



THE DEVELOPER'S CONFERENCE

Implementing Security into Agile SDLC

Anderson Dadario, CISSP, CSSLP

Flare Security



FLARE SECURITY
Securing People, Process and Technology



whoami



THE
DEVELOPER'S
CONFERENCE

- Anderson Dadario
- Consultant at Flare Security
- 5+ years working with development & infosec



FLARE SECURITY
Securing People, Process and Technology



What you will learn



THE
DEVELOPER'S
CONFERENCE

- Motivations for Secure SDLC
- A little about Waterfall SDLC Security
- Agile SDLC Security
 - Security Resources Allocation
 - Risk Management
 - How to scale security resources
- Software Assurance Maturity Model



FLARE SECURITY
Securing People, Process and Technology



What's your security program?



THE
DEVELOPER'S
CONFERENCE

- Nothing but a scan after release?
 - Automated?
 - Looking for a badge or seal?
 - Manual?
 - *Ad hoc?*



FLARE SECURITY
Securing People, Process and Technology

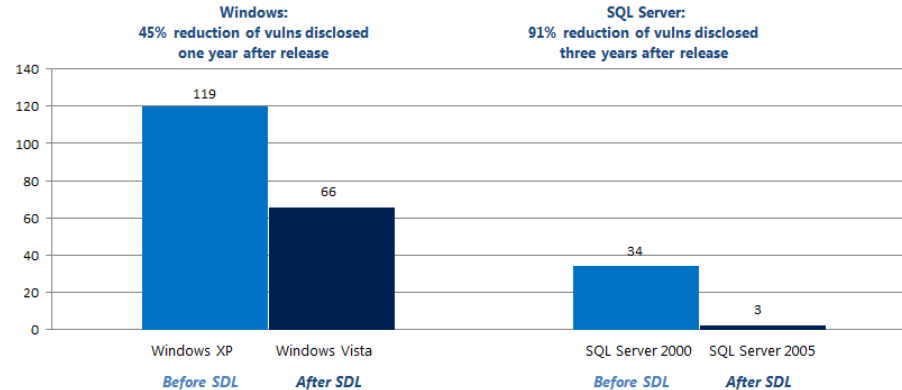


Motivations for Secure SDLC (1-2)



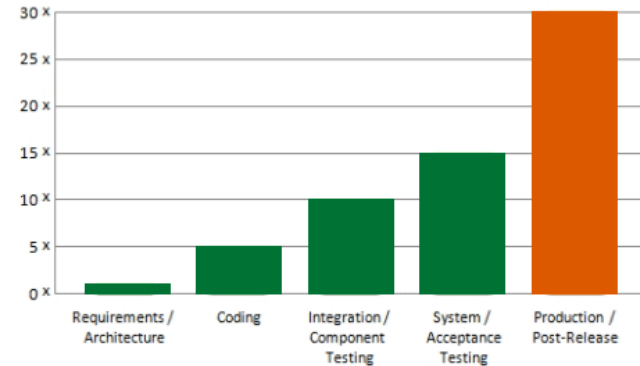
THE
DEVELOPER'S
CONFERENCE

Microsoft products: Vulnerabilities reduction after SDL implementation



Sources: Microsoft Security Blog and Microsoft TechNet Security Blog

Relative cost to fix, based on time of detection



Source: National Institute of Standards and Technology

<http://www.microsoft.com/security/sdl/about/benefits.aspx>



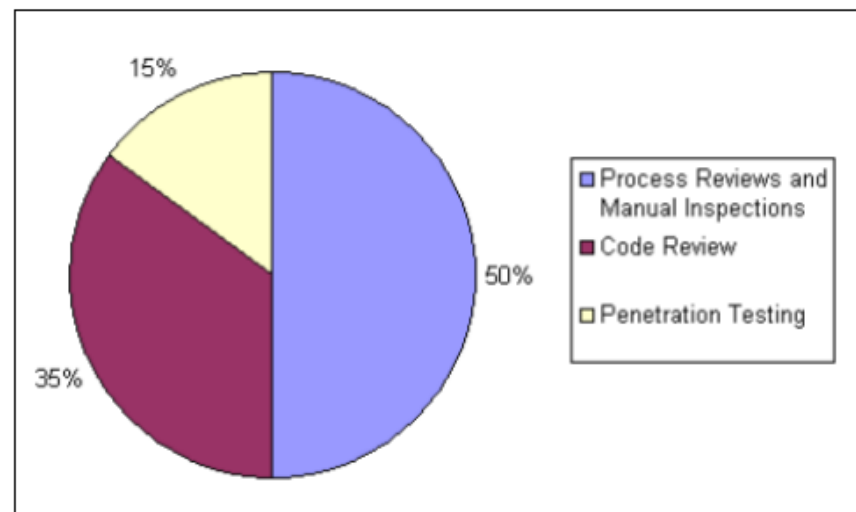
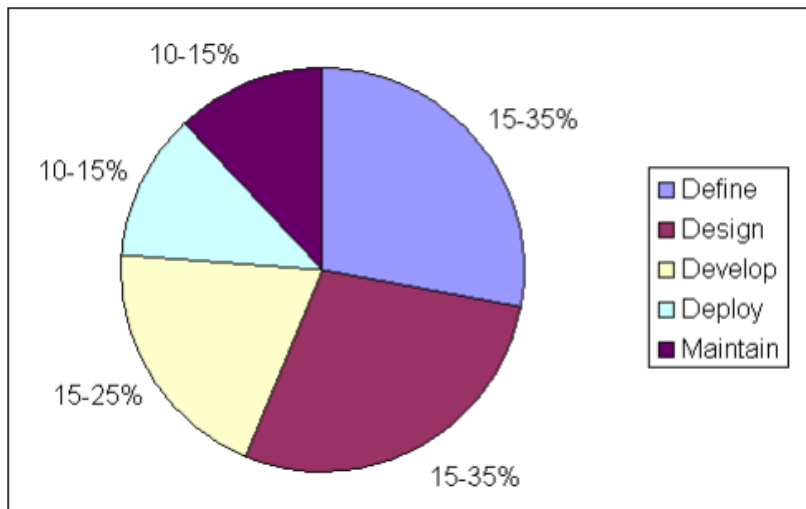
FLARE SECURITY
Securing People, Process and Technology



Motivations for Secure SDLC (2-2)



THE
DEVELOPER'S
CONFERENCE



https://www.owasp.org/images/5/56/OWASP_Testing_Guide_v3.pdf



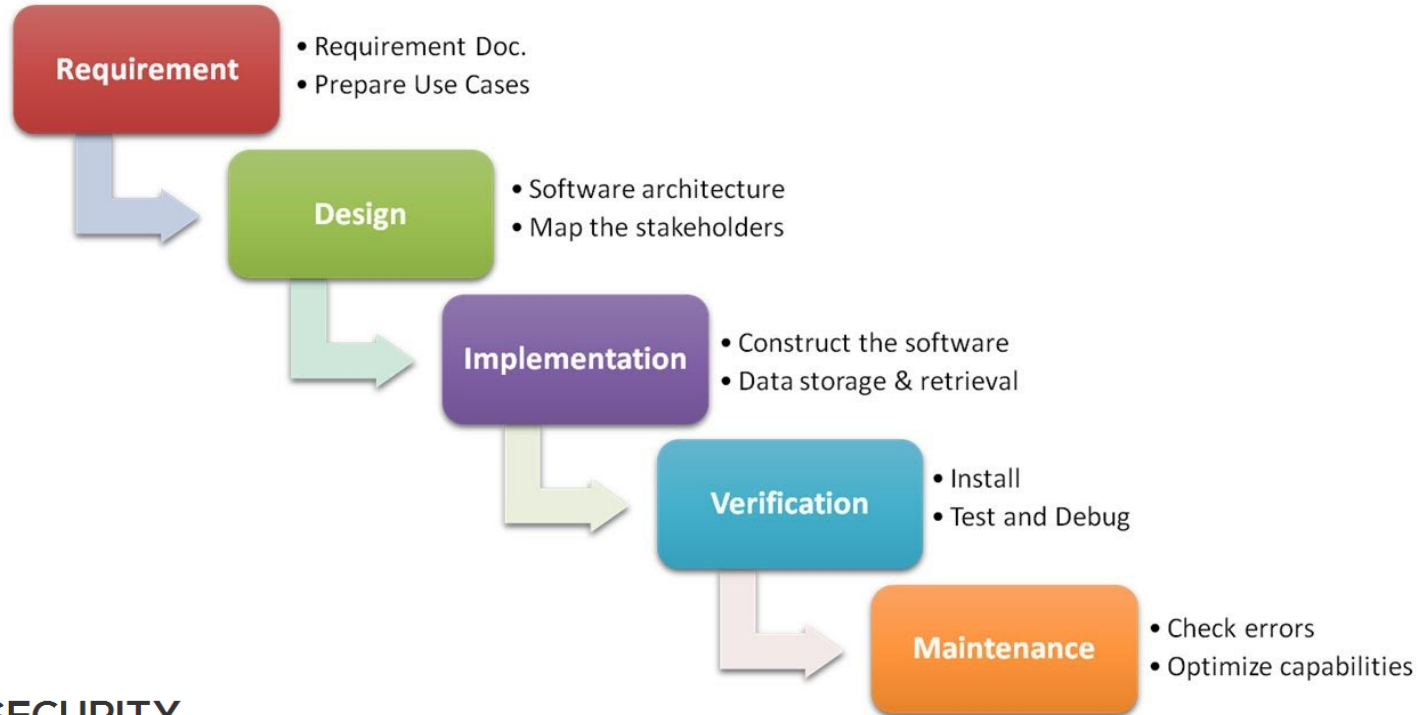
FLARE SECURITY
Securing People, Process and Technology



Waterfall Methodology



THE
DEVELOPER'S
CONFERENCE



FLARE SECURITY
Securing People, Process and Technology





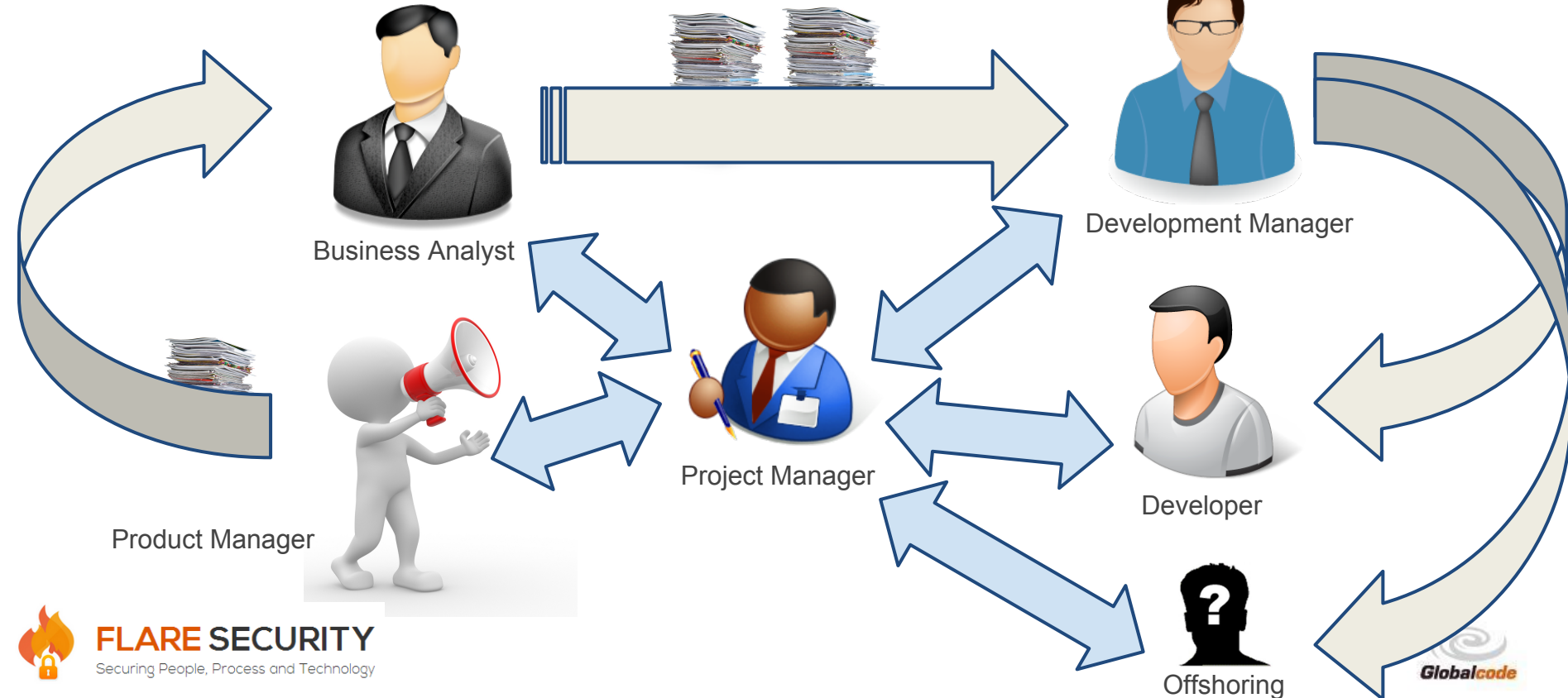
- Well-defined sequential phases;
- Significant part of the project must be planned upfront;
- Stresses the importance of requirements;
- Changes are controlled. Major changes are only allowed if the CCB (Change Control Board) approves them.



Waterfall in the Real World



THE
DEVELOPER'S
CONFERENCE



FLARE SECURITY

Securing People, Process and Technology

Globalcode

It's time to ...



THE
DEVELOPER'S
CONFERENCE

INJECT SECURITY



FLARE SECURITY

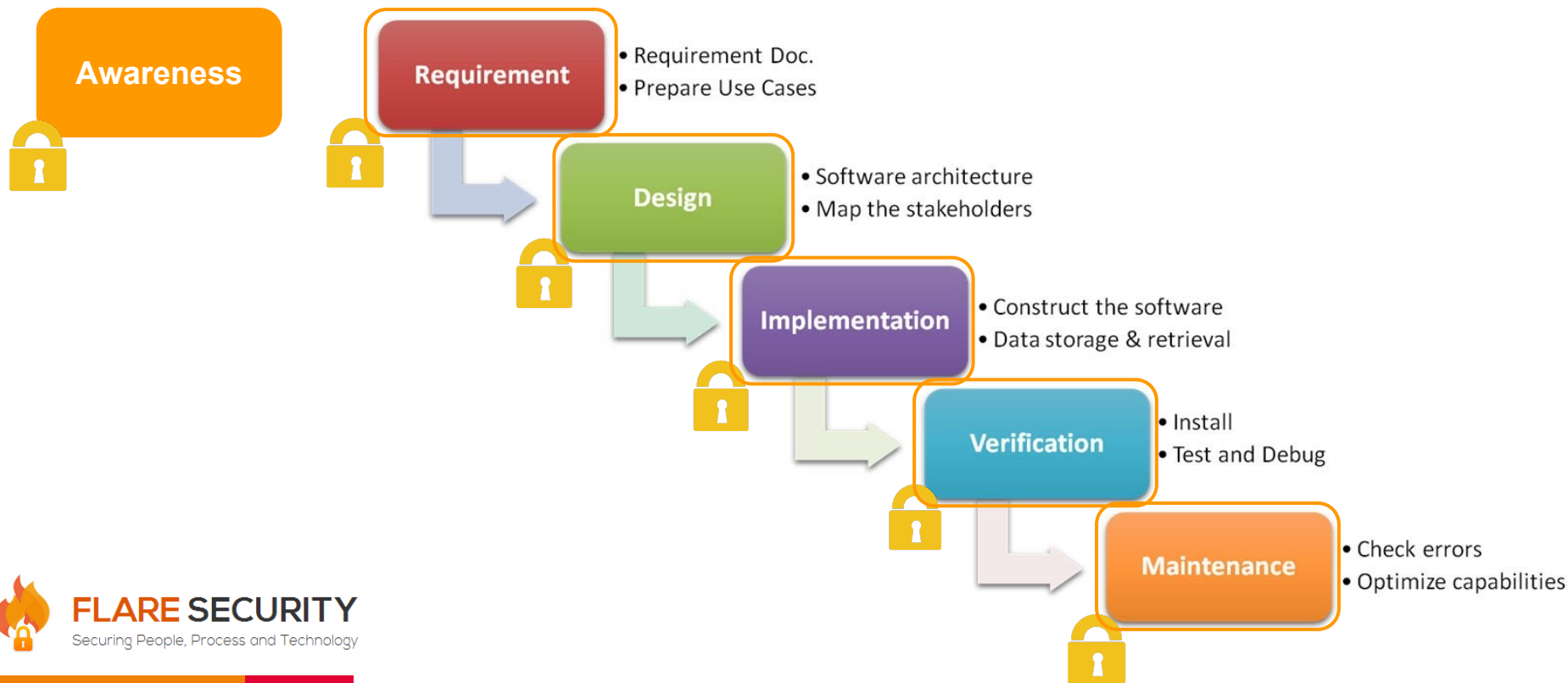
Securing People, Process and Technology



Waterfall Security



THE
DEVELOPER'S
CONFERENCE



FLARE SECURITY

Securing People, Process and Technology

Waterfall in the Real World



THE DEVELOPER'S CONFERENCE



FLARE SECURITY

Securing People, Process and Technology

Globalcode



- Bundled within each phase;
- Few or no meetings at all with the Security team;
- Bureaucratic as Waterfall demands to be.

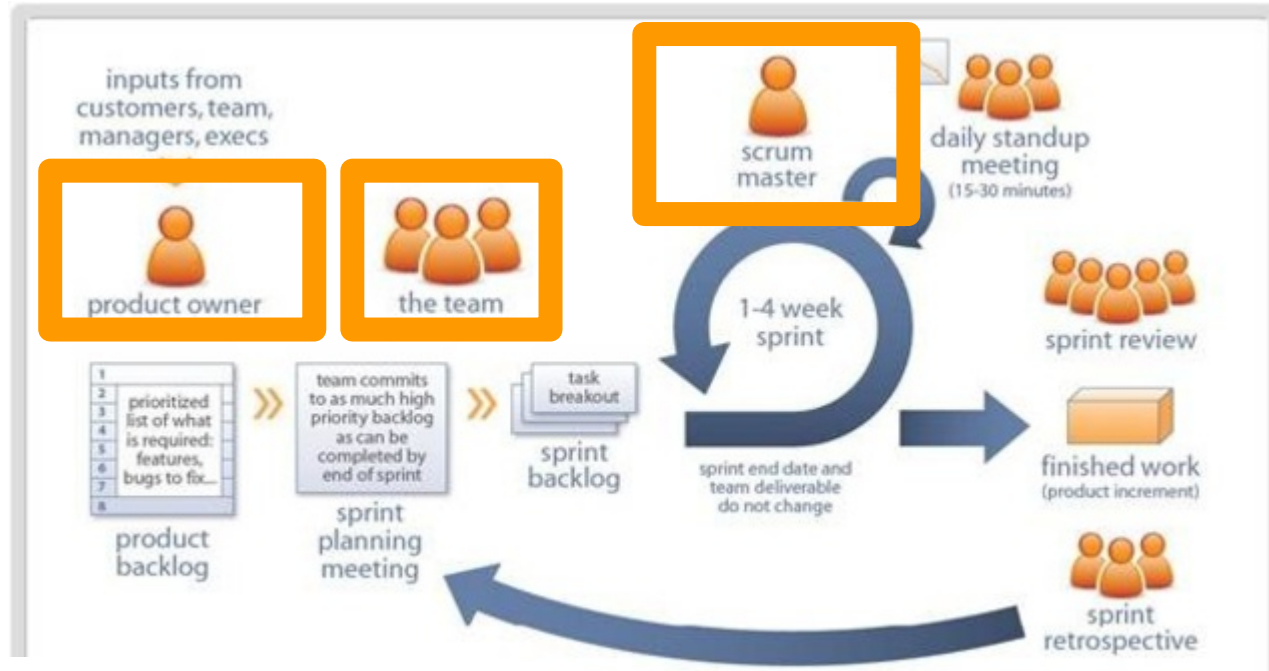


Let's Talk Agile

Scrum Roles



THE
DEVELOPER'S
CONFERENCE



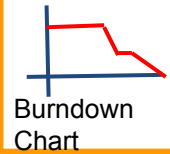
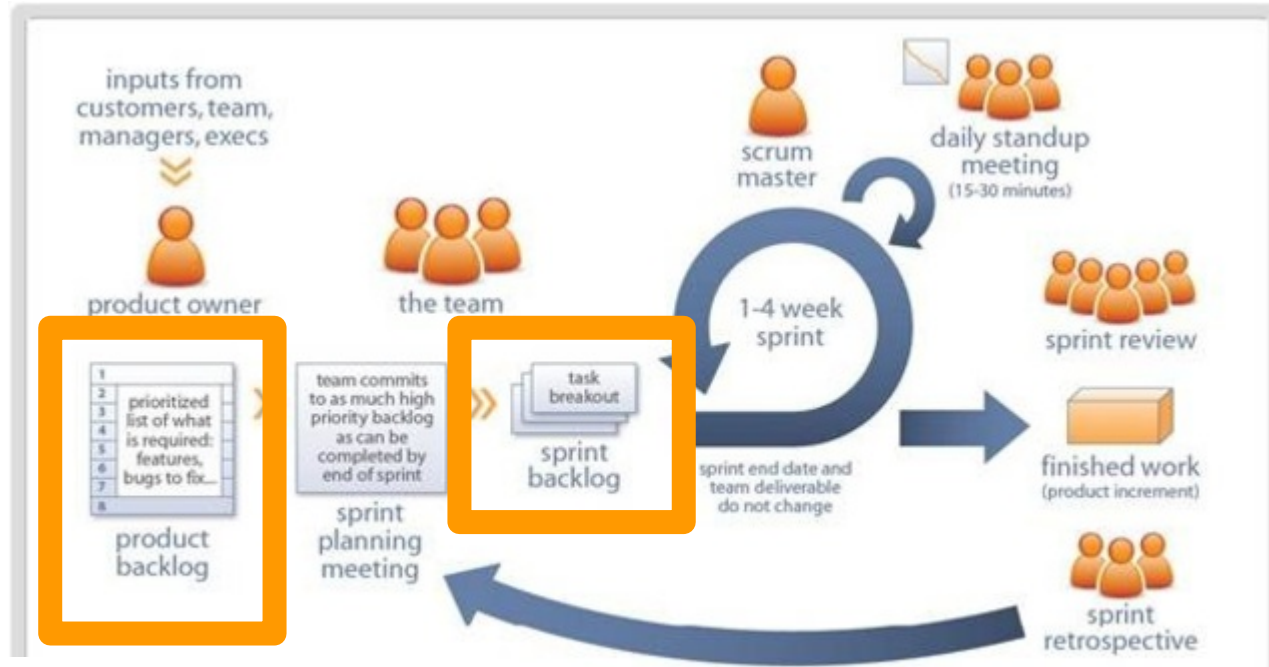
FLARE SECURITY
Securing People, Process and Technology



Scrum Artifacts



THE
DEVELOPER'S
CONFERENCE



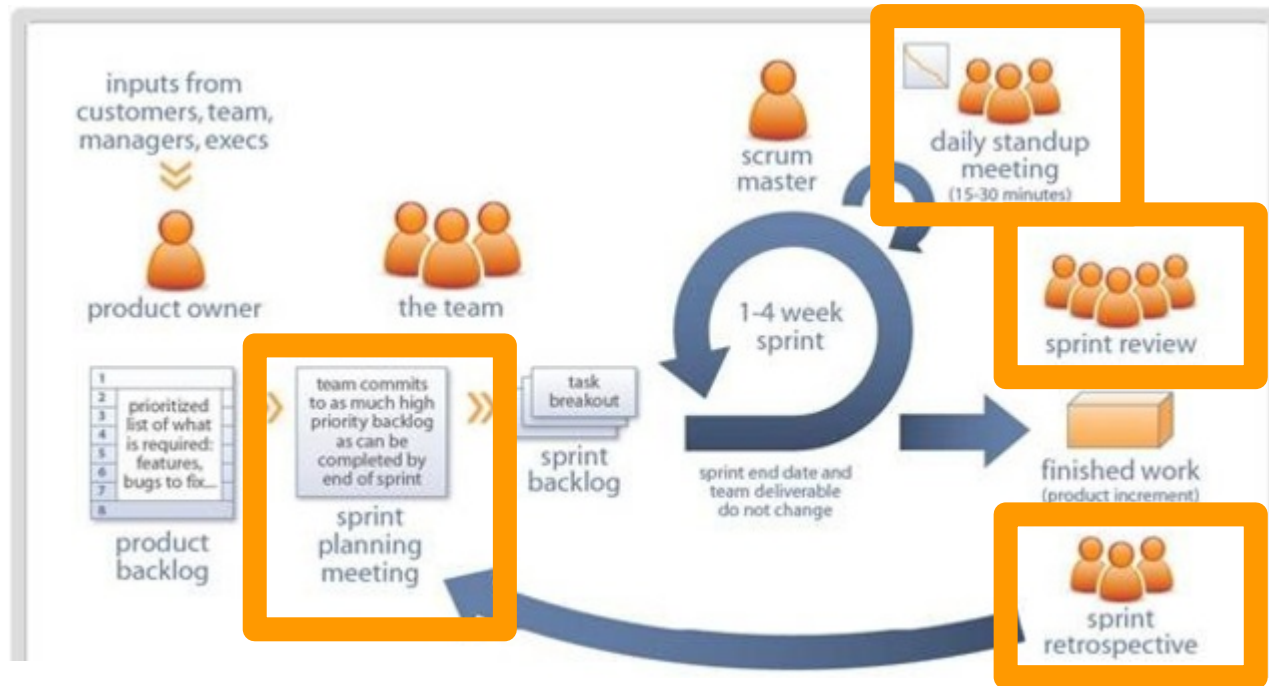
FLARE SECURITY
Securing People, Process and Technology



Scrum Ceremonies



THE
DEVELOPER'S
CONFERENCE



FLARE SECURITY
Securing People, Process and Technology



It's time to



THE
DEVELOPER'S
CONFERENCE

INJECT SECURITY



FLARE SECURITY
Securing People, Process and Technology



But first keep these points in mind



THE
DEVELOPER'S
CONFERENCE

- Understand the methodologies currently in use at your company;
- Maximize the efficiency of security injection;
- Avoid Single Point of Failure (absence of a security expert);
- There will be multiple products for limited security experts;
- Your company may hire more developers than security experts;
- The software must be rugged (**Rugged Software Manifesto**).



FLARE SECURITY

Securing People, Process and Technology



The Rugged Manifesto



THE
DEVELOPER'S
CONFERENCE

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.



FLARE SECURITY

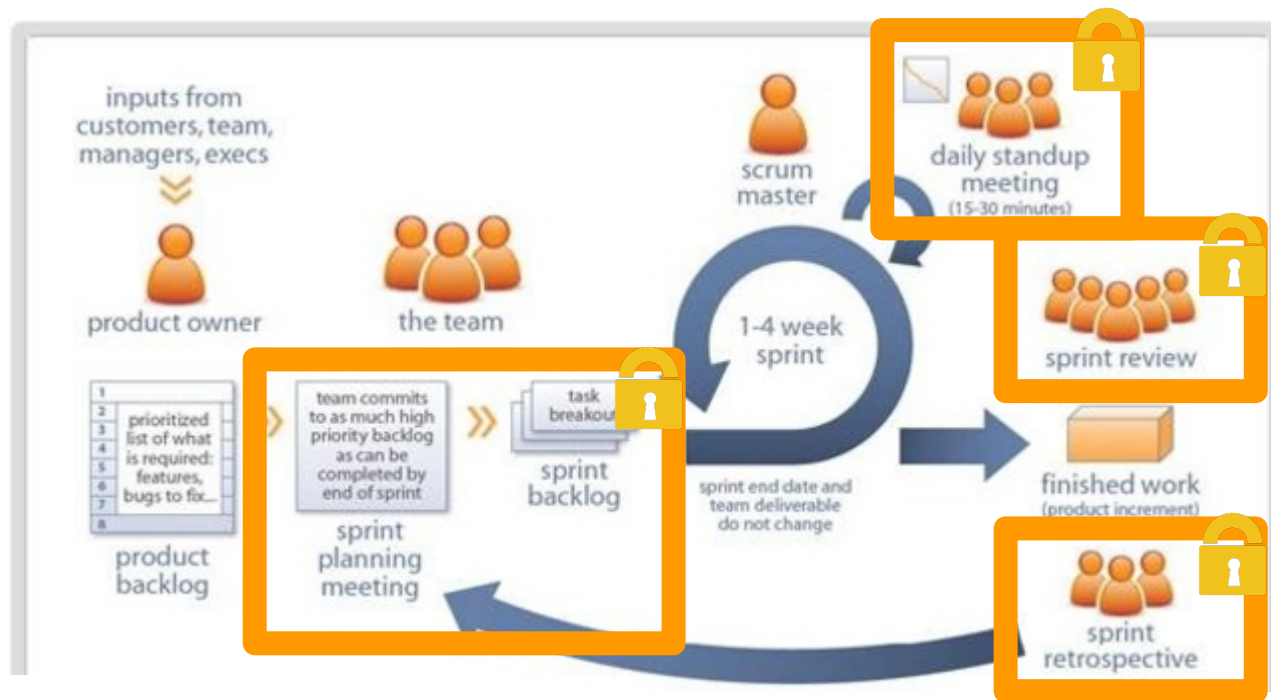
Securing People, Process and Technology



Strategy #1 Participate in everything



THE
DEVELOPER'S
CONFERENCE



FLARE SECURITY
Securing People, Process and Technology





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'



THE
DEVELOPER'S
CONFERENCE



FLARE SECURITY

Securing People, Process and Technology





Pros:

- Security Expert's time is used wisely.

Cons:

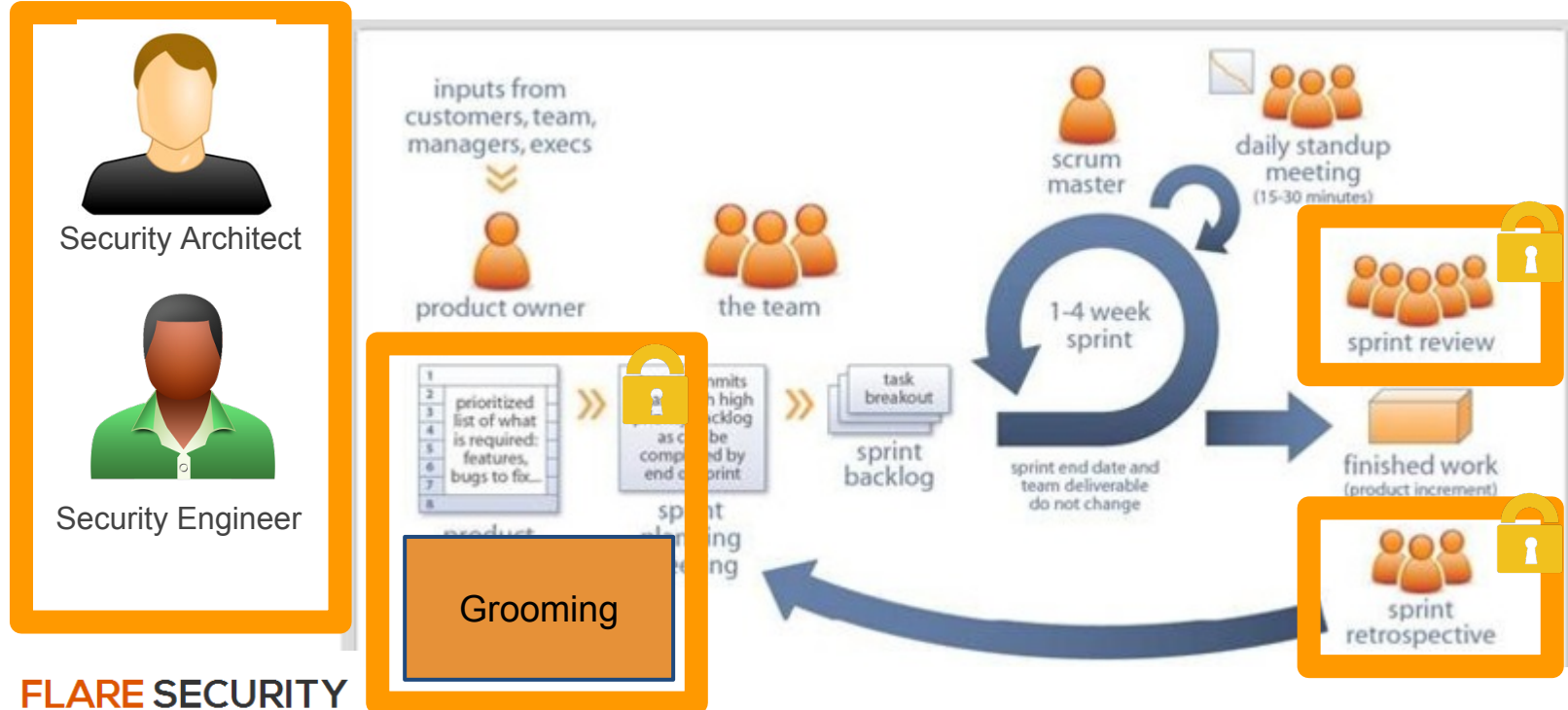
- You are messing up with Scrum methodology because stories cannot change after planning;
- Single Point of Failure persists;
- Less security awareness.



Strategy #3 Grooming, Security Roles



THE
DEVELOPER'S
CONFERENCE



FLARE SECURITY
Securing People, Process and Technology





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.



This ain't over. What about ...



THE
DEVELOPER'S
CONFERENCE

- Stories that are created after the planning?
- Security stories negotiation?
- Risk Management?
- Maximize even more the security injection?



FLARE SECURITY
Securing People, Process and Technology



Stories that are created after the planning



THE
DEVELOPER'S
CONFERENCE

- It should not be common, but it can happen;
- Define a process to handle it;
- The Information Security team must be **aware** and perform its **assessment**.



FLARE SECURITY
Securing People, Process and Technology



Security stories negotiation



THE
DEVELOPER'S
CONFERENCE

- It will always be a challenge, no matter what;
- Focus on the **risk**;
- Define the Quality Gates before publish and agree these gates with the Product Owner.

Risk Management (1-3)



THE
DEVELOPER'S
CONFERENCE

- Perform Threat Modeling on Grooming;
- Inject Security on:
 - Acceptance Criteria for specific requirements;
 - Definition of Done for generic requirements.
- Automate Security Acceptance Criteria tests;



FLARE SECURITY
Securing People, Process and Technology



Risk Management (2-3)



THE
DEVELOPER'S
CONFERENCE

- Take advantage of the agile tools:
 - Put labels on Jira stories;
- Extract the labeled stories using JQL (Jira Query Language) API;
- Integrate the extracted risks to your company risks platform / dashboard;



FLARE SECURITY

Securing People, Process and Technology



Risk Management (3-3)



THE
DEVELOPER'S
CONFERENCE

Threat Model Case #ID	05
Asset	User Credentials
Threat	Threat action aimed to illegally access and use another user's credentials, such as username and password.
Risk	High
Threat Agent	External Attacker
Threat Type (STRIDE)	Spoofing
Security Control	Authentication
Mitigation Controls	<ul style="list-style-type: none">• Appropriate authentication• Protect secret data• Don't store secrets
Incident Response Procedures	Block user account, revoke password, etc



FLARE SECURITY
Securing People, Process and Technology



Maximize even more the Security Injection



THE
DEVELOPER'S
CONFERENCE

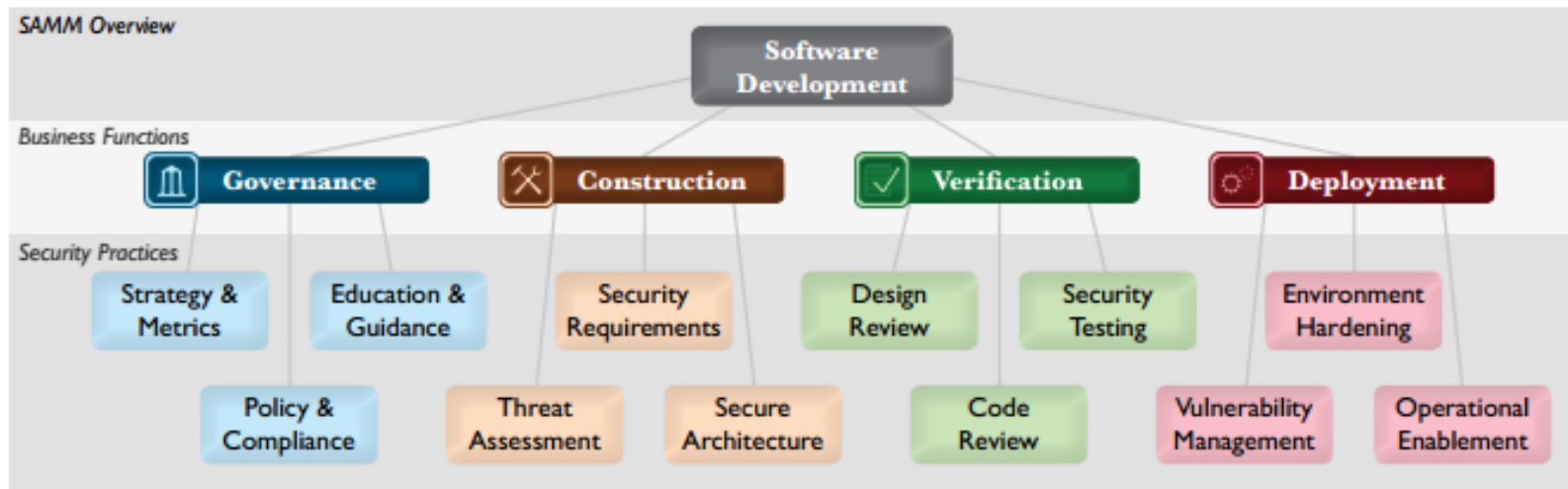
- Extreme Programming (XP) practices
 - Continuous Processes
 - Continuous Integration
 - Design Improvement
 - Shared Understanding
 - Coding Standard
 - Collective Code Ownership
 - Simple Design
- DevOps Security, Security Champions
- Mailing Lists, Tech Talks, **Software Assurance Maturity Model**




FLARE SECURITY

Securing People, Process and Technology







 OPENSAMM		Assessment Worksheet		
Business Functions	Security Practices	Activities	Answer	Ratings
Governance	Strategy & Metrics	Is there a software security assurance program already in place?	Yes ▾	1+
		Do most of the business stakeholders understand your organization's risk profile?	Yes ▾	
		Is most of your development staff aware of future plans for the assurance program?	Yes ▾	
		Are most of your applications and resources categorized by risk?	No ▾	
		Are risk ratings used to tailor the required assurance activities?	No ▾	
		Does most of the organization know about what's required based on risk ratings?	No ▾	
		Is per-project data for cost of assurance activities collected?	Yes ▾	
		Does your organization regularly compare your security spend with other organizations?	Yes ▾	
	Policy & Compliance	Do most project stakeholders know their project's compliance status?	▾	0
		Are compliance requirements specifically considered by project teams?	▾	
		Does the organization utilize a set of policies and standards to control software development?	▾	
		Are project teams able to request an audit for compliance with policies and standards?	▾	
		Are projects periodically audited to ensure a baseline of compliance with policies and standards?	▾	
		Does the organization systematically use audits to collect and control compliance evidence?	▾	





- The more you respect the developers process, the more they will respect yours;
- Scrum is about constant learning so always be thinking how you can tweak your process to make it better;
- Apply the concepts to the way of your company builds software since **there is no silver bullet.**



References & Resources



THE
DEVELOPER'S
CONFERENCE

- Scrum.org: <https://www.scrum.org/>
- Extreme Programming: <http://www.extremeprogramming.org/>
- 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>
- RSA Conference Europe: http://www.rsaconference.com/writable/presentations/file_upload/asec-107.pdf
- Gotham: <http://pt.slideshare.net/SOURCEConference/are-agile-and-secure-development-mutually-exclusive-source-2011>
- Microsoft SDL: <http://microsoft.com/sdl>
- OWASP: <https://www.owasp.org>
- OpenSAMM: <http://www.opensamm.org/>
- Flare Security: <http://flaresecurity.com>
- Anderson Dадario's blog: <http://dadario.com.br>
- Rugged Software: <https://www.ruggedsoftware.org/>



FLARE SECURITY

Securing People, Process and Technology





THE DEVELOPER'S CONFERENCE

Thank You

Anderson Dadario, CISSP, CSSLP

<http://dadario.com.br>

<http://flaresecurity.com>



FLARE SECURITY

Securing People, Process and Technology

