Week 1 Workshop

# FIT5230 Malicious AI

All about AI vs Security

# Overview

★ The case for AI+Security

★ AI vs Security

- AI for Security: AI → Sec
- Security attacks AI: AI ⇤ Sec
- Security meets AI: AI ↔ Sec
- AI attacks Security: AI ⇥ Sec

Case Scenario

# Balancing Security and AI in a Smart City

Imagine a modern smart city where AI systems are integrated to improve urban living. These systems include traffic management, public safety, energy distribution, and environmental monitoring.

Activity 1

# What you need to do: (20 mins)

1. **Form** a group of 4 to 6.
2. **Discuss** and **decide** on the system that you think it can improve the urban living.
3. **Explain** the elements of AI and security in the chosen system.
4. Teams will be randomly selected to **present** their ideas.

Include your ideas here: https://shorturl.at/j1h0S

Activity 2

Include your ideas here: https://shorturl.at/d0p0K

# What you need to do: (20 mins)

1. Within the same team, divide into 2 subgroup: the **Good Guy Team** and the **Bad Guy Team**.
2. Join other team to form **new** Good Guy Team / Bad Guy Team.
3. Good Guy Team:
    a. Brainstorm on the attacks that could be launched by the Bad Guy Team.
    b. **Improve** the system chosen in Activity 1.
4. Bad Guy Team:
    a. Discuss on the **attacks** could be launched based on the knowledge of what has been achieved in the system chosen in Activity 1.
5. Teams will be randomly selected to **present** their ideas.