THE DEVELOPER'S CONFERENCE

Implementando Segurança no Ciclo de Desenvolvimento Ágil

Anderson Dadario, CISSP, CSSLP

Flare Security

FLARE SECURITY

Securing People, Process and Technology

Globalcode

whoami

THE DEVELOPER'S CONFERENCE

- Anderson Dadario
- Fundador e Consultor da Flare Security
- Mais de 5 anos trabalhando com desenvolvimento e segurança da informação

FLARE SECURITY

Securing People, Process and Technology

Globalcode

Por que devo me importar?

THE DEVELOPER'S CONFERENCE

- Desenvolvedor
- Arquiteto de Software
- Gerente de Projeto
- Área de Negócio
- Etc

FLARE SECURITY

Securing People, Process and Technology

Globalcode

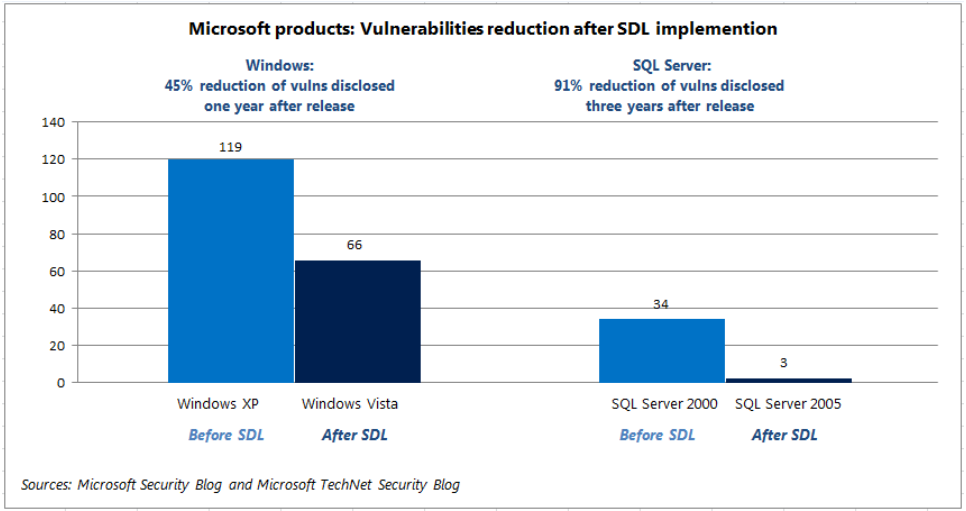
O que você vai aprender

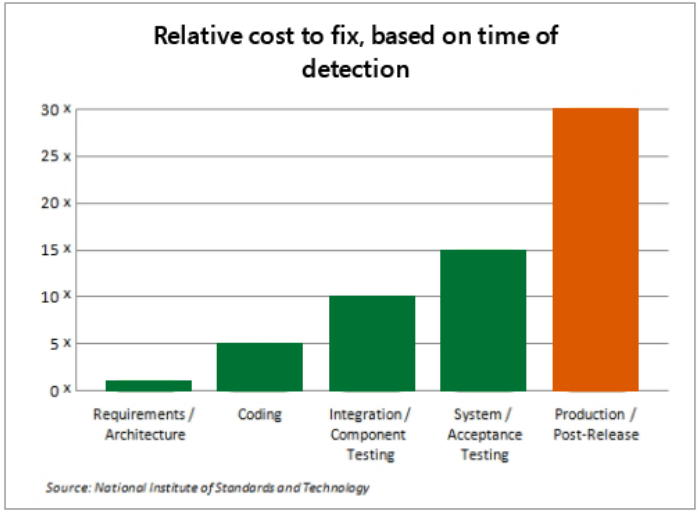
THE DEVELOPER'S CONFERENCE

- Motivações para o SDLC Seguro
- Um pouco sobre segurança do SDLC Waterfall
- Segurança do SDLC Ágil
  - Alocação de Recursos de Segurança
  - Gerenciamento de Riscos
  - Como Escalar Recursos de Segurança
- Modelo de Maturidade de Segurança de Software

- Nada além de testes após o *release*?
  - Testes automatizados?
    - Buscando apenas um selo de segurança?
  - Testes manuais?
    - *Ad hoc*?

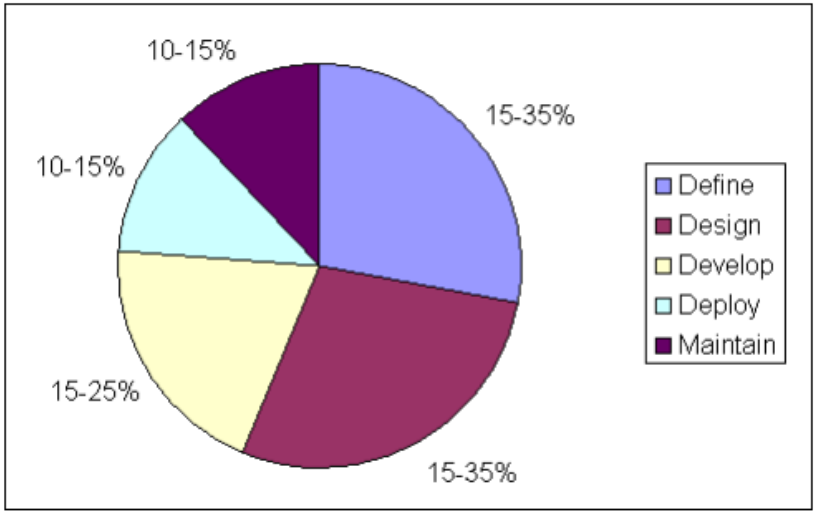
Motivações para Segurança no SDLC (1-2)

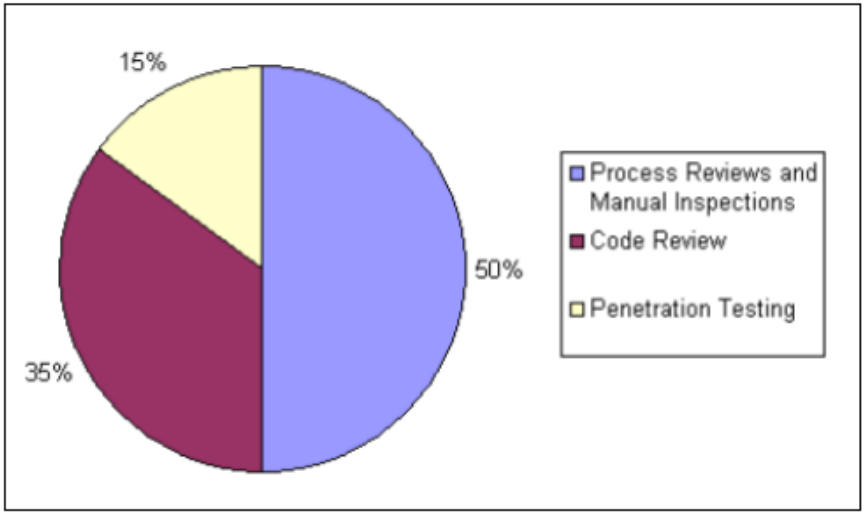




http://www.microsoft.com/security/sdl/about/benefits.aspx

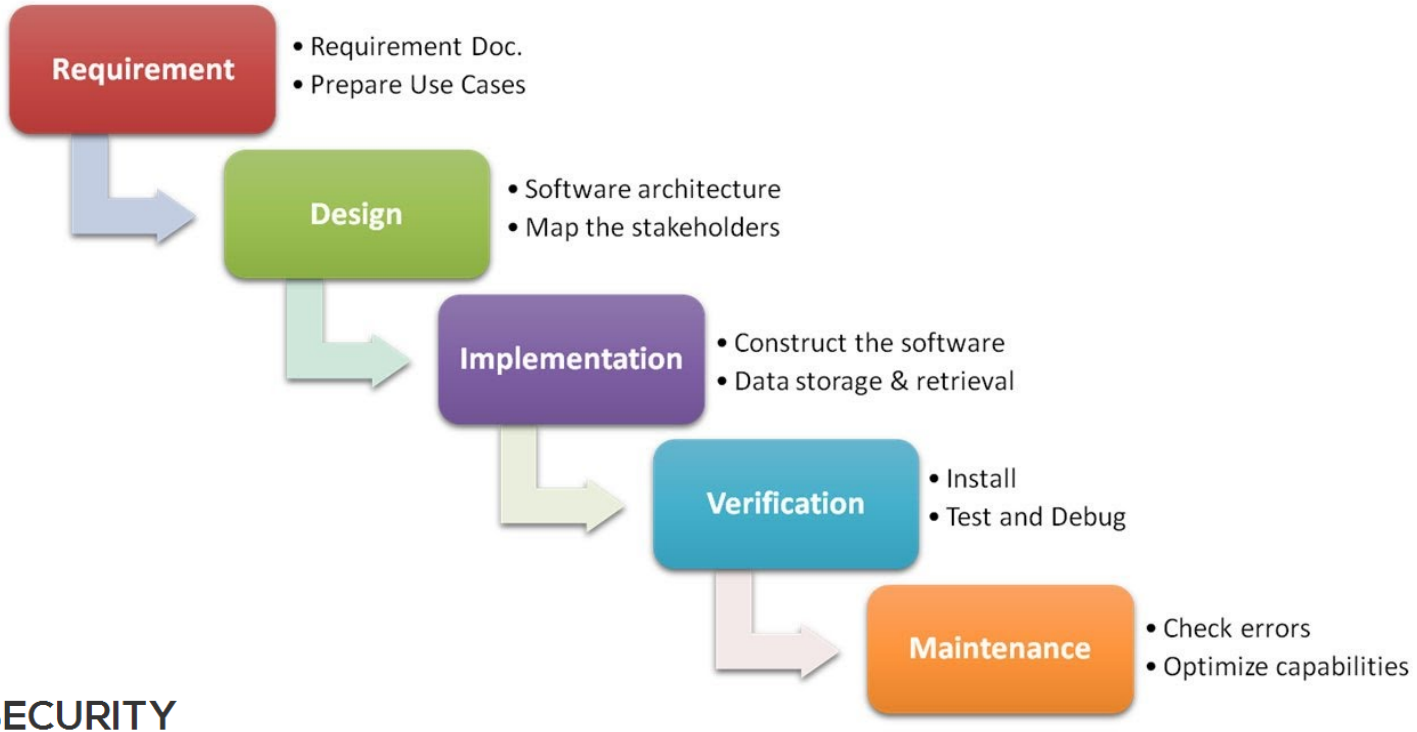
Motivações para Segurança no SDLC (2-2)





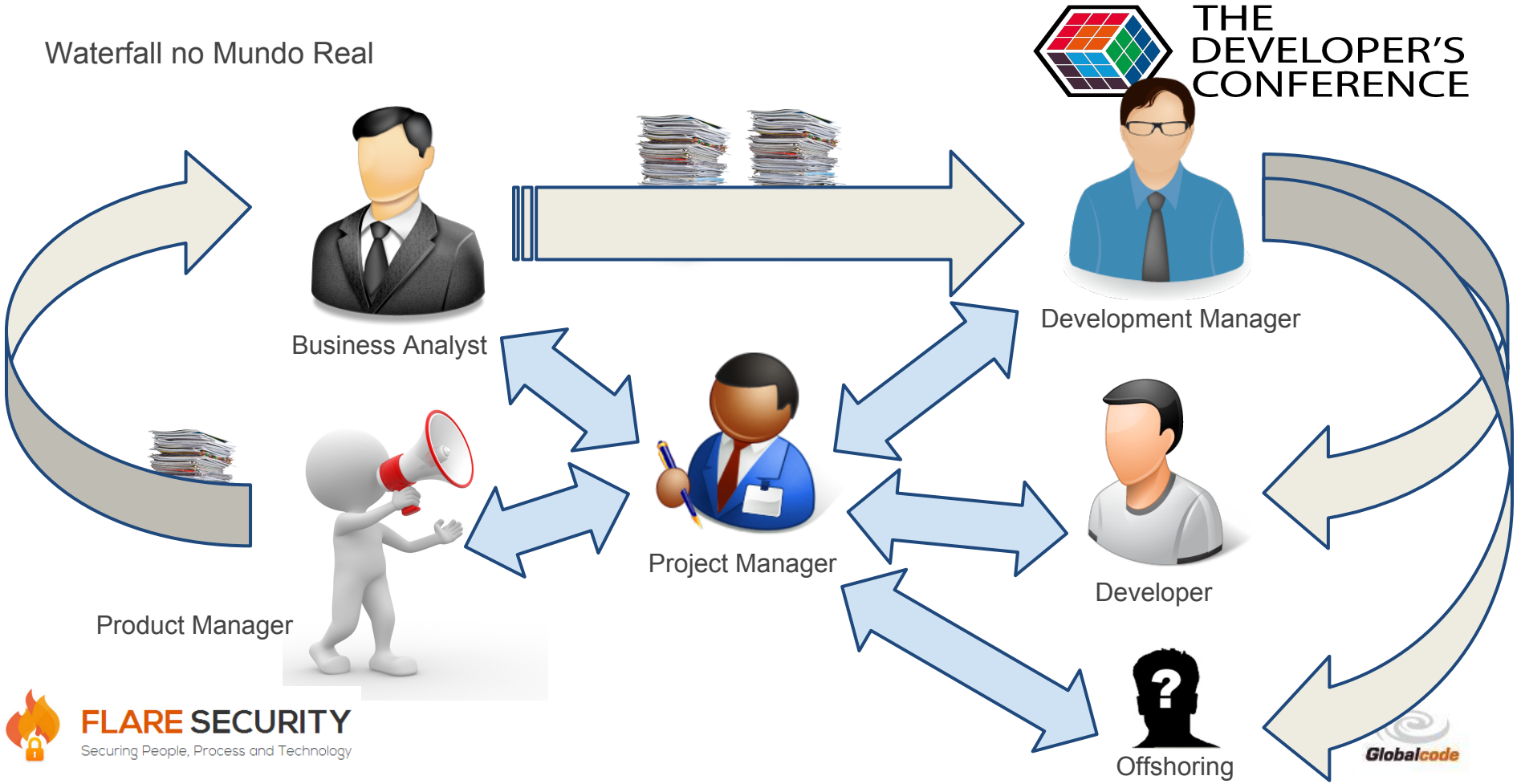
https://www.owasp.org/images/5/56/OWASP_Testing_Guide_v3.pdf

Metodologia Waterfall



- Fases sequenciais bem definidas;
- Parte significante do projeto é planejada logo no início;
- Estressa a importância dos requisitos;
- Mudanças são controladas. Mudanças significativas são permitidas apenas se o CCB (Change Control Board) aprová-las.

Waterfall no Mundo Real



É hora de

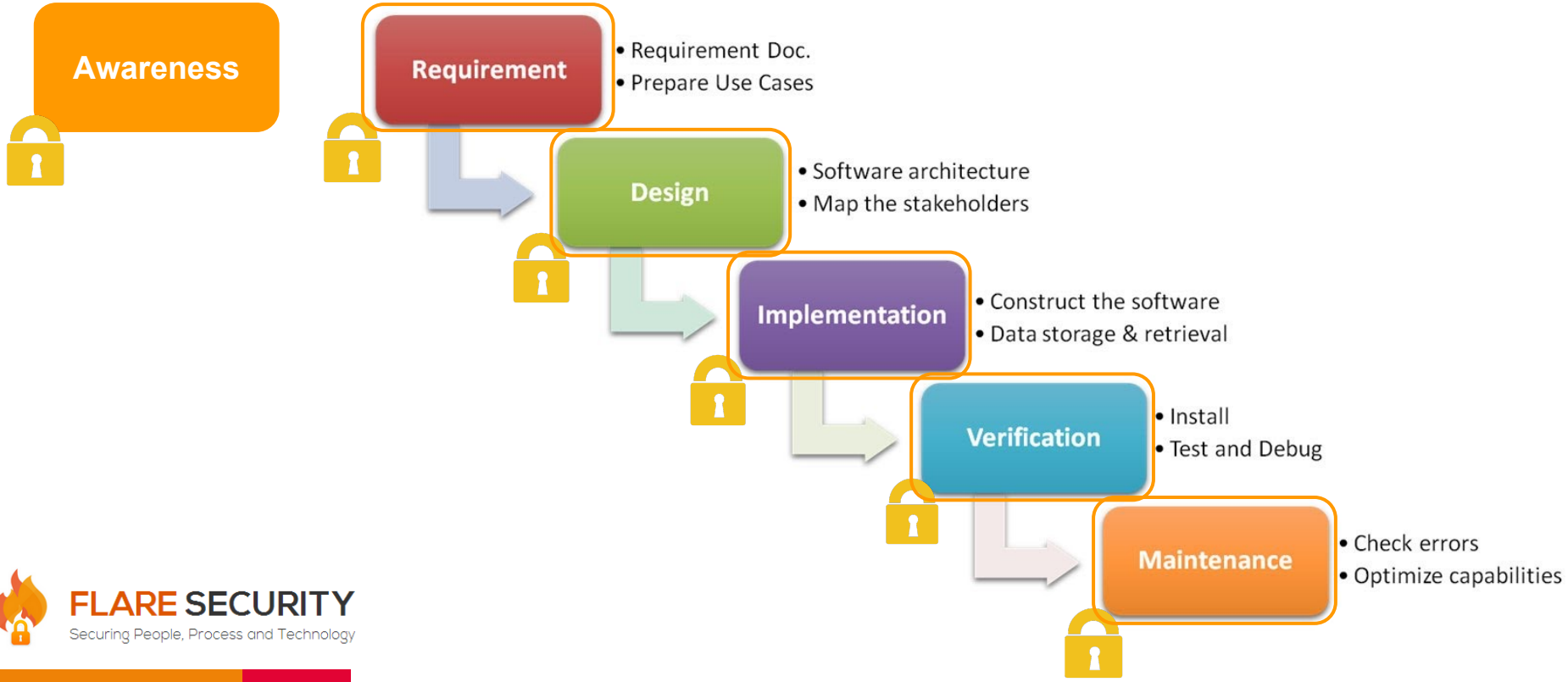
THE DEVELOPER'S CONFERENCE

INJETAR SEGURANÇA

FLARE SECURITY

Securing People, Process and Technology

Globalcode

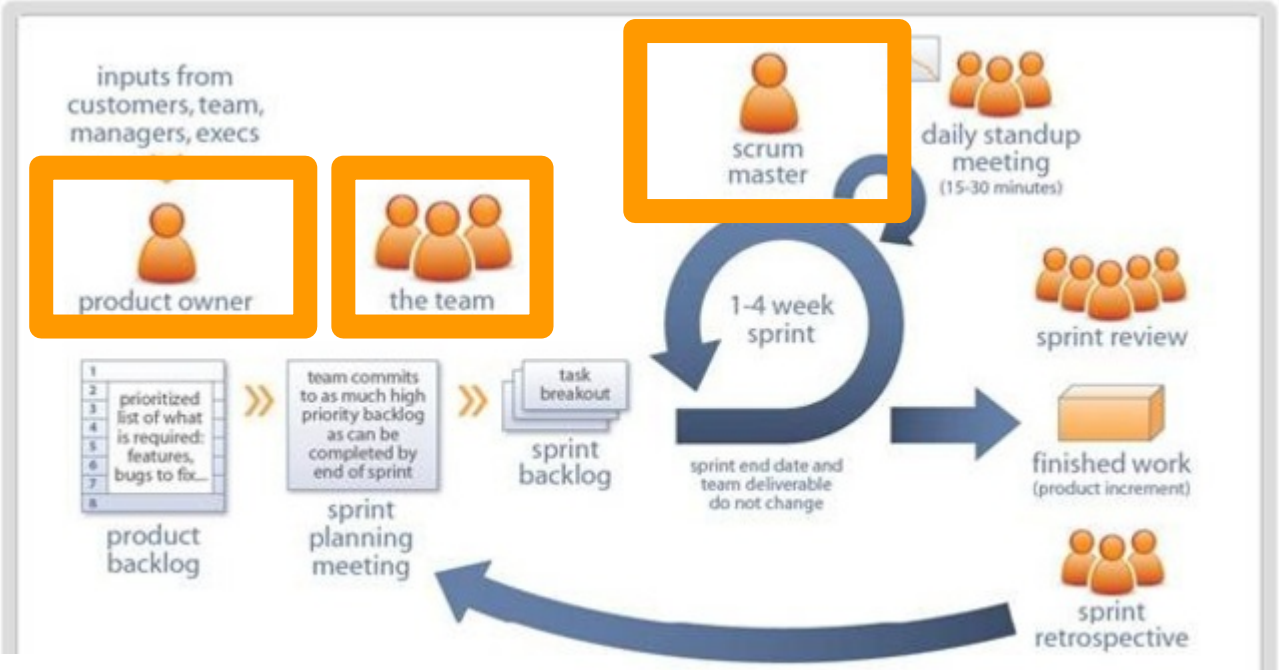

Awareness
Requirement
• Requirement Doc.
• Prepare Use Cases
Design
• Software architecture
• Map the stakeholders
Implementation
• Construct the software
• Data storage & retrieval
Verification
• Install
• Test and Debug
Maintenance
• Check errors
• Optimize capabilities

Waterfall no Mundo Real

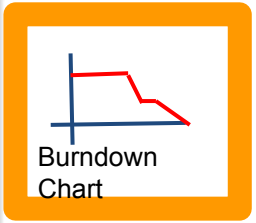
- Acoplado em cada fase;
- Poucas ou nenhuma reunião com o time de segurança;
- Burocrática como a Waterfall demanda ser.

Let’s Talk Agile

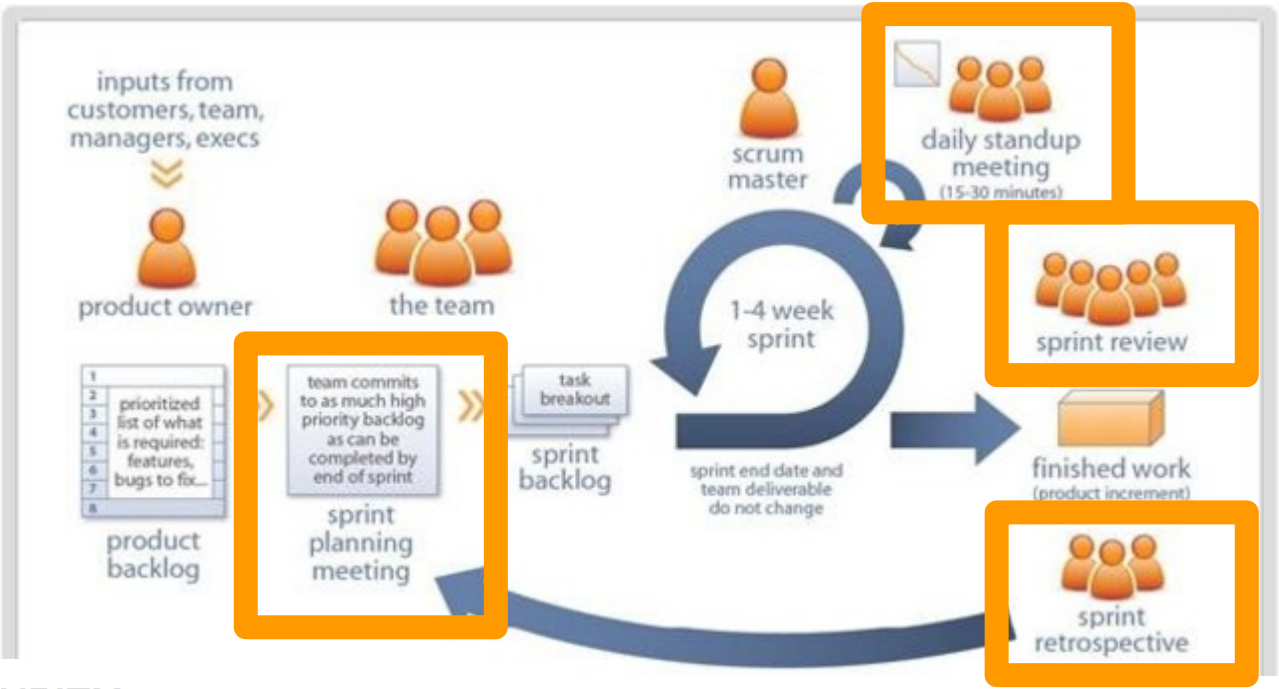
Scrum - Papéis




inputs from customers, team, managers, execs
product owner
the team
scrum master
daily standup meeting
(15-30 minutes)
1-4 week sprint
sprint review
finished work
(product increment)
sprint retrospective
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


Burndown Chart

Scrum - Cerimônias



É hora de

THE DEVELOPER'S CONFERENCE

INJETAR SEGURANÇA

FLARE SECURITY

Securing People, Process and Technology

Globalcode

Mas antes tenha estes pontos em mente ...

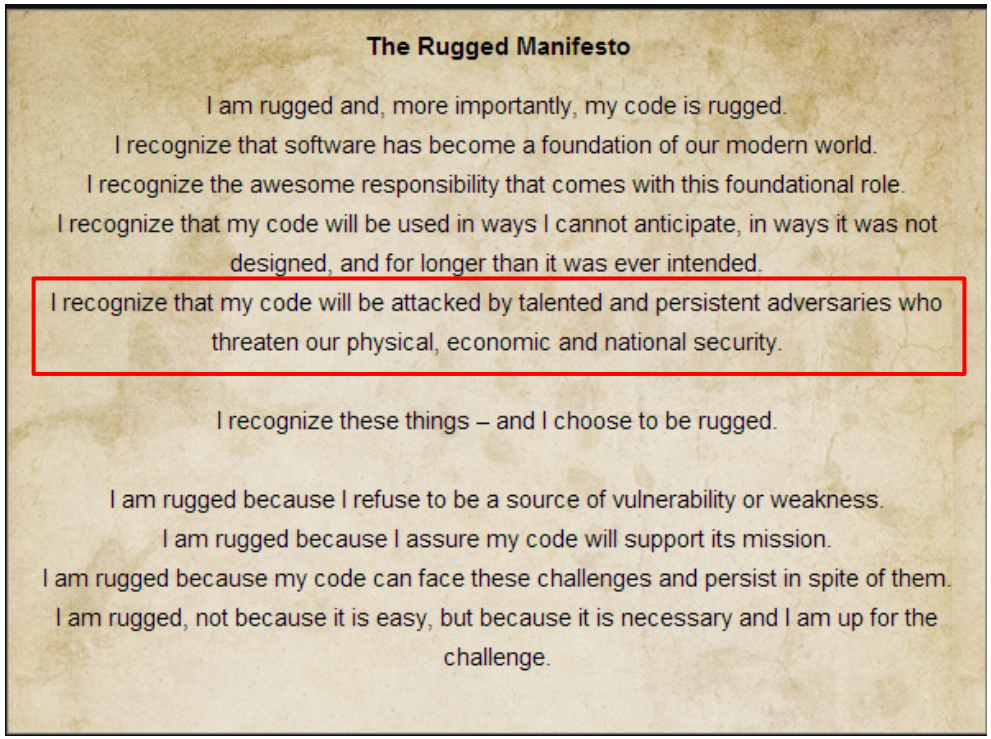
THE DEVELOPER'S CONFERENCE

- Entenda as metodologias em uso em sua empresa;
- Maximize a eficiência da injeção de segurança;
- Fuja do Ponto Único de Falha (ausência de eng. de segurança);
- Haverá múltiplos produtos para poucos engenheiros de segurança;
- Sua empresa pode contratar mais desenvolvedores que especialistas de segurança;
- O software deve ser robusto (**Rugged Software Manifesto**).

FLARE SECURITY
Securing People, Process and Technology

Globalcode

The Rugged Manifesto



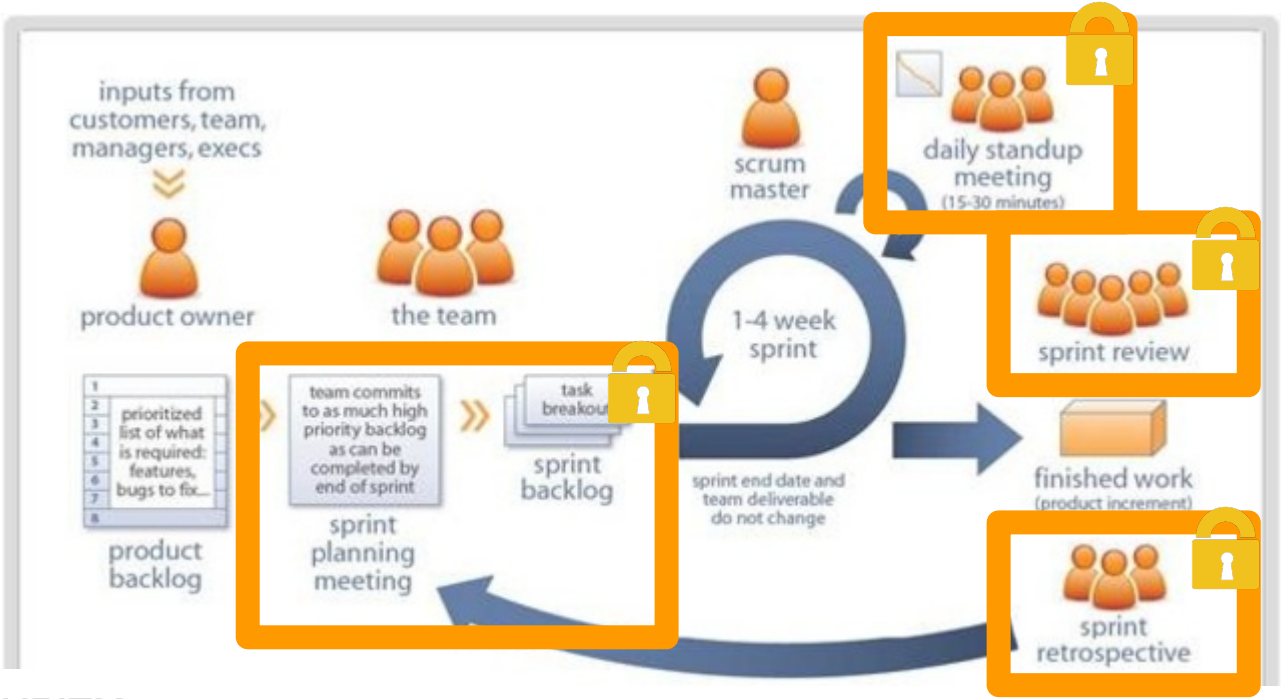
The Rugged Manifesto

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.

Estratégia #1 Participar de tudo



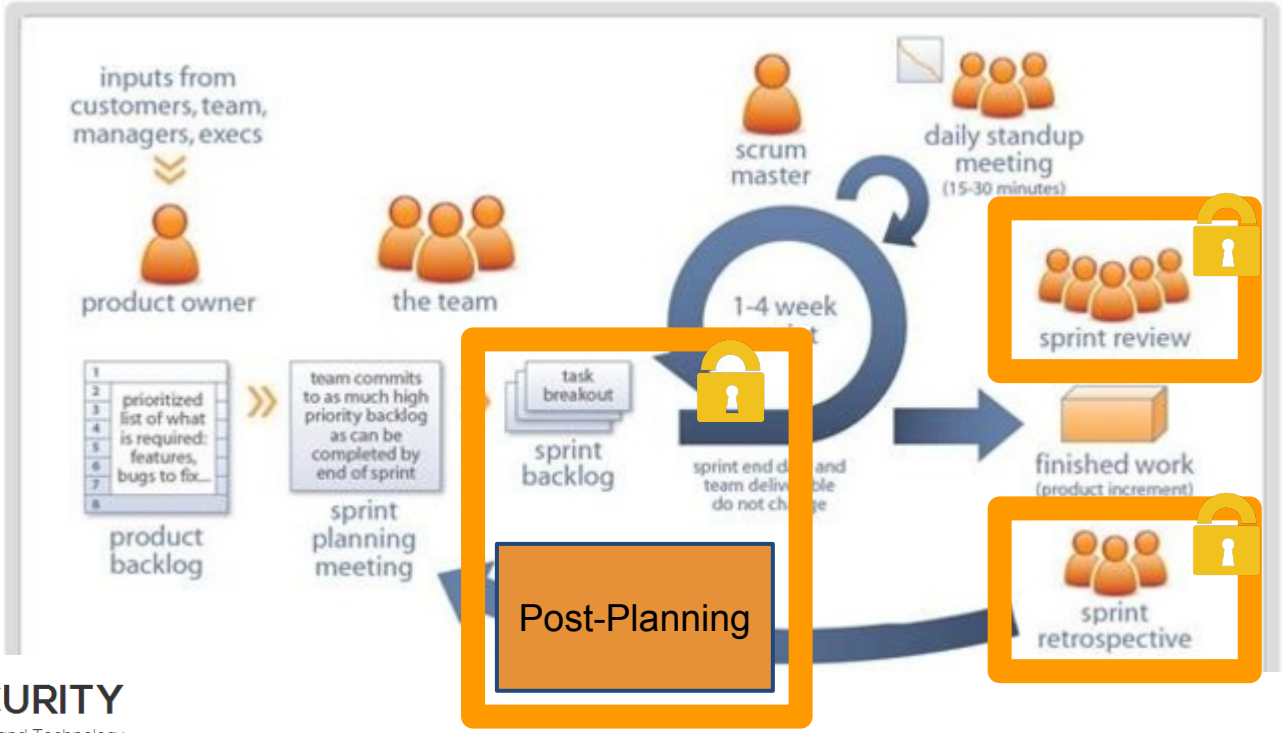
Pros:

- Engenheiro de Segurança está ciente do projeto e pode rapidamente injetar segurança:
  - nas estórias do backlog;
  - conscientizando o time durante as cerimônias.

Cons:

- Tempo dos Eng. de Segurança é bastante consumido;
- Ponto Único de Falha;
- Maior parte do tempo do Planning é desperdiçada;
- Muitos Dailys atrapalham.

Estratégia #2 Post-Planning e sem Daily



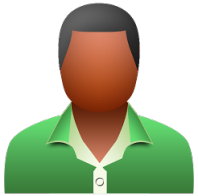
Pros:

- Tempo dos Engenheiros de Segurança é bem aproveitado.

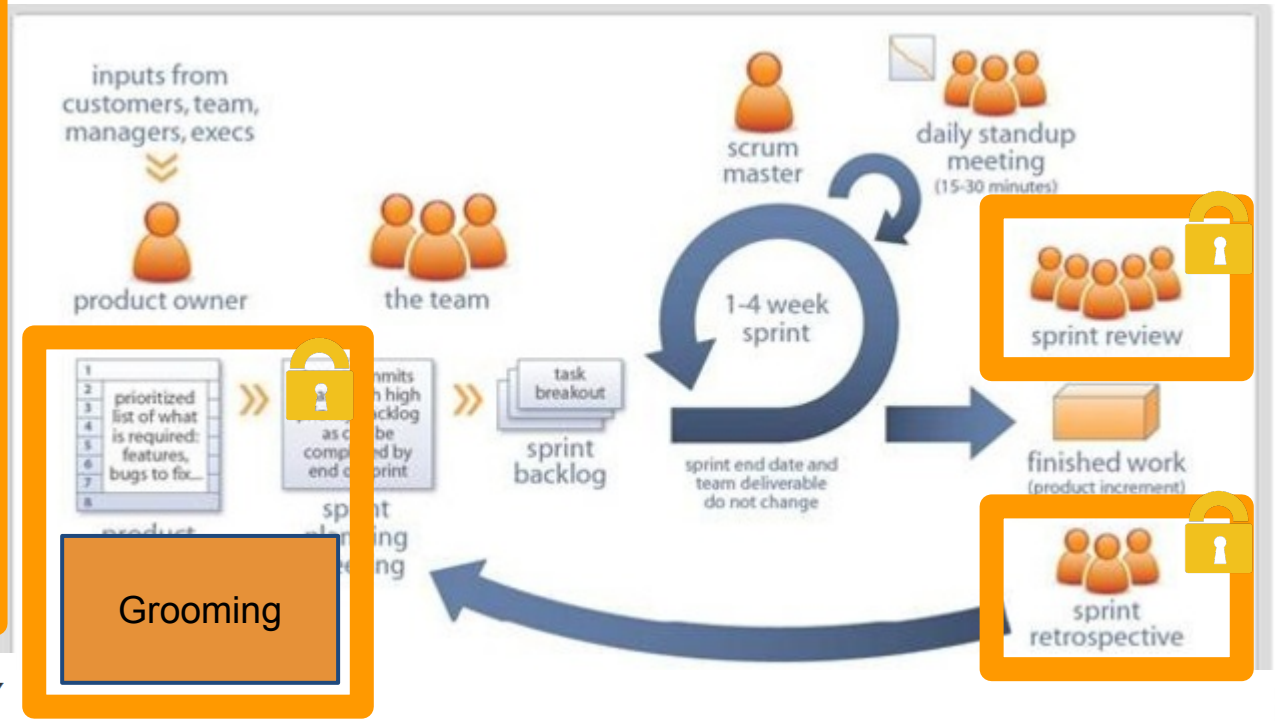
Cons:

- Você está bagunçando a metodologia Scrum porque as estórias não podem ser alteradas após o planning;
- Ponto Único de Falha persiste;
- Menos conscientização de segurança.

Security Architect



Security Engineer



Pros:

- Tempo dos Engenheiros de Segurança é bem aproveitado;
- Sem Ponto Único de Falha;
- Injeção de Segurança respeita o processo de desenvolvimento.

Cons:

- Mais pessoas estão envolvidas, tornando a injeção mais complexa.

Isso ainda não acabou. E sobre ...

THE DEVELOPER'S CONFERENCE

- Estórias que são criadas após o planning?
- Negociação de estórias de segurança?
- Gerência de Riscos?
- Como maximizar ainda mais a injeção de segurança?

FLARE SECURITY

Securing People, Process and Technology

Globalcode

Estórias que são criadas depois do planning

THE DEVELOPER'S CONFERENCE

- Não deveria ser comum, mas pode acontecer;
- Defina um processo para esta exceção;
- O time de Segurança da Informação deve estar ciente desta estória e adicionar as considerações de segurança.

FLARE SECURITY
Securing People, Process and Technology

Globalcode

- Sempre será desafiador, não importa a metodologia;
- Foque no **risco**;
- Defina Quality Gates antes de publicar a aplicação e combine estes Quality Gates com o Product Owner.

Gerenciamento de Riscos (1-3)

- Modelagem de Ameaças no Grooming;
- Injete Segurança:
  - No Critério de Aceite das estórias para requisitos específicos;
  - Na Definição de Pronto para requisitos genéricos.
- Automatize os testes de critério de aceitação de segurança.

Gerenciamento de Riscos (2-3)

THE DEVELOPER'S CONFERENCE

- Tire proveito das ferramentas ágeis:
  - Coloque labels nas estórias do Jira.
- Extraia os labels das estórias usando JQL (Jira Query Language) API;
- Integre os riscos extraídos para a plataforma / dashboard de riscos de sua empresa.

FLARE SECURITY
Securing People, Process and Technology

Globalcode

Gerenciamento de Riscos (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	• 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

Globalcode

Maximize ainda mais a Injeção de Segurança

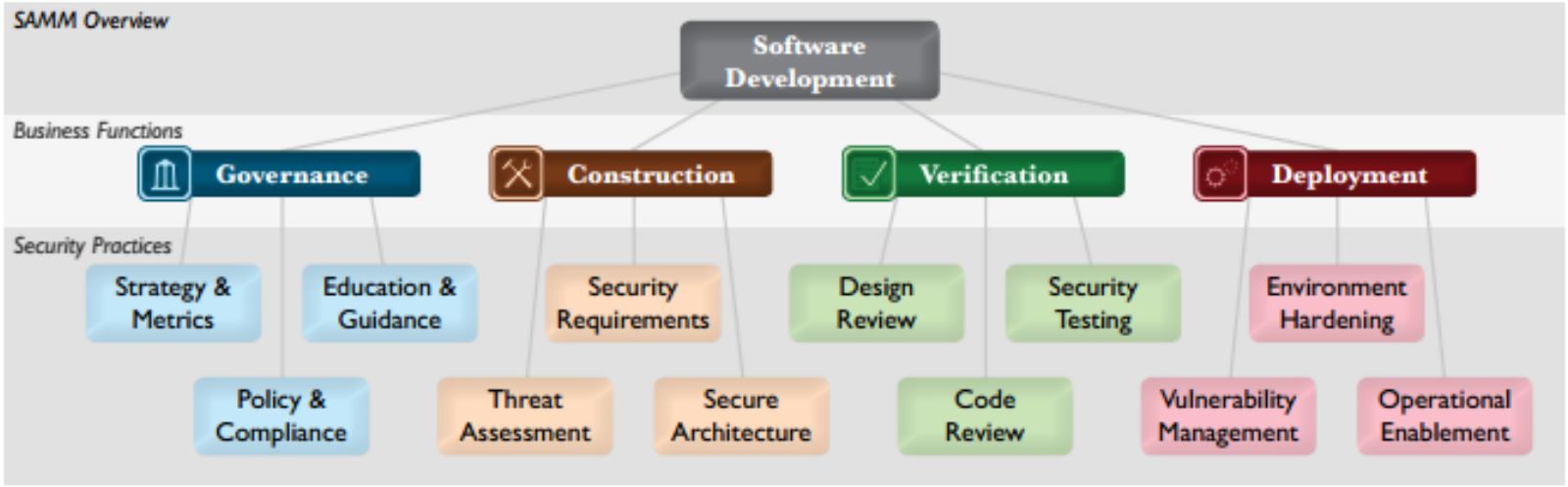
THE DEVELOPER'S CONFERENCE

- 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

Globalcode

OpenSAMM (1-2)


SAMM Overview
Software Development
Business Functions
Governance
Construction
Verification
Deployment
Security Practices
Strategy & Metrics
Education & Guidance
Security Requirements
Design Review
Security Testing
Environment Hardening
Policy & Compliance
Threat Assessment
Secure Architecture
Code Review
Vulnerability Management
Operational Enablement

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?		

- Quanto mais você respeitar o processo dos desenvolvedores, mais eles respeitarão os de segurança;

- Scrum é sobre aprendizado contínuo, então sempre pense em como você pode ajustá-lo para tornar o processo melhor;

- Aplique os conceitos da maneira que sua empresa faz software, porque ***there is no silver bullet***.

Referências e Links Úteis

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 Dadario's blog: http://dadario.com.br
- Rugged Software: https://www.ruggedsoftware.org/

FLARE SECURITY
Securing People, Process and Technology

Globalcode

THE DEVELOPER'S CONFERENCE

Obrigado

Anderson Dadario, CISSP, CSSLP

http://dadario.com.br

http://flaresecurity.com

FLARE SECURITY

Securing People, Process and Technology

Globalcode