DevSecOps

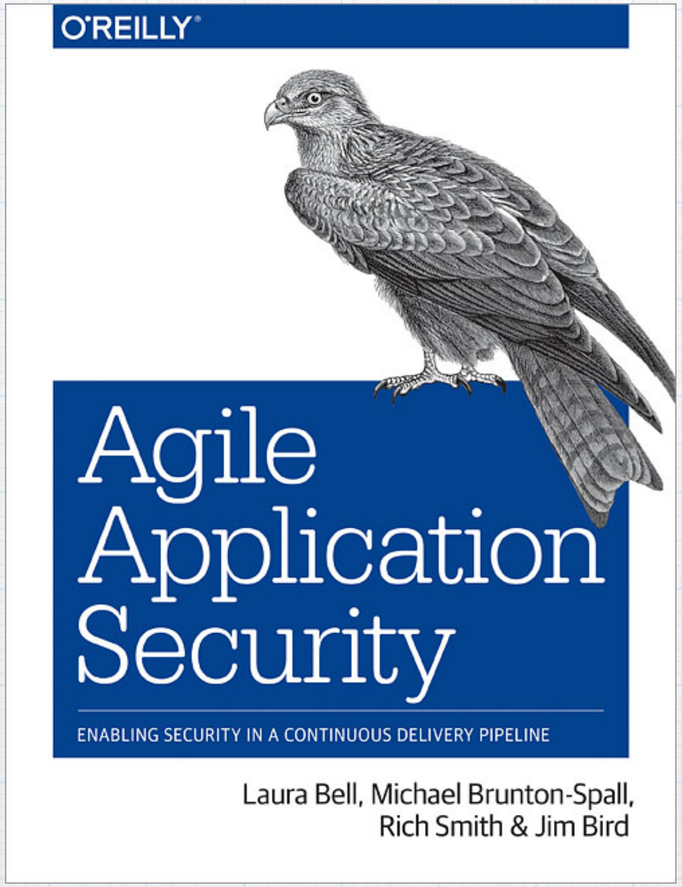
Building an Culture of Agile Security

"Approach security as a journey, not a destination — one that starts with a small number of fundamentals upon which you will continue to build iteratively, relating new developments back to familiar concepts."

Bell, Laura. Agile Application Security: Enabling Security in a Continuous Delivery Pipeline (Kindle Locations 137-138). O'Reilly Media. Kindle Edition.

Motivation

* Personal experiences as a security focused software architect
* Issues integrating security team into our DevOps Process
* Affirmation and further learning based on Agile Application Security


O'REILLY
Agile Application Security
ENABLING SECURITY IN A CONTINUOUS DELIVERY PIPELINE
Laura Bell, Michael Brunton-Spall,
Rich Smith & Jim Bird

Why should we care?

Technology Empowers

* Crime existed long before computers
* Computers, however has made it easier
* Motivations remain unchanged: money, politics, power, thrill

We can make it worse

* Speed to Market drives everything
* Quality and Security often suffer
* Management cares all too often more about artificial deadlines

How can we help?

* We have to drive change from the bottom up
* We must change the culture in the agile team
* We must take the first steps in education and process
* We must think different

What does Security really mean in today's world?

Risk Management

* Security today is all about managing risks
* Compromises must be made
* Compromises must be informed to be valid!
* Everyone involved has a role in risk management

Protect What is Important

* Protect our customers
* Protect our employers
* Protect our reputation
* Protect our profession

Agile to DevOps

Development becomes Agile

* Waterfall ruled the world
* Agile began to take hold, allowing teams to move faster
* Process of small teams, tightly integrated, moving forward quickly took hold

Ops was left behind

* Dev teams moved fast and consumed infrastructure
* Ops couldn't keep up with the needs of dev
* Microservices architectures exasperated the issues
* Cloud Native made it almost impossible

Dev and Ops joined

* We then moved ops teams in with the dev teams
* Dev teams became DevOps teams
* Responsible for development, deployment, and operations
* Speed to market increased but security was left behind

What is DevSecOps?

* Bringing security into the DevOps team
* Can be a focus on security within the team
* Can also be a trained security professional
* The key is integrating that person fully into the team

Culture

* Security is a culture
* DevOps is a culture
* DevSecOps is a culture -> hard to build in the current landscape
* Must be deliberate, must be grassroots

How do you get started?

Any security processes that slow down the path to production, without significant business gains, are a net liability for the organization and encourage value-driven teams to route around them.

Bell, Laura. Agile Application Security: Enabling Security in a Continuous Delivery Pipeline (Kindle Locations 587-588). O'Reilly Media. Kindle Edition.

Find a Champion

* You must find a security champion on your team
* Ideally a security professional, someone trained
  * penetration testing
  * attack trees
  * vulnerability mangement

Be the Champion

* If you don't have a security program, become the champion
* Read blogs, OWASP, books on hacking
* Take courses on secure coding, pen testing,

Making the barrier to interacting with the security team as low as possible is key to ensuring that security does not get in the way of delivery. Security needs to provide quick and informal guidance, and answers to questions through instant messaging or chat platforms, email, and wherever possible in person so that security is not seen as a blocker.

Bell, Laura. Agile Application Security: Enabling Security in a Continuous Delivery Pipeline (Kindle Locations 1049-1051). O'Reilly Media. Kindle Edition.

Security in Requirements

Another way to include security in requirements is through attacker stories or misuse cases

Bell, Laura. Agile Application Security: Enabling Security in a Continuous Delivery Pipeline (Kindle Locations 1484-1487). O'Reilly Media. Kindle Edition.

Building requirements with security

* Requirements should be focused on risk mitigation as well as the business needs
* Risk register should be consulted and updated as needed
* Requirements should address security at the core
* Champion can help review requirements

Security in Design

Security happens in the thought processes and design of stories, not just during coding. Be involved early and educate everyone to think about security.

Bell, Laura. Agile Application Security: Enabling Security in a Continuous Delivery Pipeline (Kindle Locations 1667-1668). O'Reilly Media. Kindle Edition.

Designing with security

* Design should leverage risk mitigation
* Design should not introduce new risk without appropriate mitigations
* Design must focus on business, ops, and security

Leverage the champion

* During design phases, consider levering your champion
* Help bounce ideas with respect to security
* Focus on collaboration

Security in testing

Testing automation

* Automate everything
* Unit tests have value, especially on input validation
* Integration testing should focus on your attack trees
* Leverage champion

Penetration testing

* Security team adds huge value here
* Leverage their tools and techniques as part of your testing process
* Look for ways to use pen testing in your CI/CD pipeline

Security in coding

Development

* Focus on secure coding principles
* Leverage CVE and OWASP during development
* Learn from you mistakes, track bugs and share them
* Leverage the champion when needed

Controls

* Technical controls - prevent the attack succeeding
* Deterrent controls - deter the attack
* Resistive controls - slow down the attack
* Protective controls - prevent the attack from happening
* Detective controls - simply detect the attack
* Compensating controls - cannot solve so you put other controls in place

Code reviews

* Do not take them lightly
* Should not be casual inspections
* Leverage champions when needed
* Pair programming shouldn't substitute for reviews

Static code analysis

* Evaluates you code looking for common patterns
* Can produce false positives
* When automation is added value is increased
* Champion can help review results

Summary

Summary

* Be the agent of change
* Build a culture
* Focus on integrating security into the dev processes
* Work with security, not against them

When security stops being the team that says no, and becomes the team that enables reliable code to ship, then that's true Agile security.

Bell, Laura. Agile Application Security: Enabling Security in a Continuous Delivery Pipeline (Kindle Locations 1122-1123). O'Reilly Media. Kindle Edition.

Questions?