TOP SECRET

SECUREBRASIL

Onde conhecimento e oportunidade se encontram

4ª EDIÇÃO

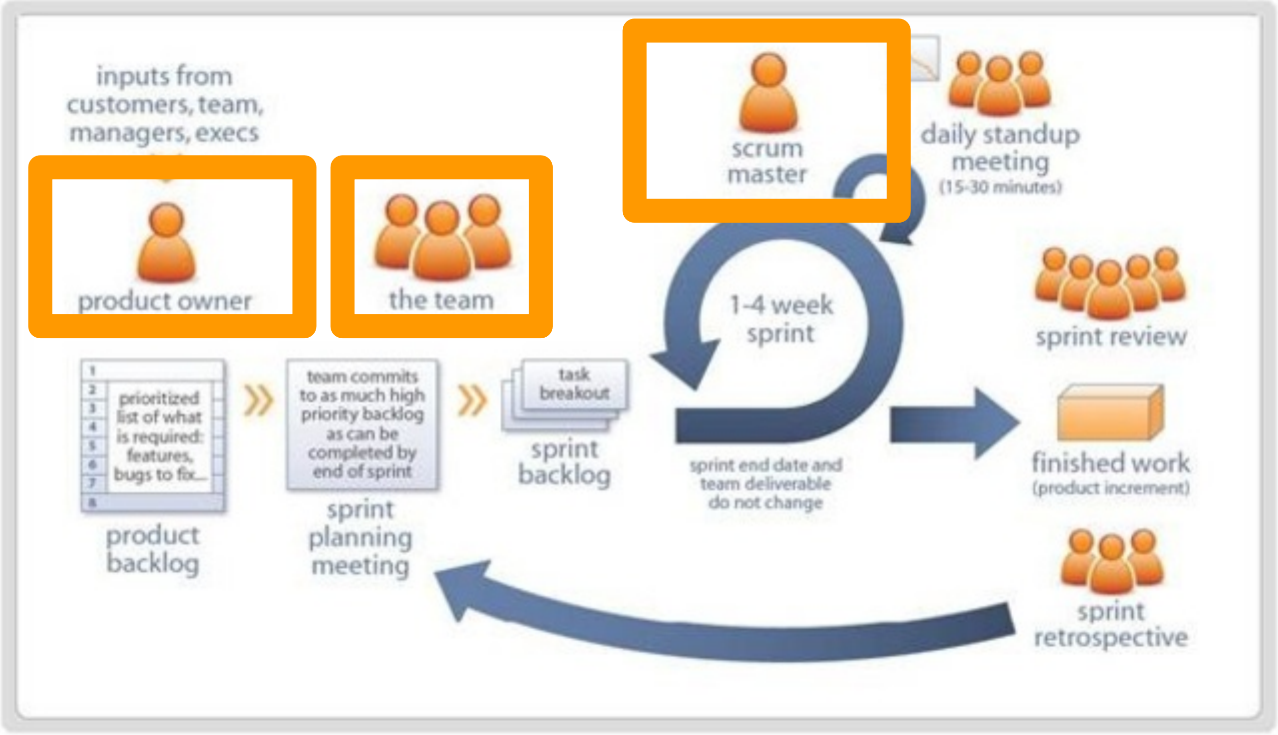
REPENSANDO CONFIANÇA EM TEMPOS DE PARANOIA

Strategies to Maximize the Security Efforts into the Agile SDLC without increasing the headcount

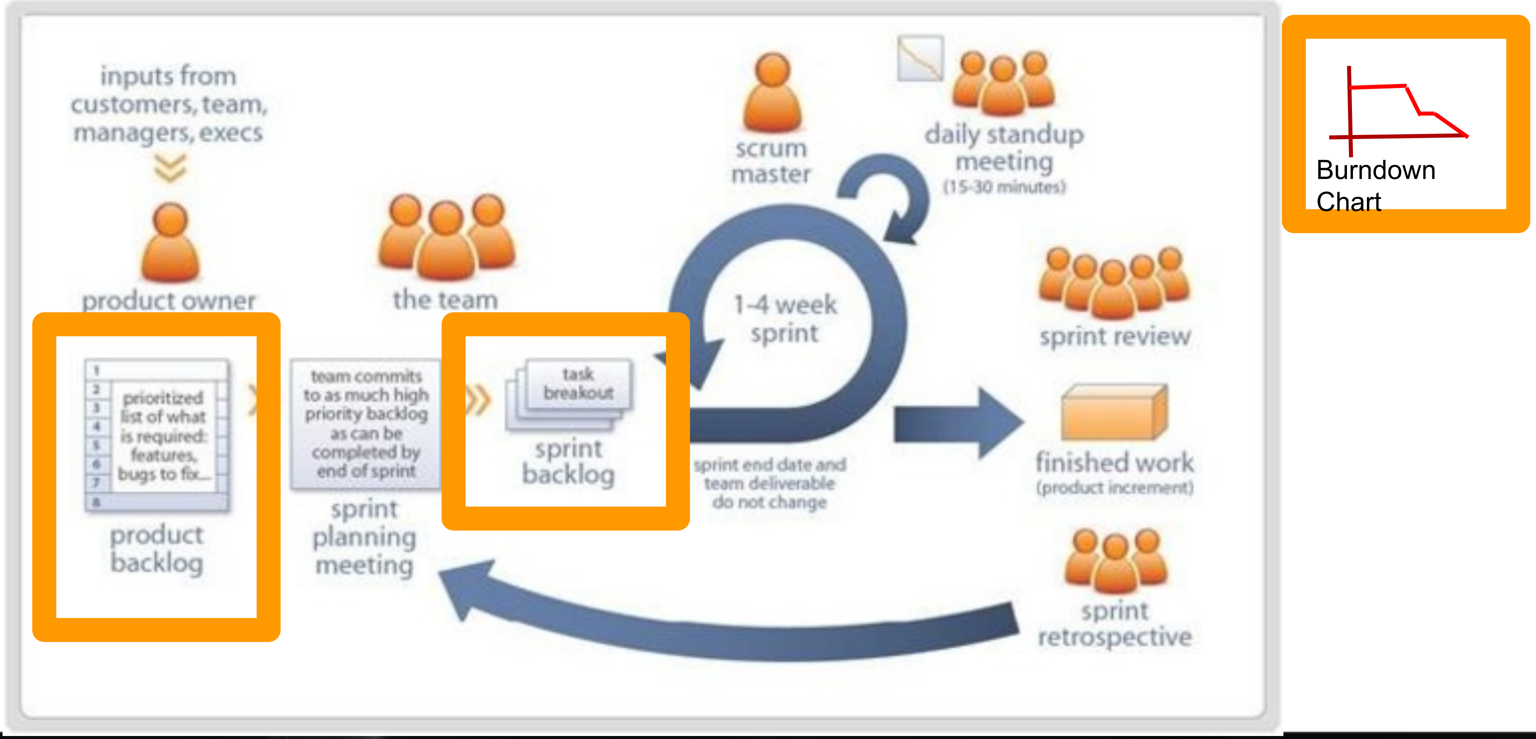
Anderson Dadario, CISSP, CSSLP

First, a little about Scrum

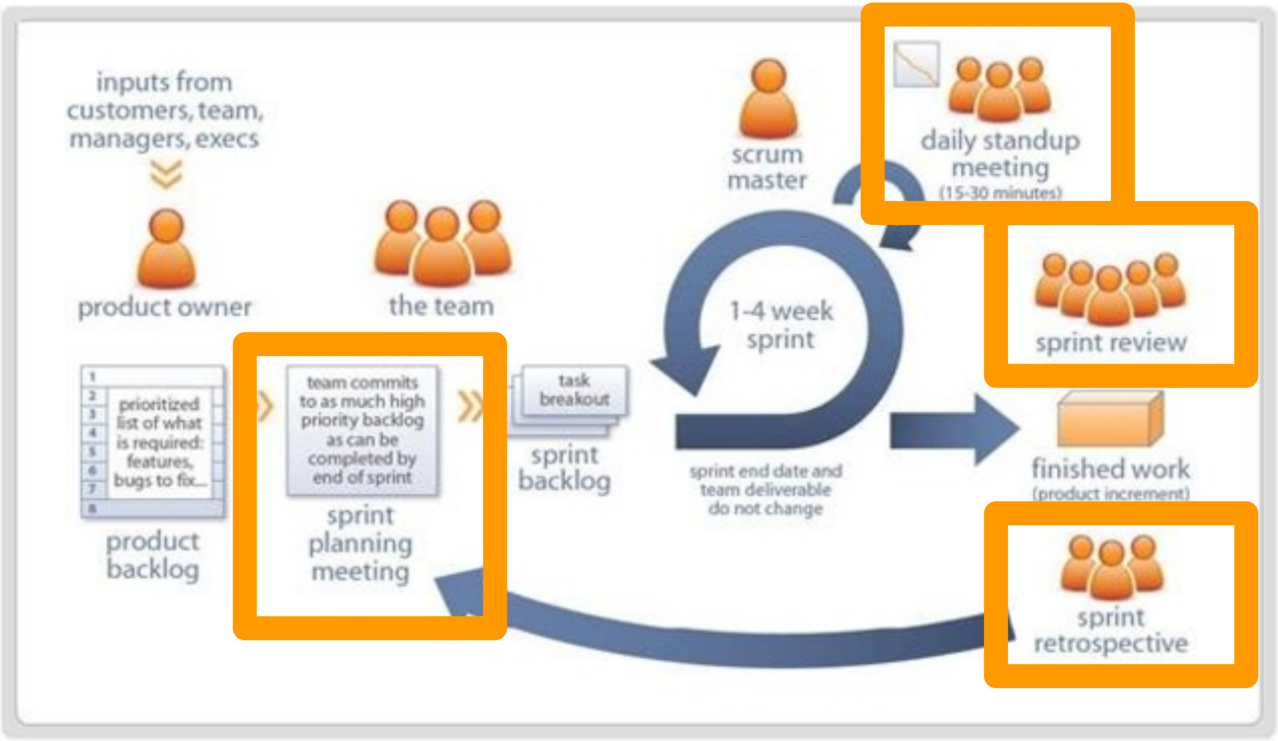
Scrum Roles


inputs from customers, team, managers, execs
product owner
the team
scrum master
daily standup meeting
(15-30 minutes)
1-4 week sprint
sprint review
1
2
3
4
5
6
7
8
prioritized list of what is required: features, bugs to fix...
product backlog
team commits to as much high priority backlog as can be completed by end of sprint
sprint planning meeting
task breakout
sprint backlog
sprint end date and team deliverable do not change
finished work
(product increment)
sprint retrospective

Scrum Artifacts


inputs from customers, team, managers, execs
product owner
the team
scrum master
daily standup meeting
(15-30 minutes)
1-4 week sprint
sprint review
1
2
3
4
5
6
7
8
prioritized list of what is required: features, bugs to fix...
product backlog
team commits to as much high priority backlog as can be completed by end of sprint
sprint planning meeting
task breakout
sprint backlog
sprint end date and team deliverable do not change
finished work
(product increment)
sprint retrospective
Burndown Chart

Scrum Ceremonies


inputs from customers, team, managers, execs
product owner
the team
scrum master
daily standup meeting
(15-30 minutes)
1-4 week sprint
sprint review
prioritized list of what is required: features, bugs to fix...
product backlog
team commits to as much high priority backlog as can be completed by end of sprint
sprint planning meeting
task breakout
sprint backlog
sprint end date and team deliverable do not change
finished work
(product increment)
sprint retrospective

Topics

1. Delegation
2. Awareness
3. Security Team Allocation
4. Team Members Assessment
5. Automation
6. Bug Bounty
7. Security Champions/Advisors

1. Delegation

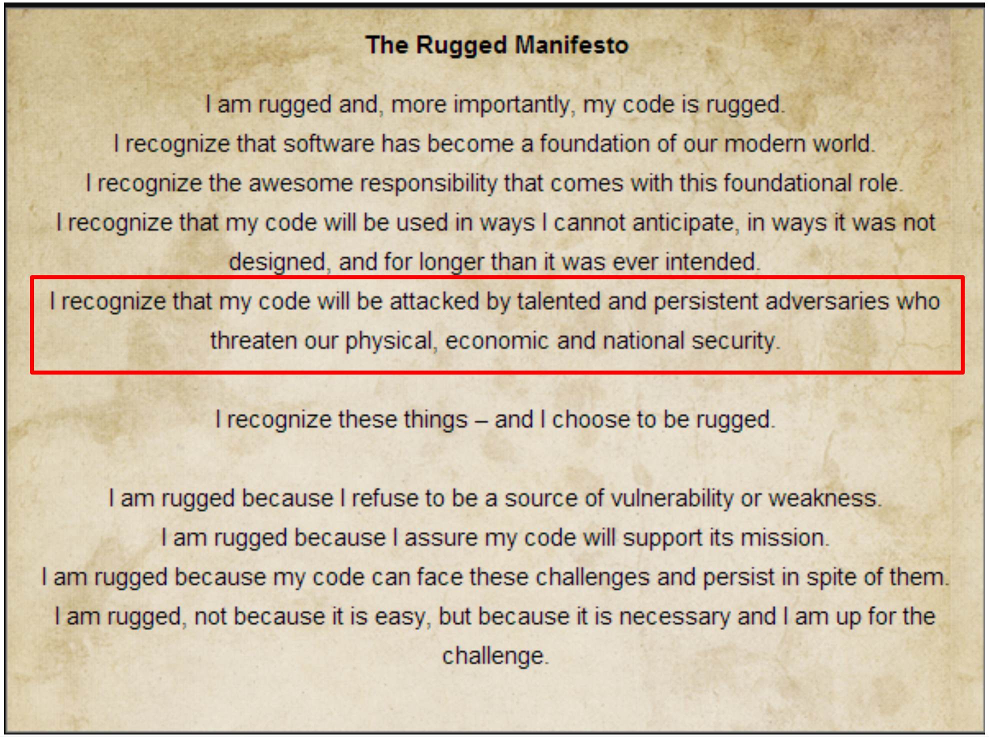
- Access Control Execution;
- Firewall Rules Execution;
- And so on, but there is no free lunch:
  - prepare an audit process.

2. Awareness

- Talk the developer language;
- Mailing lists;
- Tech talks;
- Coding standards and guidelines;
- Rugged Software Manifesto.

- The awareness campaign should:
  - NOT be a one-size-fits-all;
  - Be divided into modules;
  - Be prioritized by hierarchy;
  - Be kept alive (e.g. CTF games).

Rugged Software Manifesto



The Rugged Manifesto

I am rugged and, more importantly, my code is rugged.
I recognize that software has become a foundation of our modern world.
I recognize the awesome responsibility that comes with this foundational role.
I recognize that my code will be used in ways I cannot anticipate, in ways it was not designed, and for longer than it was ever intended.
I recognize that my code will be attacked by talented and persistent adversaries who threaten our physical, economic and national security.

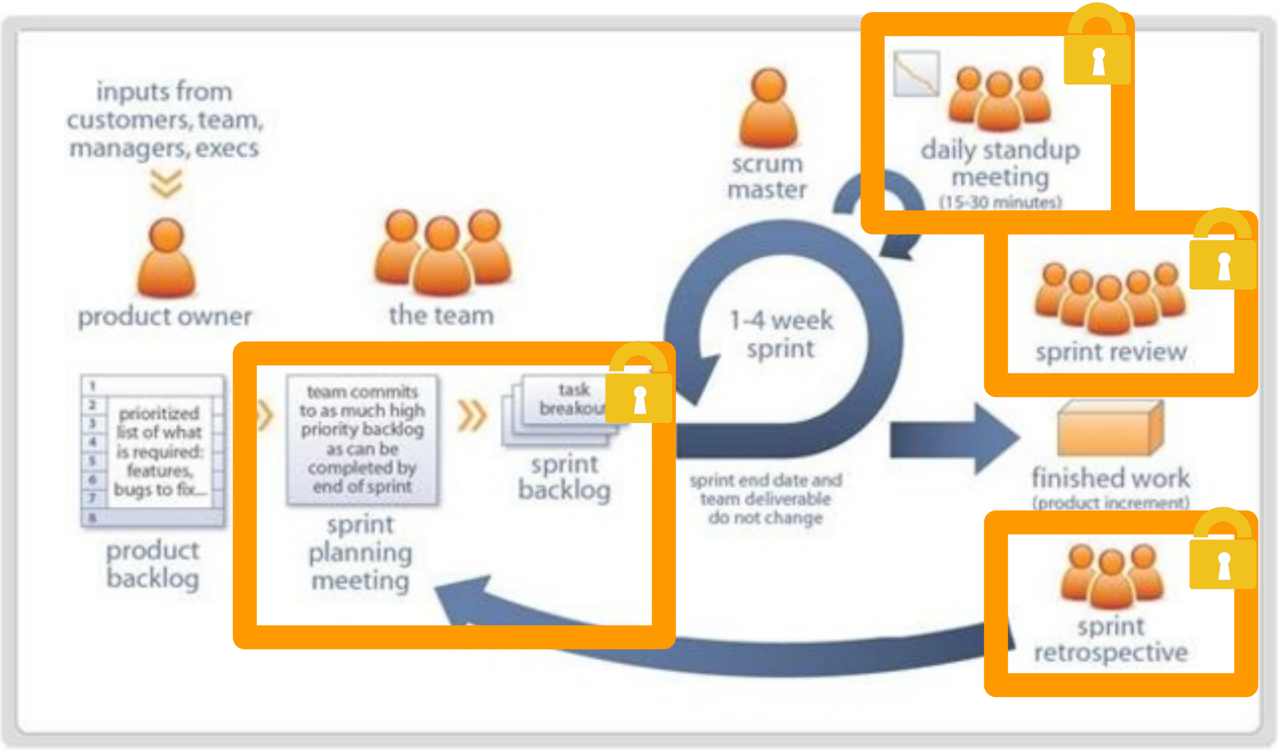
I recognize these things – and I choose to be rugged.

I am rugged because I refuse to be a source of vulnerability or weakness.
I am rugged because I assure my code will support its mission.
I am rugged because my code can face these challenges and persist in spite of them.
I am rugged, not because it is easy, but because it is necessary and I am up for the challenge.

3. Security Team Allocation

- Points to be aware:
  - Maximize the efficiency of the security injection;
  - Avoid Single Point of Failure (absence of a security expert);
  - There will be multiple products for limited security experts.

Strategy #1 Participate in everything


inputs from customers, team, managers, execs
product owner
the team
scrum master
daily standup meeting (15-30 minutes)
1-4 week sprint
sprint review
prioritized list of what is required: features, bugs to fix...
product backlog
team commits to as much high priority backlog as can be completed by end of sprint
sprint planning meeting
task breakou
sprint backlog
sprint end date and team deliverable do not change
finished work (product increment)
sprint retrospective

Strategy #1 Analysis

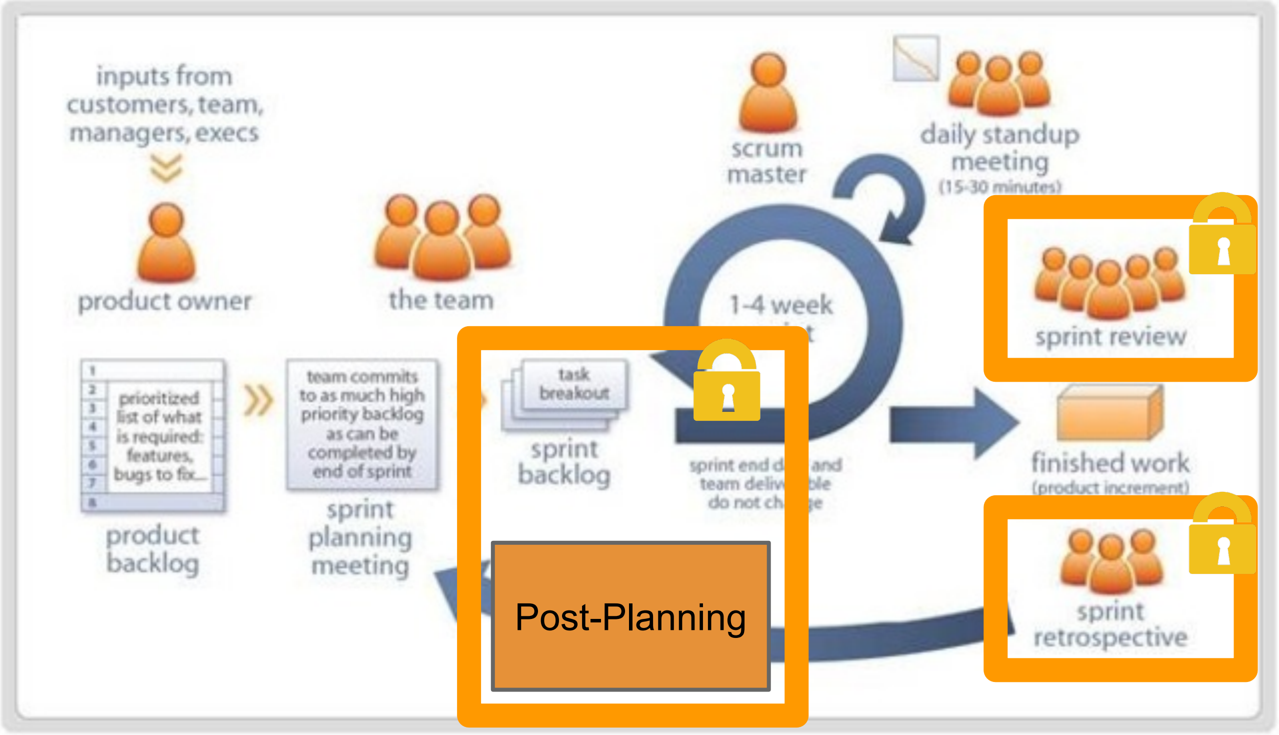
Pros:

- Security Expert is complete aware of the project and can rapidly inject security:
  - in the sprint backlog stories;
  - doing security awareness during the ceremonies.

Cons:

- Security Expert's time got too much consumed;
- Single Point of Failure;
- Planning participation is most of the part a waste of time;
- Too much daily become troublesome.

Strategy #2 Post-Planning, ‘Dailyless’



Strategy #2 Analysis

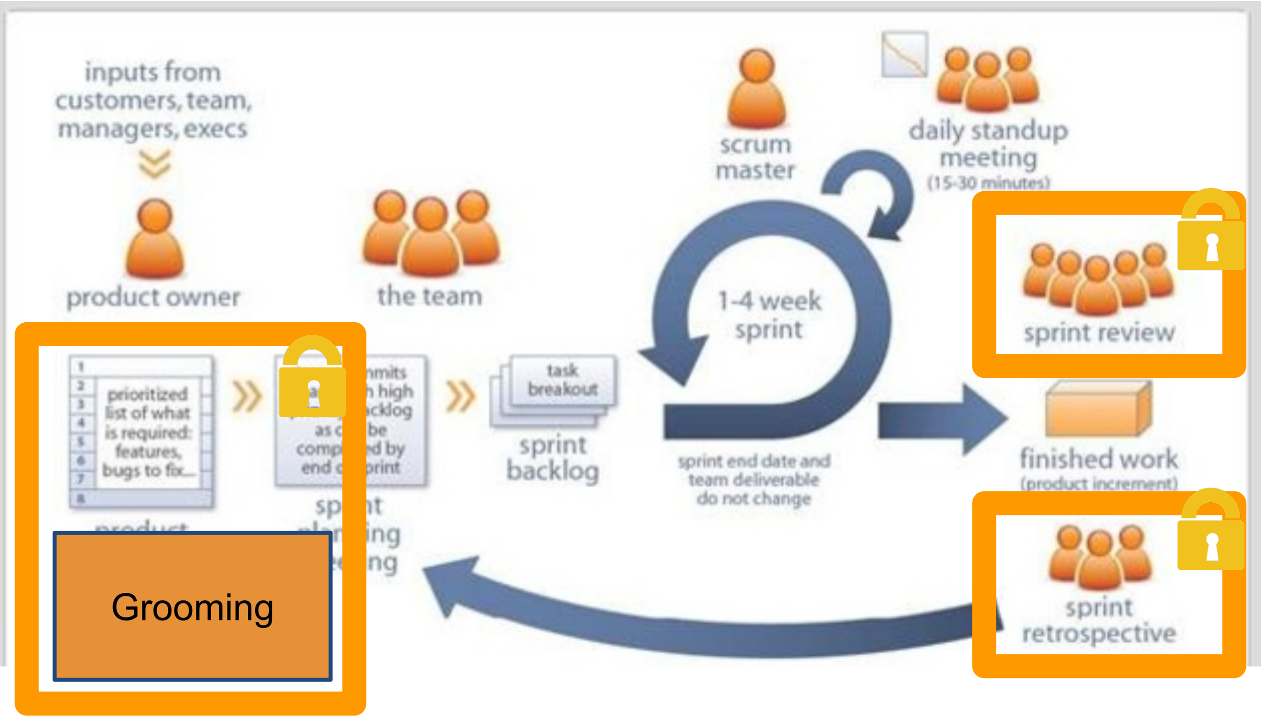
Pros:

- Security Expert’s time is used wisely.

Cons:

- You are messing up with Scrum methodology because stories cannot change after planning;
- Single Point of Failure persists;
- Less security awareness.

Strategy #3 Grooming, Security Roles



Strategy #3 Analysis

Pros:

- Security Expert’s time is used wisely;
- No Single Point of Failure;
- Security injection that respects the development process.

Cons:

- More people are involved, then the security injection become more complex.

4. Team Members Assessment

People are different, so is their performance in certain tasks:

- Some do better awareness than security testing;
- Some do better code review than threat modeling;
- And so on;

Improve your team:

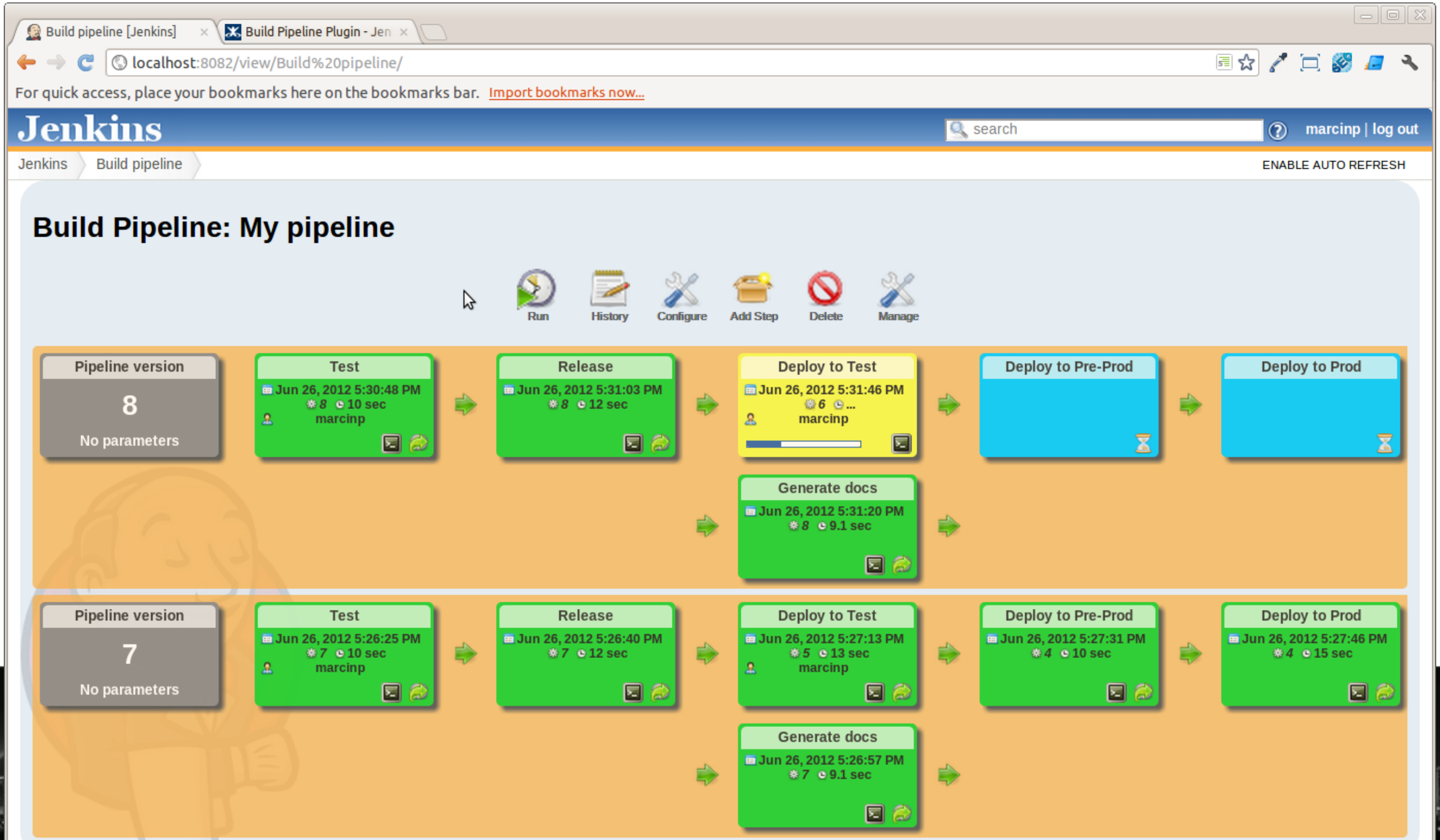
- Map their weakness and strengths;
- Give room to grow and learn (training, events, researches).

5. Automation

- SAST plugin for developer’s IDE;
- IAST Scanning;
- SAST and DAST inside the Jenkins Build Pipeline;
- Jira API and Plugins;
- Chef/Puppet hardened recipes;
- Log correlation rules;
- Open Source components and licenses management;
- Repository Audit, Checksum.

SECUREBRASIL

Jenkins Build Pipeline


Build pipeline [Jenkins]
Build Pipeline Plugin - Jen
localhost:8082/view/Build%20pipeline/
For quick access, place your bookmarks here on the bookmarks bar. Import bookmarks now...
Jenkins
search
marcinp | log out
Jenkins
Build pipeline
ENABLE AUTO REFRESH
Run
History
Configure
Add Step
Delete
Manage

Build Pipeline: My pipeline

Pipeline version
8
No parameters

Test
Jun 26, 2012 5:30:48 PM
8 10 sec
marcinp

Release
Jun 26, 2012 5:31:03 PM
8 12 sec

Deploy to Test
Jun 26, 2012 5:31:46 PM
6 ...
marcinp

Deploy to Pre-Prod

Deploy to Prod

Generate docs
Jun 26, 2012 5:31:20 PM
8 9.1 sec

Pipeline version
7
No parameters

Test
Jun 26, 2012 5:26:25 PM
7 10 sec
marcinp

Release
Jun 26, 2012 5:26:40 PM
7 12 sec

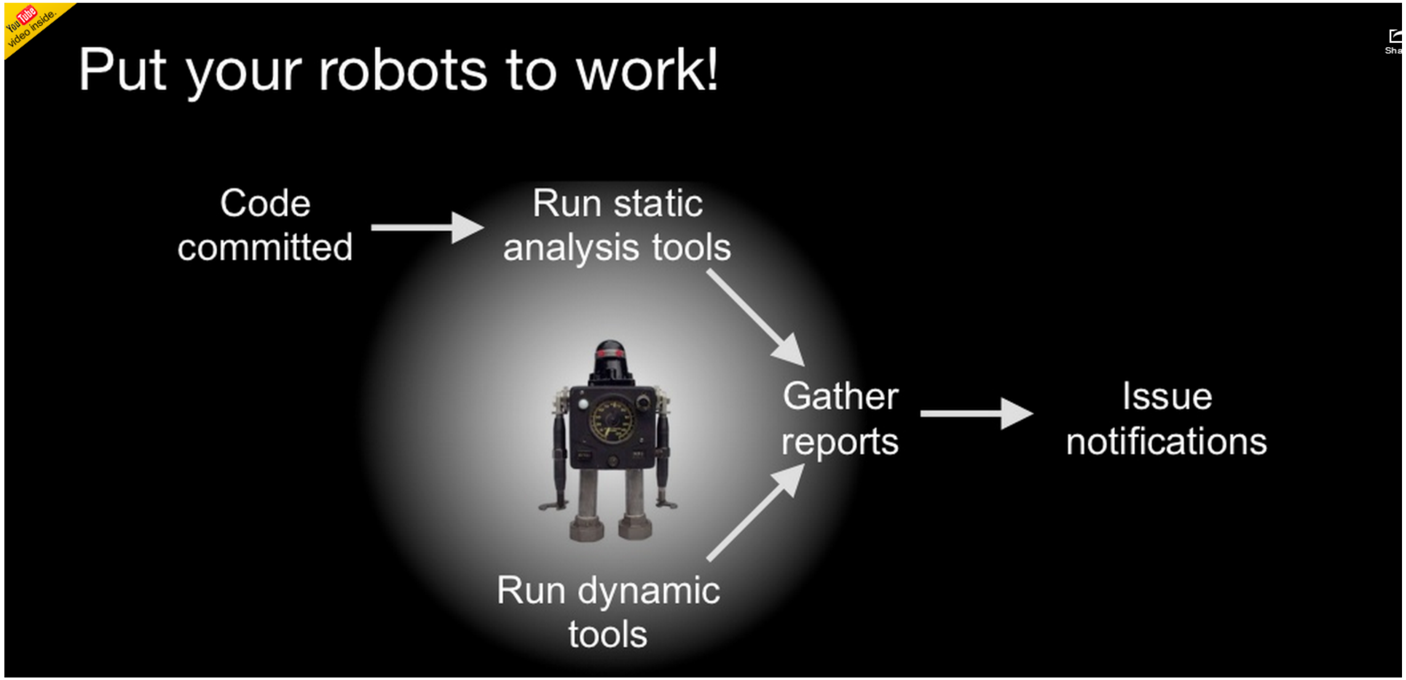
Deploy to Test
Jun 26, 2012 5:27:13 PM
5 13 sec
marcinp

Deploy to Pre-Prod
Jun 26, 2012 5:27:31 PM
4 10 sec

Deploy to Prod
Jun 26, 2012 5:27:46 PM
4 15 sec

Generate docs
Jun 26, 2012 5:26:57 PM
7 9.1 sec

Security Automation at Twitter (1-2)

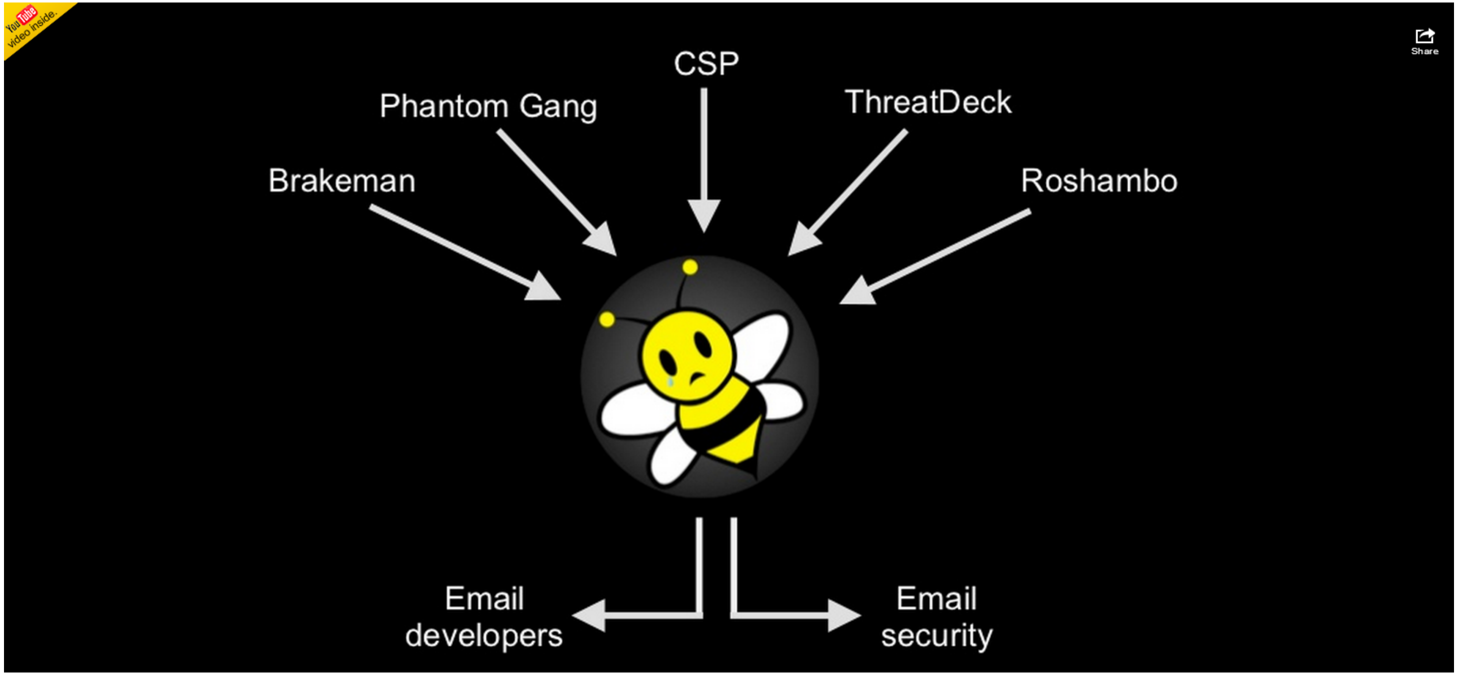


Put your robots to work!

Code committed → Run static analysis tools → Gather reports → Issue notifications

Run dynamic tools → Gather reports

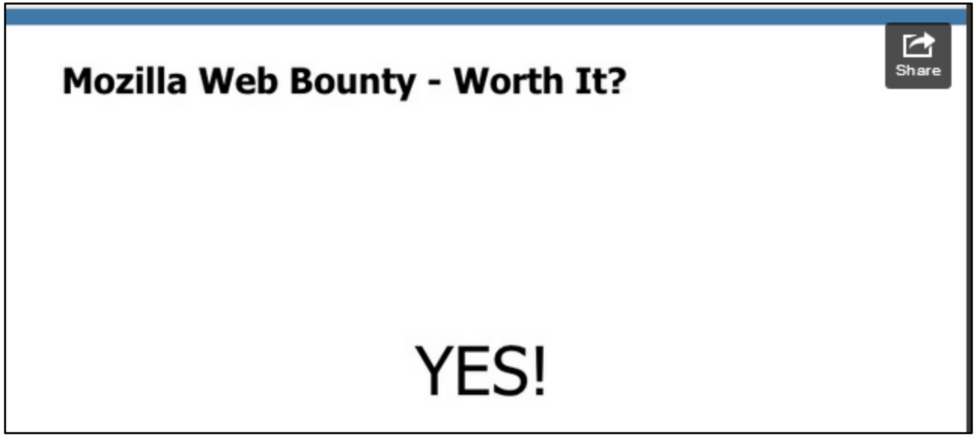
Security Automation at Twitter (2-2)



6. Bug Bounty

- Can either be Internal or External;
- Define a strict policy for bug bounty;
- Spare a day or period for bug hunting;
- Offer rewards:
    - Free holiday, T-Shirts, Mugs, Money, etc.

Worth it? Mozilla says YES



Mozilla Web Bounty - Worth It?

YES!

7. Security Champions/Advisors

- Requires special awareness training;
- Improve security awareness of the team;
- Explain security bugs details;
- Take action on low level bugs;
- Reports to the Security Team.

Takeaways

- Every strategy has a trade-off (e.g. automation vs manual code review);
- Certain strategies require more maturity than others (e.g. delegation, automation, etc);
- *There is no silver bullet*: assess your organization today and find out what fits better.

References & Further Reading

- 2012: Putting your robots to work: security automation at Twitter:
  - Slides: http://pt.slideshare.net/xplodersuv/putting-your-robots-to-work-14901538
  - Video: http://videos.2012.appsecusa.org/video/54250716
- Microsoft SDL: http://microsoft.com/sdl
- Veracode Webinars:
  - https://info.veracode.com/webinar-secure-agile-through-an-automated-toolchain-how-veracode-rd-does-it.html
  - https://info.veracode.com/webinar-building-security-into-the-agile-sdlc.html
- Continuous Delivery (Rodrigo Russo): http://pt.slideshare.net/zrusso
- Anderson Dadario's blog: http://dadario.com.br
- Mozilla Bug Bounty:
  - http://pt.slideshare.net/michael_coates/bug-bounty-programs-for-the-web

TOP SECRET

Thank You!

anderson@dadario.com.br
dadario.com.br
flaresecurity.com
@andersonmvd