Il ciclo di vita dell'indagine OSINT: Dal requisito al report

Maria Cattini | 26/01/2026 | Open source intelligence

Un analista siede davanti a uno schermo nel silenzio di una stanza semibuia. Digita un nome o un indirizzo IP. In pochi secondi, una cascata di dati inonda il monitor. Per un profano, questa è l'essenza della ricerca online. Per un professionista, questo è solo rumore bianco. La differenza tra un utente comune e un esperto risiede nella capacità di navigare questo oceano senza annegare. L'Open Source Intelligence non riguarda il semplice reperimento di informazioni. Si tratta di un processo strutturato che trasforma dati grezzi in conoscenza strategica per i decisori. Senza un metodo rigoroso, qualsiasi indagine è destinata a fallire sotto il peso del sovraccarico informativo o, peggio, a causa di conclusioni errate derivanti da fonti manipolate.

In questo report esploreremo **Il Ciclo di Vita dell'Indagine OSINT**, analizzando ogni passaggio tecnico e logico necessario per trasformare un'esigenza informativa in un dossier accurato. Comprendere questo percorso è fondamentale per chiunque operi nella cybersecurity, nelle investigazioni aziendali o nel giornalismo d'inchiesta.

Le fondamenta dell'Intelligence: Oltre la ricerca web

L'intelligence delle fonti aperte consiste nell'acquisizione e nell'analisi di dati pubblicamente accessibili. Questo termine include tutto ciò che può essere ottenuto legalmente senza ricorrere a metodi clandestini o intercettazioni protette. Storicamente, l'OSINT ha radici nelle agenzie governative durante la Seconda Guerra Mondiale e la Guerra Fredda. In quell'epoca, gli analisti setacciavano giornali stranieri e trasmissioni radiofoniche per carpire le intenzioni degli avversari.

Oggi, la digitalizzazione ha cambiato radicalmente il volume e la velocità dei dati. Le fonti non sono più solo testuali. Includono immagini satellitari, post sui social network, flussi di dati finanziari e metadati nascosti nei file. È essenziale distinguere tra Open Source Information (OSINF) e Open Source Intelligence (OSINT). La prima rappresenta la materia prima grezza: un tweet, un registro pubblico o un articolo di giornale. La seconda è il risultato di un'elaborazione analitica che attribuisce significato a quel dato.

Le Discipline Correlate

L'OSINT non opera in un vuoto. Si integra con altre discipline per fornire una visione d'insieme. Le agenzie di sicurezza nazionale utilizzano una classificazione specifica per definire questi ambiti.

Acronimo	Disciplina	Fonte Principale
HUMINT	Human Intelligence	Fonti umane e contatti diretti.
SIGINT	Signal Intelligence	Segnali elettromagnetici e comunicazioni.
IMINT	Imagery Intelligence	Immagini da satelliti o droni.
SOCMINT	Social Media Intelligence	Dati provenienti dai social network.
GEOINT	Geospatial Intelligence	Dati legati a coordinate geografiche.

© 2026 Coondivido — Tutti i diritti sono riservati

Acronimo	Disciplina	Fonte Principale
TECHINT	Technical Intelligence	Analisi di equipaggiamenti e tecnologie.

Tabella 1: Panoramica delle discipline di intelligence correlate.

La crescita esponenziale delle informazioni disponibili ha reso l'OSINT il punto di partenza quasi obbligatorio per ogni altra attività di intelligence. Un'indagine moderna raramente ignora la componente digitale, poiché i residui lasciati dalle persone online offrono una traccia indelebile delle loro attività.

Fase 1: Pianificazione e Definizione dei Requisiti

Il ciclo di vita inizia prima di toccare la tastiera. La pianificazione è il momento in cui si definiscono le priorità e i requisiti dell'indagine. Un errore frequente è lanciarsi nella raccolta senza aver chiarito l'obiettivo finale. Questo porta a una dispersione di energie e alla raccolta di dati inutili che complicano l'analisi successiva.

Identificazione dei Priority Intelligence Requirements (PIR)

L'analista deve collaborare con il destinatario del report per stabilire cosa sia davvero importante. Se un'azienda richiede una verifica su un fornitore, i requisiti non possono essere generici. Bisogna porsi domande precise: "Esistono legami con entità sanzionate?", "Qual è lo storico legale dei soci fondatori?", "Ci sono evidenze di violazioni della sicurezza informatica nei loro sistemi?". La definizione dei PIR permette di focalizzare la ricerca e di stabilire i parametri di successo dell'operazione.

Disambiguazione e Identificatori Unici

Prima di avviare la ricerca, è necessario isolare i dati che rendono un target unico. In un mondo popolato da miliardi di utenti, il rischio di omonimia è altissimo. Un analista esperto raccoglie inizialmente una massa critica di identificatori univoci.

• Dati Anagrafici: Nome completo, alias, data e luogo di nascita.
• Identificatori Digitali: Indirizzi email, handle dei social media, numeri di telefono, indirizzi IP.
• Elementi Fisici: Immagini del volto (per il riconoscimento facciale), città di residenza, legami familiari.

Avere più identificatori consente di eliminare i risultati duplicati o errati fin dall'inizio. Se si cerca "Mario Rossi", l'aggiunta di una data di nascita o di una città specifica riduce drasticamente il rumore. Questa fase di preparazione protegge anche l'analista da tentativi di inganno messi in atto da avversari che utilizzano identità sintetiche o società di facciata per nascondere le proprie tracce.

Fase 2: Identificazione delle Fonti e Raccolta (Harvesting)

Con gli obiettivi chiari e gli identificatori isolati, si passa alla fase operativa della raccolta dati. Questo passaggio richiede una strategia di sourcing diversificata. Le informazioni non risiedono tutte nello stesso posto. Il World Wide Web è uno spazio disomogeneo, strutturato in strati di accessibilità.

La Stratificazione del Web

L'accesso alle informazioni segue una logica di sicurezza crescente. Gli strati più esterni sono visibili a tutti, mentre quelli interni richiedono software o protocolli dedicati.

1. Surface Web: Comprende i siti indicizzati dai motori di ricerca come Google o Bing. È la parte più visibile ma spesso la più superficiale.
2. Deep Web: Contiene dati non indicizzati, come database privati, riviste accademiche protette da

© 2026 Coondivido — Tutti i diritti sono riservati

paywall, registri governativi o documenti legali non pubblici.
3. Dark Web: Richiede reti criptate come Tor o I2P. È il luogo dove spesso finiscono i dati sottratti tramite attacchi hacker o dove avvengono scambi illeciti.

Tipologie di Fonti OSINT

Un'indagine completa deve attingere da diverse categorie di dati per essere considerata attendibile.

• Media Tradizionali: Giornali, riviste, trasmissioni radiofoniche e televisive.
• Registri Governativi: Documenti delle camere di commercio, registri delle proprietà immobiliari, database delle sanzioni e documenti giudiziari.
• Social Media (SOCMINT): Piattaforme come LinkedIn, Facebook, X (Twitter) e Instagram. Questi canali offrono insight comportamentali e reti di contatti che i registri ufficiali ignorano.
• Letteratura Grigia: Studi universitari, rapporti tecnici non pubblicati ufficialmente, brevetti e tesi accademiche.
• Dati Geos spaziali: Immagini satellitari e mappe digitali che permettono di verificare posizioni fisiche o infrastrutture.

Tutorial Strumenti: Automazione della Raccolta

Svolgere la ricerca manualmente è un compito titanico che espone l'analista a errori e omissioni. Per questo motivo, l'utilizzo di strumenti di automazione è diventato uno standard professionale.

Maltego: L'Analisi Relazionale

Maltego è una piattaforma di visualizzazione e link analysis che permette di mappare le relazioni tra entità diverse. Funziona attraverso il concetto di "Trasformate", che sono query automatiche inviate verso database esterni o API.

1. Apertura del Grafico: Si inizia inserendo un'entità centrale, come un dominio o il nome di una persona.
2. Esecuzione delle Trasformate: Con un clic, è possibile richiedere a Maltego di trovare tutti gli indirizzi email associati a quel nome o tutti gli IP associati a quel dominio.
3. Espansione dell'Infrastruttura: Maltego può risalire dai DNS Name agli IP, e dagli IP trovare altri siti web ospitati sulla stessa macchina, rivelando infrastrutture nascoste.
4. Visualizzazione: Il risultato è un grafo interattivo dove nodi e frecce mostrano chiaramente le connessioni. È ideale per scoprire se due aziende apparentemente distinte condividono lo stesso server email o lo stesso numero di telefono.

SpiderFoot: L'Impronta Digitale Automatica

Mentre Maltego eccelle nella visualizzazione, SpiderFoot è impareggiabile nella scansione massiva di fonti. È uno strumento open-source che interroga oltre 200 fonti diverse in pochi minuti.

1. Impostazione del Target: Si inserisce l'obiettivo, ad esempio un indirizzo email sospetto.
2. Scelta del Profilo di Scansione: È possibile scegliere tra "Footprint" (mappatura generale), "Investigate" (focus su indicatori malevoli) o "Passive" (raccolta che non interagisce direttamente con il target per non allertarlo).
3. Raccolta Modulare: SpiderFoot attiva moduli per cercare riferimenti nel Dark Web, fughe di dati (leaks), account social e informazioni WHOIS.
4. Export dei Risultati: I dati possono essere visualizzati in tabelle o esportati in formati come JSON o CSV per essere integrati in altri sistemi.

Strumento	Punto di Forza	Limite Principale
Maltego	Mappatura delle relazioni umane e tecniche.	Costo elevato per le API; curva di apprendimento ripida.
SpiderFoot	Automazione estrema; scansione di massa.	Rischio di data overload; richiede filtraggio manuale.

© 2026 Coondivido — Tutti i diritti sono riservati

Strumento	Punto di Forza	Limite Principale
OSINT Framework	Mappa completa dei tool disponibili online.	È una risorsa consultativa, non un software analitico.
Shodan	Ricerca di dispositivi IoT e infrastrutture esposte.	Richiede competenze tecniche di rete avanzate.

Tabella 2: Comparazione degli strumenti OSINT per uso professionale.

Fase 3: Elaborazione e Normalizzazione (Processing)

I dati raccolti nella fase precedente sono disomogenei e spesso "sporchi". L'elaborazione è il processo che trasforma questi dati grezzi in un formato leggibile e pronto per l'analisi. Senza questa fase, l'investigatore si troverebbe di fronte a una montagna di screenshot, file di testo e log di sistema impossibili da sintetizzare.

Pulizia e Selezione

Il primo passo è eliminare le informazioni ridondanti o non pertinenti. Questo include la rimozione di fake news, dati obsoleti o errori di sistema che potrebbero inquinare l'indagine. Se un'azienda sta conducendo una due diligence su un partner commerciale, deve assicurarsi che le recensioni negative trovate online non siano state create ad arte da competitor o bot.

Analisi dei Metadati e Residui Digitali

Un aspetto cruciale dell'elaborazione riguarda l'estrazione di informazioni nascoste nei file. Ogni azione digitale lascia dei residui che raccontano una storia diversa dal contenuto visibile.

• Dati EXIF: Estrarre i metadati dalle immagini può rivelare le coordinate GPS del luogo in cui è stata scattata la foto, il modello di smartphone utilizzato e l'ora esatta dell'acquisizione.
• Analisi delle Email: Esaminare gli header delle comunicazioni permette di tracciare il percorso dei server, identificare gli indirizzi IP di origine e verificare i meccanismi di autenticazione come SPF o DKIM.
• Cronologia dei Documenti: File Word o PDF possono contenere la cronologia delle revisioni, rivelando nomi di autori o percorsi di cartelle interne che l'organizzazione non voleva rendere pubblici.

Traduzione e Contestualizzazione

In un'indagine globale, è frequente imbattersi in dati in lingue diverse. L'affidarsi ciecamente a traduttori automatici è un errore metodologico grave. Questi strumenti spesso mancano di comprendere lo slang locale, i codici culturali o le sfumature ironiche. L'analista deve contestualizzare l'informazione per evitare che una frase innocua venga interpretata come una minaccia o viceversa.

Fase 4: Analisi e Produzione (Intelligence Evaluation)

L'analisi è il cuore pulsante del ciclo OSINT. In questa fase, l'investigatore mette insieme i pezzi del puzzle per generare insight azionabili. Non si tratta solo di descrivere cosa è stato trovato, ma di interpretarlo per anticipare eventi o confermare ipotesi.

Il Sistema Admiralty (Scala NATO)

Per garantire l'oggettività, l'intelligence professionale non si basa sull'istinto. Utilizza un sistema standardizzato per valutare la qualità delle informazioni: l'Admiralty Code. Questo metodo separa l'affidabilità della fonte dalla credibilità del dato singolo.

© 2026 Coondivido — Tutti i diritti sono riservati

Codice Fonte	Affidabilità della Fonte	Codice Dato	Credibilità dell'Informazione
A	Completamente affidabile.	**1**	Confermata da fonti indipendenti.
B	Solitamente affidabile.	**2**	Probabilmente vera.
C	Abbastanza affidabile.	**3**	Possibilmente vera.
D	Di solito non affidabile.	**4**	Dubbia.
E	Inaffidabile.	**5**	Improbabile.
F	Non giudicabile.	**6**	Verità non giudicabile.

Tabella 3: Griglia di valutazione dell'intelligence secondo il codice Admiralty.

Utilizzare questa griglia permette di assegnare un valore preciso a ogni informazione. Ad esempio:

• B2: Un report proveniente da un analista noto con informazioni molto probabili.
• C3: Un'informazione proveniente da una fonte che ha fornito dati corretti in passato, ma che in questo caso non ha conferme esterne.
• F6: Un post anonimo su un forum del Dark Web senza alcuno storico di affidabilità e senza prove a supporto. È un dato che viene registrato ma non utilizzato per decisioni strategiche immediate.

Mitigare i Bias Cognitivi

L'analista deve lottare contro le trappole mentali intrinseche alla natura umana. Il cervello tende a cercare conferme a ciò che già pensa, ignorando le prove contrarie. Questo fenomeno è noto come bias di conferma. In un'indagine OSINT, è facile cadere in "camere d'eco" dove gli algoritmi dei motori di ricerca o dei social media continuano a proporre dati simili a quelli già visualizzati, rinforzando una narrazione potenzialmente errata.

Un metodo efficace per contrastare questi errori è l'Analysis of Competing Hypotheses (ACH). L'analista non cerca la spiegazione più probabile, ma elenca tutte le ipotesi possibili e cerca attivamente di smentirle. Vince l'ipotesi che resiste meglio ai tentativi di confutazione, non quella che sembra più intuitiva.

Fase 5: Disseminazione e Feedback

Un'indagine non si conclude quando l'analista ha trovato la risposta. Termina quando quella risposta viene comunicata efficacemente al destinatario. Senza una comunicazione chiara, anche la ricerca più brillante perde valore strategico.

La Redazione del Report

Il report finale deve essere un documento denso ma leggibile, privo di frasi inutili e focalizzato sui fatti. Un dossier professionale segue solitamente questa struttura:

1. Executive Summary: Un riassunto di poche righe che presenta i risultati principali. Il decisore deve capire immediatamente il livello di rischio o l'opportunità rilevata.
2. Metodologia e Limiti: Descrive quali fonti sono state interrogate e quali sono state le difficoltà. Essere onesti su ciò che "non è stato possibile verificare" è fondamentale per costruire fiducia.
3. Analisi delle Relazioni: Utilizzo di grafici e tabelle per mostrare legami tra persone, aziende e infrastrutture digitali.
4. Conclusioni e Raccomandazioni: L'analista suggerisce le azioni successive basate sulle evidenze raccolte.

L'Importanza del Feedback

Il ciclo OSINT è iterativo. Una volta consegnato il report, il destinatario potrebbe avere nuove domande o il contesto potrebbe cambiare. Il feedback permette di capire se l'indagine deve

© 2026 Coondivido — Tutti i diritti sono riservati

ricominciare con nuovi parametri o se può considerarsi conclusa. Questo flusso continuo assicura che l'intelligence rimanga dinamica e sempre allineata alle necessità operative dell'organizzazione.

Casi Studio e Fallimenti: Imparare dagli Errori

Analizzare casi reali permette di comprendere l'impatto di una cattiva metodologia.

Il Fallimento del "Dato Casuale"

In molti casi, l'errore non risiede nella mancanza di dati, ma nella loro cattiva interpretazione. Un esempio classico riguarda l'analisi dei rischi basata solo sull'osservazione superficiale. Nel 2017, a Mosul, una donna riuscì a passare i controlli di sicurezza portando in braccio un bambino. Le guardie, influenzate dal bias che vede le madri come innocue, non controllarono le sue mani, dove stringeva il detonatore. Questo errore di valutazione dimostra come i pregiudizi umani possano accecare anche di fronte all'evidenza fisica. In ambito OSINT, questo si traduce nel fidarsi ciecamente di una fonte "autorevole" senza verificare i dati specifici che sta fornendo.

Il Successo del Tracciamento Finanziario

D'altro canto, l'OSINT ha permesso di smascherare reti criminali complesse. Investigazioni recenti sui flussi di fentanyl tra aziende farmaceutiche cinesi e mercati internazionali hanno dimostrato come l'incrocio tra dati doganali, registri societari e forum del Dark Web possa rivelare sistemi di corruzione globale che sfuggono alle agenzie di polizia tradizionali. In questo caso, la capacità di seguire la traccia digitale attraverso diversi continenti è stata la chiave del successo.

L'Era dell'IA e il Futuro dell'OSINT

L'intelligenza artificiale sta cambiando le regole del gioco. Se da un lato l'IA generativa può aiutare a scrivere codice per automatizzare la raccolta, dall'altro introduce nuovi pericoli. I malintenzionati utilizzano l'IA per creare deepfake o per generare campagne di disinformazione su vasta scala, rendendo il compito dell'analista ancora più arduo.

Inoltre, i testi generati da intelligenze artificiali tendono a seguire pattern linguistici prevedibili, come l'uso eccessivo di termini neutri o costruzioni passive. Un analista moderno deve essere in grado di riconoscere queste tracce per distinguere tra contenuti autentici e manipolazioni artificiali. La sfida del futuro sarà l'integrazione di sistemi di difesa basati sull'IA per validare i dati alla velocità della luce, mantenendo però sempre l'uomo come ultimo giudice della verità.

L'attività OSINT non è una semplice sequenza di ricerche su Google. È una disciplina che richiede rigore metodologico, capacità tecniche e una profonda consapevolezza psicologica dei propri limiti. Dalla definizione chirurgica dei requisiti alla valutazione secondo il codice Admiralty, ogni passaggio è essenziale per garantire che l'intelligence prodotta sia solida e azionabile. Il sovraccarico di informazioni e la disinformazione sono i nemici principali, ma possono essere sconfitti attraverso l'uso consapevole di strumenti come Maltego e SpiderFoot, abbinati a un pensiero critico instancabile.

Se vuoi approfondire come queste tecniche possono proteggere la tua azienda o supportare le tue indagini, inizia oggi stesso a strutturare il tuo metodo. Non limitarti a raccogliere dati: trasformali in conoscenza.

Vuoi approfondire strumenti, tecniche e casi reali?
Iscriviti alla newsletter **OSINT & AI per tutti** su Substack: https://coondivido.substack.com/
Unisciti al canale Telegram: https://t.me/osintaipertutti
Un analista siede davanti a uno schermo nel silenzio di una stanza semibuia. Digita un nome o un indirizzo IP. In pochi secondi, una cascata di dati inonda il monitor. Per un profano, questa è l'essenza della ricerca online. Per un professionista, questo è solo rumore bianco. La differenza tra un utente comune e un esperto risiede nella capacità di navigare questo oceano senza annegare.
L'Open Source Intelligence non riguarda il semplice reperimento di informazioni. Si tratta di un processo strutturato che trasforma dati grezzi in conoscenza strategica per i decisori. Senza un

© 2026 Coondivido — Tutti i diritti sono riservati

metodo rigoroso, qualsiasi indagine è destinata a fallire sotto il peso del sovraccarico informativo o, peggio, a causa di conclusioni errate derivanti da fonti manipolate.

In questo report esploreremo **Il Ciclo di Vita dell'Indagine OSINT**, analizzando ogni passaggio tecnico e logico necessario per trasformare un'esigenza informativa in un dossier accurato. Comprendere questo percorso è fondamentale per chiunque operi nella cybersecurity, nelle investigazioni aziendali o nel giornalismo d'inchiesta.

Le fondamenta dell'Intelligence: Oltre la ricerca web

L'intelligence delle fonti aperte consiste nell'acquisizione e nell'analisi di dati pubblicamente accessibili. Questo termine include tutto ciò che può essere ottenuto legalmente senza ricorrere a metodi clandestini o intercettazioni protette. Storicamente, l'OSINT ha radici nelle agenzie governative durante la Seconda Guerra Mondiale e la Guerra Fredda. In quell'epoca, gli analisti setacciavano giornali stranieri e trasmissioni radiofoniche per carpire le intenzioni degli avversari.

Oggi, la digitalizzazione ha cambiato radicalmente il volume e la velocità dei dati. Le fonti non sono più solo testuali. Includono immagini satellitari, post sui social network, flussi di dati finanziari e metadati nascosti nei file. È essenziale distinguere tra Open Source Information (OSINF) e Open Source Intelligence (OSINT). La prima rappresenta la materia prima grezza: un tweet, un registro pubblico o un articolo di giornale. La seconda è il risultato di un'elaborazione analitica che attribuisce significato a quel dato.

Le Discipline Correlate

L'OSINT non opera in un vuoto. Si integra con altre discipline per fornire una visione d'insieme. Le agenzie di sicurezza nazionale utilizzano una classificazione specifica per definire questi ambiti.

Acronimo	Disciplina	Fonte Principale
HUMINT	Human Intelligence	Fonti umane e contatti diretti.
SIGINT	Signal Intelligence	Segnali elettromagnetici e comunicazioni.
IMINT	Imagery Intelligence	Immagini da satelliti o droni.
SOCMINT	Social Media Intelligence	Dati provenienti dai social network.
GEOINT	Geospatial Intelligence	Dati legati a coordinate geografiche.
TECHINT	Technical Intelligence	Analisi di equipaggiamenti e tecnologie.

Tabella 1: Panoramica delle discipline di intelligence correlate.

La crescita esponenziale delle informazioni disponibili ha reso l'OSINT il punto di partenza quasi obbligatorio per ogni altra attività di intelligence. Un'indagine moderna raramente ignora la componente digitale, poiché i residui lasciati dalle persone online offrono una traccia indelebile delle loro attività.

Fase 1: Pianificazione e Definizione dei Requisiti

Il ciclo di vita inizia prima di toccare la tastiera. La pianificazione è il momento in cui si definiscono le priorità e i requisiti dell'indagine. Un errore frequente è lanciarsi nella raccolta senza aver chiarito l'obiettivo finale. Questo porta a una dispersione di energie e alla raccolta di dati inutili che complicano l'analisi successiva.

Identificazione dei Priority Intelligence Requirements (PIR)

L'analista deve collaborare con il destinatario del report per stabilire cosa sia davvero importante. Se un'azienda richiede una verifica su un fornitore, i requisiti non possono essere generici. Bisogna porsi

© 2026 Coondivido — Tutti i diritti sono riservati

domande precise: "Esistono legami con entità sanzionate?", "Qual è lo storico legale dei soci fondatori?", "Ci sono evidenze di violazioni della sicurezza informatica nei loro sistemi?". La definizione dei PIR permette di focalizzare la ricerca e di stabilire i parametri di successo dell'operazione.

Disambiguazione e Identificatori Unici

Prima di avviare la ricerca, è necessario isolare i dati che rendono un target unico. In un mondo popolato da miliardi di utenti, il rischio di omonimia è altissimo. Un analista esperto raccoglie inizialmente una massa critica di identificatori univoci.

• Dati Anagrafici: Nome completo, alias, data e luogo di nascita.
• Identificatori Digitali: Indirizzi email, handle dei social media, numeri di telefono, indirizzi IP.
• Elementi Fisici: Immagini del volto (per il riconoscimento facciale), città di residenza, legami familiari.

Avere più identificatori consente di eliminare i risultati duplicati o errati fin dall'inizio. Se si cerca "Mario Rossi", l'aggiunta di una data di nascita o di una città specifica riduce drasticamente il rumore. Questa fase di preparazione protegge anche l'analista da tentativi di inganno messi in atto da avversari che utilizzano identità sintetiche o società di facciata per nascondere le proprie tracce.

Fase 2: Identificazione delle Fonti e Raccolta (Harvesting)

Con gli obiettivi chiari e gli identificatori isolati, si passa alla fase operativa della raccolta dati. Questo passaggio richiede una strategia di sourcing diversificata. Le informazioni non risiedono tutte nello stesso posto. Il World Wide Web è uno spazio disomogeneo, strutturato in strati di accessibilità.

La Stratificazione del Web

L'accesso alle informazioni segue una logica di sicurezza crescente. Gli strati più esterni sono visibili a tutti, mentre quelli interni richiedono software o protocolli dedicati.

1. Surface Web: Comprende i siti indicizzati dai motori di ricerca come Google o Bing. È la parte più visibile ma spesso la più superficiale.
2. Deep Web: Contiene dati non indicizzati, come database privati, riviste accademiche protette da paywall, registri governativi o documenti legali non pubblici.
3. Dark Web: Richiede reti criptate come Tor o I2P. È il luogo dove spesso finiscono i dati sottratti tramite attacchi hacker o dove avvengono scambi illeciti.

Tipologie di Fonti OSINT

Un'indagine completa deve attingere da diverse categorie di dati per essere considerata attendibile.

• Media Tradizionali: Giornali, riviste, trasmissioni radiofoniche e televisive.
• Registri Governativi: Documenti delle camere di commercio, registri delle proprietà immobiliari, database delle sanzioni e documenti giudiziari.
• Social Media (SOCMINT): Piattaforme come LinkedIn, Facebook, X (Twitter) e Instagram. Questi canali offrono insight comportamentali e reti di contatti che i registri ufficiali ignorano.
• Letteratura Grigia: Studi universitari, rapporti tecnici non pubblicati ufficialmente, brevetti e tesi accademiche.
• Dati Geos spaziali: Immagini satellitari e mappe digitali che permettono di verificare posizioni fisiche o infrastrutture.

Tutorial Strumenti: Automazione della Raccolta

Svolgere la ricerca manualmente è un compito titanico che espone l'analista a errori e omissioni. Per

© 2026 Coondivido — Tutti i diritti sono riservati

questo motivo, l'utilizzo di strumenti di automazione è diventato uno standard professionale.

Maltego: L'Analisi Relazionale

Maltego è una piattaforma di visualizzazione e link analysis che permette di mappare le relazioni tra entità diverse. Funziona attraverso il concetto di "Trasformate", che sono query automatiche inviate verso database esterni o API.

1. Apertura del Grafico: Si inizia inserendo un'entità centrale, come un dominio o il nome di una persona.
2. Esecuzione delle Trasformate: Con un clic, è possibile richiedere a Maltego di trovare tutti gli indirizzi email associati a quel nome o tutti gli IP associati a quel dominio.
3. Espansione dell'Infrastruttura: Maltego può risalire dai DNS Name agli IP, e dagli IP trovare altri siti web ospitati sulla stessa macchina, rivelando infrastrutture nascoste.
4. Visualizzazione: Il risultato è un grafo interattivo dove nodi e frecce mostrano chiaramente le connessioni. È ideale per scoprire se due aziende apparentemente distinte condividono lo stesso server email o lo stesso numero di telefono.

SpiderFoot: L'Impronta Digitale Automatica

Mentre Maltego eccelle nella visualizzazione, SpiderFoot è impareggiabile nella scansione massiva di fonti. È uno strumento open-source che interroga oltre 200 fonti diverse in pochi minuti.

1. Impostazione del Target: Si inserisce l'obiettivo, ad esempio un indirizzo email sospetto.
2. Scelta del Profilo di Scansione: È possibile scegliere tra "Footprint" (mappatura generale), "Investigate" (focus su indicatori malevoli) o "Passive" (raccolta che non interagisce direttamente con il target per non allertarlo).
3. Raccolta Modulare: SpiderFoot attiva moduli per cercare riferimenti nel Dark Web, fughe di dati (leaks), account social e informazioni WHOIS.
4. Export dei Risultati: I dati possono essere visualizzati in tabelle o esportati in formati come JSON o CSV per essere integrati in altri sistemi.

Strumento	Punto di Forza	Limite Principale
Maltego	Mappatura delle relazioni umane e tecniche.	Costo elevato per le API; curva di apprendimento ripida.
SpiderFoot	Automazione estrema; scansione di massa.	Rischio di data overload; richiede filtraggio manuale.
OSINT Framework	Mappa completa dei tool disponibili online.	È una risorsa consultativa, non un software analitico.
Shodan	Ricerca di dispositivi IoT e infrastrutture esposte.	Richiede competenze tecniche di rete avanzate.

Tabella 2: Comparazione degli strumenti OSINT per uso professionale.

Fase 3: Elaborazione e Normalizzazione (Processing)

I dati raccolti nella fase precedente sono disomogenei e spesso "sporchi". L'elaborazione è il processo che trasforma questi dati grezzi in un formato leggibile e pronto per l'analisi. Senza questa fase, l'investigatore si troverebbe di fronte a una montagna di screenshot, file di testo e log di sistema impossibili da sintetizzare.

Pulizia e Selezione

Il primo passo è eliminare le informazioni ridondanti o non pertinenti. Questo include la rimozione di fake news, dati obsoleti o errori di sistema che potrebbero inquinare l'indagine. Se un'azienda sta conducendo una due diligence su un partner commerciale, deve assicurarsi che le recensioni negative trovate online non siano state create ad arte da competitor o bot.

Analisi dei Metadati e Residui Digitali

© 2026 Coondivido — Tutti i diritti sono riservati

Un aspetto cruciale dell'elaborazione riguarda l'estrazione di informazioni nascoste nei file. Ogni azione digitale lascia dei residui che raccontano una storia diversa dal contenuto visibile.

• Dati EXIF: Estrarre i metadati dalle immagini può rivelare le coordinate GPS del luogo in cui è stata scattata la foto, il modello di smartphone utilizzato e l'ora esatta dell'acquisizione.
• Analisi delle Email: Esaminare gli header delle comunicazioni permette di tracciare il percorso dei server, identificare gli indirizzi IP di origine e verificare i meccanismi di autenticazione come SPF o DKIM.
• Cronologia dei Documenti: File Word o PDF possono contenere la cronologia delle revisioni, rivelando nomi di autori o percorsi di cartelle interne che l'organizzazione non voleva rendere pubblici.

Traduzione e Contestualizzazione

In un'indagine globale, è frequente imbattersi in dati in lingue diverse. L'affidarsi ciecamente a traduttori automatici è un errore metodologico grave. Questi strumenti spesso mancano di comprendere lo slang locale, i codici culturali o le sfumature ironiche. L'analista deve contestualizzare l'informazione per evitare che una frase innocua venga interpretata come una minaccia o viceversa.

Fase 4: Analisi e Produzione (Intelligence Evaluation)

L'analisi è il cuore pulsante del ciclo OSINT. In questa fase, l'investigatore mette insieme i pezzi del puzzle per generare insight azionabili. Non si tratta solo di descrivere cosa è stato trovato, ma di interpretarlo per anticipare eventi o confermare ipotesi.

Il Sistema Admiralty (Scala NATO)

Per garantire l'oggettività, l'intelligence professionale non si basa sull'istinto. Utilizza un sistema standardizzato per valutare la qualità delle informazioni: l'Admiralty Code. Questo metodo separa l'affidabilità della fonte dalla credibilità del dato singolo.

Codice Fonte	Affidabilità della Fonte	Codice Dato	Credibilità dell'Informazione
A	Completamente affidabile.	**1**	Confermata da fonti indipendenti.
B	Solitamente affidabile.	**2**	Probabilmente vera.
C	Abbastanza affidabile.	**3**	Possibilmente vera.
D	Di solito non affidabile.	**4**	Dubbia.
E	Inaffidabile.	**5**	Improbabile.
F	Non giudicabile.	**6**	Verità non giudicabile.

Tabella 3: Griglia di valutazione dell'intelligence secondo il codice Admiralty.

Utilizzare questa griglia permette di assegnare un valore preciso a ogni informazione. Ad esempio:

• B2: Un report proveniente da un analista noto con informazioni molto probabili.
• C3: Un'informazione proveniente da una fonte che ha fornito dati corretti in passato, ma che in questo caso non ha conferme esterne.
• F6: Un post anonimo su un forum del Dark Web senza alcuno storico di affidabilità e senza prove a supporto. È un dato che viene registrato ma non utilizzato per decisioni strategiche immediate.

Mitigare i Bias Cognitivi

L'analista deve lottare contro le trappole mentali intrinseche alla natura umana. Il cervello tende a cercare conferme a ciò che già pensa, ignorando le prove contrarie. Questo fenomeno è noto come bias di conferma. In un'indagine OSINT, è facile cadere in "camere d'eco" dove gli algoritmi dei

© 2026 Coondivido — Tutti i diritti sono riservati

motori di ricerca o dei social media continuano a proporre dati simili a quelli già visualizzati, rinforzando una narrazione potenzialmente errata.

Un metodo efficace per contrastare questi errori è l'Analysis of Competing Hypotheses (ACH). L'analista non cerca la spiegazione più probabile, ma elenca tutte le ipotesi possibili e cerca attivamente di smentirle. Vince l'ipotesi che resiste meglio ai tentativi di confutazione, non quella che sembra più intuitiva.

Fase 5: Disseminazione e Feedback

Un'indagine non si conclude quando l'analista ha trovato la risposta. Termina quando quella risposta viene comunicata efficacemente al destinatario. Senza una comunicazione chiara, anche la ricerca più brillante perde valore strategico.

La Redazione del Report

Il report finale deve essere un documento denso ma leggibile, privo di frasi inutili e focalizzato sui fatti. Un dossier professionale segue solitamente questa struttura:

1. Executive Summary: Un riassunto di poche righe che presenta i risultati principali. Il decisore deve capire immediatamente il livello di rischio o l'opportunità rilevata.
2. Metodologia e Limiti: Descrive quali fonti sono state interrogate e quali sono state le difficoltà. Essere onesti su ciò che "non è stato possibile verificare" è fondamentale per costruire fiducia.
3. Analisi delle Relazioni: Utilizzo di grafici e tabelle per mostrare legami tra persone, aziende e infrastrutture digitali.
4. Conclusioni e Raccomandazioni: L'analista suggerisce le azioni successive basate sulle evidenze raccolte.

L'Importanza del Feedback

Il ciclo OSINT è iterativo. Una volta consegnato il report, il destinatario potrebbe avere nuove domande o il contesto potrebbe cambiare. Il feedback permette di capire se l'indagine deve ricominciare con nuovi parametri o se può considerarsi conclusa. Questo flusso continuo assicura che l'intelligence rimanga dinamica e sempre allineata alle necessità operative dell'organizzazione.

Casi Studio e Fallimenti: Imparare dagli Errori

Analizzare casi reali permette di comprendere l'impatto di una cattiva metodologia.

Il Fallimento del "Dato Casuale"

In molti casi, l'errore non risiede nella mancanza di dati, ma nella loro cattiva interpretazione. Un esempio classico riguarda l'analisi dei rischi basata solo sull'osservazione superficiale. Nel 2017, a Mosul, una donna riuscì a passare i controlli di sicurezza portando in braccio un bambino. Le guardie, influenzate dal bias che vede le madri come innocue, non controllarono le sue mani, dove stringeva il detonatore. Questo errore di valutazione dimostra come i pregiudizi umani possano accecare anche di fronte all'evidenza fisica. In ambito OSINT, questo si traduce nel fidarsi ciecamente di una fonte "autorevole" senza verificare i dati specifici che sta fornendo.

Il Successo del Tracciamento Finanziario

D'altro canto, l'OSINT ha permesso di smascherare reti criminali complesse. Investigazioni recenti sui flussi di fentanyl tra aziende farmaceutiche cinesi e mercati internazionali hanno dimostrato come l'incrocio tra dati doganali, registri societari e forum del Dark Web possa rivelare sistemi di corruzione globale che sfuggono alle agenzie di polizia tradizionali. In questo caso, la capacità di seguire la traccia digitale attraverso diversi continenti è stata la chiave del successo.

© 2026 Coondivido — Tutti i diritti sono riservati

L'Era dell'IA e il Futuro dell'OSINT

L'intelligenza artificiale sta cambiando le regole del gioco. Se da un lato l'IA generativa può aiutare a scrivere codice per automatizzare la raccolta, dall'altro introduce nuovi pericoli. I malintenzionati utilizzano l'IA per creare deepfake o per generare campagne di disinformazione su vasta scala, rendendo il compito dell'analista ancora più arduo.

Inoltre, i testi generati da intelligenze artificiali tendono a seguire pattern linguistici prevedibili, come l'uso eccessivo di termini neutri o costruzioni passive. Un analista moderno deve essere in grado di riconoscere queste tracce per distinguere tra contenuti autentici e manipolazioni artificiali. La sfida del futuro sarà l'integrazione di sistemi di difesa basati sull'IA per validare i dati alla velocità della luce, mantenendo però sempre l'uomo come ultimo giudice della verità.

L'attività OSINT non è una semplice sequenza di ricerche su Google. È una disciplina che richiede rigore metodologico, capacità tecniche e una profonda consapevolezza psicologica dei propri limiti. Dalla definizione chirurgica dei requisiti alla valutazione secondo il codice Admiralty, ogni passaggio è essenziale per garantire che l'intelligence prodotta sia solida e azionabile. Il sovraccarico di informazioni e la disinformazione sono i nemici principali, ma possono essere sconfitti attraverso l'uso consapevole di strumenti come Maltego e SpiderFoot, abbinati a un pensiero critico instancabile.

Se vuoi approfondire come queste tecniche possono proteggere la tua azienda o supportare le tue indagini, inizia oggi stesso a strutturare il tuo metodo. Non limitarti a raccogliere dati: trasformali in conoscenza.

Vuoi approfondire strumenti, tecniche e casi reali?
Iscriviti alla newsletter **OSINT & AI per tutti** su Substack: https://coondivido.substack.com/
Unisciti al canale Telegram: https://t.me/osintaipertutti

© 2026 Coondivido — Tutti i diritti sono riservati