

# OSINT INVESTIGATION REPORT

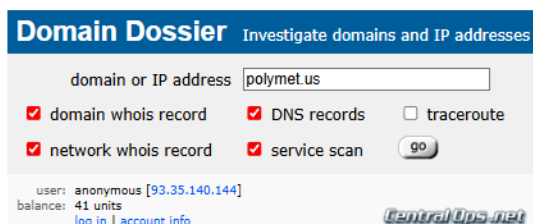
Target: *Polymet Corporation*      Domain: *polymet.us*

## 1. Target Overview

Il target designato per l'attività di Open Source Intelligence (OSINT) è Polymet Corporation, il cui dominio principale è polymet.us. L'organizzazione è una Manufacturing Company con sede negli Stati Uniti.

## 2. Domain Intelligence & Infrastructure

Utilizzando la risorsa OSINT Framework (nello specifico il tool *Domain Dossier*), è stata effettuata un'analisi dei record di registrazione e dell'infrastruttura di rete. Di seguito l'evidenza raccolta:



To obtain Whois data redacted because of the GDPR or privacy services, try ICANN's RDRS. [more information]

### Address lookup

canonical name **polymet.us.**  
aliases  
addresses **208.109.214.23**

### Domain Whois record

Queried **whois.nic.us** with "polymet.us"...

```
Domain Name: polymet.us
Registry Domain ID: D2744575-US
Registrar WHOIS Server: whois.ionos.com
Registrar URL: https://ionos.com
Updated Date: 2025-09-22T00:00:09Z
Creation Date: 2002-08-08T18:25:33Z
Registry Expiry Date: 2026-08-07T23:59:59Z
Registrar: IONOS SE
Registrar IANA ID: 83
Registrar Abuse Contact Email: abuse@ionos.com
Registrar Abuse Contact Phone: +1.8772064253
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Registry Registrant ID: C60276248-US
Registrant Name: Steve Wilson
Registrant Organization: Polymet Corporation
Registrant Street: 7397 Union Centre Blvd
Registrant Street:
Registrant Street:
Registrant City: West Chester
Registrant State/Province: OH
Registrant Postal Code: 45014
Registrant Country: US
Registrant Phone: +1.5138741123
Registrant Phone Ext:
Registrant Fax:
Registrant Fax Ext:
Registrant Email: helpdesk@polymet.us
Registrant Application Purpose: P1
Registrant Nexus Category: C21
Registry Admin ID: C60276249-US
Admin Name: Steve Wilson
Admin Organization: Polymet Corporation
Admin Street: 7397 Union Centre Blvd
```

```
Admin City: West Chester
Admin State/Province: OH
Admin Postal Code: 45014
Admin Country: US
Admin Phone: +1.5138741123
Admin Phone Ext:
Admin Fax:
Admin Fax Ext:
Admin Email: helpdesk@polymet.us
Admin Application Purpose: P1
Admin Nexus Category: C21
Registry Tech ID: C4543631-US
Tech Name: Hostmaster ONEANDONE
Tech Organization: 1&1 Internet Inc.
Tech Street: 701 Lee Rd.
Tech Street: Suite 300
Tech Street:
Tech City: Chesterbrook
Tech State/Province: PA
Tech Postal Code: 19087
Tech Country: US
Tech Phone: +1.8774612631
Tech Phone Ext:
Tech Fax: +1.6105601501
Tech Fax Ext:
Tech Email: hostmaster@1and1.com
Name Server: ns1069.ui-dns.com
Name Server: ns1069.ui-dns.de
Name Server: ns1069.ui-dns.org
Name Server: ns1069.ui-dns.biz
DNSSEC: unsigned
```

### Service scan

```
FTP - 21      Error: Timeout
SMTP - 25     Error: Timeout
HTTP - 80     HTTP/1.1 301 Moved Permanently
               Date: Sat, 29 Nov 2025 16:20:49 GMT
               Server: Apache
               Expires: Sat, 29 Nov 2025 17:20:50 GMT
               Cache-Control: max-age=3600
               X-Redirect-By: WordPress
               Upgrade: h2,h2c
               Connection: Upgrade, close
               Location: https://www.polymet.us/
               Vary: Accept-Encoding
               Content-Type: text/html; charset=UTF-8
```

L'analisi dell'output ha evidenziato le seguenti informazioni critiche:

- **Network Address:** Il dominio risolve sull'indirizzo IP **208.109.214.23**.

- **WHOIS Exposure:** I dati di registrazione non sono offuscati da servizi di privacy (GDPR redaction assente per i dati US), esponendo dettagli diretti dell'organizzazione.
- **Key Individuals:** È stato identificato **Steve Wilson** come *Registrant* e *Admin Name*.
- **Contact Vectors:** È presente un indirizzo email funzionale **helpdesk@polymet.us** e un numero di telefono diretto (+1.513...), oltre alla localizzazione fisica confermata a West Chester, OH.

### 3. Ricognizione Google Dorks

In questa fase è stata condotta un'attività di ricognizione utilizzando operatori di ricerca avanzata (**Google Dorks**) per identificare informazioni indicizzate pubblicamente.

#### 3.1 Site Structure Enumeration

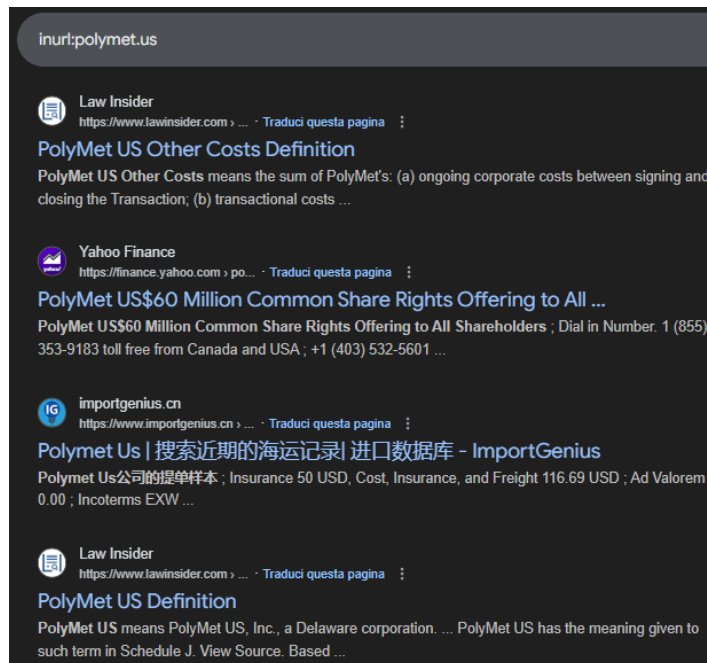
Dork Used: *site:polymet.us*



**Funzione del comando:** Questo operatore restringe la ricerca esclusivamente al dominio target, permettendo di elencare tutte le pagine e le risorse pubblicamente indicizzate da Google per mappare la struttura del sito.

### 3.2 External URL Enumeration

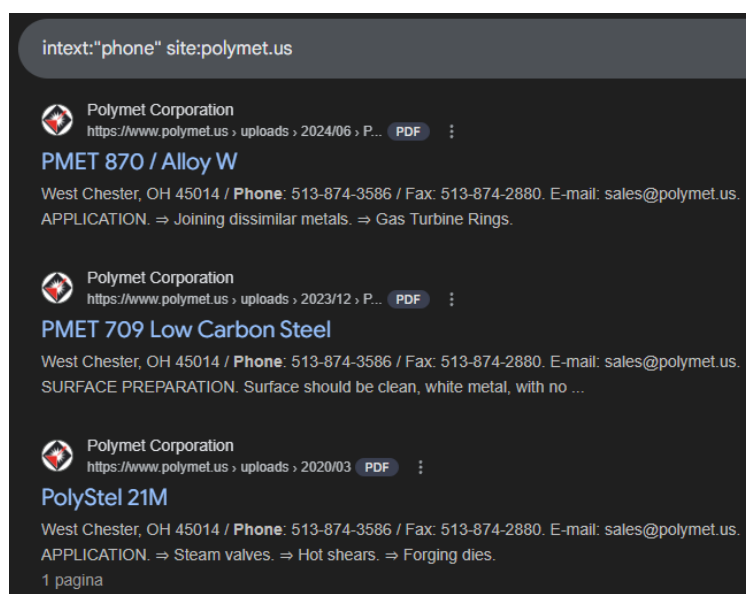
Dork Used: *inurl:polymet.us*



**Funzione del comando:** Questo operatore ricerca la stringa "polymet.us" all'interno degli URL di qualsiasi dominio indicizzato. È essenziale per individuare riferimenti esterni come documenti legali, report finanziari o record logistici ospitati su piattaforme terze.

### 3.3 Contact Information Extraction

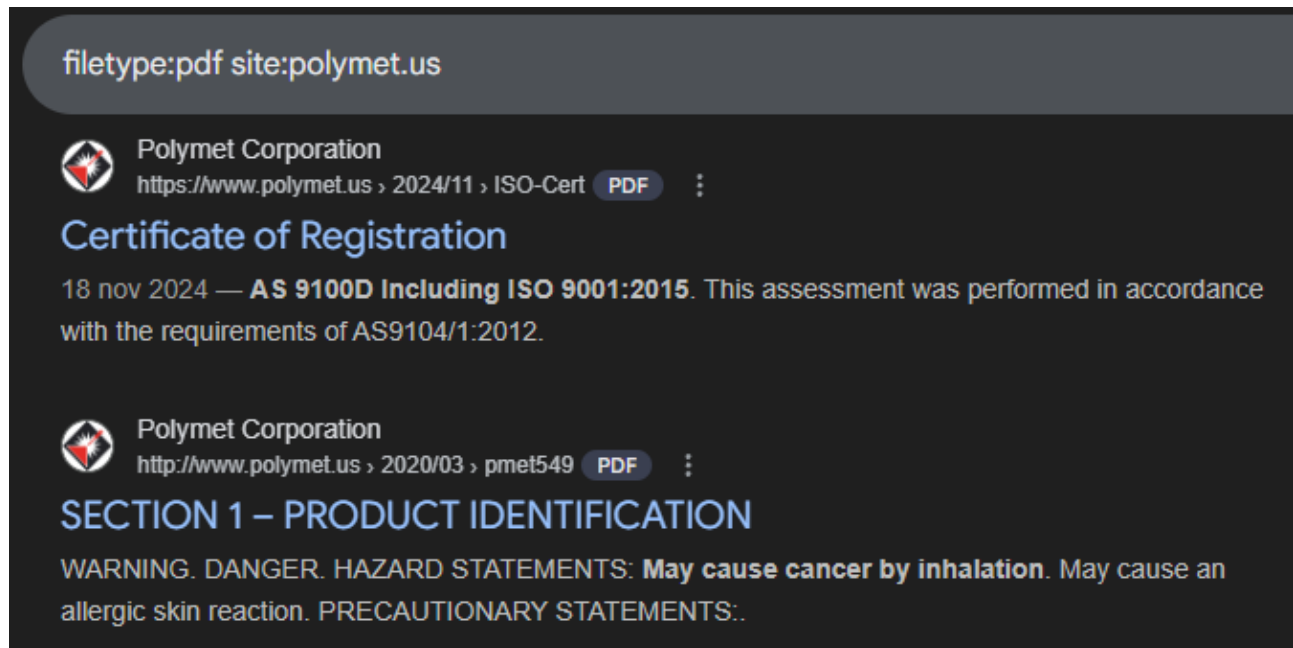
Dork Used: *intext:"phone" site:polymet.us*



**Funzione del comando:** Questo operatore forza la ricerca della stringa "phone" all'interno del testo visibile delle pagine o dei documenti ospitati sul dominio target. È una tecnica efficace per isolare rapidamente contatti telefonici, indirizzi email (come [sales@polymet.us](mailto:sales@polymet.us)) ecc.

### 3.4 File Type Enumeration

Dork Used: *filetype:pdf site:polymet.us*



**Funzione del comando:** Questo operatore isola i file con estensione .pdf ospitati sul dominio target. Permette l'esfiltrazione di documentazione aziendale statica come certificazioni di qualità, schede tecniche e manuali operativi che spesso contengono metadati o dettagli procedurali non presenti nelle pagine web standard.

### 3.5 Directory Listing

Dork Used: *site:polymet.us intitle:index.of inurl:admin*



**Funzione del comando:** Questo operatore combina la ricerca di directory aperte ("index.of") con keyword legate a percorsi amministrativi ("admin"). Il risultato evidenzia una directory esposta, permettendo in questo caso di identificare il Content Management System in uso (**WordPress**).

### 4. Content Discovery: Directory Listing Exploration

Facendo seguito all'identificazione della directory esposta, è stata eseguita una navigazione manuale del percorso /wp-content/themes/enfold/framework/php

## Index of /wp-content/themes/enfold/framework/php

Name	Last modified	Size	Description
<a href="#">Parent Directory</a>		-	
<a href="#">admin-notices/</a>	2024-09-02 21:12	-	
<a href="#">auto-updates/</a>	2024-08-22 20:25	-	
<a href="#">base-classes/</a>	2024-08-22 20:25	-	
<a href="#">class-accessibility.php</a>	2024-08-22 20:25	1.7K	
<a href="#">class-admin-notices.php</a>	2024-08-22 20:25	23K	
<a href="#">class-adminpages.php</a>	2024-08-22 20:25	8.9K	
<a href="#">class-breadcrumb-tra.&gt;</a>	2024-08-22 20:25	26K	
<a href="#">class-cpt-support.php</a>	2024-08-22 20:25	15K	
<a href="#">class-database-optio.&gt;</a>	2024-08-22 20:25	2.4K	
<a href="#">class-duplicate-post.&gt;</a>	2024-08-22 20:25	8.0K	
<a href="#">class-form-generator.&gt;</a>	2024-08-22 20:25	50K	
<a href="#">class-gmaps.php</a>	2024-08-22 20:25	19K	
<a href="#">class-grecaptcha.php</a>	2024-08-22 20:25	32K	
<a href="#">class-htmlhelper.php</a>	2024-08-22 20:25	96K	
<a href="#">class-media.php</a>	2024-08-22 20:25	15K	
<a href="#">class-megamenu.php</a>	2024-08-22 20:25	25K	
<a href="#">class-metabox.php</a>	2024-08-22 20:25	8.9K	
<a href="#">class-responsive-ima.&gt;</a>	2024-08-22 20:25	36K	
<a href="#">class-sidebar-genera.&gt;</a>	2024-08-22 20:25	6.3K	
<a href="#">class-style-generato.&gt;</a>	2024-08-22 20:25	24K	
<a href="#">class-superobject.php</a>	2024-08-22 20:25	14K	
<a href="#">class-svg-images.php</a>	2024-08-22 20:25	16K	
<a href="#">font-management/</a>	2024-08-22 20:25	-	
<a href="#">function-set-avia-aj.&gt;</a>	2024-08-22 20:25	34K	
<a href="#">function-set-avia-ba.&gt;</a>	2024-08-22 20:25	29K	
<a href="#">function-set-avia-fr.&gt;</a>	2024-08-22 20:25	72K	
<a href="#">inc-autoconfig.php</a>	2024-08-22 20:25	8.5K	
<a href="#">inc-avia-download-de.&gt;</a>	2024-08-22 20:25	4.1K	
<a href="#">inc-avia-importer.php</a>	2024-08-22 20:25	7.9K	
<a href="#">widgets/</a>	2024-08-22 20:25	-	
<a href="#">wordpress-importer/</a>	2024-08-22 20:25	-	

**Analisi tecnica:** L'assenza di protezioni sul server permette a chiunque di vedere l'elenco dei file che compongono il sito. L'analisi rivela due problemi principali:

- **Accesso ai file di programmazione:** Sono visibili file interni (come *class-database-options.php* e *class-form-generator.php*) che dovrebbero rimanere nascosti. Questo permette a un malintenzionato di studiare "come è fatto" il sito per trovare punti deboli.
- **Mancata manutenzione del sito:** Le date di ultima modifica dei file risalgono ad agosto 2024, è evidente che il sistema non viene aggiornato da oltre un anno, rendendolo vulnerabile a problemi di sicurezza già noti.

**Conclusione:** Sono state rilevate numerose vulnerabilità con una fase di OSINT abbastanza superficiale, se dovessi analizzare tramite altri tool la gerarchia dell'azienda (possibilmente partendo dall'admin name individuato) potrei scoprire altre cose sulla compagnia e su chi ne fa parte.