# SIEM Use Cases Outline

* Introduction to SIEM:
  + Brief overview of SIEM (Security Information and Event Management).
  + Importance of SIEM in cybersecurity.
* SIEM Use Cases:
  + Identify and describe specific use cases relevant to your organization.
  + Examples may include:
    - Detection of abnormal login activity.
    - Anomaly detection in network traffic.
    - Malware detection and response.
* Implementation Strategy:
  + Discuss how these use cases will be implemented in your organization.
  + Consideration of log sources, correlation rules, and incident response procedures.
* Metrics and Key Performance Indicators (KPIs):
  + Define metrics to measure the effectiveness of each SIEM use case.
  + Establish KPIs for monitoring and improving security posture.