Methodology to Examine Different Data Sources for Insider Threat Identification

1. Data Collection and Integration

Network Logs: Review VPN access timing, suspicious data transfers, connectivity to malicious IPs, or unusual bandwidth use.

-Employee Access Logs: Review login times, access to sensitive files/systems (especially outside working hours), and privilege escalation.

- Email Communications: Use NLP/topic modeling to detect phishing attacks, data exfiltration, or unusual communication activity (e.g., spikes in emails to outside locations suddenly).

- Integration: Correlate information from several sources (e.g., an employee looking at confidential files and sending them out later by email).

2. Anomaly Detection Methods

- Baseline Creation: Create typical behavior (e.g., normal times of access, use of data) against reference data.

- Machine Learning: Use unsupervised methods (e.g., clustering, isolation forests) to identify outliers. Supervised learning can be utilized if labeled data is available.

- Rule-Based Alerts: Identify actions like successive failed logins, mass downloads, or access of other department's files to which the user has no connection.

3. Behavioral Analysis

- User and Entity Behavior Analytics (UEBA): Model pattern like "time spent on systems" or "sequence of actions" to find out-of-pattern behaviors (e.g., employee in finance suddenly querying HR databases).

- Temporal Analysis: Identify actions performed at odd hours or before/after resignation.

Challenges in distinguishing Legitimate vs. Malicious Actions

1. False Positives: Innocent actions (e.g., doing late work for a deadline) could appear as threats. Mitigation: Contextual inspection (e.g., review of project schedules) and model tuning in iterations.

2. Data Volume: Too much noise in large data can conceal signals. Use feature selection and concentrate on high-risk systems/roles.

3. Evolving Tactics: Insiders may imitate normal behavior. Combine multiple low-severity indicators (e.g., slight increase in data access + emails sent to personal accounts).

Balancing Cybersecurity and Privacy

1. Minimization: Restrict analysis to relevant data (e.g., don't analyze personal web surfing unless specified).

2. Anonymization: Pseudonymize for preliminary screening; de-anonymize only for high-confidence warning.

3. Policy Alignment: Conform to legislation (e.g., GDPR, corporate policies) and obtain legal/HR permission for intrusive techniques (e.g., examination of email contents).

4. Proportionality: Tackle high-risk positions/systems first in order to limit mass surveillance.

Ensuring Transparency and Ethics

1. Transparent Policies: Educate employees on surveillance practices (e.g., via training) to avoid covert surveillance.

2. Regulation: Involve HR, legal, and ethics committees in investigative processes.

3. Prevention of Bias: Test models against biases (e.g., bias against remote employees) and confirm results objectively.

4. Record Keeping: Document each investigative step for transparency.

Communicating Findings to Stakeholders

1. Technical Teams:

- Style: Detailed reports with metrics (e.g., anomaly scores, timelines) and visualizations (e.g., heatmaps of access patterns).

- Emphasis: Evidence strength, methodology (e.g., "This user's activity is a 4σ outlier in volume of data transferred").

2. Non-Technical Stakeholders (Executives, HR):

- Simplify: Use analogies (e.g., "This is an employee copying all client data when leaving").

- Risk Context: Emphasize impact (e.g., "This could reveal customer SSNs").

- Actionable Steps: Suggest responses (e.g., "Revoke access and interview").

3. Legal/Compliance:

- Evidence Chain: Supply forensically sound information for possible disciplinary/legal action.

- Privacy Impact: Provide justification for actions taken (e.g., "Email review was warranted due to correlated file access").

Example Workflow

1. Initial Triage: Flag an employee downloading 10GB of data at 3 AM.

2. Correlation: Cross-reference against email logs of sends to external domains following download.

3. Review: Involve HR to determine if the employee had a legitimate reason (e.g., scheduled migration).

4. Escalation: Otherwise, recommend account suspension and further investigate.