

# Secure Agile Development

Jeffery Payne

[jeff.payne@coveros.com](mailto:jeff.payne@coveros.com)

Chief Executive Officer



# Contents

- About Coveros
- SecureAgile development process
- Integrating security into Agile development
- Q&A

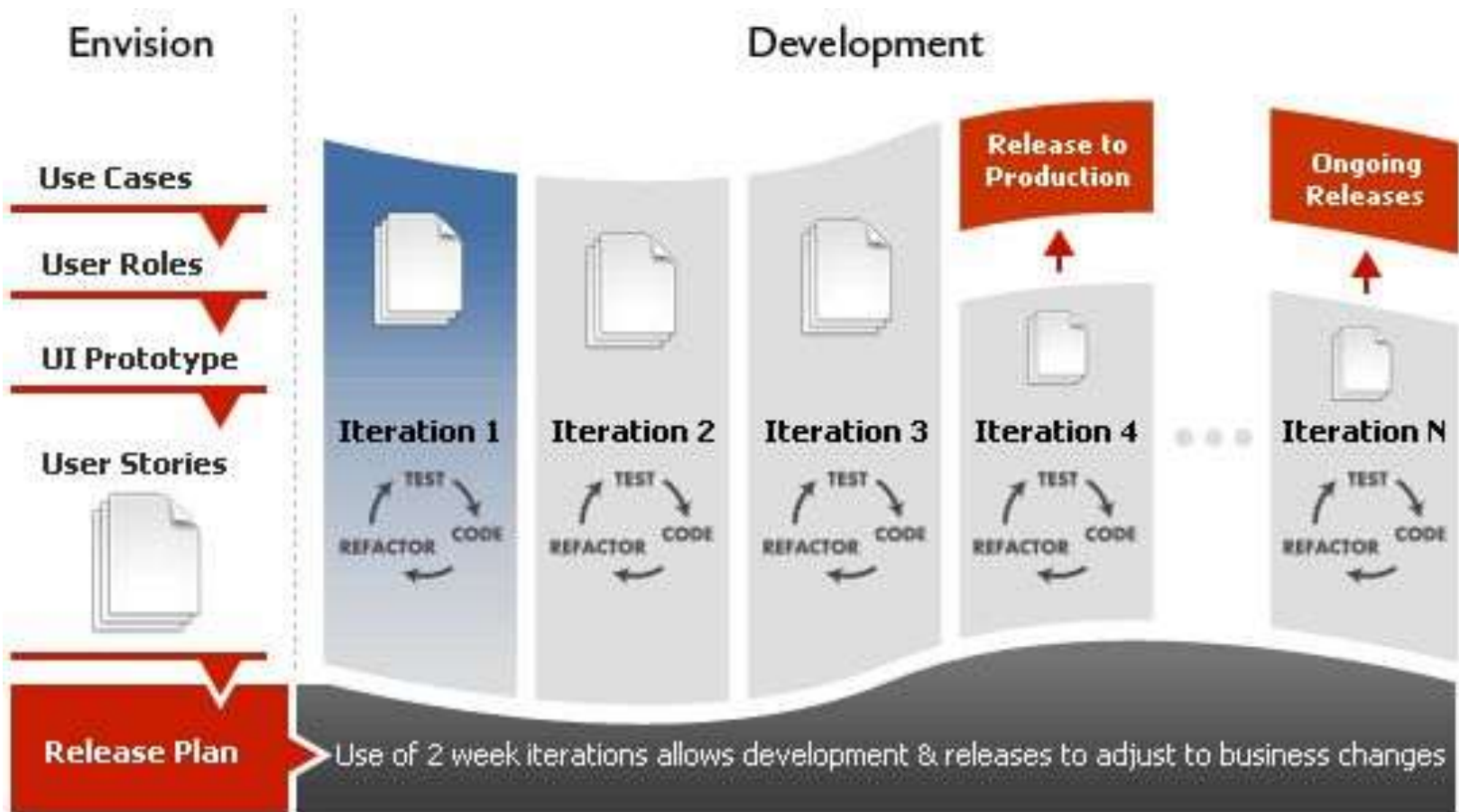
## Who we are

- Coveros helps organizations accelerate the delivery of secure, reliable software
- SecureAgile Services
  - Secure software development services
  - Application vulnerability remediation
  - Application security assessments and testing
  - Agile software process improvement
- SecureCI Product
  - Open source secure continuous integration product
- Our primary markets
  - Defense systems
  - National security
  - Healthcare
  - Financial services

### Corporate Partners



# SecureAgile™ Development Process



*Assures time-to-market while achieving security objectives*

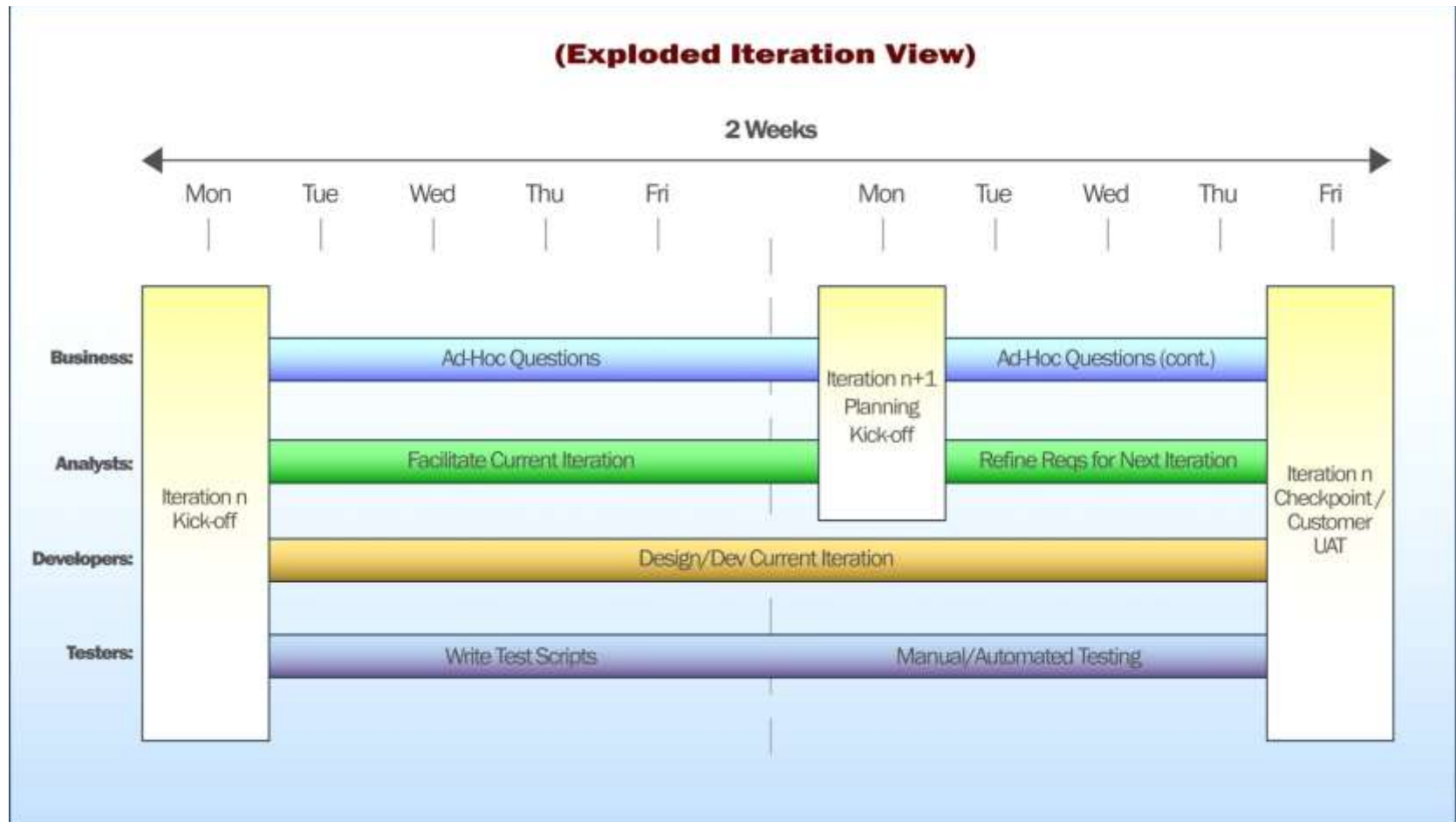
## Envision Process (aka Initial Planning)

- Create User Personas to keep the customer top of mind
- Develop Use Cases to understand overall business process
- Build Global Backlog of User Stories with priority
- Prototype UI as appropriate / necessary
- Define initial application architecture and address initial research spikes
- Develop Release Plan comprised of Stories within Iterations
- Create test strategy / master test plan for project

## Security Activities within Envision

- Threat modeling / Architectural Risk Analysis to understand threats, possible attacks, and value of assets
- Misuse / Abuse Case development
- Incorporate security requirements into User Stories
  - “User will not” nomenclature as needed
- Develop high level security test strategy / plan
- Understand compliance & regulatory needs

# Iterative Development Process



## Defensive design and coding

- Incorporation of security controls into software design and code
  - Security frameworks like OWASP ESAPI
- Use of vetted components
  - Libraries of secure components
- Examination of design / code looking for realization of architectural risks



# Software Assurance

- Secure code review
  - Both automated and manual
  
- Security testing
  - Risk-based testing
  - Testing of security functionality
  
- Penetration testing

## Continuous Integration

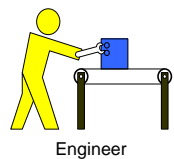
- Automation of build, test, deploy process
  - Check-in builds / tests
  - Nightly code integrations and regression tests
  - Automated promotion between test stages
  - Automated notification of build failures
- A critical capability to have when building software using agile
- Many good open source products available



Create code

IntelliJ IDEA/  
Eclipse

Version code



Engineer

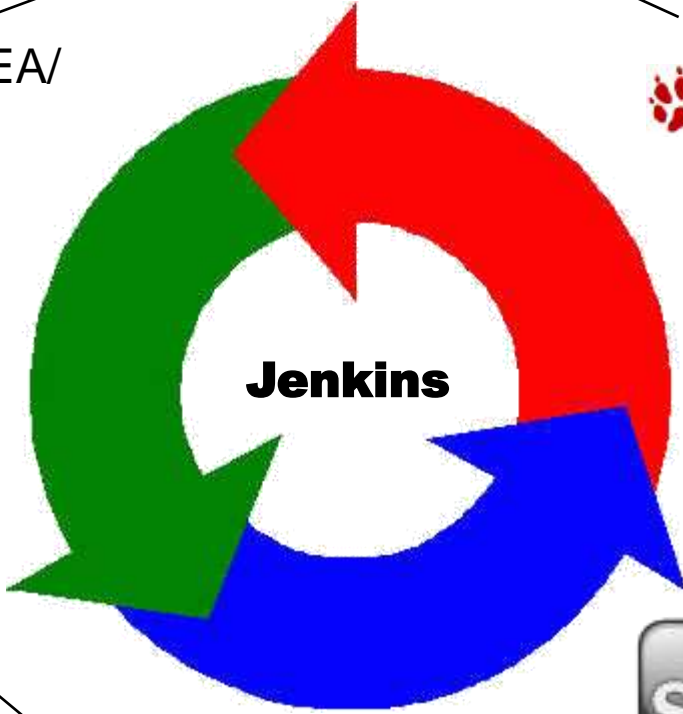
Track progress



Test security

FindBugs

Jenkins



Build application



Test application

**Questions?**

**Thank You**