Methodology for Reviewing Diverse Data Sources to Discover Insider Threats

1. Data Collection and Consolidation

Network Logs: Review for unusual login times, excessive data transfer, access to unauthorized systems, or foreign IP connections.

Employee Access Records: Look for unauthorized access to sensitive files, repeated failed access attempts, or access out of job scope.

Email Communications: Use NLP and metadata analysis to detect unusual communication patterns (e.g., too many emails to competitors, large attachments, or out-of-the-blue timing).

Techniques:

Behavioral Baselines: Establish baseline normal patterns for all employees (e.g., routine login patterns, usual file access) based on past behavior.

Anomaly Detection: Use ML models (e.g., isolation forests, clustering) to flag anomalies from baselines.

Correlation Analysis: Group signals from various sources of data (e.g., an employee reading confidential documents + sending voluminous emails).

2. Difficulty in Separating Legitimate vs. Malicious Behavior

False Positives: Standard but occasional activities (e.g., late-night work) could be suspicious.

Context Dependence: An activity may be legitimate (e.g., IT staff reading confidential systems for maintenance).

Data Volume: It can hide actual signals in large data volumes.

Mitigations:

Contextual Rules: Put job titles and projects into consideration for analysis.

Human Review: Anomaly highlights reviewed with HR/management input.

Iterative Refinement: Tune models in terms of feedback to reduce noise.

3. Cybersecurity vs. Privacy

Minimization: Get/datamine only required data (e.g., do not read email content unless at-risk from metadata).

Anonymization: Use pseudonymization during initial screening; de-anonymize only for high-risk cases.

Policy Alignment: Ensure compliance with laws (e.g., GDPR) and internal policies (e.g., employee monitoring disclosures).

### 4. Transparency and Ethics

Clear Policies: Communicate monitoring practices to employees upfront.

Oversight: Involve legal/HR teams to review investigation scope.

Bias Mitigation: Report on biased targeting models (e.g., over-flagging distant workers).

### 5. Reporting Findings

Technical Stakeholders (e.g., IT Security):

Detailed reports with quantifiers (e.g., anomaly scores, timelines).

Visualizations (e.g., network graphs of suspicious activity).

Non-Technical Stakeholders (e.g., Executives/HR):

High-level summaries with a risk focus (e.g., "X employees had high-risk patterns").

Actionable recommendations (e.g., "Review access for Employee Y").

Ethical Reporting: Avoid mentioning names until verified; prioritize evidence over suspicion.

### Example Workflow

Initial Triage: Flag employees who have >3 SD deviations in frequency of data access.

Deep Dive: For suspected cases, cross-reference network logs (e.g., VPN connections during unusual hours) and email metadata (e.g., exfiltration indicators).

Review: Report results to HR with qualifications (e.g., "May be due to project need or abuse").

Action: Escalate if evidence is compelling; otherwise, lower monitoring thresholds.

### Key Considerations

Proportionality: Target high-risk users to minimize unwarranted privacy intrusions.

Documentation: Document all the steps of the investigation in order to be accountable.

Feedback Loop: Use consequences to increase detection (e.g., tighten baselines for roles with variable workloads).