Secure Architecture Process

Memi Lavi
www.memilavi.com

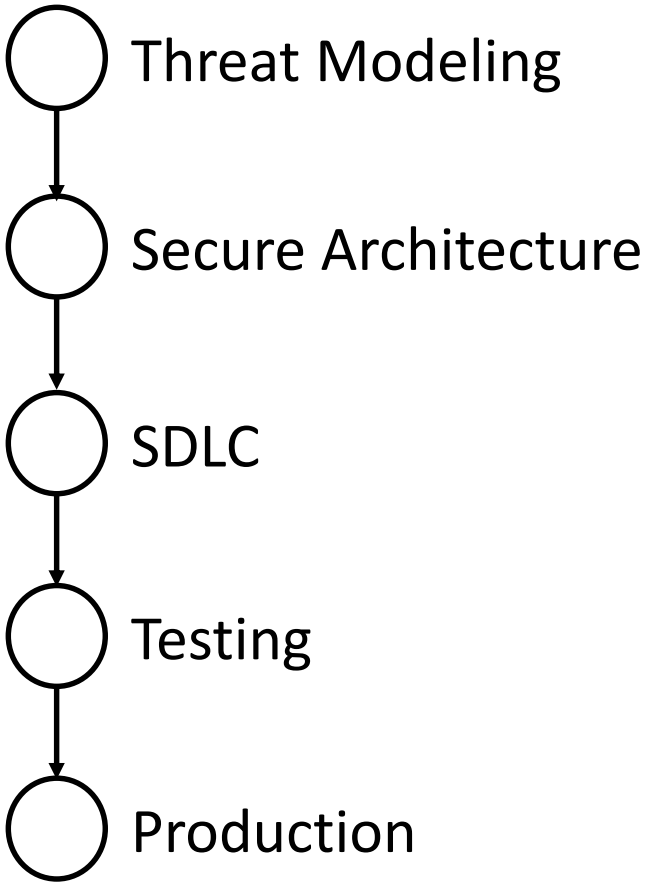
Secure Architecture Process

- A well defined process for ensuring the system is as secure as possible
- Goes through all the system's phases
- Should be led by the project manager / dev manager
- Architect should be involved in all stages

Secure Architecture Process

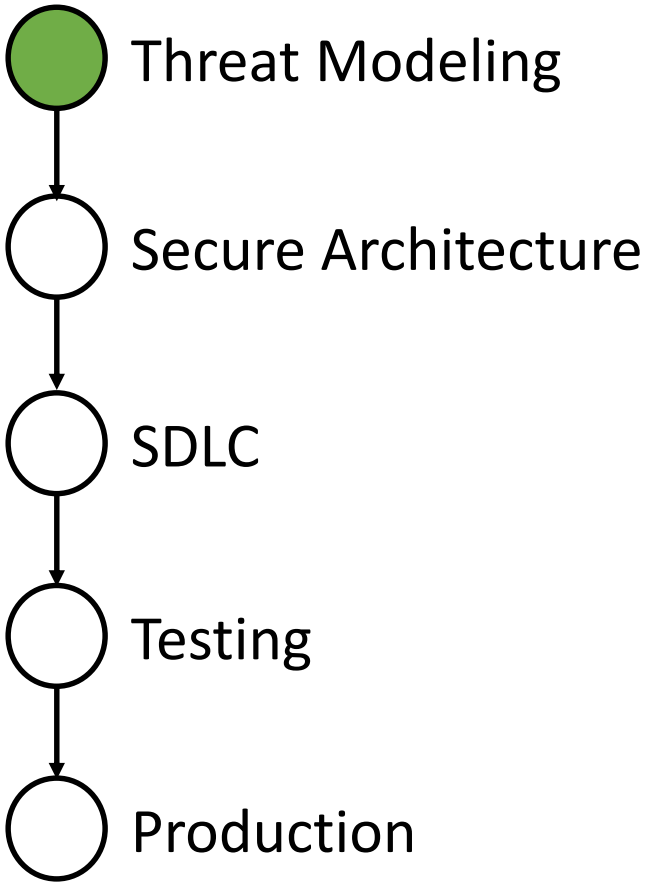
- Total of 5 stages
- For each one we'll describe:
  - Goal
  - Participants
  - Complete details about execution

Secure Architecture Process



Before diving in – a quick overview…

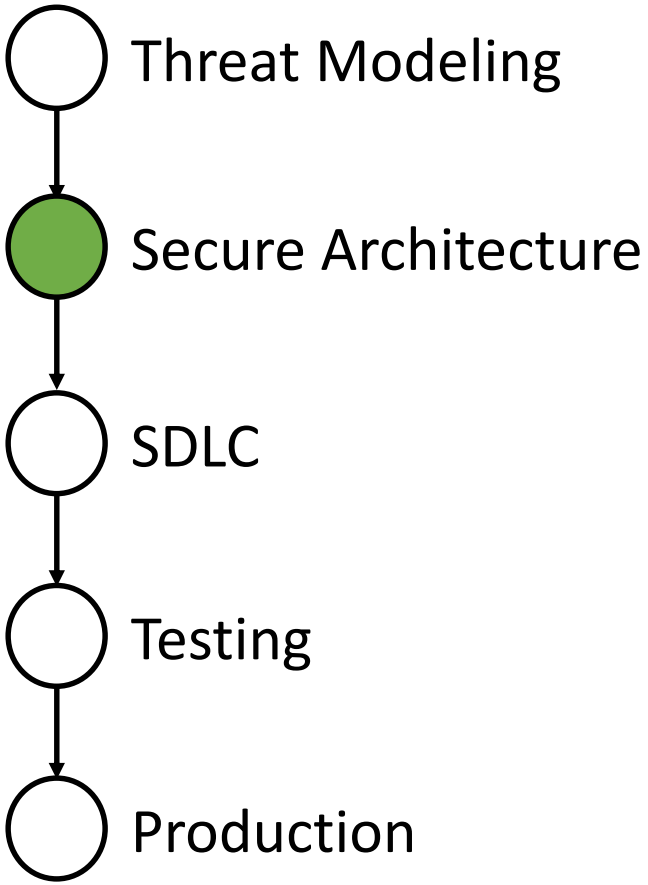
Secure Architecture Process



Threat Modeling

- A process for identifying potential threats for the system
- Prioritizes mitigations measures
- Has a great effect on the work plan
- Involves almost everyone in the team
- Might utilize formal methods and tools

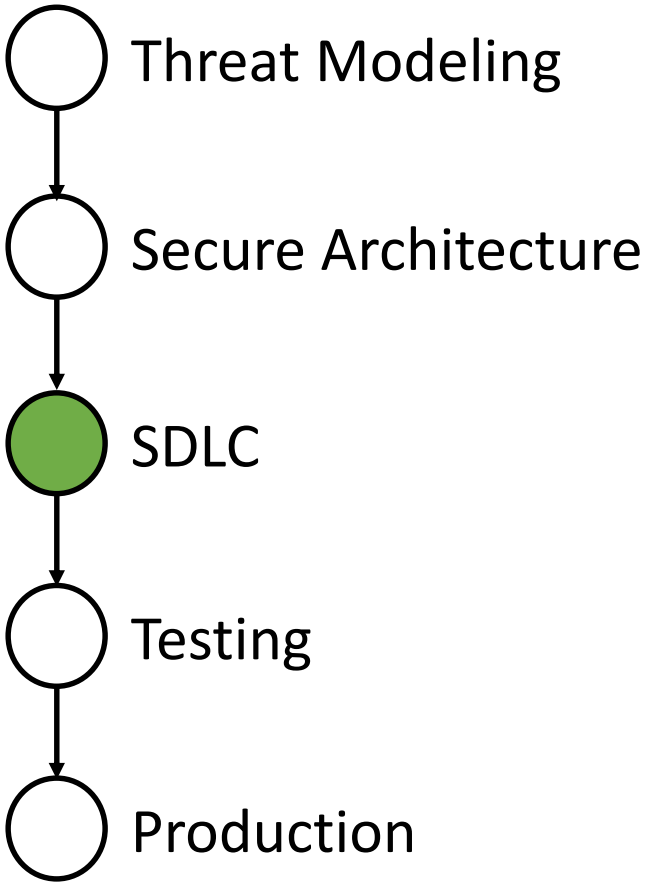
Secure Architecture Process



Secure Architecture

- The most important step for the architect (yay!)
- Based on the Security Perimeters paradigm
- Integrates security defenses into the core architecture
- Touches all aspects of the system

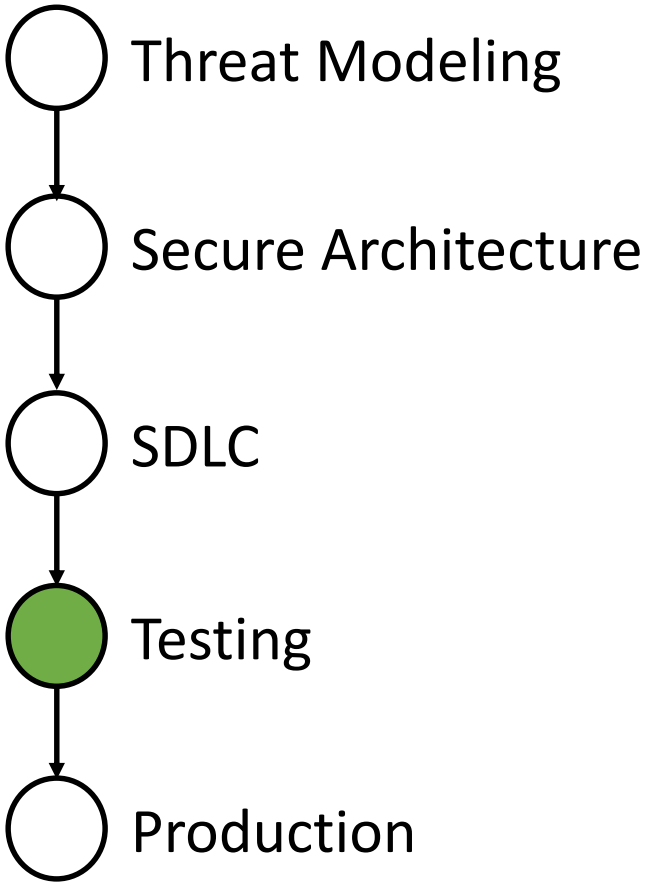
Secure Architecture Process



SDLC

- Secure Development Life Cycle
- The actual development of the system
- Implements code-level security measures
  - ie. SQL Injection, XSS, etc.

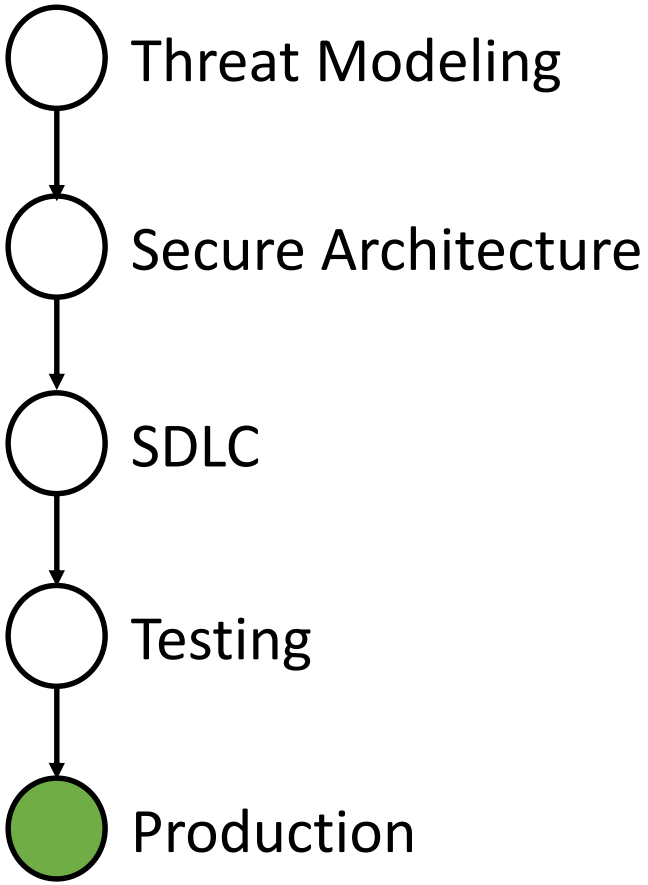
Secure Architecture Process



Testing

- Implement security-oriented testing
- Analyze the results
- Compare to the Threat Modeling

Secure Architecture Process



Production

- Continuous monitoring
- Get up-to-date