Method for Detecting Insider Threats in Cybersecurity Using Data Science   
Step 1: Gathering and Preparing Data   
I would begin by compiling information from several sources:   
  
Network logs can be used to spot odd access trends, big data transfers, or access from unapproved sources.   
Employee Access Records: Monitor file access, privilege escalation, and login/logout times.   
Email Communications: Look for odd communication patterns, unauthorised data sharing, or phishing efforts.   
I would preprocess the data from these sources because they can be noisy by:   
  
eliminating fields that aren't important.   
standardising user IDs and timestamps.   
using imputation to deal with missing data.   
Step 2: Techniques for Detecting Anomalies   
I would use the following to spot suspicious behaviour:   
  
Analysis of Statistics   
Determine the baseline behaviours and identify any deviations, such as when an employee logs in at three in the morning.   
Models for Machine Learning   
Unmonitored Education: Employ clustering techniques (like DBSCAN) or isolate forests to find irregularities.  
Learning Under Supervision: If there is labelled threat data available, train a classification model.  
Analysis of Graphs  
To map interactions and uncover hidden links, create network graphs.  
Step 3: Difficulties in Recognising Insider Dangers  
Differentiating Malicious versus Lawful Conduct:  
Workers who are late because of deadlines rather than because of data exfiltration.  
Use domain knowledge to prevent false positives.  
Privacy Issues:  
ensuring that the rights of employees are not violated by data monitoring.  
revealing aggregated and anonymised insights rather than individual communications.  
Step 4: Transparency & Ethical Issues  
Compliance with Data Privacy Laws (e.g., GDPR, HIPAA)  
Unambiguous Employee Monitoring Policies  
Reducing Detection Algorithm Bias  
Step 5: Sharing Results With Technical Teams: Give thorough logs, an analysis of the features' relevance, and model justifications.  
Regarding Non-Technical Participants: Utilise heatmaps, visual dashboards, and executive summaries.