Segurança Ágil

Security Week 2018
29/10/2018

daniel.melo@serpro.gov.br

Quem sou eu?

Daniel Araujo Melo

Baterista - 1989

Analista do Serpro - 2004

Professor - 2005

CISSP – 2012

Mestre - 2014

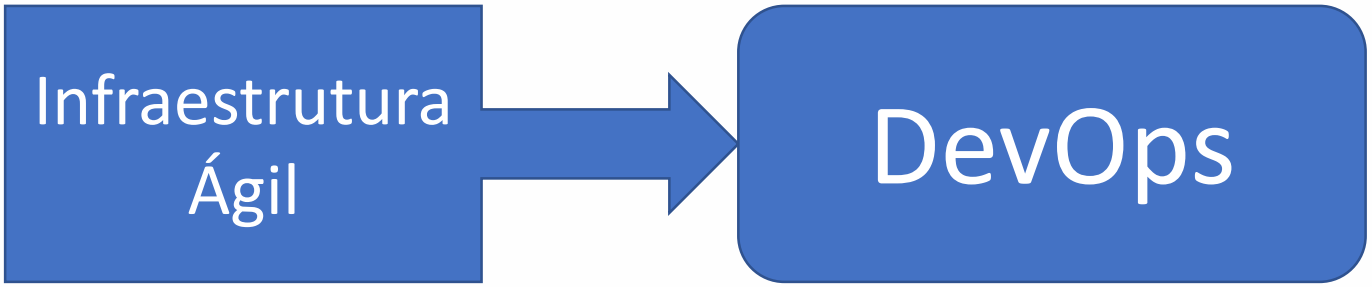
Equipe do Estaleiro - 2016

Manifesto Ágil

- Em 2001, Manifesto Ágil propõe mudança de mentalidade
  - **Indivíduos e interações** mais que processos e ferramentas
  - **Software em funcionamento** mais que documentação abrangente
  - **Colaboração com o cliente** mais que negociação de contratos
  - **Responder a mudanças** mais que seguir um plano

DevOps

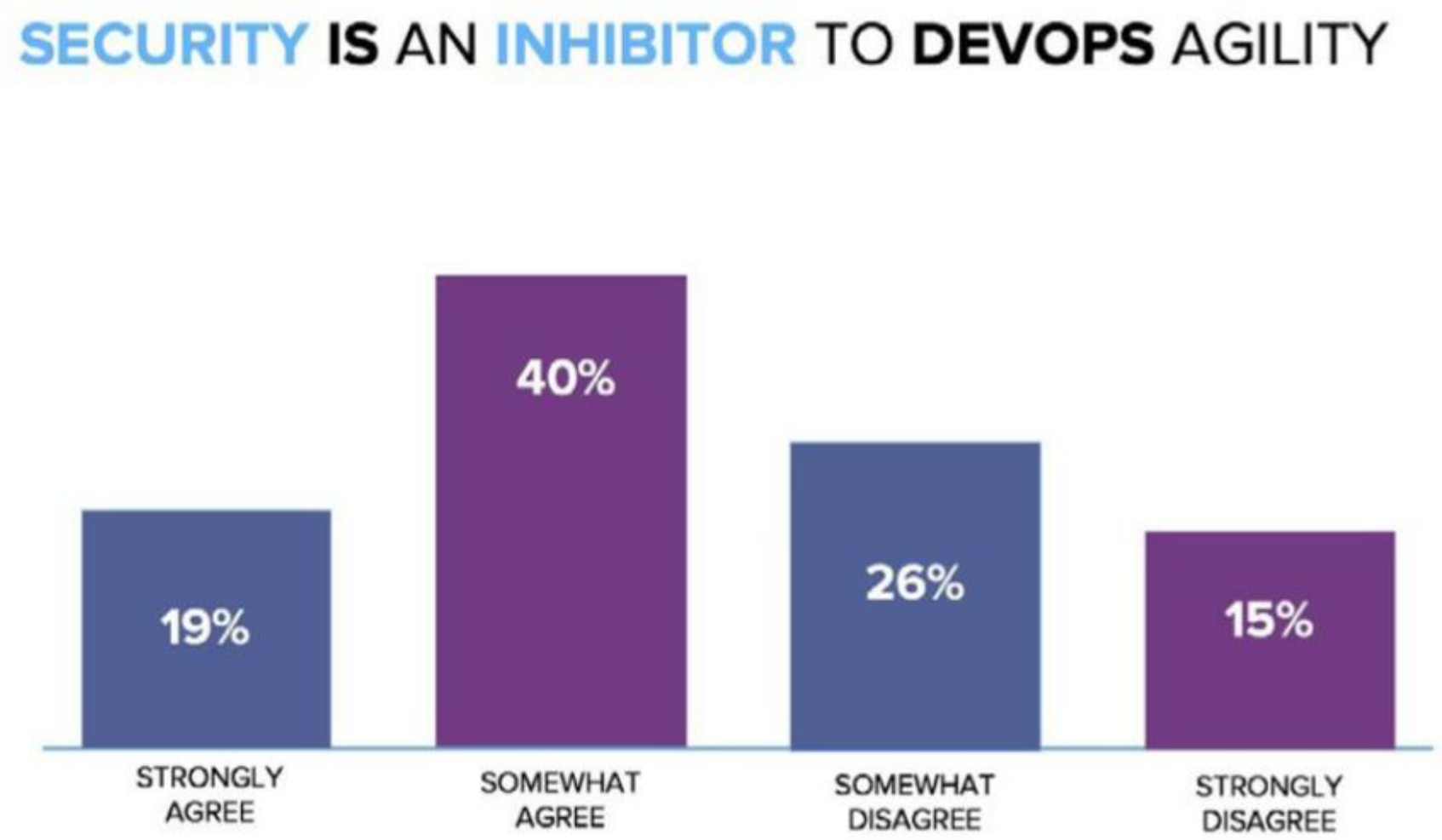
Em 2007, Patrick Debois propôs a utilização do Ágil no processo de gerenciamento da infraestrutura.



Cultura, Entrega Contínua de Valor e Ferramentas

Fonte: https://www.oreilly.com/ideas/the-evolution-of-devops

Historicamente



Fonte: DevOps Community Survey 2017

Segurança Ágil

Ágil é sobre **pessoas em primeiro lugar**

Segurança - Intersecção de Tecnologia, Processos e **Pessoas**

Desenvolvimento de uma **Cultura de Segurança**

Cultura de Segurança

"Cultura inclui um conjuntos de **valores compartilhados**, **objetivos** e **princípios** que guiam **comportamentos**, **atividades**, **prioridades** e **decisões** de um grupo de pessoas em direção a um **objetivo comum**"

Karl Wiegers – Creating a software engineering culture

SERPRO

Cultura de Segurança

Lado das pessoas na Segurança

Como construir valores Ágeis:

Empatia,

Abertura,

Transparência

e Colaboração.

De uma forma Pragmática

Cultura de Segurança

Segurança
vista como provedora de soluções
e não como geradora de problemas

Habilitar ao invés de Bloquear

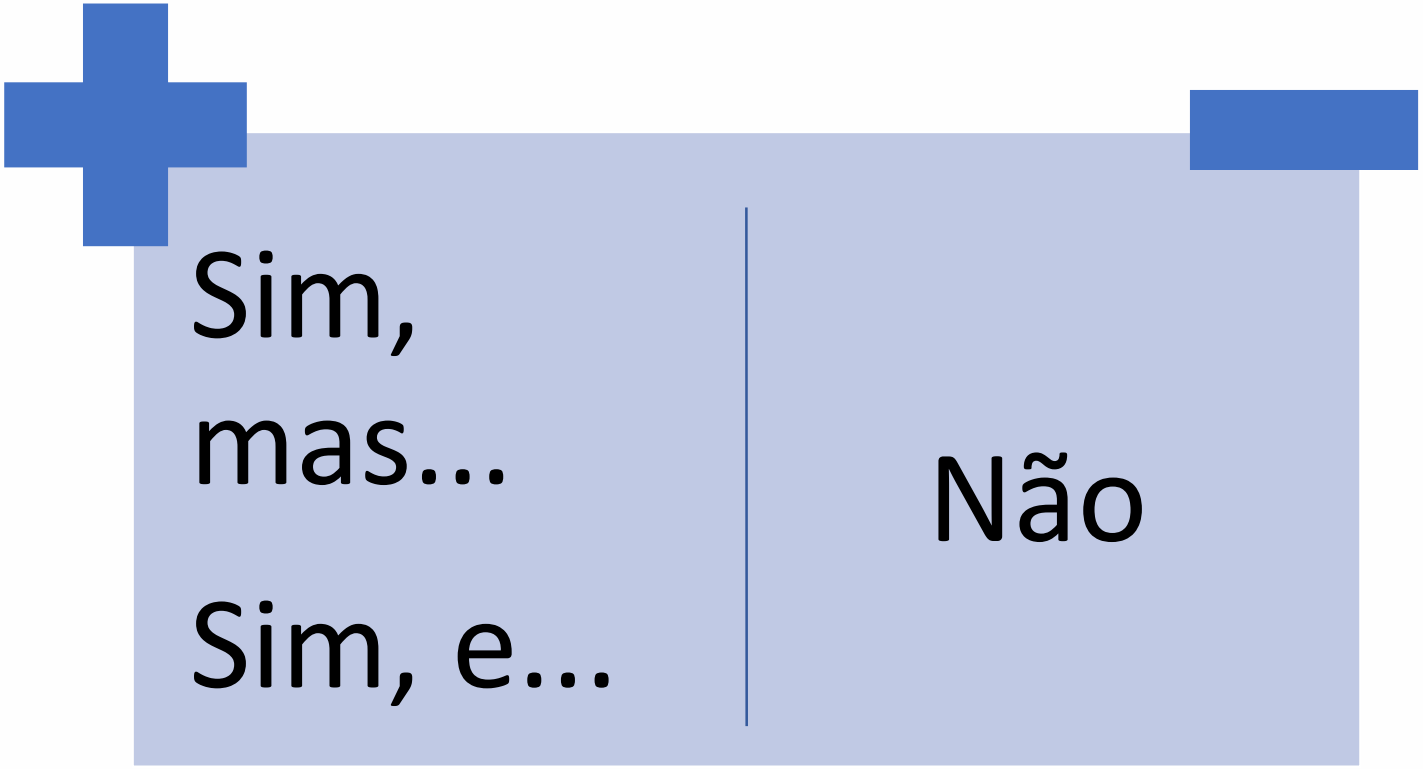
Equipes de segurança eficientes são avaliadas pelo que habilitam ao invés do que bloqueiam.

Se a segurança for considerada um bloqueio, será evitada a qualquer custo.

Fonte:http://www.securecoding.cert.org

Habilitar ao invés de Bloquear

Quanto mais a segurança bloqueia, menos eficaz se torna, pois mais atividades são ocultas.




A
Não
A

Gestão de Risco

Segurança perfeita é uma ilusão

Risco Consciente

Aceitação Consciente >>>> Ignorância cega

Análise de Risco:

Momento para determinar o risco aceitável

Oportunidade para diálogo criativo

Gestão de Risco

Attacker Stories – Histórias de Atacantes

Misuse cases – Casos de Mau Uso

Desenvolvedores devem pensar como atacantes

Modelagem de Ameaças

1. What are you building?
2. What can go wrong?
3. What should you do about those things that can go wrong?
4. Did you do a decent job of analysis

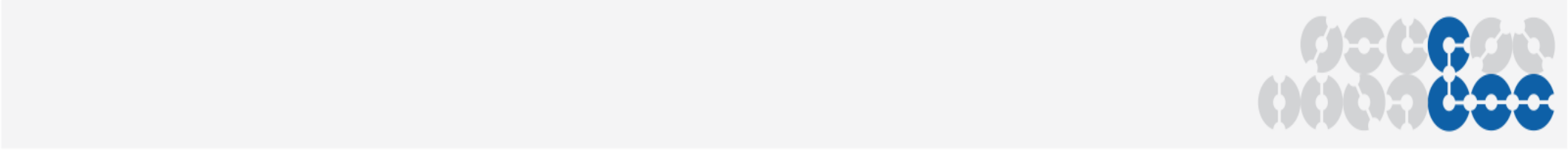
Modelagem de Ameaças

Stride – Classificação de Ameaças

- **S**poofing Identity
- **T**ampering with Data
- **R**epudiation
- **I**nformation Disclosure
- **D**enial of Service
- **E**levation of Privilege

Gamification
Elevation Of Privilege

SERPRO



Histórias de Atacantes

- Ponto de vista do usuário
- Black-box

Modelagem de Ameaças

- Ponto de vista do desenvolvedor
- White-box

SERPRO

Seguro e Transparente

Uma equipe de Segurança que abraça a transparência e abertura a respeito do que faz e porque faz, espalha consciência e compreensão.

Blameless Postmortem

Investigação com o principal objetivo de detectar falhas e aprimorar a segurança

Princípio da Engenharia de Confiabilidade (Software Reliability Engineering)

Falhas de segurança acontecerão

Diga não ao jogo da culpa.

Hardening

"Segurança é fundamentalmente a redução da superfície de ataque. Você cobre 90% do trabalho apenas focando nisto. Os outros 10% é sorte."

Justin Schuch

SERPRO

Hardening

Práticas reconhecidas

- Least Privilege
- Remover Pacotes não utilizados
- Parar serviços não utilizados
- Templates Seguros para VMs

Gestão de Vulnerabilidades

Postura defensiva.

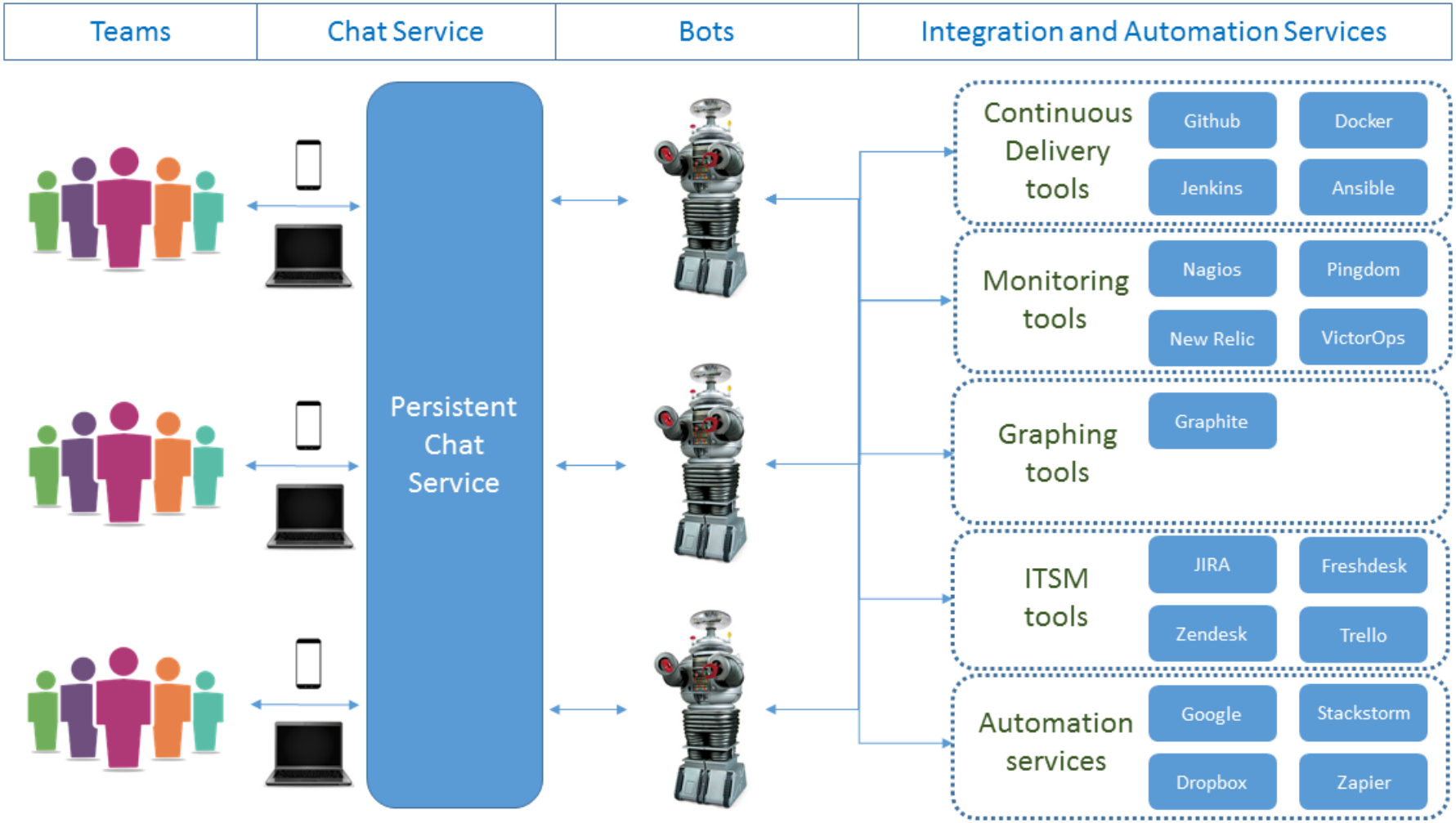
Ao invés de mapear as vulnerabilidades de um ativo,

Onde estão as vulnerabilidades?

Mapeamento Contínuo de Vulnerabilidades

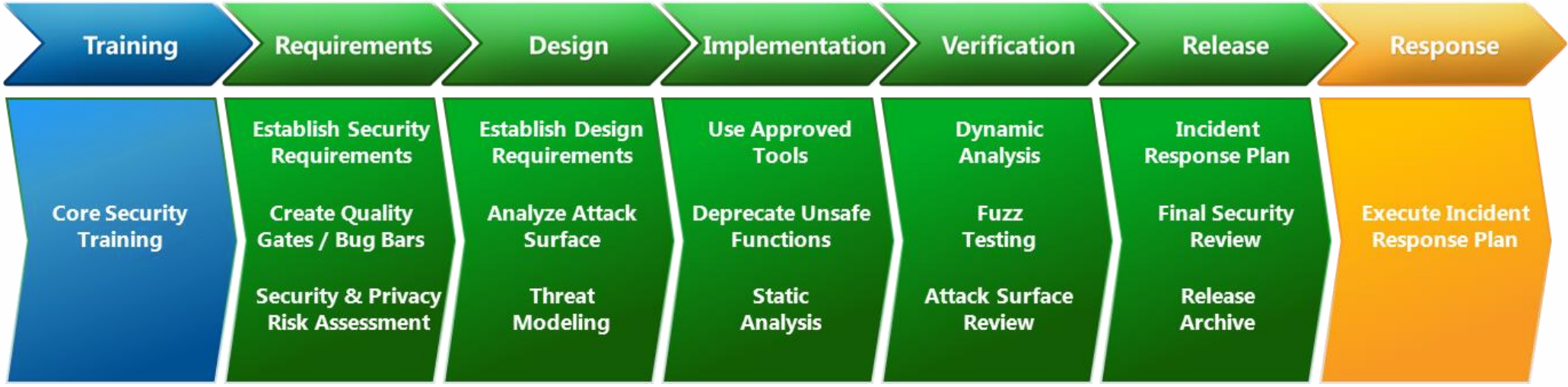
Resposta a Incidentes

ChatOps e ChatBots



Resposta a Incidentes

Integração com Ciclo de Vida de Desenvolvimento



Fonte: https://www.microsoft.com/en-us/sdl

Resposta a Incidentes

Integração com Ciclo de Vida de Desenvolvimento

Fonte: https://www.microsoft.com/en-us/sdl

DEVSECOPS | SECURITY AS CODE

www.devsecops.org

Leaning in over Always Saying “No”

Data & Security Science over Fear, Uncertainty and Doubt

Open Contribution & Collaboration over Security-Only Requirements

Consumable Security Services with APIs over Mandated Security Controls & Paperwork

Business Driven Security Scores over Rubber Stamp Security

Red & Blue Team Exploit Testing over Relying on Scans & Theoretical Vulnerabilities

24x7 Proactive Security Monitoring over Reacting after being Informed of an Incident

Shared Threat Intelligence over Keeping Info to Ourselves

Compliance Operations over Clipboards & Checklists

SERPRO

DevSecOps e Krav Maga

Positioning

Ruggedness

Drills

Situation Awareness

Chaos

http://www.devsecops.org/blog/2016/9/8/devsecops-is-the-krav-maga-of-security

Obrigado!