OPEN SOURCE INTELLIGENCE

TOOLS, TECHNIQUES, BEST PRACTICES & METHODOLOGIES

For Insider Threat • Insider Breach • Insider Risk Management

A Practitioner's Reference Guide

Date: June 2026 | Version 1.0

Classification: RESTRICTED – Security Practitioners Only

Presented by: Wolfhound Consulting and Investigation Services (WCIS)
https://wolfhoundcis.com

Table of Contents

1. Executive Summary

This guide is a practitioner-level reference for security analysts, HR professionals, corporate investigators, legal counsel, and insider risk programme managers who need to apply Open Source Intelligence (OSINT) systematically to detect, investigate, and manage insider threats, breaches, and ongoing risk.

Unlike introductory OSINT texts, this document focuses on applied methodology: the step-by-step techniques, specific tools, and structured workflows that translate raw open-source data into actionable insider risk intelligence. Every methodology described here must be executed within a legally authorised framework and with documented investigative purpose.

SCOPE NOTE

This guide covers all three Web tiers (surface, deep, and dark web), SOCMINT, technical footprinting, behavioural analysis, UEBA integration, and four detailed investigation playbooks. It complements an organisation's Insider Risk Management policy and the companion document OSINT in the Context of Insider Threat, Breach & Risk Management (Canadian Legal Perspectives).

2. How to Use This Guide

This guide mirrors the lifecycle of an insider threat investigation. Practitioners should:

- Start with Section 3 (Methodology) to understand the governing framework before touching any tools.
- Use Section 4 (Preparation) as a checklist before beginning any investigation.
- Follow Phases 1–5 (Sections 5–9) sequentially for new investigations; return to individual phases for follow-on work.
- Use Section 10 (Tool Catalogue) as a reference when selecting tools for specific investigative tasks.
- Apply the Playbooks in Section 11 for common scenario types – adapt to your specific context.
- Consult Sections 12–14 for evidence handling, best practices, and programme performance.

LEGAL PREREQUISITE

Before conducting any OSINT investigation involving an identified individual, confirm: (1) legal authority or organisational policy authorises the investigation; (2) a documented purpose and proportionality assessment is complete; (3) a chain-of-custody log has been opened; (4) findings will be reviewed by legal counsel before any adverse action.

3. OSINT Intelligence Cycle and Core Methodologies

3.1 The OSINT Intelligence Cycle (Six-Phase)

All OSINT investigations follow a structured intelligence cycle. This prevents undirected data hoarding and ensures collection serves a specific analytical requirement:

1	**Planning & Direction (Requirements)** Define the specific intelligence question: Who is the subject? What indicators triggered the investigation? What is the legal authority? What information is needed and why?
2	**Collection (Gathering)** Execute passive and active collection across defined OSINT sources using Phases 1–5. Document each source, URL, query, and timestamp contemporaneously.
3	**Processing & Exploitation** Organise and normalise raw data. Remove duplicates, convert formats, extract key indicators (email addresses, usernames, IP addresses, phone numbers, aliases).
4	**Analysis** Apply analytical frameworks (Diamond Model, ACH, timeline analysis) to identify patterns, anomalies, and associations. Assign confidence levels to each finding.
5	**Production (Reporting)** Produce a structured intelligence product appropriate to the audience: a brief for HR, a detailed report for legal, or a case file for law enforcement referral.
6	**Dissemination & Feedback** Share findings through appropriate channels to decision-makers. Obtain feedback on whether intelligence answered the requirement; adjust collection if not.

3.2 The OWASP OSINT Framework

The OWASP Testing Guide and OSINT Framework (osintframework.com) provide a structured taxonomy of sources by investigative category. The most relevant categories for insider threat are:

OWASP Category	Insider Threat Relevance	Example Sources/Tools
Username / Handle	Identify aliases used on social media, forums, and dark web platforms	Sherlock, WhatsMyName, Namechk
Email Address	Verify identity, find associated accounts, check breach exposure	Hunter.io, EmailRep, HaveIBeenPwned, Holehe
IP Address / Domain	Trace shadow IT, unauthorised cloud services, exfiltration destinations	Shodan, Censys, VirusTotal, WhoisXML API
Social Networks	Map associations, detect disgruntlement, foreign contacts, job-seeking	Maltego, Skopenow, SocialLinks, ShadowDragon
Public Records	Background verification, financial distress, prior misconduct	CanLII, SEDAR+, provincial court registries
Dark Web	Credential sale, insider-for-hire offers, exfiltrated data listings	DarkOwl, Recorded Future, Flashpoint, IntelX
Geospatial	Verify travel claims, map access patterns, confirm locations	Google Earth, Creepy, EXIF analysis, Yandex Maps

3.3 The Diamond Model Applied to Insider Threats

The Diamond Model of Intrusion Analysis, adapted for insider threats, provides a structured framework for understanding the four core vertices of any insider incident:

Vertex	Insider Threat Interpretation	OSINT Collection Focus
Adversary (Insider)	The individual with authorised access who poses the threat. Includes motivation, capability, and intent.	Digital identity, social media, professional history, associations, behavioural indicators
Capability	The insider's technical or physical ability to cause harm: skills, access level, and available tools.	GitHub/technical forums, certifications, job postings, skills listed on professional profiles
Infrastructure	The channels, systems, or intermediaries the insider uses or plans to use.	Shadow IT, cloud storage, dark web accounts, email accounts, communication channels
Victim	The specific asset, system, or person targeted – what the insider is trying to access or harm.	Cross-reference with internal asset inventory; dark web data listing content analysis

3.4 Passive / Semi-Passive / Active – Decision Framework

Method	Description	Risk Level	When to Use
Passive	Review publicly indexed content. No direct system or platform interaction. No queries directed at subject's infrastructure.	Low	Always appropriate; use as default for all investigations.
Semi-Passive	Targeted queries of public APIs, database searches, or platform searches that leave minimal footprint.	Medium	Appropriate when passive methods are insufficient; document each query.
Active	Direct interaction with subject's online presence, systems, or contacts. May generate notifications or access logs.	High	Use only with legal authorisation; assess alerting risk before proceeding.

ACTIVE OSINT – SPECIAL CAUTION

Active techniques such as creating test accounts to follow a subject, directly querying a subject's exposed infrastructure, or sending connection requests to a person under investigation may constitute unauthorised access under Criminal Code s. 342.1 or trigger privacy law liability. All active techniques must be reviewed by legal counsel before deployment.

4. Pre-Investigation Preparation

4.1 Defining Requirements and Legal Authority

Document the following in a Case Initiation Record before opening an investigation:

- Investigation Trigger: The specific indicator that prompted the investigation (e.g., DLP alert, manager report, access anomaly, HR referral).
- Subject Identification: Name, employee ID, role, access level, and relevant HR status.
- Intelligence Requirement: The specific questions this investigation must answer.
- Legal Basis: Applicable authorisation – organisational policy, PIPEDA s.7(1)(b), provincial equivalent, or national security authority.
- Scope Limitation: What sources may and may not be collected; what information categories are in scope.

- Handling Instructions: Classification level, authorised recipients, and retention period.
- Review Checkpoint: Date by which findings must be reviewed by legal or HR before any adverse action.

4.2 Investigator Operational Security (OPSEC)

Investigators must protect their identities from detection by the subject. A compromised investigation can alert an insider, trigger evidence destruction, accelerate exfiltration, or expose the organisation to legal liability.

OPSEC FUNDAMENTALS

Use dedicated investigative infrastructure – never personal accounts or devices for OSINT on a subject.

Deploy a VPN with an appropriate exit node before any online investigation activity.

Use a hardened browser (Firefox with privacy extensions, or Tor Browser for dark web) with JavaScript disabled where possible.

Create investigative cover personas ('sock puppet' accounts) that are aged, plausible, and disconnected from the organisation. Document their creation and use.

Never 'like', follow, or interact with subject accounts on social media – this creates evidence of investigation and may alert the subject.

Review EXIF metadata before sharing any screenshots – they may contain investigator device or location data.

Use full-page screenshot tools (e.g. Hunchly, Fireshot, HTTrack) with timestamps for evidential capture.

4.3 Infrastructure and Tool Hygiene

- Operating System: A dedicated VM (e.g., TAILS, Whonix, or Kali Linux) isolated from corporate networks during investigation sessions.
- Browser Configuration: Firefox with uBlock Origin, Privacy Badger, Canvas Blocker, and User-Agent Switcher. Disable WebRTC to prevent IP leaks.
- Proxy / VPN: Route all traffic through a commercial VPN (not the corporate VPN). Consider Tor for high-sensitivity investigations.
- Evidence Storage: Encrypted, access-controlled storage for all OSINT artefacts. Folder structure by case reference and date.

- Tool Licensing: Confirm that all commercial tools are properly licensed for investigative use. Some platform licences restrict HR or employment screening use.
- Data Retention: Apply the organisation's data retention policy to all collected OSINT data.

5. Phase 1 – Subject Identification and Digital Footprint Mapping

Phase 1 establishes the subject's digital identity and maps their presence across the open web. This baseline intelligence picture informs all subsequent phases and reduces wasted effort by identifying which platforms are most likely to yield relevant intelligence.

5.1 Identity Resolution Techniques

Technique	Description	Tools
Email Pivot	Use a known email to find associated accounts, breach exposure, and registration history.	Hunter.io, EmailRep.io, HaveIBeenPwned, Holehe
Username Enumeration	Search known usernames or likely variants across 300+ platforms simultaneously.	Sherlock (CLI), WhatsMyName.app, Namechk, KnowEm
Reverse Phone Lookup	Identify names, addresses, and associated social accounts from a phone number.	NumLookup, TrueCaller, SpiderFoot (phone module)
Reverse Image Search	Identify other online uses of a profile photograph to uncover aliases or alternate accounts.	Google Images, TinEye, Yandex Images, PimEyes
Digital Identity Graph	Build a visual map of all confirmed and suspected accounts, email addresses, and usernames.	Maltego (Person entity), SpiderFoot HX
Metadata Extraction	Extract hidden metadata from public documents (EXIF, PDF author fields, GPS coordinates).	ExifTool, FOCA, Metagoofil

5.2 Professional Network Analysis

- LinkedIn Profile Deep Dive: Review full employment history, education, endorsements, publications, and connections for inconsistencies or undisclosed affiliations. Note recent posts and activity patterns.
- Job Seeking Signals: Active job applications, profile set to 'open to work', or sudden profile updates signal imminent departure and elevated exfiltration risk.

- Competitor Connections: Identify connections to competitor employees, foreign government-linked organisations, or persons of concern.
- Skills Review: Technical skills may reveal capabilities relevant to a suspected breach method (database administration, cloud architecture, cryptography).
- Temporal Analysis: Review post timestamps for anomalies (unusual activity at night, posting during claimed sick leave).

LINKEDIN OPSEC NOTE

Do NOT use a personal or corporate LinkedIn profile to view a subject's profile – LinkedIn notifies users of profile viewers unless the investigator's account is set to private browse mode. Use a properly constructed cover persona account or access the profile through a cached search engine version (e.g., Google cache).

5.3 Open Records and Corporate Intelligence

- Court Records: Search provincial court registries and CanLII for civil litigation, criminal history, restraining orders, and bankruptcy proceedings. Financial distress is a key insider risk indicator.
- Corporate Registry: Search the Canada Business Registry and provincial equivalents for companies the subject has incorporated, directorships, and registered addresses.
- SEDAR+ / Securities Filings: For subjects involved in publicly traded companies, review insider trading filings, director disclosures, and regulatory submissions.
- Property Records: Provincial land registry searches reveal undisclosed real estate holdings or sudden property acquisitions indicating unexplained wealth.
- Sanctions and Watchlists: Screen against Global Affairs Canada designated persons list, OFAC SDN list, UN consolidated sanctions list, and Interpol Red Notices.

6. Phase 2 – Social Media Intelligence (SOCMINT)

Social media platforms are among the richest and most time-sensitive OSINT sources for insider threat investigations. SOCMINT must be collected quickly – subjects frequently delete content when they become aware of an investigation.

6.1 Platform-by-Platform Approach

Platform	Key Intelligence Value	Key Techniques	OPSEC
LinkedIn	Employment history, job-seeking, professional associations, skills	Profile review, connection analysis, activity timeline	Private mode or sock puppet; do not connect
X / Twitter	Real-time views, grievances, ideological indicators, posting patterns	Advanced search, follower analysis, timeline review	Logged out or cached; avoid interactions
Facebook	Personal associations, life events, travel, financial signals	Public profile, event attendance, photo geolocation	Sock puppet; do not friend/follow
Instagram	Location data in photos, lifestyle/wealth, association networks	EXIF from public photos, tagged locations	Logged out; do not like or comment
Reddit	Anonymous candid views, financial discussions, forum participation	Username search, subreddit history, Pushshift archive	Public content; no login needed
Telegram	Extremist community membership, foreign contact channels	Public channel/group monitoring, username search	Review public channels only; joining creates footprint
GitHub	Technical capability, code commits, exposed credentials	Repository review, commit history, gist analysis	No login needed for public repos

6.2 Behavioural and Sentiment Analysis

- Disgruntlement Indicators: Posts expressing anger, resentment, or grievance about the organisation, management, pay, or colleagues. Escalating negativity over time is a key precursor.
- Financial Distress Signals: Posts referencing debt, financial hardship, missed payments, or requests for financial help. Cross-reference with public court records.
- Foreign Contact Indicators: Sudden increased communication with individuals in countries associated with state-sponsored threat activity.
- Dual Employment Signals: Mentions of secondary employment, consulting, or projects that may conflict with obligations, particularly with competitors.

- Exfiltration Precursors: Posts referencing job offers, career transitions, or starting competing businesses while still employed.
- Ideological Radicalisation: Content expressing extremist or foreign-state-aligned positions directed at the employer or industry.

AUTOMATION TIP: SENTIMENT ANALYSIS AT SCALE

Enterprise SOCMINT platforms (e.g., Skopenow, ShadowDragon, DigitalStakeout, Babel X) provide automated sentiment scoring, behavioural change alerts, and keyword-triggered notifications. These significantly reduce analyst time compared to manual monitoring. All automated monitoring requires a governance framework ensuring proportionate, documented, legally authorised use.

6.3 Network and Association Mapping

Understanding a subject's social network identifies potential co-conspirators or recipients of exfiltrated information; foreign-state linked individuals who may have recruited or directed the insider; organised crime associations; and competitors who may be the ultimate beneficiary of insider activity.

- Follower/Following Analysis: Who follows the subject and who do they follow? Identify unusual, foreign-government-linked, or criminal-adjacent accounts.
- Mutual Connection Analysis: Which connections are shared with known persons of concern?
- Mention and Tag Analysis: Who does the subject publicly interact with, and in what context?
- Graph Visualisation: Use Maltego to build a visual network graph of online associations, overlaid with intelligence from other phases.

7. Phase 3 – Dark Web and Deep Web Monitoring

7.1 Understanding the Web Tiers

Tier	Definition	Insider Threat Relevance	Access Method
Surface Web	Publicly indexed content accessible via standard search engines.	Social media, professional profiles, news, court records, corporate filings.	Standard browser; no special access required.

Deep Web	Non-indexed content requiring authentication or direct URLs, but not inherently illicit.	Paywalled databases, academic repositories, some paste sites, subscription databases.	Direct URL, credentials, or database subscription.
Dark Web	Content on Tor (.onion), I2P, or Freenet networks – predominantly anonymous.	Credential markets, insider-for-hire forums, ransomware sites, exfiltrated data repos.	Tor Browser with VPN; hardened environment; documented authorisation required.

7.2 Credential Exposure and Breach Monitoring

Monitoring for exposed employee credentials is one of the highest-value dark web OSINT activities. Credentials in breach databases indicate compromised insider scenarios, password reuse risk, or potentially deliberate self-exposure by a disgruntled employee.

- Corporate email domain monitoring: all @organisation.ca addresses in breach databases.
- Executive and high-privilege user credential monitoring with priority alerting.
- Hash monitoring: where passwords are hashed, platforms such as SpyCloud perform pre-computation to recover the original password.
- Alert thresholds: define what credential exposures trigger immediate investigation vs routine password rotation.

7.3 Insider-for-Hire and Data Marketplace Monitoring

Dark web forums regularly contain posts from disgruntled employees offering insider access, and from threat actors actively recruiting insiders at specific organisations. Key monitoring indicators:

- Posts advertising ‘legitimate access’ to specific organisations, sectors, or system types on cybercriminal forums.
- Data listings that include organisation-specific file naming conventions, internal terminologies, or proprietary data structures – suggesting an insider source.
- Recruitment threads targeting specific job roles (‘seeking IT admin at Canadian bank’) that may be used to recruit current employees.
- Identity data sets matching the organisation’s customer or employee profile – suggesting an ongoing or completed exfiltration.

DARK WEB INVESTIGATION CAUTION

Direct participation in dark web forums, making purchases, or direct contact with threat actors may constitute criminal activity and could compromise any prosecution. Dark web monitoring should be conducted exclusively through passive observation of public content or through licensed commercial monitoring platforms. Investigators must not create accounts on dark web markets or engage in any transaction.

8. Phase 4 – Technical Footprinting and Cyber Intelligence

8.1 Domain and Infrastructure Intelligence

Technique	Intelligence Value	Tools
WHOIS / RDAP Lookups	Identify domain registrants, registration dates, and name servers that may link a subject to external infrastructure.	WhoisXML API, DomainTools, ICANN RDAP
Reverse WHOIS	Find all domains registered by a specific email or registrant name – exposing undisclosed businesses or foreign affiliations.	DomainTools, ViewDNS.info, SecurityTrails
Certificate Transparency (CT) Logs	Identify TLS certificates for shadow IT services or subdomains used as exfiltration endpoints.	crt.sh, Censys, Facebook CT Monitor
Passive DNS Analysis	Review historical DNS resolution to identify when a domain appeared, associated IPs, and name server changes.	SecurityTrails, PassiveTotal (RiskIQ), Farsight DNSDB
Shodan / Censys Scanning	Identify publicly exposed servers, services, and IoT devices associated with a subject or their external contacts.	Shodan.io, Censys.io
BGP / ASN Lookup	Determine if traffic is routed through foreign state-controlled infrastructure by identifying the owning ASN.	BGPView, Team Cymru IP-ASN Mapping

8.2 Code Repository Monitoring

- Secret / Credential Scanning: Monitor GitHub for commits containing API keys, database credentials, tokens, or connection strings. Tools: GitGuardian, TruffleHog, Gitleaks.
- Source Code Leakage: Watch for commits containing proprietary algorithm implementations, internal system documentation, or code with corporate copyright headers.
- Attribution: Review commit metadata (email addresses, usernames) to attribute repositories to specific subjects.
- Timing Analysis: Examine commit timestamps for activity outside business hours or during periods of concern (notice periods, disciplinary proceedings).

8.3 Email and Communication Intelligence

- Email Existence Validation: Tools such as Hunter.io verify whether an email address exists and is associated with a specific domain.
- Email Header Analysis: If an email from the subject is publicly available, extract originating IP, mail client, and routing from Received: headers.
- Email Breach Exposure: Submit corporate and personal email addresses to HaveIBeenPwned, DeHashed, or IntelX to identify breach dataset appearances.
- Email Permutation Discovery: Use theHarvester or Hunter.io to enumerate all email addresses at an organisation's domain, revealing previously undisclosed accounts or aliases.

9. Phase 5 – Behavioural Pattern Analysis and UEBA Integration

9.1 Connecting OSINT to Internal UEBA Signals

The full power of OSINT in insider risk is realised when open-source intelligence is fused with internal behavioural data from UEBA platforms, SIEM, DLP, and access control systems. OSINT provides the contextual explanation for anomalies that internal tools detect but cannot interpret:

Internal UEBA/SIEM Signal	Corroborating OSINT Investigation
Unusual data download volume outside business hours	Check dark web for related credential listings; review social media for job seeking or grievance indicators; review court records for financial distress.

Access to systems outside normal role scope	Review LinkedIn for skills/interests that do not match declared role; check technical forums for posts about the accessed systems.
Bulk email forwards to personal address	Check personal email in breach databases; review social media for competitor contacts; check GitHub for recent public repository activity.
VPN access from unusual geographic location	Cross-reference with public social media check-ins, flight booking confirmations posted publicly, or LinkedIn location updates.
Sudden resignation or notice period	Elevate monitoring immediately; review LinkedIn for job application signals; check for recent GitHub commits; monitor dark web for data listings.
Repeated failed privilege escalation attempts	Check technical forums and GitHub for the subject's posts about system administration; review for dark web forum activity related to the targeted systems.
Printing or USB transfer of large file volumes	Review for job interview signals on public platforms; check for competitor employee connections on LinkedIn; check for freelance service listings.

9.2 Insider Risk Indicator Scoring Framework

OSINT findings should be structured against a defined Insider Risk Indicator framework to produce a consistent, defensible risk score:

Risk Domain	OSINT-Observable Indicators	Weight
Financial Distress	Bankruptcy filings, court judgements, social media posts about debt/hardship, unexplained new wealth (property, luxury goods).	High
Disgruntlement	Social media grievance posts, negative employer reviews, forum complaints, escalating negative tone over time.	High
Foreign Contact	LinkedIn connections to foreign government employees, social media contact with sanctioned-country nationals, unexplained foreign travel.	High
Dual Employment	LinkedIn secondary job listings, GitHub projects for competing organisations, freelance platform profiles (Upwork, Toptal).	Medium
Ideological Alignment	Public support for extremist, foreign state, or anti-establishment ideologies; membership in relevant online communities.	Medium

Technical Capability	Advanced skills in data exfiltration, anonymization, or cryptography demonstrated on technical forums or code repositories.	Medium
Life Stressors	Divorce filings, custody disputes, bereavement posts – indicative of personal stress that may elevate susceptibility to exploitation.	Low–Medium
Credential Exposure	Employee email/password found in dark web breach databases – indicates either compromise or deliberate sharing.	Medium–High

SCORING CAUTION

Risk scoring based on OSINT must never be used as the sole basis for adverse employment action. Indicators are probabilistic, not deterministic. Each finding must be corroborated, individually assessed for accuracy, and reviewed by HR and legal before any action is taken.

10. Tool Reference Catalogue

All tools should be evaluated for licensing compliance, data handling terms, and compatibility with applicable privacy law before deployment.

10.1 Free / Open-Source Tools

■ theHarvester *[Email / DNS / OSINT Aggregator]* Access: Free / Open Source

Use Case: Gather email addresses, subdomains, employee names, and open ports. Ideal for domain-based reconnaissance.

- Queries Google, Bing, LinkedIn, Shodan, and 25+ sources simultaneously
- Returns email addresses, subdomains, IPs, and banner data
- CLI-based; integrates with Python OSINT toolchains
- Useful to enumerate all corporate email addresses for cross-checking

■ Sherlock *[Username Enumeration]* Access: Free / Open Source

Use Case: Search for a username across 300+ social media platforms to identify all accounts a subject may hold.

- Single CLI command returns results for 300+ platforms within minutes

- Essential for mapping digital identity beyond declared accounts
- Combines with Maltego for visual network mapping
- Actively maintained; regularly updated with new platforms

■ SpiderFoot *[Automated OSINT Aggregator]* Access: Free (Community) / Commercial (HX Edition)

Use Case: Automates collection across 100+ data sources given a domain, email, username, IP, or name. API integration with SIEM.

- Modules covering DNS, WHOIS, social media, breach databases, paste sites, and more
- Web-based interface (HX Edition) provides collaborative investigation workspaces
- Generates graph visualisations of discovered relationships
- API enables automated enrichment of SIEM/UEBA alerts with OSINT context

■ Maltego Community Edition *[Link Analysis and Visualisation]* Access: Free (Community, 12 results/transform) / Commercial

Use Case: Gold standard for visualising relationships between people, domains, IPs, and social accounts.

- Transform-based architecture integrates with 60+ third-party data providers
- Visual graph interface maps connections between entities at scale
- Pivoting: start with email → social accounts → infrastructure → associates
- Community Edition free; commercial editions remove result limits

■ ExifTool *[Metadata Extraction]* Access: Free / Open Source

Use Case: Extract hidden metadata from documents, images, PDFs, and other files shared publicly.

- Supports 100+ file formats: JPEG, PDF, DOCX, XLSX, MP4, and more
- Reveals GPS coordinates embedded in photos – critical for location verification
- Document metadata reveals authorship, organisation name, software, and edit history
- Essential for verifying provenance of any document attributed to a subject

■ Recon-ng *[Modular Web Reconnaissance Framework]* Access: Free / Open Source

Use Case: Modular framework for web-based reconnaissance with 35+ modules covering search engines, social media, and public databases.

- Python-based; CLI-driven; fully extensible module architecture
- Modules for Shodan, BuiltWith, GitHub, LinkedIn, Twitter, and more
- Database back-end stores results for cross-module analysis
- Ideal for structured, repeatable collection workflows in corporate investigations

10.2 Commercial Platforms

■ Skopenow *[Social Media / Deep Web Investigation Platform]* Access: Commercial (Subscription)

Use Case: AI-driven SOCMINT and public records investigation platform used by corporate investigators and HR teams for due diligence and insider threat.

- Automated subject profiling across social media, news, court records, and public databases
- Behavioural analysis and flagging for high-risk content (violence, extremism, substance abuse)
- Customisable report generation for HR and legal audiences
- Compliant data handling features designed for employment screening use cases

■ ShadowDragon *[Social Media & Dark Web Intelligence Platform]* Access: Commercial (Subscription)

Use Case: Provides deep social media analysis, dark web monitoring, and entity tracking. Strong on platform-native API access and historical data.

- SocialNet module searches 200+ social media platforms for a single identifier
- OSINT Industries integration for comprehensive identity pivot
- Historical data access for retrospective investigation
- Designed by and for investigative professionals

■ Palantir Gotham *[Enterprise Intelligence Platform]* Access: Commercial (Enterprise Licence)

Use Case: Enterprise-grade intelligence management and link-analysis. Deployed by major Canadian financial institutions, government agencies, and law enforcement.

- Integrates OSINT data with internal structured data (HR records, access logs, financial transactions)
- Advanced graph analytics and anomaly detection at scale
- Role-based access controls and full audit trail for regulatory compliance
- Requires significant implementation investment and analyst training

■ DigitalStakeout *[Multi-Source OSINT Investigation Platform]* Access: Commercial (Subscription)

Use Case: Practitioner-focused platform combining people search, social media monitoring, dark web scanning, and breach data access.

- Unified search across people, companies, domains, email addresses, and phone numbers
- Continuous monitoring with automated alerting for subject mentions

- Data breach search with direct access to breach database integrations
- Includes case management and structured reporting features

10.3 Dark Web and Credential Monitoring

■ Recorded Future *[Threat Intelligence Platform]* Access: Commercial (Enterprise)

Use Case: Comprehensive TI platform using ML and human analysis. Real-time intelligence from open, deep, and dark web sources.

- Real-time dark web forum and marketplace monitoring for credential exposures and insider-for-hire
- Predictive risk scoring and prioritised alert feeds
- Integration with SIEM, SOAR, and identity management platforms
- Widely deployed across Canadian critical infrastructure and financial sector

■ DarkOwl Vision *[Dark Web Data Provider]* Access: Commercial (API / Platform)

Use Case: World's largest commercially available darknet data index. Search engine-like access to raw dark web content for investigations.

- Continuous indexing of Tor, I2P, and ZeroNet; billions of indexed documents
- Historical archive for retrospective searches – when did data first appear?
- REST API for automated monitoring pipelines
- Best for teams needing raw darknet access for manual deep-dive analysis

■ SpyCloud *[Credential Monitoring and ATO Prevention]* Access: Commercial (Enterprise)

Use Case: Specialised credential recapture platform with 53+ billion identity records. Optimised for enterprise credential and account takeover prevention.

- Automated monitoring for corporate domain credentials in breach databases
- Pre-computation of password hashes to recover plaintext credentials
- Employee-level alerting with actionable remediation recommendations
- Integration with identity management for automated password reset triggers

■ Flashpoint *[Business Risk Intelligence Platform]* Access: Commercial (Enterprise)

Use Case: Deep and dark web intelligence focused on business risk including insider threat, fraud, and physical security.

- Access to closed and restricted criminal forums not covered by standard dark web tools
- Analyst-curated intelligence on threat actor TTPs relevant to specific sectors
- Insider threat and fraud intelligence feeds for financial, healthcare, and government sectors

- SIEM and SOAR integration for automated alert enrichment

■ Have I Been Pwned (HIBP) *[Credential Breach Check]* Access: Free / Commercial API

Use Case: Most widely used public credential breach database. Free lookups at haveibeenpwned.com; domain monitoring via commercial API.

- Domain Search feature notifies security teams of new employee credential exposures
- Covers 12+ billion records across hundreds of historical breaches
- Commercial API enables bulk checking and continuous domain-level monitoring
- Notification Emails alert the registered domain owner on new breach appearances

10.4 Link Analysis and Technical Tools

■ Maltego Full Edition *[Link Analysis and Graph Intelligence]* Access: Commercial (Subscription)

Use Case: Full commercial version removes Community Edition limitations. Access to premium transform packs.

- Unlimited entity pivot and transform results
- Premium transforms: Shodan, VirusTotal, DomainTools, LexisNexis, FullContact, Recorded Future
- Collaboration features for team-based investigations
- Automated transform workflows for repeatable investigative patterns

■ Shodan *[Internet-Connected Device Search Engine]* Access: Free (limited) / Commercial

Use Case: Search engine for internet-connected devices. Identifies exposed services, default credentials, and vulnerable infrastructure.

- Real-time indexing of internet-connected devices worldwide
- Search by organisation name, ASN, IP range, or service type
- Historical data API to see when a device or service first appeared publicly
- Essential for identifying shadow IT, exposed cloud buckets, or exfiltration endpoints

■ IntelX (Intelligence X) *[Search Engine for Rare Data Sources]* Access: Free (limited) / Commercial

Use Case: OSINT search engine providing access to dark web content, Tor sites, I2P data, data leaks, and historical web archives.

- Indexes Tor, I2P, data leak sites, pastes, and historical web archives
- Email, phone, domain, and IP-based searches across all indexed sources
- Historical archive reaching back decades for retrospective investigation

- Sensitive data handling: access to breach data requires documented legitimate use case

11. Investigation Playbooks

The following playbooks provide step-by-step guidance for the four most common OSINT investigation scenarios in insider risk management. Each must be adapted to the specific organisational context and executed under documented authorisation.

Playbook A – Pre-Employment OSINT Screening

SCENARIO

Enhanced due diligence on a candidate for a sensitive role: privileged IT access, access to classified information, executive position, or critical infrastructure.

Step	Action	Tools	Output
A1	Obtain written consent (where required) or document legal basis for collection without consent.	—	Consent form or legal basis memo
A2	Identity resolution: verify name, email, phone, and aliases. Map all known digital identities.	Sherlock, Holehe, theHarvester, Maltego	Identity profile with confirmed accounts
A3	Professional history verification: check LinkedIn, company websites, and professional registries against CV claims.	LinkedIn, CanLII, professional licensing DBs	Verified/disputed career timeline
A4	Social media review: review all confirmed public accounts for risk indicators. Screenshot and document.	Manual + Skopenow / DigitalStakeout	SOCMINT summary report with screenshots
A5	Public records check: court records, bankruptcy, litigation, regulatory sanctions.	CanLII, provincial court registries, SEDAR+	Public records summary

A6	Sanctions screening: check against Canadian, US, and UN sanctions lists, Interpol notices.	Global Affairs Canada, OFAC, UN Sanctions, Interpol	Clear/match screening result
A7	Credential breach check: check known email addresses for breach exposure.	HaveIBeenPwned, SpyCloud, IntelX	Breach exposure report
A8	Document all findings, assign confidence levels, prepare structured screening report.	Case management system	Completed Pre-Employment OSINT Report
A9	Legal review before use in employment decision. Retain per policy then securely destroy.	—	Legal sign-off; retention action documented

Playbook B – Triggered Insider Risk Investigation

SCENARIO

A behavioural trigger has been identified for a current employee (UEBA alert, manager referral, DLP event, HR concern). An investigation is warranted to determine whether insider threat activity is occurring or imminent.

Step	Action	Tools	Output
B1	Open Case Initiation Record. Document trigger, subject details, legal basis, scope, and assigned investigator.	—	Case file opened
B2	Establish investigative infrastructure: VPN, isolated VM, sock puppet accounts if needed.	TAILS/Whonix, commercial VPN	Secure investigation environment confirmed
B3	Digital footprint mapping: enumerate all online accounts and digital identities.	Sherlock, SpiderFoot, Maltego	Digital identity map
B4	SOCMINT review: systematic review of all identified social media	Manual + Skopenow, ShadowDragon	SOCMINT findings with timestamps

	accounts. Screenshot all relevant content immediately.		
B5	Credential exposure check: determine if subject's credentials are in breach databases or dark web markets.	SpyCloud, DarkOwl, HaveIBeenPwned	Credential exposure status
B6	Technical footprinting: shadow IT, personal cloud services, GitHub activity, domain registrations.	Shodan, Censys, crt.sh, DomainTools, GitHub	Technical intelligence summary
B7	Public records review: recent court filings, corporate registry changes, property transactions.	CanLII, provincial registries, SEDAR+	Financial/legal indicator summary
B8	Fuse OSINT findings with internal UEBA/SIEM/DLP signals. Update insider risk score.	UEBA platform, SIEM	Integrated risk assessment
B9	Produce Investigation Intelligence Report. Recommend: continue monitoring, HR review, legal escalation, or closure.	—	Report with recommendations

Playbook C – Active Insider Breach Response

SCENARIO

A confirmed or highly suspected insider breach is underway or has recently occurred. Rapid OSINT is required to determine scope, identify the insider, and assess external distribution of compromised data.

Step	Action	Tools	Output
C1	Immediately preserve all available internal evidence. Suspend suspect's access if warranted.	—	Evidence preservation actions documented
C2	Dark web sweep: search for any listing or discussion of organisation data,	DarkOwl, Recorded Future, Flashpoint, IntelX	Dark web findings report

	credentials, or insider access within the last 30–90 days.		
C3	Compromised data scope: if data appears on dark web or paste sites, document format, content type, volume, and listing date.	DarkOwl, Pastebin, IntelX	Data exposure scope assessment
C4	Insider attribution: conduct full OSINT investigation against suspect(s) using Playbook B (expedited).	Full Phase 1–4 toolkit	Attribution intelligence report
C5	External entity mapping: identify likely recipients or purchasers of exfiltrated data via dark web listing context and communication intelligence.	Maltego, DarkOwl, Recorded Future	External entity intelligence
C6	Assess breach notification obligation: use OSINT-derived data scope to inform Real Risk of Significant Harm (RROSH) analysis under PIPEDA.	—	Breach notification assessment memo
C7	Prepare evidence package for potential RCMP referral. Ensure full chain-of-custody documentation.	—	RCMP/law enforcement referral package
C8	Establish ongoing automated dark web monitoring for continued data distribution post-breach.	Recorded Future, DarkOwl, SpyCloud	Ongoing monitoring programme confirmed

Playbook D – Post-Incident Threat Intelligence

SCENARIO

An insider incident is resolved (employee terminated/resigned/prosecuted). Post-incident OSINT is required to monitor for ongoing risk, inform programme improvements, and support legal proceedings.

Step	Action	Tools	Output
D1	Continue dark web monitoring for 90–180 days post-incident for new data listings attributable to the breach.	Recorded Future, DarkOwl, SpyCloud	Ongoing monitoring alerts
D2	Monitor subject's public activities post-departure for evidence of data use (product launches, publications, role content).	LinkedIn, social media monitoring	Post-departure activity log
D3	Track any legal proceedings publicly: court filings, charges, and outcomes.	CanLII, provincial court registries	Legal proceedings summary
D4	Threat landscape: did exfiltrated data appear in the hands of a competitor, foreign state, or threat actor?	Threat intelligence platforms	Threat actor attribution report
D5	Programme lessons-learned: use OSINT findings to identify detection gaps and improve monitoring indicators.	Internal programme review	Programme improvement recommendations
D6	Securely archive case file per retention policy. Destroy personal data no longer required.	—	Case archived; destruction documented

12. Evidence Handling and Chain of Custody

OSINT evidence is only as valuable as its legal integrity. Without rigorous chain-of-custody documentation, OSINT findings may be inadmissible in employment tribunals, civil proceedings, or criminal prosecutions.

12.1 Collection Standards

- Timestamp Everything: Record the exact date, time (UTC timezone), and URL for every piece of collected content.
- Capture Full Context: Always capture the full page, not just the relevant extract. Use full-page screenshot tools (e.g., Fireshot) that preserve the URL bar and timestamp.

- Archive Independently: Use web archiving services (Wayback Machine, archive.ph) to create a third-party-hosted copy of collected content as independent corroboration.
- Hash Evidence Files: Generate SHA-256 hashes for all screenshots and files immediately upon capture. Record hashes in the case log to demonstrate files have not been altered.
- Original File Preservation: Never edit or annotate original evidence files. Maintain originals and create working copies for analysis.

12.2 Documentation Standards

- Case Log: A contemporaneous log of every investigative action: by whom, at what time, using which tool, and what was found.
- Source Record: For each artefact, record source URL, access date/time, collection method, tool used, and chain of custody from collection to storage.
- Analyst Notes: Separate analytical conclusions from raw evidence. Clearly distinguish facts from inferences.
- Handling Instructions: Every case file must be marked with handling and classification instructions, authorised recipients, and retention period.

12.3 Storage and Retention

- Encrypted Storage: All OSINT evidence must be stored in encrypted, access-controlled repositories. Never in personal email, consumer cloud storage, or unencrypted USB drives.
- Access Log: Maintain a log of every access to the case file, by whom and when.
- Retention Period: Apply the organisation's defined retention schedule. For files that may support legal proceedings, retain until all proceedings including appeals are concluded.
- Secure Deletion: At end of retention, use certified secure deletion. Document destruction.

13. Best Practices and Common Pitfalls

13.1 Best Practices

TOP 10 OSINT BEST PRACTICES FOR INSIDER RISK
1. Always begin with a documented requirement. If you cannot articulate the specific intelligence question, do not collect.

2. Collect only what is necessary. Data minimisation applies to OSINT – do not gather information beyond what is required for the stated purpose.

3. Protect your OPSEC rigorously. A compromised investigation can destroy weeks of work, alert an insider, and expose the organisation to legal liability.

4. Screenshot immediately. Social media content is frequently deleted, edited, or made private. Capture relevant content at the first opportunity.

5. Never rely on a single source. Corroborate every significant finding across at least two independent sources before reporting or taking action.

6. Assign confidence levels to every finding: Confirmed, Probable, Possible, or Unconfirmed. Be explicit about the basis for each level.

7. Separate collection from analysis. The analyst who evaluates evidence should ideally not be the same person who collected it – confirmation bias is a significant risk.

8. Legal review before action. No adverse employment action, access revocation, or law enforcement referral should be taken without legal review of OSINT-derived evidence.

9. Train and certify your investigators. Consider SANS FOR578, CREST CPIA, or dedicated OSINT certifications. Untrained investigators make errors that destroy evidential value.

10. Measure your programme. Use the metrics in Section 14 to assess whether your OSINT programme delivers value and improves over time.

13.2 Common Pitfalls

PITFALLS THAT DESTROY INVESTIGATIONS

Confirmation Bias: Collecting only evidence that confirms a pre-existing suspicion. Actively seek exculpatory evidence and alternative explanations.

Misattribution: Assuming an account belongs to the subject without rigorous identity verification. This is especially dangerous with common names or popular usernames.

Stale Data Reliance: Using cached or archived content without checking whether it reflects the current state. Confirm that captures are recent and still live.

Legal Overreach: Conducting active OSINT (fake accounts, querying internal systems, interacting with the subject) without legal authority. Can result in criminal liability and destroy the investigation.

Inadequate Documentation: Failing to maintain contemporaneous notes, case logs, or chain-of-custody records. Without documentation, even valid evidence becomes unusable.

Tool Over-Reliance: Assuming automated OSINT tools are complete and accurate. All automated output requires analyst validation – tools produce false positives and miss content regularly.

14. Programme Effectiveness Metrics

Measuring the effectiveness of an OSINT-enabled insider risk programme requires balanced process, output, and outcome metrics:

Metric	Description	Target / Benchmark
Mean Time to Detection (MTTD)	Average time between when an insider threat indicator first becomes observable and when the programme detects it.	< 30 days for high-risk indicators; < 90 days for medium-risk
Investigation Completion Rate	Percentage of triggered investigations completed within the defined SLA.	Target > 90% within 30 business days
False Positive Rate	Percentage of triggered investigations that found no substantiated insider risk.	< 25%; excessive false positives indicate over-sensitive triggers
Dark Web Hit Rate	Percentage of active investigations where relevant OSINT was found on dark web sources.	Trend is more valuable than absolute value; benchmark against prior period
Credential Exposure Coverage	Percentage of employees whose credentials are covered by continuous dark web monitoring.	100% for privileged users; > 80% organisation-wide
Evidence Admissibility Rate	Percentage of cases where OSINT evidence met chain-of-custody standards for legal proceedings.	100% target – all evidence should be collected to legal standard

Programme ROI	Cost of incidents prevented vs cost of programme operation (using Ponemon CIRGR benchmarks).	Positive ROI based on even one prevented incident at $7.98M+ (Canadian, 2024)

15. References and Training Resources

OSINT Frameworks and Methodology

- OSINT Framework – Justin Nordine, osintframework.com, maintained 2025.
- OWASP Testing Guide v4.2, Testing for Information Gathering – OWASP Foundation, 2022.
- The Diamond Model of Intrusion Analysis – Caltagirone, Pendergast, Betz (2013).
- CERT Common Sense Guide to Mitigating Insider Threats, 7th Edition – Carnegie Mellon SEI, 2022.

Tools Documentation

- SpiderFoot Documentation – github.com/smicallef/spiderfoot.
- Maltego Documentation – docs.maltego.com. Maltego Techonologies GmbH.
- Hunchly documentation – support.hunch.ly. Maltego Techonologies GmbH (2025)
- Shodan – developer.shodan.io. Shodan.io.
- theHarvester – github.com/laramies/theHarvester.
- Sherlock – github.com/sherlock-project/sherlock.
- ExifTool – exiftool.org (Phil Harvey).
- Have I Been Pwned – haveibeenpwned.com (Troy Hunt).
- Recon-ng – github.com/lanmaster53/recon-ng.

Threat Intelligence and Research

- Recorded Future. Threat Intelligence Platform Documentation. recordedfuture.com, 2025.
- DarkOwl. Vision Platform Overview. darkowl.com, 2025.
- SpyCloud. 2025 Annual Identity Exposure Report.
- Ponemon Institute. 2025 Cost of Insider Risks Global Report. Proofpoint.
- Vectra AI. UEBA Explained: User and Entity Behavior Analytics Guide, 2026.
- ShadowDragon. OSINT Techniques: Expert Tactics for Investigators. shadowdragon.io, 2026.
- Opsimathy Limited. Comprehensive Guide to Open-Source Intelligence Tools for 2026.
- DigitalStakeout. A Practitioner's Guide to OSINT Investigation, June 2025.

Training and Certification Resources

- SANS FOR578: Cyber Threat Intelligence – sans.org/cyber-security-courses/cyber-threat-intelligence/
- GIAC Cyber Threat Intelligence (GCTI) – giac.org/certifications/cyber-threat-intelligence-gcti/
- OSINT Curious (osintcurio.us) – community training resources and webinars.
- Bellingcat Online Investigations Toolkit – toolkit.bellingcat.com.
- CREST Practitioner Intrusion Analyst (CPIA) – crest-approved.org.
- Michael Bazzell's OSINT Techniques (inteltechniques.com) – annual practitioner handbook updated 2025.
- OSMOSIS Institute: OSINT Certification – https://osmosisassociation.org/certifications

Contact the Insider Risk Management Centre of Excellence

For more information on Insider Risk Management, consult the Canadian Insider Risk Management Centre of Excellence (CInRM COE), your regional centre, or the Insider Risk Practitioner Alliance (IRPA) at:

- Insider Risk Practitioner Alliance (IRPA) – https://www.irpa.org/
- Canadian Insider Risk Management Centre of Excellence (CInRM COE) – https://www.cinrmcoe-cdecgrin.ca/
- United States Insider Risk Management Center of Excellence (USInRM CoE) – https://www.usinrmcoe.org/
- Australian Insider Risk Centre of Excellence (AIR CoE) – https://www.cybercollaboration.org.au/collaboration-partnerships/australian-insider-risk-centre-of-excellence-air-coe/
- UK Insider Risk Management Collaboration Centre (UKInRM CC) – https://www.ukinrmcc.uk/
- Norwegian Insider Risk Management Centre of Excellence (NInRM CoE) – https://www.ninrmcoe-nie.no/
- Swedish Insider Risk Management Centre of Excellence (SInRM CoE) – https://www.sinrmcoe-ski.se/
- Coming soon: New Zealand