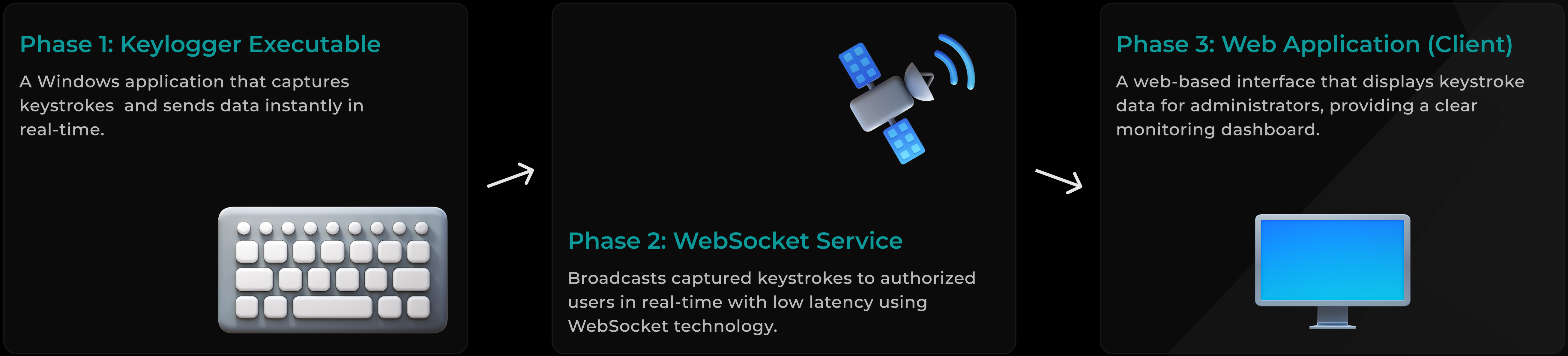
Keylogger: Simulating Cyberattacks for System Monitoring

An ethical tool for real-time system monitoring, penetration testing, and forensic investigation in cybersecurity.



Phase 1: Keylogger Executable

A Windows application that captures keystrokes and sends data instantly in real-time.

Phase 2: WebSocket Service

Broadcasts captured keystrokes to authorized users in real-time with low latency using WebSocket technology.

Phase 3: Web Application (Client)

A web-based interface that displays keystroke data for administrators, providing a clear monitoring dashboard.

Ethics and Responsible Use

The keylogger is designed for ethical applications like penetration testing and insider threat monitoring, always with user consent.

Security and Compliance

Data is encrypted to ensure privacy, with compliance to legal frameworks like GDPR for safe, authorized use.

Technology Used

- Python
- Reactjs
- Websocket

University of Kent