1. Threat investigation.
2. Data Collection & Integration.

**i. Network Logs**: Capture login times, IP addresses, file transfers, and access patterns.

**ii. employee access records:** **Track badge swipes, system logins, and resource usage.**

**iii. email communications:** **detect suspicious keywords, mass attachments, or external domain communications.**

1. How **to detect anomalous or suspicious behavior.**
2. **compare user behavior against historical baselines.**
3. **identify outliers.**
4. **cross-check if abnormal logins correlate with unusual email/file transfers.**
5. **see if an employee’s activity deviates significantly from peers in similar roles.**
6. **challenges that might face in distinguishing between legitimate and malicious actions.**
7. **Context Sensitivity**
8. **False positives: unusual activity might be legitimate.**
9. **Data volume:** **High-frequency logs and diverse formats require scalable processing.**
10. **Bias & Assumptions:** **Risk of profiling or unfair targeting without sufficient evidence.**
11. **importance of maintaining transparency and ethical standards throughout the investigation process.**
12. **Document Procedures**: Maintain audit trails of analysis steps and decisions.
13. **Avoid Overreach**: Focus only on data relevant to the investigation.
14. **Independent Review**: Involve HR or legal teams to validate findings
15. **Respect Confidentiality**: Anonymize data where possible during analysis
16. **strategies for effectively communicating your findings to both technical and non-technical stakeholders within the organization.**
17. To Technical Stakeholders: Use dashboards to visualize anomalies, Share model metrics and Provide reproducible notebooks or scripts.
18. To Non-Technical Stakeholders: Use Plain language explanation of findings and recommended actions.