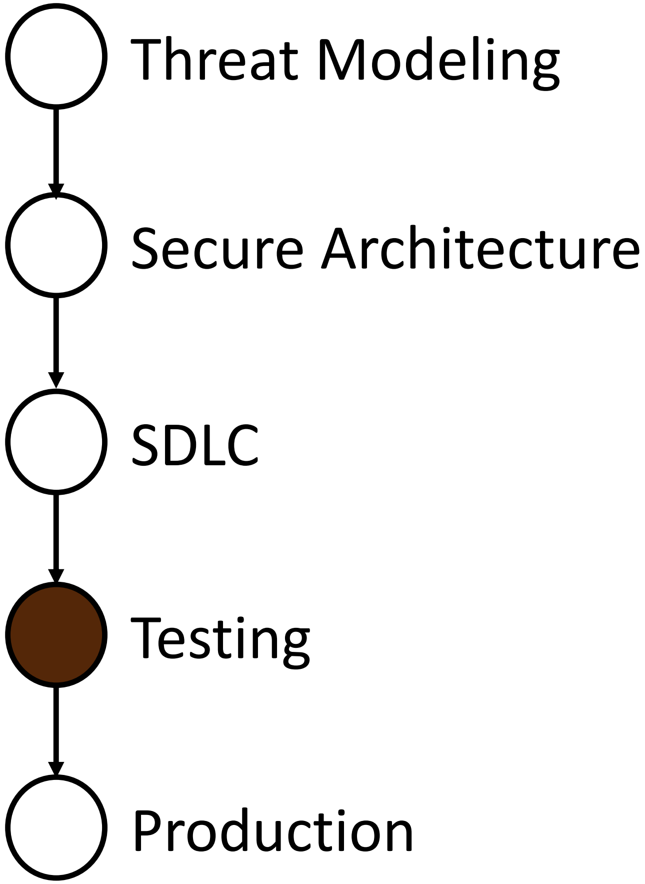
Testing

Memi Lavi
www.memilavi.com

Secure Architecture Process



○ Threat Modeling

○ Secure Architecture

○ SDLC

● Testing

○ Production

Testing

Be Aware / Recommend

Goal: To make sure the system is really secure

Participants:

Architect
QA
Dev Manager
Developers

Testing and Security

- Testing is an integral part of the development process
- Usually used to make sure the system works as expected
- Testing should be used to make sure the system is secure

Security Related Test Types

Penetration Testing

Load Testing

Penetration Testing

- A special type of test which simulates an attack on the system
- Its purpose:
  - to find weaknesses in the system that allow attackers to gain unauthorized access

Penetration Testing

- Protects against:
  - Data leak
  - Data loss
  - Data inconsistency
  - Disruption of service

Types of Penetration Testing

Black Box

White Box

Black Box Testing

- The attacker (tester) has no prior knowledge on the system
- He's handed the URL or endpoint and that's it
- Might miss some important vulnerabilities
- Takes long time
- Best simulates real-world attacks

White Box Testing

- The attacker (test) is given full details and access
- Can see the source code, network, database, etc.
- Should scan everything for vulnerabilities
- Not simulates real world attacks

Grey Box Testing

- The attacker (tester) has some knowledge on the system
- Mainly around network and credentials
- Used to simulate an attack where the hacker already penetrated the network perimeter

Which One to Choose?

Black Box

- When main threats are from the outside (ie. Public website)
- No time constraints

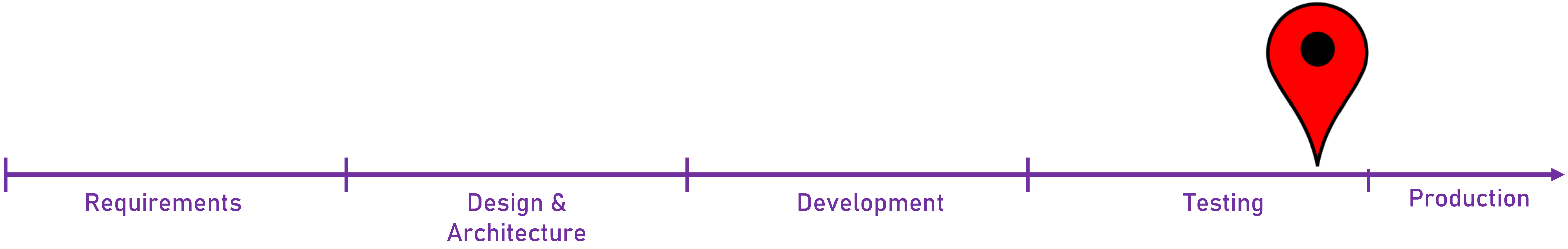
Grey Box

- When main threat is from the outside
- Want to focus on the app’s penentration testing

White Box

- When main threat is from the inside (ie. Internal org system)
- Don’t want to miss any potential vulnerability

When to Do Penetration Testing?



Also – After major changes

Who Conducts Penetration Testing?

- White Hat Hackers

- For black box tests – preferably outside expert

Penetration Testing Process

- Information Gathering
- Vulnerability Assessment
- Penetration Testing
- Report Results

Penetration Testing Results

- Detailed report outlining:
  - Background
  - Objectives
  - Scope
  - Approach
  - Findings
  - Recommendations

Automated Penetration Testing

- Offered by some companies
- Much faster than manual pen test
- Less flexible
- Usually costs less

nessus® Professional

Qualys.

RAPID7

Cymulate

Load Testing

- A test that simulates heavy load on the system and makes sure it functions properly
- Is a standard part in the testing lifecycle
  - Not just security related

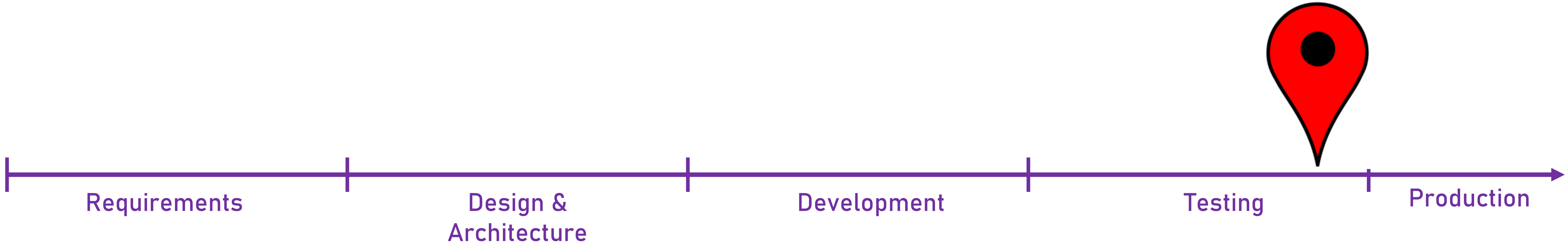
Load Testing

- Protects against:
  - Disruption of service

Conducting Load Testing

- Preparing a number of computers
  - Around the world or in the organization
- Each computer makes a large number of requests according to pre-prepared scenario
- Continuously monitoring the server

When to Do Load Testing?



Also - After major changes

Who Conducts Load Testing?

- Expert testers
- Developers must be involved

Load Test Process

- Preparing Scenarios
- Building Scenarios
- Configuring Machines
- Load Testing
- Report Results

Automated Load Testing

- Load Testing must be automated

- There are a lot of tools for that

APACHE JMeter™

BlazeMeter

WEBLOAD

Load Testing Results

- Automated report outlining:
  - Execution Details
  - Monitoring Results

Security Testing and the Architect

- Make sure there are planned penetration and load testing
- Work with the testers to ensure they test the right things
- Look closely at the results
- Fine tune the architecture as needed