# Controls

* **Network Sniffing on Kafka Streaming Cluster:**
  + Implement encryption for data in transit within the Kafka cluster to prevent interception.
  + Utilize network segmentation to restrict access to the Kafka cluster only to authorized users.
  + Enable strong authentication mechanisms such as mutual TLS for communication within the cluster.
* **SQL Injection on Data Lake (Cassandra):**
  + Input validation and parameterized queries should be implemented to prevent SQL injection attacks.
  + Regularly patch and update the Cassandra database to address any known vulnerabilities.
  + Implement least privilege access controls to limit the impact of a successful SQL injection attack.
* **Phishing Attacks on Web/Mobile App Users:**
  + Conduct regular security awareness training for users to recognize and report phishing attempts.
  + Implement multi-factor authentication to add an extra layer of security for user login credentials.
  + Use email filtering solutions to detect and block phishing emails before they reach users.
* **Denial of Service (DoS) on Spark Streaming Nodes:**
  + Implement rate limiting and request validation to mitigate the impact of excessive requests.
  + Utilize load balancers to distribute incoming traffic and prevent overwhelming specific nodes.
  + Monitor network traffic and system performance to detect and respond to potential DoS attacks.
* **Man-in-the-Middle Attacks on Direct Data Push Communication:**
  + Implement end-to-end encryption for data transmission to protect against interception and tampering.
  + Use digital signatures to verify the integrity and authenticity of data exchanged between systems.
  + Implement certificate pinning to ensure secure communication channels and prevent MITM attacks.