**Data Science Use Case Document Template**

**1. Problem Statement**

**Description:**  
Telecom networks are constantly targeted by cyber threats such as DDoS attacks, SIM swap fraud, and unauthorized access attempts. Traditional security systems struggle to adapt to the evolving nature of these threats, leaving networks and customer data vulnerable. An AI-driven advanced network security solution is needed to proactively identify, analyze, and mitigate potential risks in real-time.

**2. Target Variable / Number of Clusters**

**Definition:**  
The target outcomes include real-time threat detection, mitigation actions, and network security score improvement. Clustering can be used to group similar threat patterns for analysis and response.

**3. Input Variables / Parameters**

**Key Influencers:**

* Network traffic data (e.g., packet types, volume, origin/destination)
* Historical security incident logs
* User authentication and access data
* Real-time system alerts and anomalies
* Device and endpoint metadata
* Threat intelligence feeds (external and internal)

**4. Sector**

**Telecom**

**5. Approach / Technology Used**

**Technology Stack:**

* **Anomaly Detection Models:** For identifying unusual patterns in network traffic.
* **Machine Learning Models:** To predict and classify potential security breaches.
* **Threat Intelligence Platforms:** To integrate external threat data for enhanced analysis.
* **Automated Incident Response Systems:** To mitigate threats in real-time.
* **Blockchain Technology:** For secure transaction logging and data integrity.

**6. Benefits**

* Proactive protection against emerging cyber threats.
* Enhanced trust and confidence among customers due to improved security.
* Reduced financial and reputational losses from breaches.
* Faster detection and response times for incidents.
* Insights into evolving threat patterns for future prevention.

**7. Expected Outcome**

* **Reduced Incidents:** 40-60% reduction in successful cyberattacks.
* **Faster Response:** Real-time threat mitigation within seconds.
* **Improved Security Posture:** Enhanced compliance with security standards.
* **Operational Efficiency:** Lower manual intervention due to automation.

**8. Challenges / Risks**

* High computational requirements for real-time processing.
* Potential false positives leading to unnecessary actions.
* Balancing privacy concerns with threat analysis.
* Integration complexity with existing systems.