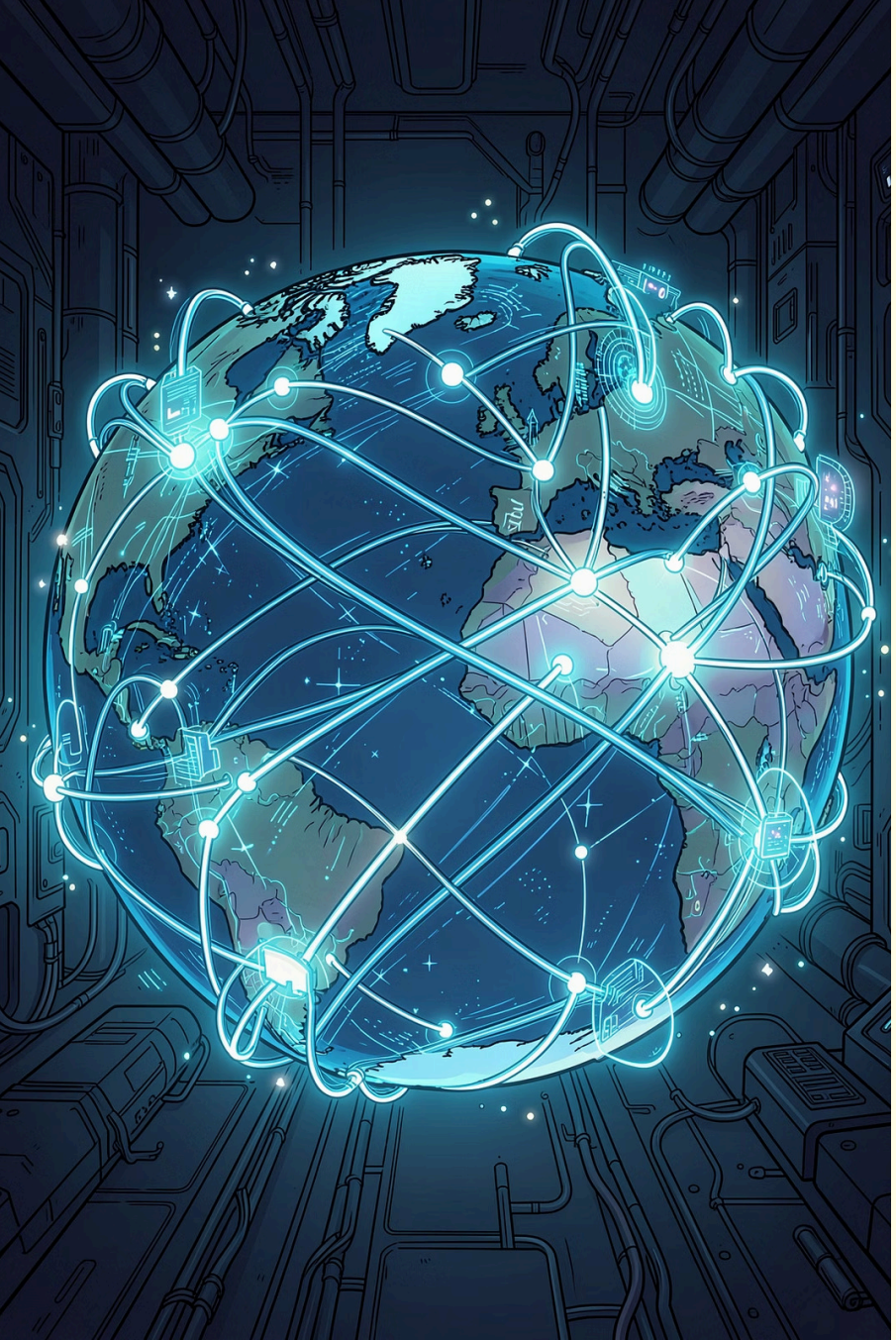


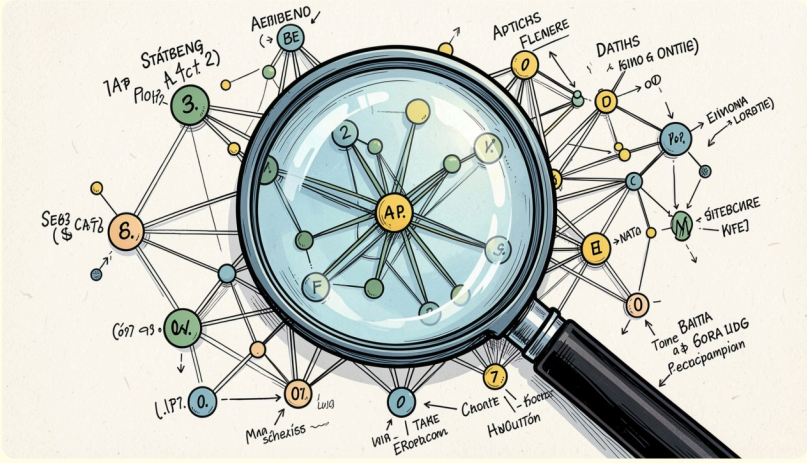
Maltego: Як розкрити таємниці інтернету

Інструмент для візуалізації та аналізу відкритих джерел інформації

Що таке Maltego?

Maltego — це **потужний інструмент OSINT** (розвідка за відкритими джерелами), призначений для збору, аналізу та візуалізації інформації з публічно доступних джерел.

- Він перетворює хаотичні фрагменти даних на **зрозумілий граф**, що допомагає виявити приховані зв'язки.
- Завдяки своїй здатності візуалізувати логічні зв'язки, Maltego стає незамінним помічником у складних розслідуваннях.



Три стовпи роботи Maltego

Entities (Об'єкти)

Це основні елементи, які ви досліджуєте: люди, домени, IP-адреси, телефонні номери, електронні пошти та багато іншого. Кожен об'єкт є вузлом у вашому графі.

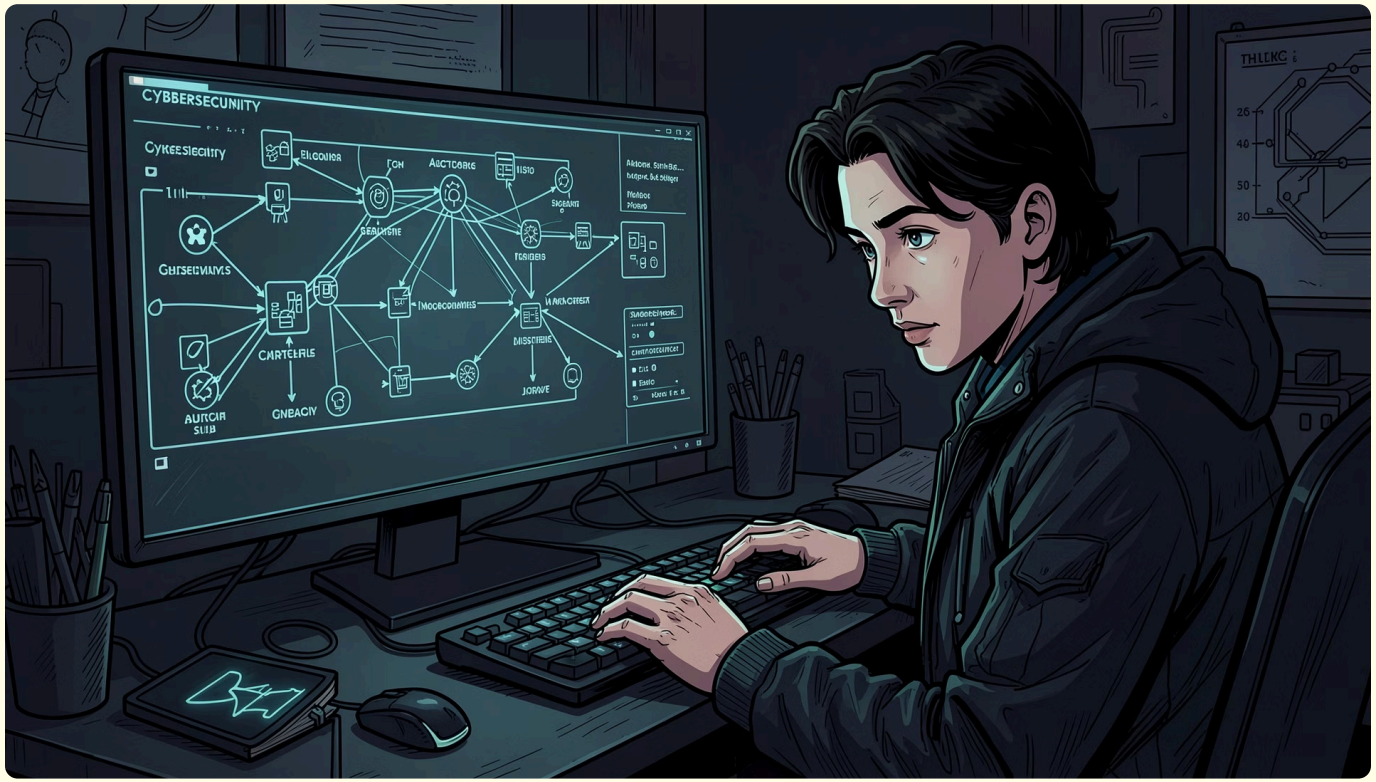
Transforms (Трансформації)

Автоматизовані запити, які Maltego виконує для збору інформації про об'єкти. Вони взаємодіють з базами даних та API, розширюючи ваш граф новими даними.

Links (Зв'язки)

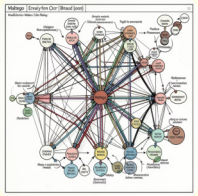
Візуальні лінії, що поєднують знайдені факти та об'єкти. Вони показують взаємозв'язки між різними частинами інформації, допомагаючи будувати повну картину.

Де це використовується?



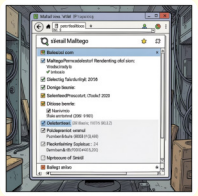
- **Кібербезпека:** аналіз інфраструктури, виявлення вразливостей, розслідування інцидентів та відстеження кіберзлочинців.
- **Правоохоронні органи:** розслідування злочинів, пошук підозрюваних та збір доказів за допомогою відкритих джерел.
- **OSINT-розвідка:** перевірка фактів, пошук людей, аналіз репутації та збір даних для бізнес-розвідки.
- **Журналістські розслідування:** викриття корупції, пошук прихованих зв'язків між компаніями та особами.

Інтерфейс: ваш робочий простір



Graph View

Це центральна область, де ви будуєте та візуалізуєте свої розслідування. Тут відображаються всі об'єкти та зв'язки між ними, формуючи інтерактивний граф.



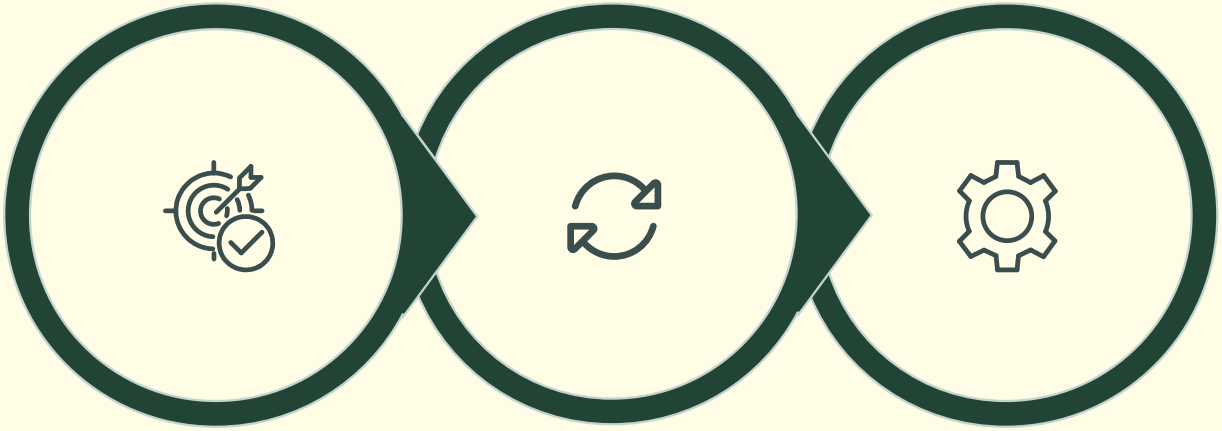
Detail View

Ця панель надає детальну інформацію про обраний об'єкт. Ви можете переглядати його властивості, атрибути та інші релевантні дані, що допомагає глибше зануритися в дослідження.

Transform Output

Тут відображається лог виконання всіх операцій та пошукових запитів. Це дозволяє відстежувати хід розслідування, перевіряти результати Transforms та виявляти можливі помилки.

Перші кроки: збір інформації



Вибір точки

Запуск Transforms

Машини аналізу

Почніть з вибору ключової інформації, наприклад, доменного імені або електронної пошти. Запустіть відповідні Transforms, щоб автоматично зібрати пов'язані дані, такі як IP-адреси, інші домени або контактні дані. Для більш глибокого аналізу використовуйте вбудовані "Machines", які проводять комплексні розслідування за вас.

Головні поради для ефективності

- **Використовуйте Community Edition**

  Для початківців та навчання ідеально підійде безкоштовна версія Maltego Community Edition. Вона надає достатньо функціоналу для освоєння основ OSINT.

- **Регулюйте "Number of Results"**

  У налаштуваннях Transforms ви можете контролювати кількість результатів, що повертаються. Це допоможе уникнути перевантаження графа надмірною інформацією.

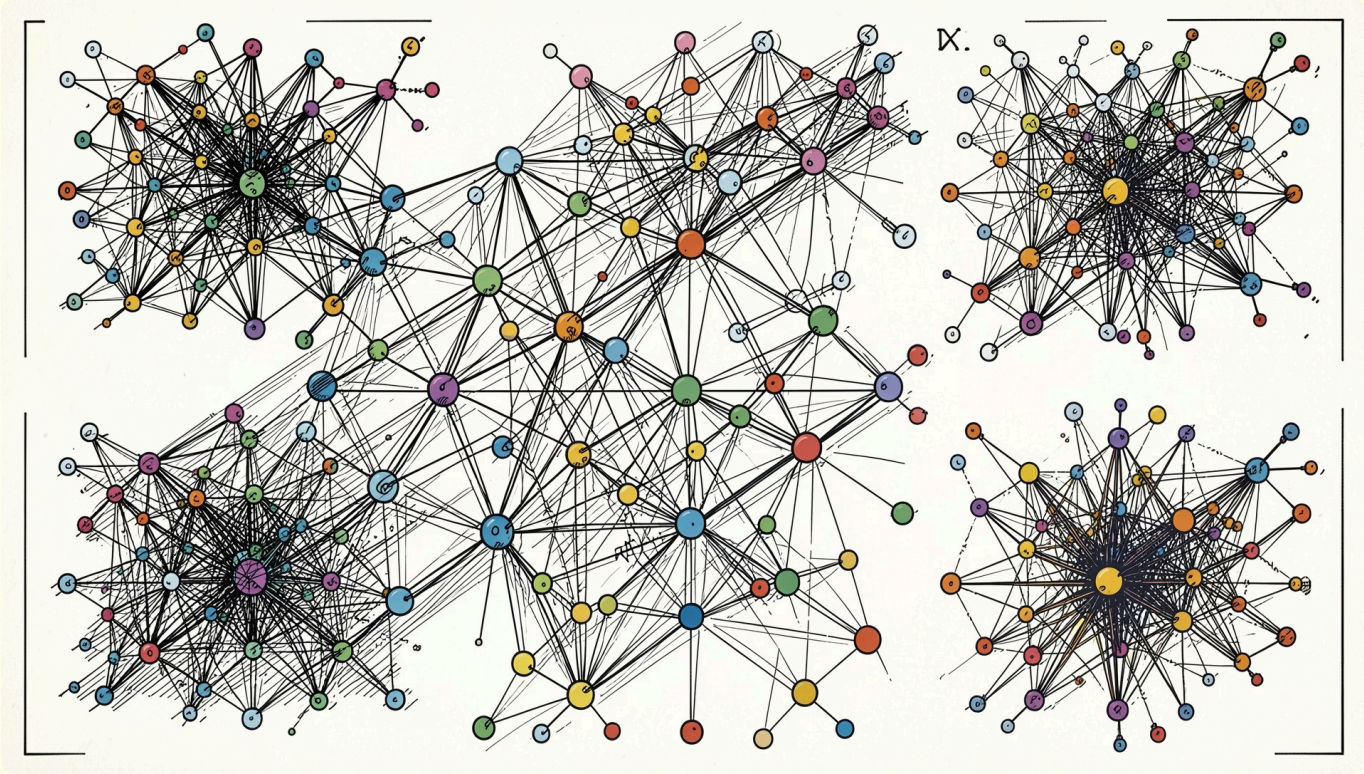
- **Завжди перевіряйте результати**

  Maltego показує зв'язки, але не робить остаточних висновків. Критично оцінюйте отримані дані та перевіряйте їх з інших джерел, щоб уникнути помилок.

Візуалізація як ключ до розуміння

Maltego пропонує різноманітні способи візуалізації даних, що дозволяє краще зрозуміти складні взаємозв'язки:

- Змінюйте вигляд графів: від кругових до ієрархічних, щоб знайти найбільш вдале представлення.
- Групуйте дані для виявлення прихованих патернів та аномалій, які можуть бути неочевидними у розрізнених даних.
- Використовуйте інструменти панелі **Investigate** для швидкого пошуку вузлів, фільтрації та аналізу структури графа.



Безпека та етика у OSINT

⚠ Відповідальне використання

Пам'ятайте, що Maltego працює з реальними даними. Завжди дотримуйтесь етичних норм та законів щодо конфіденційності та захисту даних.

OSINT — це потужний інструмент, який вимагає критичного мислення та відповідального підходу. Завжди оцінюйте результати перед ухваленням рішень, особливо якщо вони стосуються приватних осіб або компаній.

Використання Maltego має бути спрямоване на підвищення безпеки та прозорості, а не на порушення прав інших.

Ваш шлях дослідника

Розпочніть свою подорож у світ OSINT з Maltego. Почніть з малого: перевірте власний цифровий слід, щоб зрозуміти, як працює інструмент. Досліджуйте безмежні зв'язки мережі та відкривайте приховані дані. Maltego — це не просто програмне забезпечення, це ваш спосіб бачити те, що приховано від інших, і розкривати істину.