Using OSINT for Insider Threat Scanning

Specifically for Predictive Indicators, *NOT* for Insider Threat *Investigations*

Scott Foote

Last Updated: 15 August 2026

Phenomenati Consulting
www.phenomenati.com

6 Liberty Square, #2736
Boston, MA 02109
(508) 709-7990 (office)

<this page is intentionally blank>

Contents

1 Purpose, Scope, and Governing Principle

The most defensible insider-risk program looks for observable conduct connected to enterprise access, information, systems, people, or facilities. It should not attempt to identify a supposed "insider-threat personality." Potential indicators are not diagnostic, may have innocent explanations, and can involve legally protected activity. Research and operational guidance consistently emphasize that malicious and non-malicious insiders do not fit a single reliable demographic or personality profile; relevant anomalies must be evaluated against context, source reliability, authorized role, and corroborating evidence. [1][2][3][4]

A second distinction is essential. A malicious insider intentionally misuses authorized access. A negligent insider creates exposure through unsafe behavior. A compromised or coerced insider is a victim whose credentials, device, identity, or authority are being exploited. A credential appearing in a breach dump or access marketplace should normally be treated first as evidence of compromise, not employee malice. Criminal access ecosystems routinely trade stolen credentials, sessions, and unauthorized access obtained without the account holder's cooperation. [1][5][6][7]

Governing principle: Evidence of access, intent, action, proof, transaction, and proximity should drive insider-risk decisions - not identity, ideology, hardship, ordinary dissent, or opaque behavioral scores. [2][4][15][21]

2 Suggested Evidence Classification

The classifications below apply to an event or intelligence artifact, not to the permanent character of an individual. They are intended to guide triage, protective action, corroboration, and escalation. [16][21]

Classification	Meaning	Appropriate Initial Response
Critical - Direct evidence	Explicit offer, sale, transaction, threat, sabotage plan, or verified unauthorized disclosure.	Immediate incident response, evidence preservation, and Legal, HR, Privacy, Physical Security, and executive engagement.
High - Strongly corroborated	Strong attribution plus proof of possession, employer-specific preparation, or repeated coordinated behavior.	Rapid internal corroboration and a controlled, multidisciplinary inquiry.
Protective - Likely compromise	Stolen credentials, device infection, identity theft, coercion, impersonation, or criminal targeting.	Contain, reset, protect, hunt, and support the affected individual.
Contextual - Weak signal	Grievance, negative sentiment, financial difficulty, outside activity, or another ambiguous fact.	No adverse action; assess only when lawfully collected and materially corroborated.
Excluded	Protected traits, lawful dissent, ordinary job seeking, anonymous allegations, or unverified broker scores.	Do not collect, score, investigate, or retain as an insider-risk indicator.

3 Sale, Rental, or Facilitation of Enterprise Access [5][6]

Potential markers include:

- An attributable online persona advertises itself as an employee, contractor, administrator, developer, help-desk worker, finance employee, or other insider at the organization.
- An offer to sell or rent access to corporate VPN, SSO, email, cloud environments, source repositories, CRM, ERP, financial systems, administrative consoles, customer portals, or production systems.
- An offer involving valid session cookies, authentication tokens, API keys, private keys, signing certificates, recovery codes, or MFA approvals.
- A willingness to approve an MFA prompt, perform a password reset, reactivate a disabled account, create a new account, or elevate privileges.
- An offer to whitelist an IP address, device, domain, application, or external account.
- An offer to install software, connect removable media, launch a payload, establish persistence, or create an externally accessible account.
- An offer to suppress alerts, disable monitoring, alter logs, bypass DLP, or prevent the organization from detecting subsequent activity.
- An offer to provide a badge, visitor credential, unattended device, physical key, floor plan, access schedule, or entry to a restricted location.
- Company-specific details about access level, geographic location, technology stack, persistence, user population, data volume, or available administrative permissions.
- Screenshots of authenticated internal systems, account banners, dashboards, directory listings, support tickets, or other proof intended to demonstrate access.
- Discussion of a price, escrow service, commission, recurring payment, ransomware percentage, or payment following successful access.
- Marketplace feedback or criminal-forum reputation suggesting that the seller has completed previous access transactions.
- Coordination around maintenance windows, holidays, off-hours, employee departures, or periods when monitoring will be reduced.
- Recruitment of coworkers or subcontractors who can provide complementary access.

Default Interpretation: Treat as critical when attribution and proof of access are both credible. A generic advertisement naming the company, without proof or reliable attribution, remains an intelligence lead rather than evidence against an individual. Access brokers may exaggerate, impersonate employees, or resell access obtained through infostealers and other compromises. [5][6][7]

4 Unauthorized Disclosure or Proof of Possession [1][2][3]

Potential markers include:

- Posting internal documents, screenshots, recordings, photographs, dashboards, chat messages, support tickets, or administrative interfaces.
- Sharing nonpublic customer, client, patient, employee, supplier, or partner information.
- Offering source code, model weights, training data, research, product designs, formulas, engineering drawings, legal materials, completed client work, or proprietary methodologies.
- Disclosing unpublished financial information, forecasts, pricing, bids, acquisition plans, litigation strategy, executive communications, or board materials.
- Posting network diagrams, identity architecture, security procedures, incident-response plans, backup configurations, vulnerability reports, or penetration-test results.
- Publicly exposing passwords, secrets, tokens, certificates, credentials, internal hostnames, private URLs, or environment files in a code repository, package registry, paste site, file-sharing platform, or support forum.
- Publishing internal data shortly after it was created, suggesting continuing or near-real-time access.
- Providing a sample of stolen material to establish credibility with a buyer or extortion victim.
- Posting information containing document identifiers, metadata, usernames, internal paths, canary values, watermarks, or other markers traceable to a specific custodian.
- Claiming to maintain private copies, backups, insurance files, or a dead-man archive for use against the organization.
- Offering information that exceeds what would reasonably be available through public sources or the individual's authorized responsibilities.
- Reposting or relocating material after a takedown, warning, or demand for return.
- Publicly claiming to have retained data or credentials after separation from the organization.
- Displaying proprietary work in a portfolio, resume, conference presentation, academic paper, training course, or sales presentation without authorization.

Default Interpretation: Treat as critical when the material is demonstrably nonpublic, attribution is strong, and possession cannot reasonably be explained by authorized activity. Lawful reporting and protected disclosures must be separated from malicious disclosure before investigative or employment action. [2][3][8][9]

5 Preparation for Exfiltration, Evasion, or Sabotage [1][2][3]

Potential markers include:

- Seeking instructions to defeat the organization's particular MFA, DLP, EDR, CASB, SIEM, logging, watermarking, USB restrictions, or access-review process.
- Requesting assistance with concealing downloads, copying large datasets, suppressing audit trails, manipulating timestamps, or removing evidence.
- Seeking malware, credential-stealing capability, anonymous infrastructure, or exploit assistance specifically matched to the employer's environment.
- Registering or controlling lookalike domains, accounts, applications, or identities intended to impersonate the employer or its executives.
- Building phishing material that uses nonpublic company terminology, projects, reporting relationships, or business processes.
- Offering to disable backups, monitoring agents, alerts, endpoint controls, administrative safeguards, or recovery processes.
- Discussing how to revoke other administrators, lock out responders, corrupt data, destroy logs, encrypt systems, or interfere with operations.
- Publishing specific internal weaknesses and encouraging external actors to exploit them.
- Recruiting an external criminal actor to perform the technical portion of an attack while the insider supplies access or information.
- Seeking a buyer for data before the data has appeared publicly.
- Coordinating activity around termination, resignation, disciplinary proceedings, a major transaction, a product launch, or another high-impact event.
- Testing whether stolen information can be sold, laundered, anonymously transferred, or monetized.
- Attempting to establish alternate accounts, covert communications, or persistent access that would survive account termination.

Default Interpretation: Treat as high to critical when the behavior is employer-specific, attributable, and accompanied by evidence of access or preparation. Generic cybersecurity discussion, authorized research, training, or professional participation in technical forums is not itself suspicious. [1][2][3][4]

6 Credential, Device, or Identity Compromise [5][6][7]

Potential markers include:

- Corporate usernames and passwords appearing in breach dumps, credential collections, combo lists, or stealer-log datasets.
- Valid session cookies, SSO tokens, refresh tokens, API keys, SSH keys, private certificates, or cloud credentials offered for sale.
- An access-broker advertisement that matches the organization, the individual's location, business unit, technology, or privilege level.
- Evidence that the person's endpoint or personal device was infected by an information stealer, remote-access Trojan, botnet agent, or malicious browser extension.
- Exposure of personal email accounts, telephone numbers, recovery addresses, identity documents, security-question answers, or other information usable in help-desk impersonation.
- SIM-swap activity, account-recovery attempts, identity theft, or unauthorized changes to personal or corporate accounts.
- Doxxing that exposes an employee's reporting line, travel, family, location, employee identifier, badge, or access responsibilities.
- A fake recruiting profile, cloned professional profile, deepfake identity, or impersonation account using the employee's name or image.
- A compromised personal social-media or email account contacting coworkers, customers, executives, or suppliers.
- Criminal posts claiming to control the employee's workstation, mailbox, identity, or MFA device.
- Reappearance of credentials or sessions after resets, suggesting persistent malware, token theft, or incomplete containment.
- Evidence that an attacker is blackmailing the person or threatening family, reputation, immigration status, finances, or employment to obtain cooperation.

Default Interpretation: Use a protective response unless separate evidence shows that the user knowingly supplied, facilitated, or monetized the access. Stolen credentials, identity data, and sessions are routinely traded without the victim's knowledge. Contain the exposure, protect the individual, and investigate the attacker before treating the employee as a suspect. [5][6][7]

7 Explicit Threats, Retaliation, Coercion, or Escalating Grievance [3][17]

Potential markers include:

- A threat identifying the employer, facility, system, executive, manager, coworker, customer, or other specific target.
- A statement identifying a proposed action, approximate time, method, access path, or intended consequence.
- Claims of having the access, knowledge, data, credentials, or authority necessary to carry out the threat.
- Statements that the person will take the company down, wipe systems, release data, expose customers, divert money, or lock others out.
- Claims to possess a dead-man switch, disclosure package, retained backup, or evidence archive intended for retaliation.
- Invitations for hackers, activists, criminals, competitors, or hostile actors to attack the organization.
- Offering inside information to make another person's attack possible.
- Targeted doxxing, stalking, harassment, or intimidation of coworkers or executives tied to workplace information.
- Statements about taking customers, source code, proprietary data, or confidential files when leaving.
- Escalation from general dissatisfaction to a specific target, plan, capability, or preparatory act.
- Public justification of theft, fraud, sabotage, or violence as deserved retaliation.
- Evidence that the individual is being coerced, blackmailed, extorted, or manipulated because of organizational access.
- Repeated posts across platforms that become progressively more specific, operational, or imminent.

Default Interpretation: For sentiment analysis, evaluate target, expressed intent, proposed action, access or capability, timing, recurrence, and escalation. Generic negativity, profanity, criticism of leadership, low morale, or a machine-generated toxicity score should not be treated as evidence. Lawful discussions of pay, benefits, management, safety, or working conditions and protected whistleblowing must not be repurposed as insider-risk evidence merely because they are adverse or embarrassing to the employer. [8][9][17][22]

8 Conflicts of Interest and Concealed Outside Activity [2][3][20]

Potential markers include:

- Corporate-registry or beneficial-ownership records showing an undisclosed interest in a supplier, bidder, customer, intermediary, or competitor where disclosure is required.
- Operating or advising a competing business while retaining privileged access to the employer's information.
- Freelance advertisements offering employer-specific data, leads, access, technical work, or influence.
- Offering to obtain contracts, approvals, purchase orders, payments, refunds, favorable audits, or confidential information in exchange for compensation.
- Soliciting kickbacks, referral fees, gifts, cryptocurrency, employment, equity, or other benefits connected to official decisions.
- Simultaneous employment in conflicting privileged roles that has been intentionally concealed.
- A side product, dataset, model, service, course, or publication that appears to incorporate employer intellectual property.
- Undisclosed paid consulting, research, speaking, or advisory activity that requires access to protected organizational information.
- Public records showing that a vendor is controlled by the employee, a close associate, or an undisclosed related party.
- Use of the employer's name, customer relationships, confidential pricing, or proprietary materials to promote a personal venture.
- A pattern of directing organizational business to an undisclosed personal interest.
- Paid participation in an external program that imposes conflicting disclosure or intellectual-property obligations.

Default Interpretation: Treat as contextual until the conflict, applicable disclosure obligation, organizational decision, and information-access nexus are established. Many outside activities are legitimate. Legal, Ethics, HR, Procurement, and the DPO should determine relevance and permissible use rather than leaving the decision to security operations alone. [2][3][15][20]

9 Employment Transition and Movement of Intellectual Property [3][4][7]

Potential markers include:

- A portfolio, job application, resume, presentation, or interview artifact containing nonpublic employer work.
- Public solicitation of employer customers or employees using information that appears to come from a confidential list.
- An announcement that the person has copied, retained, or intends to take organizational files, code, clients, or business information.
- Claims of continuing access after resignation or termination.
- Offering employer-specific datasets, models, scripts, tools, or playbooks shortly before or after departure.
- Proprietary material appearing in a new employer's product, public repository, marketing material, or presentation in a form traceable to the prior organization.
- Moving substantial internal work into a public personal repository, public file-sharing account, or portfolio.
- Offering to sell knowledge of vulnerabilities, security controls, customers, pricing, or internal processes after leaving.
- Seeking collaborators or buyers for information obtained through the former position.
- Public statements about retaining passwords, devices, archives, backups, or authentication material.

Default Interpretation: Updating a resume, seeking another job, resigning, interviewing with a competitor, criticizing the employer, or announcing a career move is not an indicator by itself. The security nexus arises from unauthorized possession, disclosure, solicitation, or continued access - not from the departure itself. [3][4][7][8]

10 Identity Deception, Proxy Working, or Fraudulent Onboarding [18][19]

Potential markers include:

- Multiple professional identities using the same photograph, telephone number, email address, portfolio, PGP key, cryptocurrency wallet, device identifier, or unusual resume content.
- Material inconsistencies between the onboarded identity and public records concerning location, work history, education, licenses, or employer history.
- Forged or altered qualifications, certifications, references, identity documents, or work samples.
- Evidence that a substitute person attended an interview, performs the work, joins video calls, or controls the company device.
- Indicators of a laptop farm, remote keyboard or video forwarding, undisclosed remote operator, or proxy worker.
- Reuse of an employee's email address, avatar, handle, PGP identity, wallet, or distinctive content by an account active on criminal forums.
- A person publicly performing work during incompatible hours or from locations materially inconsistent with the approved employment arrangement.
- A public profile showing simultaneous full-time identities that cannot reasonably coexist and that involve privileged access.
- Sale or rental of verified employment identities for remote-job applications.
- Public solicitation for someone to complete identity checks, interviews, coding tests, or work on another person's behalf.
- The individual who appears on calls or performs work differs materially from the verified employee.

Default Interpretation: Treat as high when supported by strong identity-resolution evidence. Namesakes, recycled photographs, stale broker records, profile-scraping errors, and compromised accounts are common enough that identity must be independently verified. Recent law-enforcement cases demonstrate the use of stolen identities, false personas, proxy workers, and laptop farms to obtain trusted access. [18][19]

11 External Recruitment, Inducement, or Coercion [3][7][19]

Potential markers include:

- A competitor, criminal actor, intelligence-linked entity, or intermediary asks the person for source code, research, customer data, credentials, network information, or work samples.
- An offer of money, employment, travel, honoraria, consulting work, investment, immigration assistance, or other benefits conditioned on providing internal information.
- Requests to remove classification, confidentiality, export-control, customer, or handling markings.
- Requests to use personal accounts, encrypted channels, removable media, or unauthorized transfer mechanisms.
- Instructions to conceal meetings, compensation, affiliations, or information exchanges.
- Requests to identify other employees who possess privileged or sensitive access.
- Threats to the individual's family, reputation, finances, immigration status, or personal safety tied to demands for organizational information.
- Public acknowledgement by the employee that they are being targeted or pressured.
- The employee soliciting buyers, recruiters, or sponsors for protected information.
- Undisclosed participation in an external research, investment, or talent arrangement that creates a specific reporting or access conflict.

Default Interpretation: Nationality, dual citizenship, foreign family members, international travel, friendships, language skills, political opinions, and work with foreign organizations are not indicators by themselves. The relevant markers are the specific request, concealment, inducement, coercion, unauthorized transfer, or conflict. When coercion or targeting is plausible, prioritize protection and safe reporting. [7][19][22]

12 Financial or Criminal Conduct with an Access Nexus [3][13][14]

Potential markers include:

- A credible admission, conviction, or well-substantiated public record involving fraud, bribery, embezzlement, identity theft, cybercrime, extortion, or breach of trust that is materially relevant to the current role.
- An attributable criminal-market account selling organizational access, credentials, data, refunds, accounts, or influence.
- Solicitation of payment in exchange for manipulating invoices, payroll, refunds, customer records, procurement, compliance results, or administrative approvals.
- A cryptocurrency wallet strongly linked to the person receiving payment associated with an access or data transaction.
- New wealth or spending that occurs contemporaneously with an independently documented sale, kickback, or diversion - not merely unexplained affluence in isolation.
- Evidence of criminal debt, extortion, or coercion explicitly tied to demands for organizational access.
- Public evidence of shell companies, false invoices, undisclosed vendor ownership, or payment diversion involving the employer.
- Repeated falsification or concealment directly relevant to the individual's authority, access, or fiduciary responsibilities.
- Participation in account-reshipping, money-mule, refund-fraud, credential-trafficking, or similar operations involving the organization's systems.

Default Interpretation: Debt, bankruptcy, divorce, medical expense, gambling, foreclosure, liens, reduced income, or personal hardship is not an indicator by itself. Third-party background or risk reports used for hiring, retention, promotion, reassignment, or other employment decisions may be consumer reports under the Fair Credit Reporting Act and may also implicate anti-discrimination and state-law requirements. Assess accuracy, job relevance, business necessity, disclosure, permission, dispute, and adverse-action obligations with counsel. [13][14][22]

13 Negligent Security Behavior Visible Outside the Enterprise [1][2][3][7]

Potential markers include:

- Public posting of a password, token, recovery code, private key, credential, QR code, or authentication screenshot.
- Public links to internal documents or storage locations without appropriate access restrictions.
- Screenshots exposing customer information, internal communications, administrative interfaces, or sensitive browser tabs.
- Posting photographs of badges, access cards, workstation labels, whiteboards, network equipment, visitor credentials, or restricted areas.
- Oversharing exact administrative privileges, internal technologies, vulnerabilities, security gaps, travel schedules, on-call patterns, or executive movements.
- Placing company information into a publicly shared AI conversation, public chatbot link, support forum, translation site, code assistant, or document-analysis service.
- Publishing confidential code or configuration in a personal repository, package, container image, notebook, or model.
- Using public file-transfer or collaboration links for sensitive work material.
- Publicly sharing information from an unauthorized personal email or cloud-storage account.
- Selling, donating, recycling, or returning a company device or storage medium while organizational data remains accessible.
- Allowing another person to use the employee's corporate account, identity, badge, or device.
- Repeated external exposure after specific training, corrective action, or technical remediation.

Default Interpretation: Usually treat this as negligent or compromised behavior first. Prioritize containment, removal, training, and control improvement. Repetition, concealment, monetization, or deliberate bypass may justify escalation, but intent must be established separately from the unsafe act. [1][2][3][7]

14 Threats to Physical Safety or Facilities [1][17]

Potential markers include:

- A direct threat against a workplace, executive, manager, coworker, customer, or family member.
- A plan identifying a location, date, method, entry route, access point, shift, or target.
- Photographs or diagrams showing surveillance of facilities, homes, vehicles, routes, entrances, or security measures.
- Posting badge images, access routes, shift schedules, floor plans, executive travel, or other information to facilitate harm.
- Doxxing coworkers and encouraging others to threaten or attack them.
- Statements describing sabotage of power, environmental controls, safety equipment, manufacturing systems, laboratories, transportation, or physical infrastructure.
- Weapon acquisition, rehearsal, or operational planning explicitly connected to the workplace target.
- Coordination with another person to carry out violence, property destruction, or operational disruption.
- Escalation from grievance to target selection, reconnaissance, preparation, or communicated intent.

Default Interpretation: Refer immediately to the organization's behavioral-threat-assessment process, Physical Security, Legal, HR, and, where warranted, law enforcement. Ideology, diagnosis, protected speech, or lawful weapon ownership alone should not be substituted for target-specific behavioral evidence, planning, preparation, or communicated intent. [1][17][22]

15 Cross-Source Pattern Amplifiers

A single weak signal should rarely determine the outcome. Risk rises materially when multiple dimensions reinforce each other and when independent internal evidence supports the external intelligence. [2][3][16][21]

- **Strong attribution:** Stable identifiers connect the actor to the end-user through verified accounts, unique artifacts, wallet history, internal metadata, or other reliable evidence - not merely a name or photograph.
- **Proof of possession:** The actor demonstrates access to nonpublic, current, and verifiable organizational information.
- **Role relevance:** The information or action aligns with systems and assets the person can actually access.
- **Specific intent:** The statement describes what will be stolen, changed, disclosed, disrupted, or sold.
- **Action already taken:** Data has been copied, a sample posted, a buyer contacted, a payment requested, infrastructure created, or an account modified.
- **Transaction evidence:** Price negotiation, escrow, payment, marketplace feedback, or delivery confirmation exists.
- **Evasion:** The individual discusses defeating controls, hiding activity, deleting evidence, or maintaining access.
- **Imminence:** A near-term date, event, transaction, termination, maintenance window, or operational opportunity is identified.
- **Recurrence:** Similar conduct appears repeatedly over time or across independent platforms.
- **Independent corroboration:** External intelligence aligns with internal identity, access, endpoint, network, DLP, physical-access, or case-management records.
- **Escalating sequence:** Grievance progresses to target selection, research, preparation, proof, solicitation, and action.
- **No credible benign explanation:** Authorized research, professional activity, public information, mistaken identity, protected reporting, and account compromise have been considered and reasonably excluded.

Analytic Discipline: Source veracity, attribution confidence, organizational baselines, alternative hypotheses, and documented reasoning are essential. A pattern is stronger when its components come from genuinely independent sources rather than multiple vendors republishing the same underlying data. [2][16][21]

16 Source-to-Signal Map

Different source classes answer different questions and carry different failure modes. The table below should be used to shape collection requirements and analyst skepticism. [5][6][7][18][19][21]

External Intelligence Source	Most Useful Indicators	Principal Caution
Access-broker markets and criminal forums	Sale of access, insider recruitment, data samples, credential transactions.	Sellers may exaggerate, impersonate employees, or resell compromised access.
Breach dumps and stealer telemetry	Compromised credentials, devices, sessions, tokens, and personal identity data.	Exposure ordinarily indicates victimization, not malicious intent.
Leak and extortion sites	Published data, proof samples, insider claims, and extortion communications.	Attribution to a particular employee may be speculative.
Public social media and forums	Explicit threats, disclosure, coercion, invitations to attack, and targeted doxxing.	Protected speech, sarcasm, cultural context, account compromise, and false attribution.
Code repositories, package registries, model hubs, and paste sites	Secrets, proprietary code, configuration, internal data, and unsafe work practices.	Authorized open-source contributions, forks, examples, and old public material.
File-sharing and public collaboration links	Exposed documents, datasets, client information, and internal presentations.	Misconfiguration or negligence may be more likely than malice.
Professional profiles and portfolios	Unauthorized work samples, identity conflicts, and conflicting employment.	Ordinary job seeking and resume updating are not suspicious.
Freelance and contractor marketplaces	Sale of employer-specific services, access, data, or influence.	Shared skills and generic experience do not establish IP theft.
Corporate, procurement, and beneficial-ownership records	Conflicts, related-party vendors, shell entities, and undisclosed interests.	Namesakes, stale records, and lawful outside businesses.
Court and regulatory records	Relevant fraud, bribery, cybercrime, or fiduciary misconduct.	Allegations are not convictions; legal use varies by jurisdiction.
Data brokers and employment-screening services	Identity verification, public records, and possible conflicts.	Accuracy, FCRA, discrimination, proportionality, and challenge rights.
Domain, DNS, and certificate-transparency data	Lookalike domains, phishing infrastructure, and impersonation preparation.	Registration information can be hidden, forged, or controlled by an attacker.
Blockchain intelligence	Payment associated with an access sale, kickback, or extortion.	Wallet attribution requires strong corroboration; transfers alone do not identify a person.
Threat-intelligence reporting	Targeted recruitment, coercion, identity compromise, and access-market exposure.	Vendor confidence levels, collection methods, and source independence vary.

17 Information That Should Not Be Treated as an Insider-Threat Indicator

The following information should be excluded from scoring, or should never stand alone as a basis for inquiry or adverse action. Some items are protected by law; others are too common, sensitive, inaccurate, or weakly predictive to support a defensible conclusion. [4][8][9][10][11][13][14][22]

- Race, color, ethnicity, or national origin.
- Citizenship, dual citizenship, foreign birth, or accent.
- Religion or philosophical belief.
- Political opinion or lawful political activity.
- Sex, gender identity, pregnancy, sexual orientation, or marital status.
- Age, disability, medical condition, mental-health status, genetic information, or family medical history.
- Union membership, organizing, collective employee activity, or lawful discussion of working conditions.
- Whistleblowing, ethics reporting, safety reporting, regulatory complaints, or protected disclosures.
- Foreign relatives, friendships, language ability, travel, or lawful international associations.
- Job searching, resume changes, resignation, or employment by a competitor.
- General dissatisfaction, poor morale, negative sentiment, profanity, sarcasm, or criticism of management.
- Debt, bankruptcy, divorce, illness, bereavement, foreclosure, or other personal hardship.
- Appearance of credentials in a dump without evidence that the person supplied them.
- Anonymous allegations, rumor, unverified screenshots, or a namesake match.
- A data-broker or AI-generated risk, loyalty, anger, or toxicity score without reliable underlying evidence.
- Lawful cybersecurity research, participation in technical communities, possession of security tools, or discussion of vulnerabilities consistent with the person's role.
- An arrest, accusation, or civil dispute without reliable facts, legal relevance, and a direct nexus to the person's duties.

Privacy and employment-law caution: Monitoring and intelligence use may involve sensitive or special-category information, employment screening rules, collective labor rights, whistleblower protections, anti-discrimination duties, and jurisdiction-specific consultation or notice requirements. Collection must be necessary, proportionate, accurate, purpose-limited, transparent where required, and subject to human review and challenge. [8][9][10][11][12][13][14][22]

18 Governance Requirements for Using These Indicators

External intelligence about end-users creates material security, privacy, employment, civil-liberties, evidentiary, and reputational risk. The collection and adjudication process therefore requires explicit authority, multidisciplinary oversight, analyst discipline, and documented safeguards. [1][2][15][16][20][21][22]

18.1 Begin with assets and threat scenarios, not people

Define the critical information, systems, transactions, facilities, and people being protected. Collection should answer approved questions such as whether organizational access is being sold, protected information has been disclosed, an employee is being impersonated or coerced, or someone is preparing to sabotage a critical system. A direction to find anything concerning about employees is neither a defensible intelligence requirement nor a proportionate monitoring purpose. [1][2][15]

18.2 Score the event, not the individual

Evaluate source reliability, attribution confidence, specificity of intent, relevance to authorized access, proof of possession or action, recency, imminence, independent corroboration, and possible innocent, authorized, or protected explanations. Do not maintain permanent character scores such as disloyal, angry, financially vulnerable, or high insider risk. [2][3][16][21]

18.3 Separate protective and investigative pathways

A stolen credential, infected device, impersonation account, identity theft event, or coercion attempt should enter a protective response path. Moving immediately to employee discipline can punish the victim, discourage reporting, and allow the actual attacker to remain active. [5][6][7][16]

18.4 Require corroboration before adverse action

Except for an immediate safety or containment emergency, use a defined corroboration threshold. A practical internal standard is one direct, authenticated artifact with a compelling enterprise nexus, or two reasonably independent sources plus relevant internal telemetry. A vendor alert, dark-web claim, sentiment score, or social-media post should not by itself support discipline, termination, denial of promotion, or referral to law enforcement. [2][16][21]

18.5 Use multidisciplinary adjudication

Define roles for Security Operations, Insider Risk, Threat Intelligence, HR and Employee Relations, Legal and Employment Counsel, the DPO or Privacy Office, Ethics and Compliance, Fraud or Internal Audit, Physical Security, behavioral threat assessment, business owners, and executive oversight. No single technical team should own the factual, legal, privacy, and employment judgments alone. [2][15][20]

18.6 Collect lawfully and passively

Do not buy working credentials, transact with access brokers, direct criminal activity, impersonate buyers, or acquire unlawfully obtained personal dossiers merely to investigate an employee. Use approved passive collection, vetted intelligence providers, documented legal process, and law-enforcement coordination when required. [1][5][6][16]

18.7 Apply privacy-by-design controls

Document purpose and lawful basis; conduct a PIA or DPIA where required or prudent; use the least intrusive source capable of answering the question; prefer metadata and event information over private content when feasible; minimize sensitive information; limit collection by geography and workforce population; provide notice and consultation where required; restrict access; establish short retention

periods; log searches and decisions; and prevent repurposing for general performance or loyalty monitoring. [10][11][12][15]

18.8 Address employment-screening laws

When a third party supplies background information, behavioral assessments, social-media reports, or worker risk scores for hiring, promotion, reassignment, retention, or another employment decision, the output may be a consumer report. Applicable requirements can include permissible purpose, disclosure, written authorization, accuracy, pre-adverse-action process, adverse-action notice, file access, and dispute rights, in addition to anti-discrimination and state-law restrictions. [13][14]

18.9 Preserve explainability and challenge rights

The case record should identify the exact artifact, collection date and method, source and reliability assessment, identity-attribution method, enterprise-access or asset nexus, alternative explanations, corroborating evidence, legal basis, jurisdictional limitations, human decision-makers, final disposition, and retention date. Where consistent with safety and evidence preservation, the affected individual should have a meaningful opportunity to explain or challenge inaccurate information. [10][11][12][16][21]

18.10 Prohibit automated adverse decisions

Automated matching, sentiment analysis, identity resolution, or behavioral scoring may prioritize analyst review. It should not independently determine that an employee is malicious or trigger termination, suspension, law-enforcement referral, or another material employment action. Human reviewers must examine source quality, attribution, context, protected activity, and alternative explanations. [10][11][12][13][14][21]

19 Executive Test for a Defensible Indicator

Before escalating an external signal, the decision-maker should be able to answer each of the following questions in writing. [16][21]

1. What observable act occurred?
2. How confidently is it attributed to this person?
3. What organizational asset or authorized access is involved?
4. Is there evidence of intent, preparation, transaction, or completed action?
5. Could the person instead be compromised, impersonated, coerced, mistaken for someone else, or engaged in protected activity?
6. What independent internal evidence corroborates the claim?
7. Is collection and use lawful, necessary, proportionate, and consistent with published policy?
8. Would the organization make the same decision regardless of the person's protected characteristics, views, nationality, or personal circumstances?

Decision Rule: Escalate behavior and evidence, not identity or stereotype. Where the signal is ambiguous, use the least harmful protective measure while facts are corroborated. [4][16][21][22]

Appendix A - Sources and URLs

Inline source markers in the body refer to the numbered entries below. URLs are presented as plain text to preserve a clean document package without external hyperlink relationships. Accessed 20 August 2026.

[1] Cybersecurity and Infrastructure Security Agency (CISA). Insider Threat Mitigation Guide. 2020.
URL: https://www.cisa.gov/sites/default/files/2022-11/Insider%20Threat%20Mitigation%20Guide_Final_508.pdf

[2] Software Engineering Institute, Carnegie Mellon University. Common Sense Guide to Mitigating Insider Threats, Seventh Edition. 7 September 2022.
URL: https://www.sei.cmu.edu/library/common-sense-guide-to-mitigating-insider-threats-seventh-edition/

[3] Center for Development of Security Excellence (CDSE), Defense Counterintelligence and Security Agency. Potential Risk Indicators: Insider Threat. November 2021.
URL: https://www.cdse.edu/Portals/124/Documents/jobaids/insider/INTJ0181-insider-threat-indicators-job-aid.pdf

[4] Software Engineering Institute, Carnegie Mellon University. 5 Best Practices to Prevent Insider Threat. 6 November 2017.
URL: https://www.sei.cmu.edu/blog/5-best-practices-to-prevent-insider-threat/

[5] Europol. Steal, Deal and Repeat: Cybercriminals Cash In on Your Data. Internet Organised Crime Threat Assessment spotlight report. 2025.
URL: https://www.europol.europa.eu/cms/sites/default/files/documents/Steal-deal-repeat-IOCTA_2025.pdf

[6] Europol. The Evolving Threat Landscape: How Encryption, Proxies and AI Are Expanding Cybercrime - Internet Organised Crime Threat Assessment (IOCTA) 2026. 2026.
URL: https://www.europol.europa.eu/cms/sites/default/files/documents/IOCTA-2026.pdf

[7] Center for Development of Security Excellence (CDSE). An Insider's Digital Footprint and Associated Risks. August 2026.
URL: https://www.cdse.edu/Portals/124/Documents/jobaids/insider/insiders-digital-footprint.pdf

[8] National Labor Relations Board. Social Media - Protected Concerted Activity.
URL: https://www.nlrb.gov/about-nlrb/rights-we-protect/the-law/employees/social-media-0

[9] U.S. Department of Labor. Whistleblower Protections.
URL: https://www.dol.gov/general/topics/whistleblower

[10] European Parliament and Council of the European Union. Regulation (EU) 2016/679, General Data Protection Regulation. 27 April 2016.
URL: https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng

[11] Information Commissioner's Office. Data Protection and Monitoring Workers.
URL: https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/employment/monitoring-workers/data-protection-and-monitoring-workers/

[12] National Institute of Standards and Technology. NIST Privacy Framework.
URL: https://www.nist.gov/privacy-framework

[13] Federal Trade Commission. Using Consumer Reports: What Employers Need to Know.
URL: https://www.ftc.gov/business-guidance/resources/using-consumer-reports-what-employers-need-know

[14] U.S. Equal Employment Opportunity Commission. Enforcement Guidance on the Consideration of Arrest and Conviction Records in Employment Decisions under Title VII of the Civil Rights Act. 25 April 2012.
URL: https://www.eeoc.gov/laws/guidance/enforcement-guidance-consideration-arrest-and-conviction-records-employment-decisions

[15] Software Engineering Institute, Carnegie Mellon University. The 13 Key Elements of an Insider Threat Program. 23 October 2023.
URL: https://www.sei.cmu.edu/blog/the-13-key-elements-of-an-insider-threat-program/

[16] Center for Development of Security Excellence (CDSE). Insider Threat Inquiry. February 2025.
URL: https://www.cdse.edu/Portals/124/Documents/jobaids/insider/Insider-Threat-Inquiry.pdf

[17] Center for Development of Security Excellence (CDSE). Potential Risk Indicators: Active Shooters and the Pathway to Violence. May 2022.
URL: https://www.cdse.edu/Portals/124/Documents/jobaids/insider/potential-risk-indicators-kinetic-violence-jobaid.pdf

[18] U.S. Department of Justice, U.S. Attorney's Office for the District of Columbia. Arizona Woman Sentenced in $17M IT Worker Fraud Scheme That Illegally Generated Revenue for North Korea. 24 July 2025.
URL: https://www.justice.gov/usao-dc/pr/arizona-woman-sentenced-17m-it-worker-fraud-scheme-illegally-generated-revenue-north

[19] U.S. Department of State, U.S. Department of the Treasury, and Federal Bureau of Investigation. Guidance on the Democratic People's Republic of Korea Information Technology Workers. 16 May 2022.
URL: https://ofac.treasury.gov/media/923126/download?inline=

[20] Center for Development of Security Excellence (CDSE). Human Resources and Insider Threat. October 2024.
URL: https://www.cdse.edu/Portals/124/Documents/jobaids/insider/INT_Human-Resources-and-Insider-Threat.pdf

[21] Center for Development of Security Excellence (CDSE). Critical Thinking Techniques for Insider Threat Analysts. April 2024.
URL: https://www.cdse.edu/Portals/124/Documents/jobaids/insider/INT250-critical-thinking-techniques.pdf

[22] Center for Development of Security Excellence (CDSE). Privacy and Civil Liberties Case Law Examples. May 2019.
URL: https://www.cdse.edu/Portals/124/Documents/jobaids/insider/case-law.pdf