud moderne e scalabili.

Questa mappatura geografica permette di comprendere meglio come l'organizzazione distribuisce le proprie risorse digitali, quali aree del mondo servono da punto di erogazione e quali partner tecnologici vengono utilizzati.

```
EPICODE.COM

[*] URL: https://www.bing.com/search?first=0&q=domain%3Aepicode.com
[recon-ng][default][bing_domain_web] > show hosts

+--------+-------------------------------------------------+-----------------+---------+---------+----------+-----------+-------+-------------+
| rowid  |                      host                       |    ip_address   | region  | country | latitude | longitude | notes |    module   |
+--------+-------------------------------------------------+-----------------+---------+---------+----------+-----------+-------+-------------+
| 1      | ai.epicode.com                                  | 3.124.197.171   |         |         |          |           |       | hackertarget |
| 2      | app.epicode.com                                 | 13.227.74.59    |         |         |          |           |       | hackertarget |
| 3      | auth.epicode.com                                | 128.140.65.97   |         |         |          |           |       | hackertarget |
| 4      | bucket.epicode.com                              | 128.140.65.97   |         |         |          |           |       | hackertarget |
| 5      | certificates.epicode.com                        | 52.85.61.33     |         |         |          |           |       | hackertarget |
| 6      | cms.epicode.com                                 | 3.75.45.73      |         |         |          |           |       | hackertarget |
| 7      | console-bucket.epicode.com                      | 128.140.65.97   |         |         |          |           |       | hackertarget |
| 8      | cool.epicode.com                                | 128.140.65.97   |         |         |          |           |       | hackertarget |
| 9      | app.dev.epicode.com                             | 65.8.161.115    |         |         |          |           |       | hackertarget |
| 10     | cms.dev.epicode.com                             | 3.122.14.253    |         |         |          |           |       | hackertarget |
| 11     | learn.dev.epicode.com                           | 18.244.214.103  |         |         |          |           |       | hackertarget |
| 12     | ml.dev.epicode.com                              | 18.155.192.49   |         |         |          |           |       | hackertarget |
| 13     | talent.dev.epicode.com                          | 108.138.246.111 |         |         |          |           |       | hackertarget |
| 14     | docgen.epicode.com                              | 3.122.137.127   |         |         |          |           |       | hackertarget |
| 15     | exams.epicode.com                               | 52.85.61.35     |         |         |          |           |       | hackertarget |
| 16     | gol.epicode.com                                 | 185.158.133.1   |         |         |          |           |       | hackertarget |
| 17     | instituteoftechnology.epicode.com               | 35.207.141.200  |         |         |          |           |       | hackertarget |
| 18     | www.instituteoftechnology.epicode.com           | 35.207.141.200  |         |         |          |           |       | hackertarget |
| 19     | internal.epicode.com                            | 128.140.65.97   |         |         |          |           |       | hackertarget |
| 20     | keycloak.internal.epicode.com                   | 128.140.65.97   |         |         |          |           |       | hackertarget |
| 21     | kb.epicode.com                                  | 13.225.63.36    |         |         |          |           |       | hackertarget |
| 22     | keycloak-cwo08o44kgo4gkgs0ck0880g.epicode.com   | 128.140.65.97   |         |         |          |           |       | hackertarget |
| 23     | learn.epicode.com                               | 108.138.246.104 |         |         |          |           |       | hackertarget |
| 24     | libre.epicode.com                               | 128.140.65.97   |         |         |          |           |       | hackertarget |
| 25     | microlearn.epicode.com                          | 35.207.141.200  |         |         |          |           |       | hackertarget |
| 26     | www.microlearn.epicode.com                      | 35.207.141.200  |         |         |          |           |       | hackertarget |
| 27     | parser.epicode.com                              | 3.71.147.183    |         |         |          |           |       | hackertarget |
| 28     | render.epicode.com                              | 128.140.65.97   |         |         |          |           |       | hackertarget |
| 29     | s3.render.epicode.com                           | 128.140.65.97   |         |         |          |           |       | hackertarget |
| 30     | talent.epicode.com                              | 13.227.74.103   |         |         |          |           |       | hackertarget |
| 31     | trigger.epicode.com                             | 128.140.65.97   |         |         |          |           |       | hackertarget |
| 32     | uni.epicode.com                                 | 18.244.214.19   |         |         |          |           |       | hackertarget |
+--------+-------------------------------------------------+-----------------+---------+---------+----------+-----------+-------+-------------+

[*] 32 rows returned
[recon-ng][default][bing_domain_web] >
```

L’analisi ha permesso di identificare in modo strutturato l’insieme dei servizi digitali collegati al dominio principale dell’organizzazione.

L’elenco risultante comprende 32 sottodomini attivi, ciascuno dei quali rappresenta un componente specifico dell’infrastruttura online: piattaforme didattiche, portali di autenticazione, ambienti di sviluppo, servizi amministrativi e siti informativi.

Questa mappatura dettagliata permette di comprendere la distribuzione e la suddivisione funzionale dei servizi erogati, evidenziando la presenza di diverse piattaforme operative e ambienti dedicati.

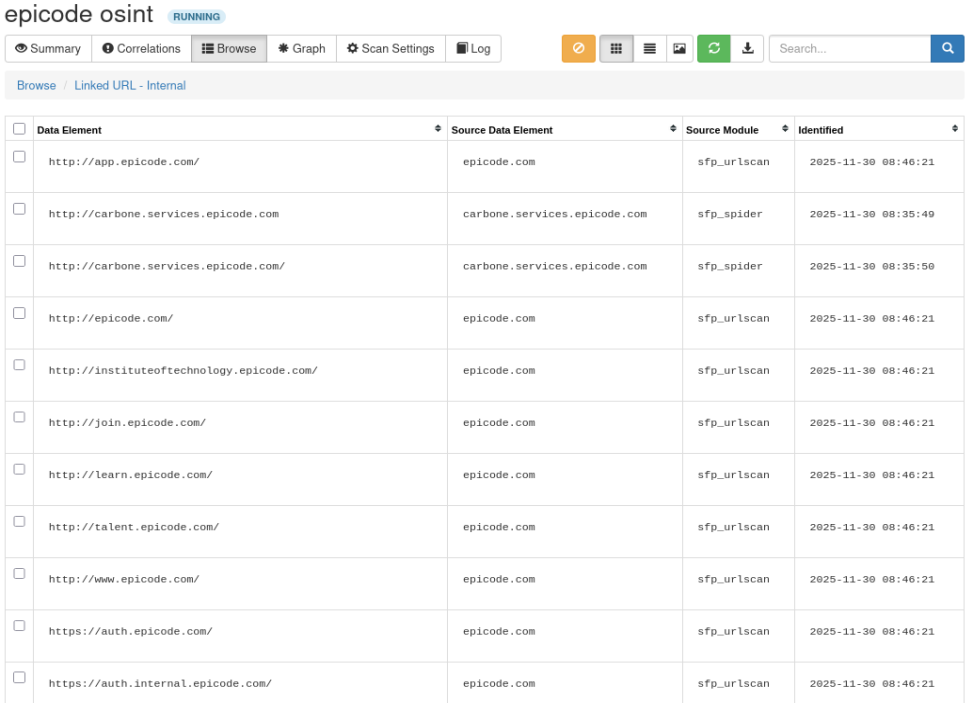
L’analisi mette inoltre in luce la varietà di indirizzi IP associati, con servizi ospitati su provider differenti, a conferma di un’architettura distribuita e articolata.

Il risultato fornisce una panoramica chiara e aggiornata della struttura online esistente, utile per qualunque attività di governance, pianificazione tecnica o ottimizzazione delle risorse digitali.

SPIDER FOOT

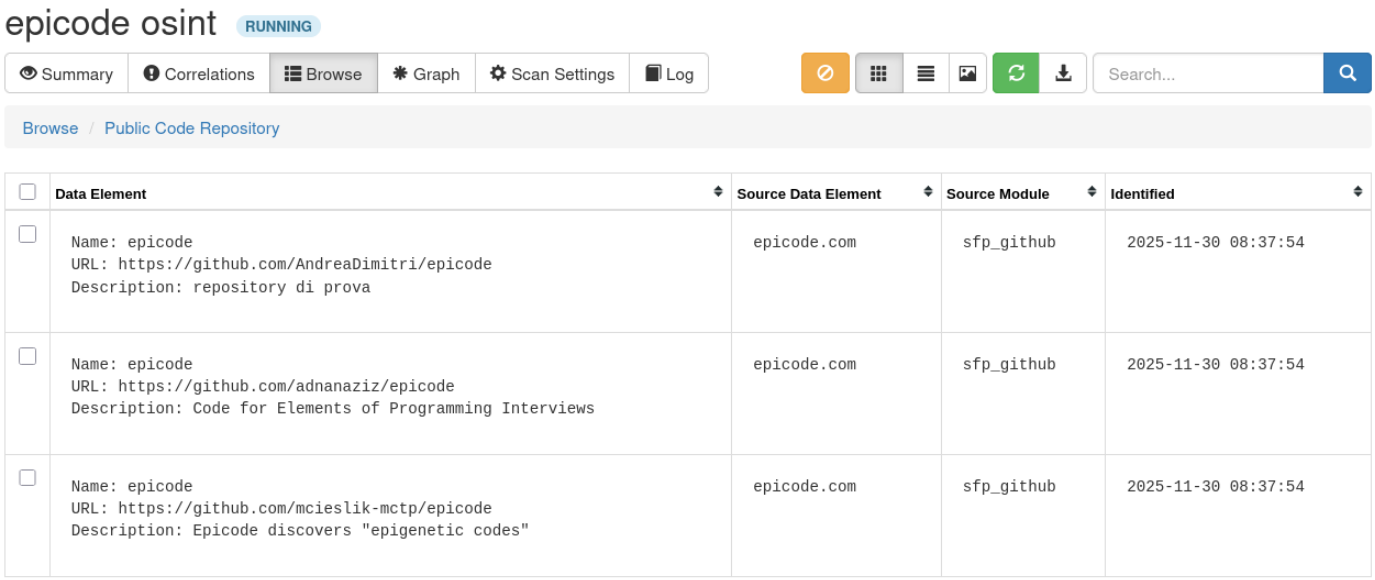
```
Session  Actions  Edit  View  Help
┌──(kali㉿kali)-[~]
└─$ sudo spiderfoot -l 127.0.0.1:5001
```

È stata attivata un'istanza locale dello strumento di analisi tramite un comando dedicato, che ha permesso l'esecuzione del servizio sulla macchina di lavoro.
L'interfaccia è stata resa disponibile in ambiente locale all'indirizzo *127.0.0.1:5001* (scovato in precedenza), consentendo di avviare le successive attività di raccolta e consultazione delle informazioni in modo centralizzato e strutturato.



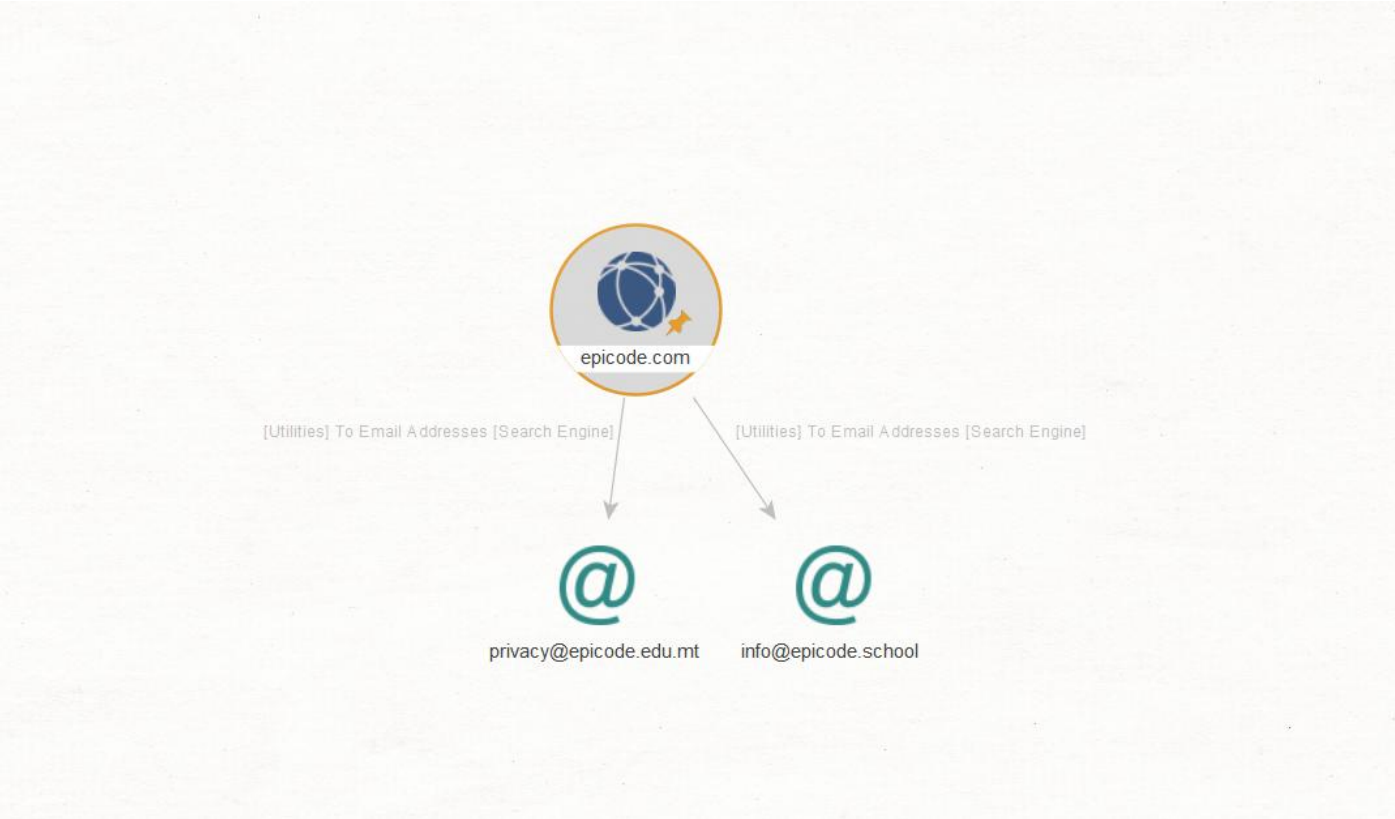
Data Element	Source Data Element	Source Module	Identified
http://app.epicode.com/	epicode.com	sfp_urlscan	2025-11-30 08:46:21
http://carbone.services.epicode.com	carbone.services.epicode.com	sfp_spider	2025-11-30 08:35:49
http://carbone.services.epicode.com/	carbone.services.epicode.com	sfp_spider	2025-11-30 08:35:50
http://epicode.com/	epicode.com	sfp_urlscan	2025-11-30 08:46:21
http://instituteoftechnology.epicode.com/	epicode.com	sfp_urlscan	2025-11-30 08:46:21
http://join.epicode.com/	epicode.com	sfp_urlscan	2025-11-30 08:46:21
http://learn.epicode.com/	epicode.com	sfp_urlscan	2025-11-30 08:46:21
http://talent.epicode.com/	epicode.com	sfp_urlscan	2025-11-30 08:46:21
http://www.epicode.com/	epicode.com	sfp_urlscan	2025-11-30 08:46:21
https://auth.epicode.com/	epicode.com	sfp_urlscan	2025-11-30 08:46:21
https://auth.internal.epicode.com/	epicode.com	sfp_urlscan	2025-11-30 08:46:21

L'analisi ha restituito un insieme di collegamenti interni riconducibili alla presenza online dell'organizzazione.
Questi indirizzi rappresentano sezioni, servizi e piattaforme operative legate al dominio principale e mostrano come l'infrastruttura web sia suddivisa in diverse aree funzionali, ciascuna dedicata a specifiche attività amministrative, formative o di accesso ai servizi.
L'elenco ottenuto evidenzia la presenza di più portali secondari (ad esempio ambienti di autenticazione, aree informative, piattaforme educative, spazi dedicati agli studenti e servizi gestionali), confermando un ecosistema digitale articolato e distribuito. Ogni elemento è stato identificato riportandone l'origine e la data di rilevazione, consentendo una visione chiara e strutturata della configurazione attuale.

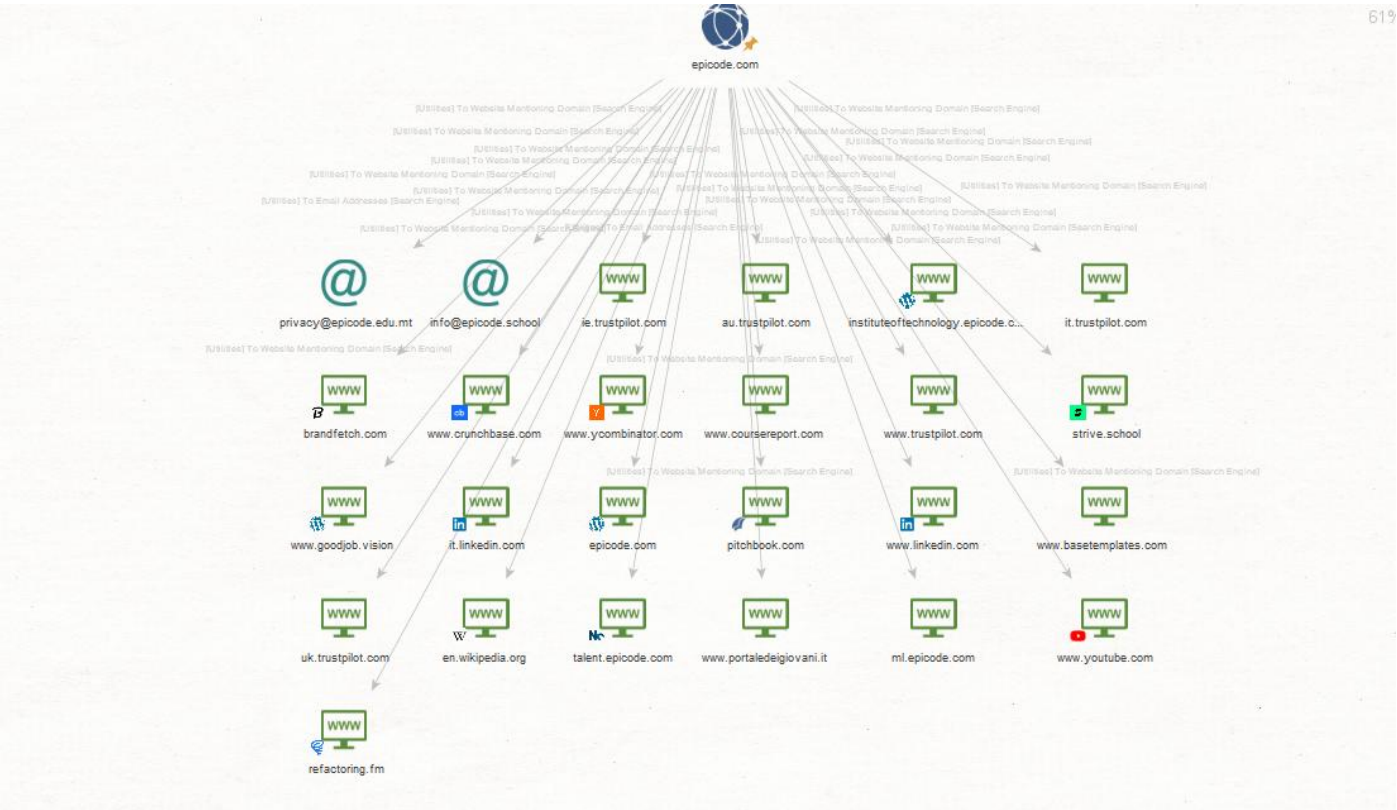


Durante l'analisi sono stati individuati alcuni repository di codice sorgente pubblicamente disponibili.
Questi elementi risultano collegati al dominio aziendale e rappresentano contenuti creati o gestiti da professionisti che operano (o hanno operato) in relazione all'organizzazione.
I repository rilevati contengono materiali quali progetti dimostrativi, componenti software e risorse didattiche.
La loro presenza offre una panoramica sulla produzione tecnica associata all'organizzazione e conferma l'esistenza di contributi distribuiti su più profili esterni, ciascuno con finalità e contenuti differenti.
Ogni voce è stata raccolta indicando il collegamento pubblico, la descrizione fornita dall'autore e il collegamento con il dominio principale, fornendo così una visione chiara e ordinata delle risorse attualmente reperibili in rete.

MALTEGO



Dall'analisi svolta emergono alcuni indirizzi di posta elettronica direttamente collegati ai domini ufficiali dell'organizzazione.
Si tratta di recapiti la cui individuazione è rilevante perché permette di comprendere **quali canali l'organizzazione espone al pubblico** e quindi quali punti risultano potenzialmente raggiungibili da interlocutori esterni.



L'analisi ha prodotto una rappresentazione strutturata delle relazioni esterne associate al dominio principale.
La mappa mostra come l'organizzazione sia richiamata, citata o collegata da diversi portali pubblici, piattaforme professionali e servizi terzi.
I domini e i servizi visualizzati includono, ad esempio, piattaforme di valutazione, canali social, siti informativi, portali dedicati alla formazione, repository pubblici e pagine istituzionali.
La loro comparsa evidenzia i punti in cui il nome dell'ente viene menzionato o referenziato, delineando così una panoramica chiara della visibilità esterna e delle interazioni digitali attualmente accessibili.
Questa mappatura consente di comprendere come il marchio e i contenuti dell'organizzazione siano distribuiti nello spazio online, quali soggetti terzi lo citino e quali portali risultino connessi alla sua identità digitale.

CONCLUSIONE

L’analisi ha fornito una visione completa dell’esposizione digitale associata al dominio, mettendo in evidenza sia la struttura interna dei servizi online sia le relazioni esterne generate da citazioni, collegamenti e riferimenti pubblici.
L’insieme dei risultati permette di delineare in modo chiaro come l’organizzazione sia rappresentata nel panorama web, quali servizi risultino attivi e quali portali terzi contribuiscano alla sua visibilità.
Questa panoramica costituisce un punto di riferimento utile per valutare la coerenza dell’identità digitale, monitorare la distribuzione delle informazioni e supportare eventuali decisioni strategiche legate alla comunicazione, alla presenza online e alla gestione dei servizi erogati. Nel complesso, la mappatura ottenuta offre una base solida per una governance digitale più consapevole ed efficace.