**What is CyberSecurity?**

**Cybersecurity** involves protecting systems, networks, and data from cyber threats. This field encompasses a wide range of practices and technologies designed to safeguard information from unauthorized access, attacks, damage, or theft. Cybersecurity includes preventive measures such as firewalls, encryption, and secure coding practices, as well as detection and response strategies like intrusion detection systems and incident response plans. This topic covers the principles, best practices, and latest trends in cybersecurity, including emerging threats and the evolving landscape of cyber defense.

Database security application

Problem statement:

**Modern enterprises face increasing threats to their databases from both external attackers and insider misuse**.

Traditional intrusion detection systems (IDS) often struggle to **differentiate between harmless probing attempts (dummy/fake attacks)** and **genuine malicious queries** that aim to exfiltrate sensitive data. This leads to either:

i)**False positives** where legitimate or test activities trigger unneccesary alerts

ii)**False negatives**, where actual attacks bypass detection

There is a pressing need for a **database intrusion detection system (DB-IDS)** that can **simulate multiple attack scenarios, analyze query behavior, and accurately distinguish genuine attacks from dummy attempts**. Such a system should also provide **automated responses** (blocking, quarantining, alerting) to minimize damage and reduce the burden on security teams.