Security Testing

John Slankas
jbslanka@ncsu.edu

What is Security Testing?

Validate security controls operate as expected

What to Test?

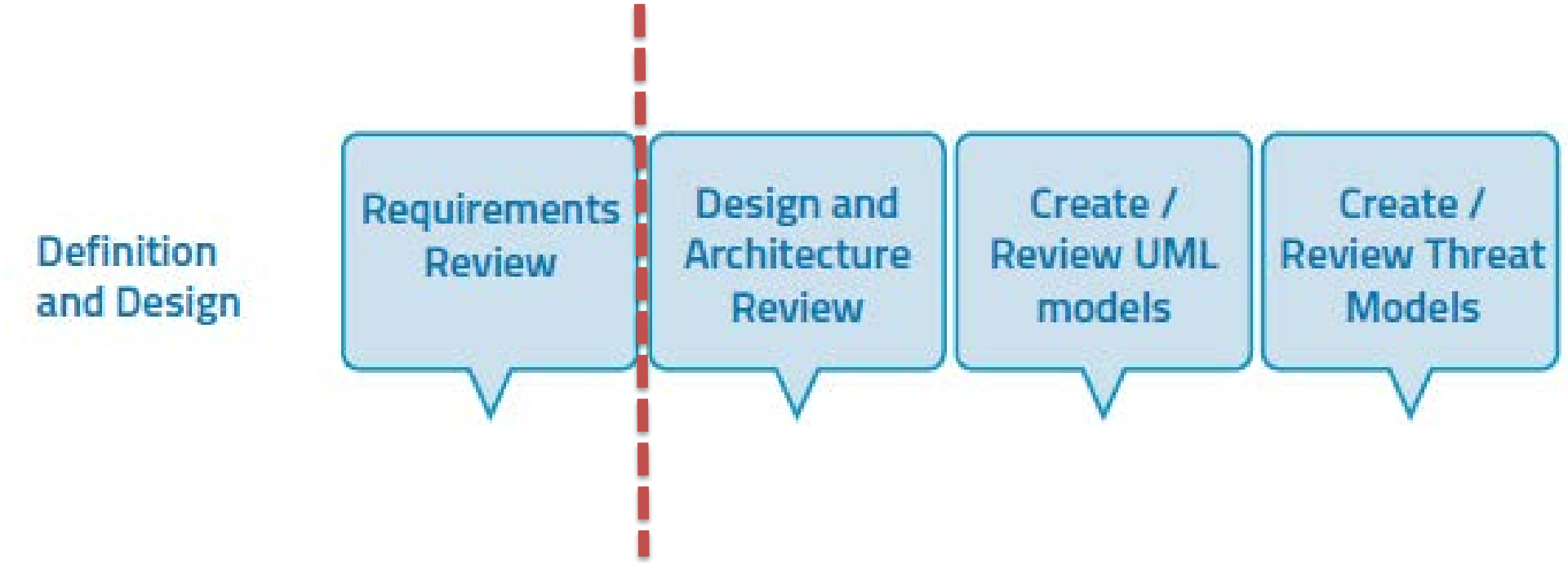
- People
  - Ensure there is adequate education and awareness
- Process
  - Ensure there are adequate policies and standards and that people know how to follow these policies
- Technology
  - Ensure that the product has been effective in its implementation

When to Perform Security Testing?

Before Development

Metrics
Criteria
Measurement
Traceability

When to Perform Security Testing



When to Perform Security Testing

When to Perform Security Testing

When to Perform Security Testing

How to Perform Security Testing

- Manual Inspections
- Threat Modeling
- Source Code Review
- Penetration Testing
- Tool-based Testing
  - Static Code Analyzers
  - Dynamic Code Analyzers
  - Fuzz Testing
- Security Test Suites

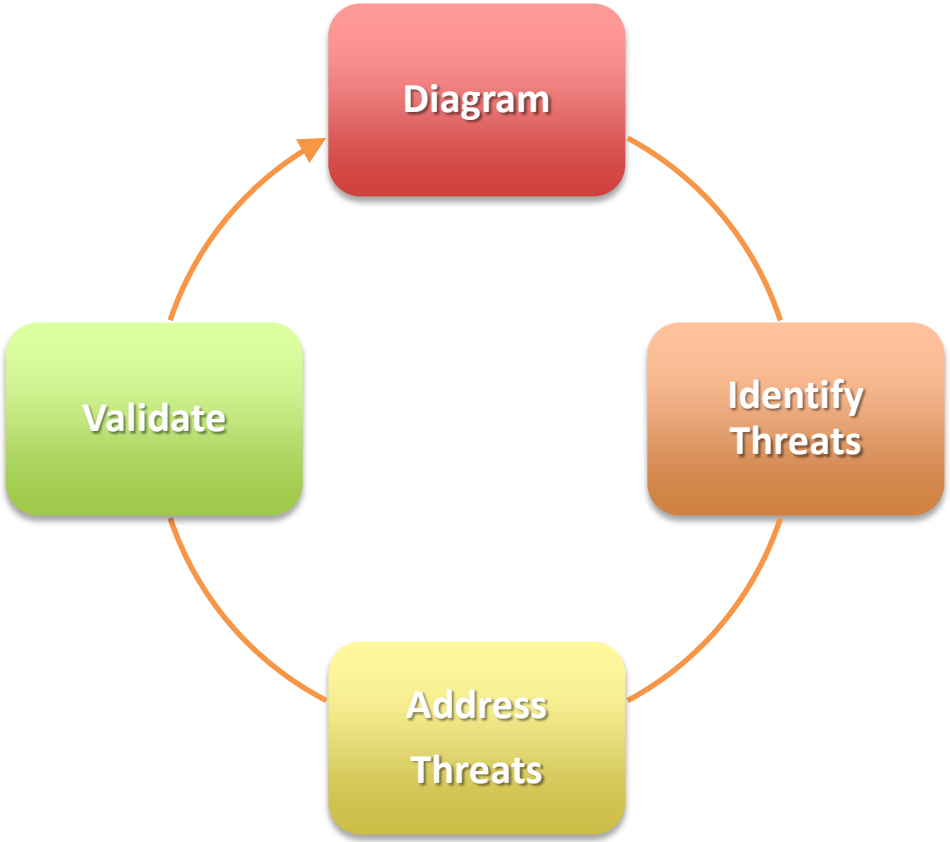
Manual Inspections

- Human reviews
- Analyze documentation, models, and other artifacts
- Interviews

- Advantages
  - No technology needed
  - Use throughout the SDLC
  - Flexible

- Disadvantages
  - Time consuming
  - May not have supporting materials
  - Requires significant security skill

Threat Modeling



- Advantages
  - Attacker's point of view
  - Early in the SDLC
- Disadvantages
  - Good threat models don't automatically mean good software

Source Code Review

- Manually check the source code for security issues
- “If you want to know what’s really going on, go straight to the source”
- Examples that can be found:
  - Concurrency issues
  - Flawed business logic
  - Backdoors (Trojans, Easter Eggs)
  - Weak cryptography
  - ….

- Advantages
  - Complete, effective, accurate

- Disadvantages
  - Requires skilled developers
  - Can’t find issues in 3rd Party or compiled libraries
  - May miss runtime issues

http://www.clipartbest.com/clipart-yikg7ajRT