OSINT su Reddit: come trasformare un social caotico in una macchina investigativa

Maria Cattini | 03/04/2026 | Open source intelligence

OSINT su Reddit: Perché Reddit è diventato un terreno di caccia per l'OSINT

Quante volte, durante un'inchiesta, ti sei resa conto che la conversazione più interessante non era su X o LinkedIn, ma nascosta in un thread anonimo su Reddit? Con decine di milioni di utenti attivi ogni giorno e migliaia di community iper-verticali, Reddit è diventato uno dei terreni più fertili per raccogliere segnali, storie e pattern utili a chi fa giornalismo investigativo, cybersecurity o analisi OSINT.

C'è però un problema: senza metodo, Reddit è solo rumore. Policy API sempre più rigide, attenzione crescente alla privacy e un ecosistema in cui troll, propaganda e shitposting convivono con testimonianze genuine rendono facile sbagliare bersaglio. L'obiettivo di questa guida è darti un framework operativo, non teorico: una sorta di "playbook OSINT" ispirato ai manuali di Reddit prospecting commerciale, ma adattato a chi deve verificare, contestualizzare e pubblicare, non vendere.

Cos'è Reddit in ottica OSINT

Reddit è una piattaforma di social news e discussione organizzata in community tematiche chiamate subreddit, ognuna con regole, moderatori e cultura propri. Gli utenti operano dietro username pseudonimi, con profili minimali ma cronologie di post e commenti spesso lunghissime, soprattutto nei contesti tecnici o di nicchia.

Per chi fa OSINT, Reddit rientra nel perimetro della **SOCMINT** (social media intelligence): sfruttare dati pubblici dei social per ricostruire comportamenti, reti e narrazioni. Il valore sta nella combinazione di due fattori: community ultra-specifiche (da r/OSINT a r/cybersecurity fino a micro-subreddit geopolitici) e discussioni lunghe, dove gli utenti condividono dettagli che non metterebbero mai in un comunicato stampa.

Come è fatto Reddit: gli elementi che un'analista deve conoscere

Subreddit: i "quartieri" dove succede tutto

Ogni subreddit vive su un URL del tipo https://www.reddit.com/r/nome_subreddit e concentra post su un tema specifico, con un proprio micro-ecosistema di regole, sanzioni e linguaggio. Alcune community chiave per l'OSINT: r/OSINT, r/cybersecurity, r/netsec, r/geopolitics, r/worldnews, ma anche subreddit più oscuri che scopri seguendo cross-post e link interni.

Profili: cosa puoi leggere (e cosa no)

I profili utente, accessibili da https://www.reddit.com/user/username, mostrano storico di post e

commenti, sub frequentati, eventuali display name, avatar e poco altro. I nickname sono in gran parte pseudonimi, ma possono contenere indizi: nomi, anni, riferimenti geografici, che vanno trattati come indizi da verificare, non come dati anagrafici scolpiti nella pietra.

Ricerca: interna, esterna e ibrida

La ricerca interna di Reddit permette di filtrare per parola chiave, subreddit, autore, intervallo temporale e tipo di contenuto; è lo strumento base per qualunque indagine mirata. In parallelo, la vecchia ma sempreverde combo site:reddit.com parola_chiave sui motori di ricerca spesso restituisce thread che il motore interno nasconde o indicizza male.

I paletti: termini d'uso, legalità e privacy

Cosa permette Reddit (e cosa decisamente no)

L'accesso massivo ai dati di Reddit è regolato dai **Data API Terms**, che concedono una licenza limitata per usare le API ufficiali, revocabile in caso di violazione dei termini. Negli ultimi anni la piattaforma ha irrigidito sensibilmente le condizioni, in particolare verso servizi che estraggono e rivendono analisi su conversazioni degli utenti, con casi di rifiuto esplicito di approvazione per app di questo tipo.

Privacy policy e anonimato relativo

La privacy policy di Reddit elenca in dettaglio quali dati vengono raccolti (username, IP, cookie, attività sulla piattaforma) e a quali scopi vengono usati o condivisi. Per giornalisti e analisti significa una cosa semplice: lavorare su contenuti pubblici non autorizza automaticamente a tentare la de-anonimizzazione di utenti qualunque, soprattutto se non sono figure pubbliche o non esiste un chiaro interesse pubblico prevalente.

Scraping "furbo" non è per forza lecito

Le guide sullo scraping legale ribadiscono sempre la stessa triade: usare API ufficiali, rispettare i rate limit, non violare i ToS e non collezionare dati sensibili per finalità abusive. In pratica: preferire strumenti e workflow che lavorano sui contenuti visibili via web o API, evitare mirror massivi dell'intero sito e chiarire internamente perché, come e dove verranno conservati i dati raccolti.

Dal playbook sales al playbook OSINT: il cambio di paradigma

I playbook di Reddit prospecting mostrano bene come impostare un sistema che monitora subreddits, filtra thread rilevanti, assegna punteggi alle conversazioni e propone risposte pronte tramite agenti AI. Nel mondo OSINT, obiettivo e metrica cambiano: non ti interessa "convertire" un lead, ma **trovare informazione verificabile, contestualizzarla e documentarla**.

Un framework operativo sensato per l'OSINT su Reddit può seguire questo flusso:

1. definire il perimetro di indagine;
2. mappare le community rilevanti;
3. costruire un vocabolario di ricerca;
4. raccogliere dati (manuale, semi-automatica, via API);
5. attribuire punteggi ai thread;
6. analizzare profili e reti;
7. verificare, contestualizzare, archiviare i risultati.

Step 1 – Definire obiettivo e perimetro (prima di aprire Reddit)

Domande guida

Prima domanda scomoda: **cosa stai cercando davvero?**
Esempi di obiettivi:

• mappare una rete di account legata a un movimento politico o a un gruppo estremista;
• seguire le discussioni su una vulnerabilità critica, un nuovo malware o una campagna di phishing;
• monitorare la percezione di un’azienda o di un’infrastruttura strategica dopo un incidente.

Un obiettivo chiaro ti evita di annegare nel feed infinito di meme e shitpost.

Vincoli espliciti (per non farti male dopo)

Definisci nero su bianco:

• periodo analizzato (es. ultimi 6 mesi);
• categorie di dati da NON collezionare (telefono, indirizzi, dati sanitari);
• regole di pubblicazione: cosa resta nel taccuino, cosa può finire in un pezzo o in un report tecnico.

Nel contesto cyber, questo è cruciale: ripubblicare dettagli tecnici non necessari può esporre ancora di più le vittime, o facilitare copycat.

Step 2 – Mappare le community giuste (e non solo r/OSINT)

Come trovare i subreddit che contano

Le guide OSINT dedicate a Reddit suggeriscono di partire da una mappa “core” di subreddits (r/OSINT, r/cybersecurity, r/netsec, r/geopolitics, r/worldnews…) e poi seguire cross-post, link consigliati e sidebar per scovare community più di nicchia.

Un trucco banale ma efficacissimo: cercare \"keyword\" \"r/qualcosa\" site:reddit.com su un motore, per intercettare menzioni di subreddit poco visibili dall’interno.

Per ogni subreddit annota:

• tema e pubblico prevalente;
• regole su leak, doxxing, contenuti illegali;
• livello di moderazione (strict, laissez-faire, deserto);
• eventuali account ufficiali o esperti riconosciuti.

Costruire una tassonomia personale

Una volta raccolta una lista di community, organizzarle in categorie (“discussione tecnica”, “aiuto utenti”, “attivismo”, “mercato grigio”) ti permette di capire rapidamente dove cercare cosa. Questo approccio è perfettamente in linea con i percorsi OSINT più seri, che insistono su mappe delle fonti e non solo su liste di tool.

Step 3 – Vocabolario di ricerca: non basta digitare il nome ufficiale

Slang, storpiature e inside joke

Su Reddit raramente i fenomeni si chiamano come nei report ufficiali. Tra meme, abbreviazioni e sarcasmo, un servizio o un gruppo possono avere tre o quattro soprannomi diversi.

Per questo ha senso costruire un mini-glossario che includa:

• nome ufficiale;
• acronimi e sigle;
• errori ortografici frequenti;
• versioni ironiche o dispregiative.

Fonti per arricchirlo:

• post “ELI5”, FAQ e “read this first” dei subreddit target;
• wiki interni delle community;
• discussioni meta su r/OSINT e r/cybersecurity che elencano tool e tecniche.

Ridurre il bias nelle query

Se cerchi solo “truffa X”, indovinerai cosa troverai.
Integrare query positive, neutre e negative (“scam”, “review”, “success story”, “issue”, “bug”) aiuta a evitare la classica conferma delle ipotesi iniziali. I percorsi OSINT consigliati alle persone alle prime armi suggeriscono anche di strutturare le query per blocchi (persona, organizzazione, luogo, evento) per non lasciarsi dietro pezzi importanti di contesto.

Step 4 – Raccolta dati: manuale, semi-automatica, automatizzata

Fase 1: raccolta manuale (per capire il terreno)

Per un caso singolo o una prima esplorazione, lavorare manualmente nell’interfaccia di Reddit resta imbattibile: vedi il thread nel suo ambiente naturale, percepisci tono, reazioni, meta-discussioni. È il momento in cui ti fai l’orecchio al linguaggio locale e capisci se quella community vale il tuo tempo.

Fase 2: strumenti OSINT e ricerca avanzata

Tutorial e corsi OSINT mostrano come usare strumenti che permettono di cercare per keyword, autore, URL o altri parametri, aggregando risultati e facilitando l’analisi temporale. Alcune piattaforme includono funzioni di “Reddit comment search” e analisi dei profili, utili per ricostruire attività di un utente su più subreddits.

Fase 3: API ufficiali e archivi

Quando il lavoro diventa sistematico (monitoraggi continuativi, ricerche longitudinali), passare alle API ufficiali – rispettando termini, rate limit e scopi consentiti – è la via meno rischiosa sul piano legale. A questo si possono affiancare archivi e dataset usati in ambito OSINT per recuperare contenuti non più facilmente accessibili via interfaccia standard.

Step 5 – Dare un punteggio ai thread

Dal “buying intent” al “valore investigativo”

Nei playbook sales si assegnano punteggi ai thread in base all’intento d’acquisto. Tu puoi fare la stessa cosa sostituendo la metrica con il **valore investigativo**.

Esempi di criteri:

• quanti dettagli verificabili contiene (nomi, domini, IP, aziende, luoghi, date);
• livello di engagement (numero di commenti, qualità della discussione);
• presenza di fonti esterne (documenti, repository, leak, articoli);
• legame con altri casi o eventi che stai già seguendo.

Dalla teoria alla tua “coda di lavoro”

Una volta attribuito un punteggio, puoi costruire una coda giornaliera o settimanale: prima i thread ad alto punteggio, poi quelli intermedi, il rumore resta in fondo. Molte community OSINT raccomandano di tenere queste priorità in un foglio di calcolo o in strumenti di link analysis, per tracciare che cosa è già stato analizzato e da chi.

Step 6 – Analizzare profili e reti (senza fare caccia alle streghe)

Guardare i pattern, non un singolo commento

Le guide su Reddit OSINT insistono sul fatto che l’unità di misura non è il post isolato, ma i **pattern**: orari, sub frequentati, temi ricorrenti, stile linguistico. L’obiettivo per giornalisti e analisti non è “smascherare” le persone, ma capire se un account è parte di una campagna coordinata, di un’operazione di influenza o di una rete tecnica.

Collegare Reddit al resto dell’ecosistema

Molti utenti linkano spontaneamente GitHub, X, Discord, blog personali o riutilizzano lo stesso nickname su più piattaforme. Tracciare queste connessioni in modo strutturato (foglio di calcolo, grafo) ti consente di costruire mappe di relazione preziose in contesti cyber, di disinformazione o di inchieste su gruppi organizzati.

Step 7 – Verifica, contestualizzazione, archiviazione

Reddit ti dà lo spunto, non il verdetto

Ogni informazione trovata su Reddit andrebbe trattata come **segnalazione** da verificare altrove, non come prova definitiva. Cross-check con documenti ufficiali, altre piattaforme, fonti umane e database tecnici è obbligatorio, soprattutto davanti a accuse, leak o dettagli sensibili.

Archiviare bene oggi per non pentirsene domani

Le community OSINT più strutturate raccomandano di usare tabelle, note strutturate e grafi per memorizzare entità (persone, organizzazioni, infrastrutture), relazioni e riferimenti ai thread originali. Conservare link, screenshot e, dove lecito, hash dei contenuti chiave ti permette di ricostruire il quadro anche se un post viene modificato o cancellato.

Strumenti e risorse per fare OSINT su Reddit con criterio

Community da seguire

Subreddit come r/OSINT e r/cybersecurity sono ottimi hub per restare aggiornati su tool, metodologie, casi reali e percorsi di formazione, con thread che spesso linkano a guide esterne e corsi gratuiti.

Guide specializzate

Alcune aziende che lavorano su OSINT e sicurezza hanno pubblicato guide dettagliate a come usare Reddit in chiave intelligence, con focus su architettura della piattaforma, tecniche di raccolta e analisi dei profili. In parallelo, articoli indipendenti illustrano interi toolkit (API, archivi, script, motori verticali) per automatizzare porzioni del processo senza uscire dal perimetro legale.

Rischi sottovalutati: disinformazione, bias e monocultura informativa

Reddit ospita campagne di disinformazione, trolling coordinato e operazioni di influenza che sfruttano l’apparenza di “discussione spontanea”. Segnali tipici: account nuovi misteriosamente

molto attivi, messaggi copia-incolla su thread diversi, pattern di upvote sospetti.

In più, i percorsi OSINT ricordano un punto spesso ignorato: costruire un'intera analisi su una sola piattaforma è il modo più rapido per distorcerla. Reddit è una fonte potente, non l'unica. Quello che non esiste lì può esistere su forum storici, Telegram, Discord, blog, database pubblici.

Dove ti porta tutto questo

Reddit è, oggi, uno dei contesti più ricchi per chi fa OSINT su persone, organizzazioni e fenomeni globali, grazie al volume di discussioni e alla granularità delle community. Ma la chiusura progressiva delle API, l'uso intensivo dei dati per l'addestramento di modelli di AI e la sensibilità crescente su privacy e anonimato obbligano chi fa giornalismo e analisi a un livello di consapevolezza superiore.

Adottare un framework "da playbook" – mappatura delle community, scoring dei thread, automazione controllata, verifica incrociata e archiviazione strutturata – ti permette di trasformare Reddit da flusso caotico a fonte solida e difendibile anche davanti a una direzione legale o a un comitato etico.

Vuoi fare il passo successivo? Scegli una singola inchiesta o un tema di cybersecurity che stai seguendo, costruisci la tua mappa di subreddit e il tuo sistema di scoring, e sperimenta un "mini-playbook Reddit OSINT". Poi, se vuoi, condividi cosa ha funzionato e cosa no: sarà materiale perfetto per il prossimo pezzo.

E se vuoi approfondire: Iscriviti alla newsletter: https://coondivido.substack.com/ - Entra nella community Telegram: https://t.me/osintaipertutti

OSINT su Reddit: Perché Reddit è diventato un terreno di caccia per l'OSINT

Quante volte, durante un'inchiesta, ti sei resa conto che la conversazione più interessante non era su X o LinkedIn, ma nascosta in un thread anonimo su Reddit? Con decine di milioni di utenti attivi ogni giorno e migliaia di community iper-verticali, Reddit è diventato uno dei terreni più fertili per raccogliere segnali, storie e pattern utili a chi fa giornalismo investigativo, cybersecurity o analisi OSINT.

C'è però un problema: senza metodo, Reddit è solo rumore. Policy API sempre più rigide, attenzione crescente alla privacy e un ecosistema in cui troll, propaganda e shitposting convivono con testimonianze genuine rendono facile sbagliare bersaglio. L'obiettivo di questa guida è darti un framework operativo, non teorico: una sorta di "playbook OSINT" ispirato ai manuali di Reddit prospecting commerciale, ma adattato a chi deve verificare, contestualizzare e pubblicare, non vendere.

Cos'è Reddit in ottica OSINT

Reddit è una piattaforma di social news e discussione organizzata in community tematiche chiamate subreddit, ognuna con regole, moderatori e cultura propri. Gli utenti operano dietro username pseudonimi, con profili minimali ma cronologie di post e commenti spesso lunghissime, soprattutto nei contesti tecnici o di nicchia.

Per chi fa OSINT, Reddit rientra nel perimetro della **SOCMINT** (social media intelligence): sfruttare dati pubblici dei social per ricostruire comportamenti, reti e narrazioni. Il valore sta nella combinazione di due fattori: community ultra-specifiche (da r/OSINT a r/cybersecurity fino a micro-subreddit geopolitici) e discussioni lunghe, dove gli utenti condividono dettagli che non metterebbero mai in un comunicato stampa.

Come è fatto Reddit: gli elementi che un'analista deve conoscere

Subreddit: i “quartieri” dove succede tutto

Ogni subreddit vive su un URL del tipo https://www.reddit.com/r/nome_subreddit e concentra post su un tema specifico, con un proprio micro-ecosistema di regole, sanzioni e linguaggio. Alcune community chiave per l’OSINT: r/OSINT, r/cybersecurity, r/netsec, r/geopolitics, r/worldnews, ma anche subreddit più oscuri che scopri seguendo cross-post e link interni.

Profili: cosa puoi leggere (e cosa no)

I profili utente, accessibili da https://www.reddit.com/user/username, mostrano storico di post e commenti, sub frequentati, eventuali display name, avatar e poco altro. I nickname sono in gran parte pseudonimi, ma possono contenere indizi: nomi, anni, riferimenti geografici, che vanno trattati come indizi da verificare, non come dati anagrafici scolpiti nella pietra.

Ricerca: interna, esterna e ibrida

La ricerca interna di Reddit permette di filtrare per parola chiave, subreddit, autore, intervallo temporale e tipo di contenuto; è lo strumento base per qualunque indagine mirata. In parallelo, la vecchia ma sempreverde combo site:reddit.com parola_chiave sui motori di ricerca spesso restituisce thread che il motore interno nasconde o indicizza male.

I paletti: termini d’uso, legalità e privacy

Cosa permette Reddit (e cosa decisamente no)

L’accesso massivo ai dati di Reddit è regolato dai **Data API Terms**, che concedono una licenza limitata per usare le API ufficiali, revocabile in caso di violazione dei termini. Negli ultimi anni la piattaforma ha irrigidito sensibilmente le condizioni, in particolare verso servizi che estraggono e rivendono analisi su conversazioni degli utenti, con casi di rifiuto esplicito di approvazione per app di questo tipo.

Privacy policy e anonimato relativo

La privacy policy di Reddit elenca in dettaglio quali dati vengono raccolti (username, IP, cookie, attività sulla piattaforma) e a quali scopi vengono usati o condivisi. Per giornalisti e analisti significa una cosa semplice: lavorare su contenuti pubblici non autorizza automaticamente a tentare la de-anonimizzazione di utenti qualunque, soprattutto se non sono figure pubbliche o non esiste un chiaro interesse pubblico prevalente.

Scraping “furbo” non è per forza lecito

Le guide sullo scraping legale ribadiscono sempre la stessa triade: usare API ufficiali, rispettare i rate limit, non violare i ToS e non collezionare dati sensibili per finalità abusive. In pratica: preferire strumenti e workflow che lavorano sui contenuti visibili via web o API, evitare mirror massivi dell’intero sito e chiarire internamente perché, come e dove verranno conservati i dati raccolti.

Dal playbook sales al playbook OSINT: il cambio di paradigma

I playbook di Reddit prospecting mostrano bene come impostare un sistema che monitora subreddits, filtra thread rilevanti, assegna punteggi alle conversazioni e propone risposte pronte tramite agenti AI. Nel mondo OSINT, obiettivo e metrica cambiano: non ti interessa “convertire” un lead, ma **trovare informazione verificabile, contestualizzarla e documentarla**.

Un framework operativo sensato per l’OSINT su Reddit può seguire questo flusso:

1. definire il perimetro di indagine;
2. mappare le community rilevanti;
3. costruire un vocabolario di ricerca;

4. raccogliere dati (manuale, semi-automatica, via API);
5. attribuire punteggi ai thread;
6. analizzare profili e reti;
7. verificare, contestualizzare, archiviare i risultati.

Step 1 – Definire obiettivo e perimetro (prima di aprire Reddit)

Domande guida

Prima domanda scomoda: **cosa stai cercando davvero?**
Esempi di obiettivi:

• mappare una rete di account legata a un movimento politico o a un gruppo estremista;
• seguire le discussioni su una vulnerabilità critica, un nuovo malware o una campagna di phishing;
• monitorare la percezione di un'azienda o di un'infrastruttura strategica dopo un incidente.

Un obiettivo chiaro ti evita di annegare nel feed infinito di meme e shitpost.

Vincoli espliciti (per non farti male dopo)

Definisci nero su bianco:

• periodo analizzato (es. ultimi 6 mesi);
• categorie di dati da NON collezionare (telefono, indirizzi, dati sanitari);
• regole di pubblicazione: cosa resta nel taccuino, cosa può finire in un pezzo o in un report tecnico.

Nel contesto cyber, questo è cruciale: ripubblicare dettagli tecnici non necessari può esporre ancora di più le vittime, o facilitare copycat.

Step 2 – Mappare le community giuste (e non solo r/OSINT)

Come trovare i subreddit che contano

Le guide OSINT dedicate a Reddit suggeriscono di partire da una mappa "core" di subreddits (r/OSINT, r/cybersecurity, r/netsec, r/geopolitics, r/worldnews…) e poi seguire cross-post, link consigliati e sidebar per scovare community più di nicchia.

Un trucco banale ma efficacissimo: cercare \"keyword\" \"r/qualcosa\" site:reddit.com su un motore, per intercettare menzioni di subreddit poco visibili dall'interno.

Per ogni subreddit annota:

• tema e pubblico prevalente;
• regole su leak, doxxing, contenuti illegali;
• livello di moderazione (strict, laissez-faire, deserto);
• eventuali account ufficiali o esperti riconosciuti.

Costruire una tassonomia personale

Una volta raccolta una lista di community, organizzarle in categorie ("discussione tecnica", "aiuto utenti", "attivismo", "mercato grigio") ti permette di capire rapidamente dove cercare cosa. Questo approccio è perfettamente in linea con i percorsi OSINT più seri, che insistono su mappe delle fonti e non solo su liste di tool.

Step 3 – Vocabolario di ricerca: non basta digitare il nome ufficiale

Slang, storpiature e inside joke

Su Reddit raramente i fenomeni si chiamano come nei report ufficiali. Tra meme, abbreviazioni e sarcasmo, un servizio o un gruppo possono avere tre o quattro soprannomi diversi.

Per questo ha senso costruire un mini-glossario che includa:

• nome ufficiale;
• acronimi e sigle;
• errori ortografici frequenti;
• versioni ironiche o dispregiative.

Fonti per arricchirlo:

• post “ELI5”, FAQ e “read this first” dei subreddit target;
• wiki interni delle community;
• discussioni meta su r/OSINT e r/cybersecurity che elencano tool e tecniche.

Ridurre il bias nelle query

Se cerchi solo “truffa X”, indovinerai cosa troverai.
Integrare query positive, neutre e negative (“scam”, “review”, “success story”, “issue”, “bug”) aiuta a evitare la classica conferma delle ipotesi iniziali. I percorsi OSINT consigliati alle persone alle prime armi suggeriscono anche di strutturare le query per blocchi (persona, organizzazione, luogo, evento) per non lasciarsi dietro pezzi importanti di contesto.

Step 4 – Raccolta dati: manuale, semi-automatica, automatizzata

Fase 1: raccolta manuale (per capire il terreno)

Per un caso singolo o una prima esplorazione, lavorare manualmente nell’interfaccia di Reddit resta imbattibile: vedi il thread nel suo ambiente naturale, percepisci tono, reazioni, meta-discussioni. È il momento in cui ti fai l’orecchio al linguaggio locale e capisci se quella community vale il tuo tempo.

Fase 2: strumenti OSINT e ricerca avanzata

Tutorial e corsi OSINT mostrano come usare strumenti che permettono di cercare per keyword, autore, URL o altri parametri, aggregando risultati e facilitando l’analisi temporale. Alcune piattaforme includono funzioni di “Reddit comment search” e analisi dei profili, utili per ricostruire attività di un utente su più subreddits.

Fase 3: API ufficiali e archivi

Quando il lavoro diventa sistematico (monitoraggi continuativi, ricerche longitudinali), passare alle API ufficiali – rispettando termini, rate limit e scopi consentiti – è la via meno rischiosa sul piano legale. A questo si possono affiancare archivi e dataset usati in ambito OSINT per recuperare contenuti non più facilmente accessibili via interfaccia standard.

Step 5 – Dare un punteggio ai thread

Dal “buying intent” al “valore investigativo”

Nei playbook sales si assegnano punteggi ai thread in base all'intento d'acquisto. Tu puoi fare la stessa cosa sostituendo la metrica con il **valore investigativo**.

Esempi di criteri:

• quanti dettagli verificabili contiene (nomi, domini, IP, aziende, luoghi, date);
• livello di engagement (numero di commenti, qualità della discussione);
• presenza di fonti esterne (documenti, repository, leak, articoli);
• legame con altri casi o eventi che stai già seguendo.

Dalla teoria alla tua "coda di lavoro"

Una volta attribuito un punteggio, puoi costruire una coda giornaliera o settimanale: prima i thread ad alto punteggio, poi quelli intermedi, il rumore resta in fondo. Molte community OSINT raccomandano di tenere queste priorità in un foglio di calcolo o in strumenti di link analysis, per tracciare che cosa è già stato analizzato e da chi.

Step 6 – Analizzare profili e reti (senza fare caccia alle streghe)

Guardare i pattern, non un singolo commento

Le guide su Reddit OSINT insistono sul fatto che l'unità di misura non è il post isolato, ma i **pattern**: orari, sub frequentati, temi ricorrenti, stile linguistico. L'obiettivo per giornalisti e analisti non è "smascherare" le persone, ma capire se un account è parte di una campagna coordinata, di un'operazione di influenza o di una rete tecnica.

Collegare Reddit al resto dell'ecosistema

Molti utenti linkano spontaneamente GitHub, X, Discord, blog personali o riutilizzano lo stesso nickname su più piattaforme. Tracciare queste connessioni in modo strutturato (foglio di calcolo, grafo) ti consente di costruire mappe di relazione preziose in contesti cyber, di disinformazione o di inchieste su gruppi organizzati.

Step 7 – Verifica, contestualizzazione, archiviazione

Reddit ti dà lo spunto, non il verdetto

Ogni informazione trovata su Reddit andrebbe trattata come **segnalazione** da verificare altrove, non come prova definitiva. Cross-check con documenti ufficiali, altre piattaforme, fonti umane e database tecnici è obbligatorio, soprattutto davanti a accuse, leak o dettagli sensibili.

Archiviare bene oggi per non pentirsene domani

Le community OSINT più strutturate raccomandano di usare tabelle, note strutturate e grafi per memorizzare entità (persone, organizzazioni, infrastrutture), relazioni e riferimenti ai thread originali. Conservare link, screenshot e, dove lecito, hash dei contenuti chiave ti permette di ricostruire il quadro anche se un post viene modificato o cancellato.

Strumenti e risorse per fare OSINT su Reddit con criterio

Community da seguire

Subreddit come r/OSINT e r/cybersecurity sono ottimi hub per restare aggiornati su tool, metodologie, casi reali e percorsi di formazione, con thread che spesso linkano a guide esterne e corsi gratuiti.

Guide specializzate

Alcune aziende che lavorano su OSINT e sicurezza hanno pubblicato guide dettagliate a come usare Reddit in chiave intelligence, con focus su architettura della piattaforma, tecniche di raccolta e analisi dei profili. In parallelo, articoli indipendenti illustrano interi toolkit (API, archivi, script, motori verticali) per automatizzare porzioni del processo senza uscire dal perimetro legale.

Rischi sottovalutati: disinformazione, bias e monocultura informativa

Reddit ospita campagne di disinformazione, trolling coordinato e operazioni di influenza che sfruttano l'apparenza di "discussione spontanea". Segnali tipici: account nuovi misteriosamente molto attivi, messaggi copia-incolla su thread diversi, pattern di upvote sospetti.

In più, i percorsi OSINT ricordano un punto spesso ignorato: costruire un'intera analisi su una sola piattaforma è il modo più rapido per distorcerla. Reddit è una fonte potente, non l'unica. Quello che non esiste lì può esistere su forum storici, Telegram, Discord, blog, database pubblici.

Dove ti porta tutto questo

Reddit è, oggi, uno dei contesti più ricchi per chi fa OSINT su persone, organizzazioni e fenomeni globali, grazie al volume di discussioni e alla granularità delle community. Ma la chiusura progressiva delle API, l'uso intensivo dei dati per l'addestramento di modelli di AI e la sensibilità crescente su privacy e anonimato obbligano chi fa giornalismo e analisi a un livello di consapevolezza superiore.

Adottare un framework "da playbook" – mappatura delle community, scoring dei thread, automazione controllata, verifica incrociata e archiviazione strutturata – ti permette di trasformare Reddit da flusso caotico a fonte solida e difendibile anche davanti a una direzione legale o a un comitato etico.

Vuoi fare il passo successivo? Scegli una singola inchiesta o un tema di cybersecurity che stai seguendo, costruisci la tua mappa di subreddit e il tuo sistema di scoring, e sperimenta un "mini-playbook Reddit OSINT". Poi, se vuoi, condividi cosa ha funzionato e cosa no: sarà materiale perfetto per il prossimo pezzo.

E se vuoi approfondire: Iscriviti alla newsletter: https://coondivido.substack.com/ - Entra nella community Telegram: https://t.me/osintaipertutti