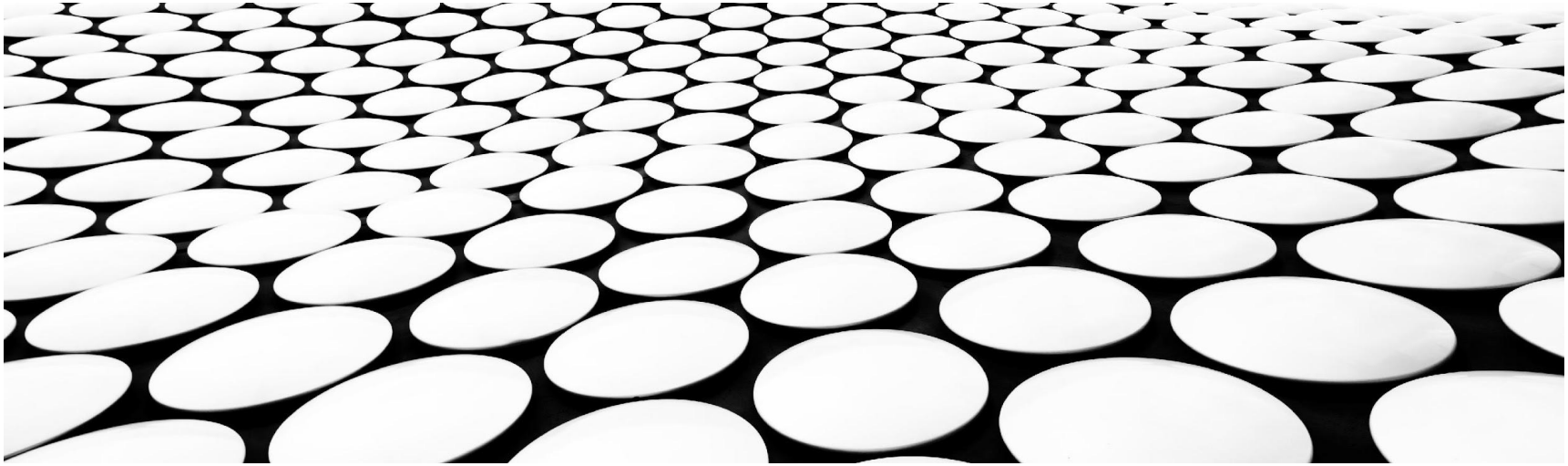
Secure AI Camera Communication

Unhackable, Offline AI Surveillance

Presented by: Steven Sereg | Solution Architect



Executive Summary

- Problem: insecure, internet-reliant AI video systems
- Solution: encrypted, offline-capable AI camera system
- Use Cases: military, law enforcement, emergency response

Problem Statement

- AI video systems depend on internet connectivity
- Vulnerabilities: MITM attacks, outages, unauthorized access
- Mission-critical ops require stronger security

Solution Overview

- Raspberry Pi 5-based AI camera
- Offline-capable secure communication protocol
- Proprietary, unbreakable encryption method

System Architecture

- Data flow: Camera → AI → Encryption → Secure Transmission → Receiver
- Modules: Camera Input, AI Processing, Encryption, Secure Channel, Receiver

Encryption Algorithm

- Custom, proprietary encryption technique
- Not based on standard mathematical algorithms
- Resistant to known cryptographic attacks
- Comparison with AES, RSA (conceptual)

Deployment Scenarios

- Military body cams in the field
- Dashcams for law enforcement vehicles
- Drones streaming secure video feeds
- Emergency areas with disrupted networks

Security Features & Benefits

- Offline functionality
- No external network dependencies
- Real-time secure video/audio transfer
- Field-tested, robust software stack

Case Study / Feedback

- Successful pilot demo: zero data compromise
- Real-time, encrypted transmission verified
- Positive stakeholder feedback
- High reliability under field conditions

Next Steps / Call to Action

- Engage for trials, demos, partnerships
- Roadmap: Certifications, integrations, scaling
- Contact Steven Sereg for full technical briefing

Q&A

- Let’s discuss how this technology fits your mission.