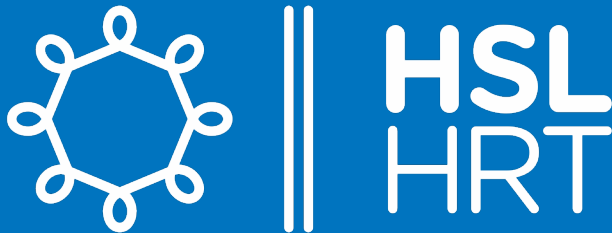


Vulnerability management



Experiences on building and running the vulnerability management process from left to right

Akseli Wiik - akseli.wiik@hsl.fi

Speakers



Akseli Wiik
Security Specialist
HSL

**Security Champion
Captain**

DevSecOps



Massimo Prencipe
Security Specialist
Solita

DevSecOps

Cloud Security

Helsinki regional transport



344M

Boardings /
Year

Income: 876M

50-55% from
municipalities

400

Workers

9

Municipalities

1,4M

Regional
Population

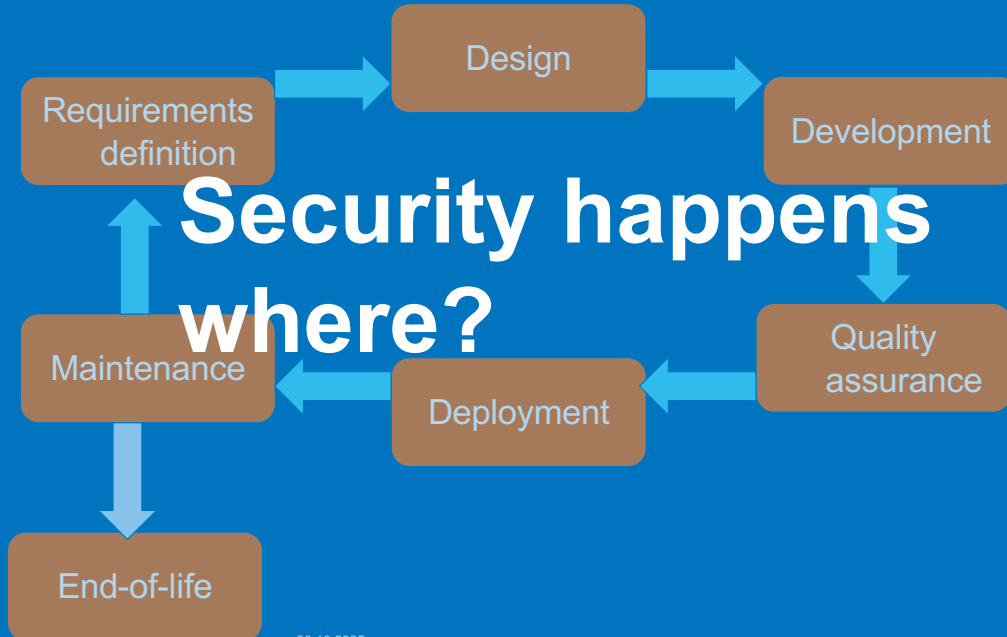


Critical function = Interesting target

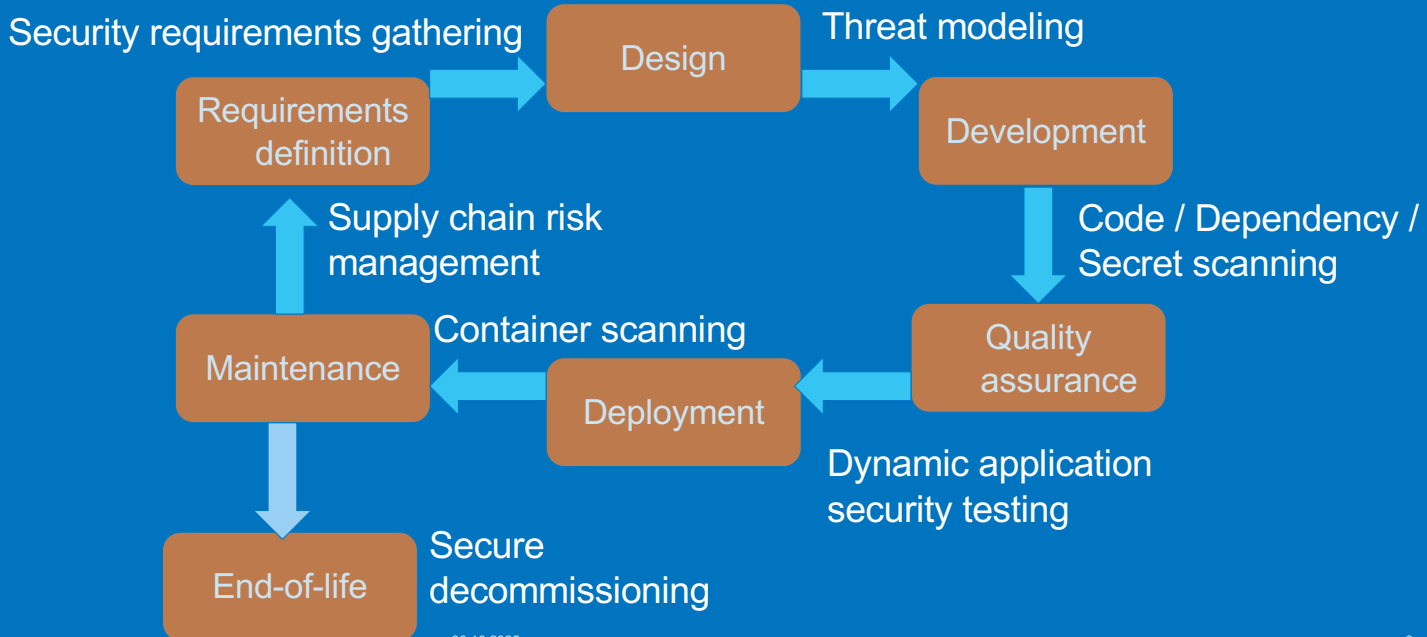
We play key role of transporting people in southern Finland

We are juicy target also for nation state actors





Secure Software Lifecycle



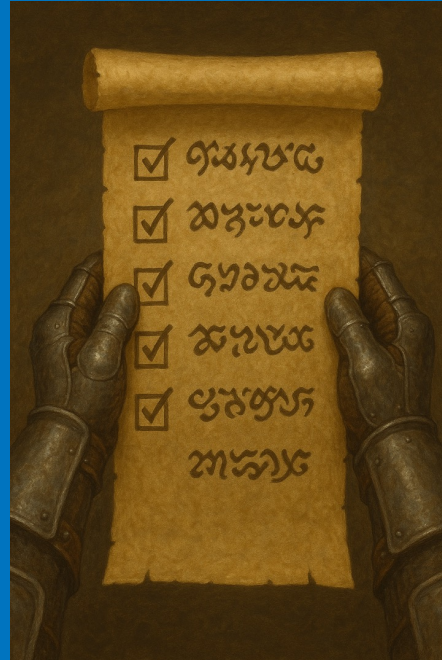
Scaling the process

- Security Champions nominated from each team
- Champs are responsible for deploying and maintaining tooling in their projects



Secure Software Development Lifecycle = SSDLC

- Centralized repository of information
- Requirements for creating an operating software securely
- Practical guidance for implementing the requirements



Fostering the Champs community

- Weekly calls
- Exclusive training on topical subjects like supply chain security, AI
- Low threshold support



Maintaining situation awareness

- Organization-level visibility to vulnerabilities
- Regular inspection of project security postures
- Ad hoc meeting with team having rising trend
- Supply chain risk management with SBOM



Challenges

- Establishing a baseline for legacy project – huge amount of findings
- Busy teams are busy
- Monorepo vs separate repos and ownership



Kiitos Thank you

