OWASP

Open Web Application Security Project

De Secure SDLC a SecDevOps

Mario Robles

Mario Robles

- Fundador WhiteJaguars Cyber Security
- OWASP Costa Rica Board member desde 2011
- Líder del proyecto OWASP Pyttacker
- Colaborador en:
  - OWASP Testing Guide, OWASP Top 10, OWASP ASVS
- +14 años experiencia en Information Security
- +300 Pentests realizados
- +50 Capacitaciones brindadas en AppSec
- +1300 apps AppSec program Tech Lead
- Global scope:
  - LATAM, CAN, US, Iberia, UK, NZ, AU, IN, Russia

mario.robles@whitejaguars.com | +506 7012-8363

WHITE JAGUARS
CYBER SECURITY

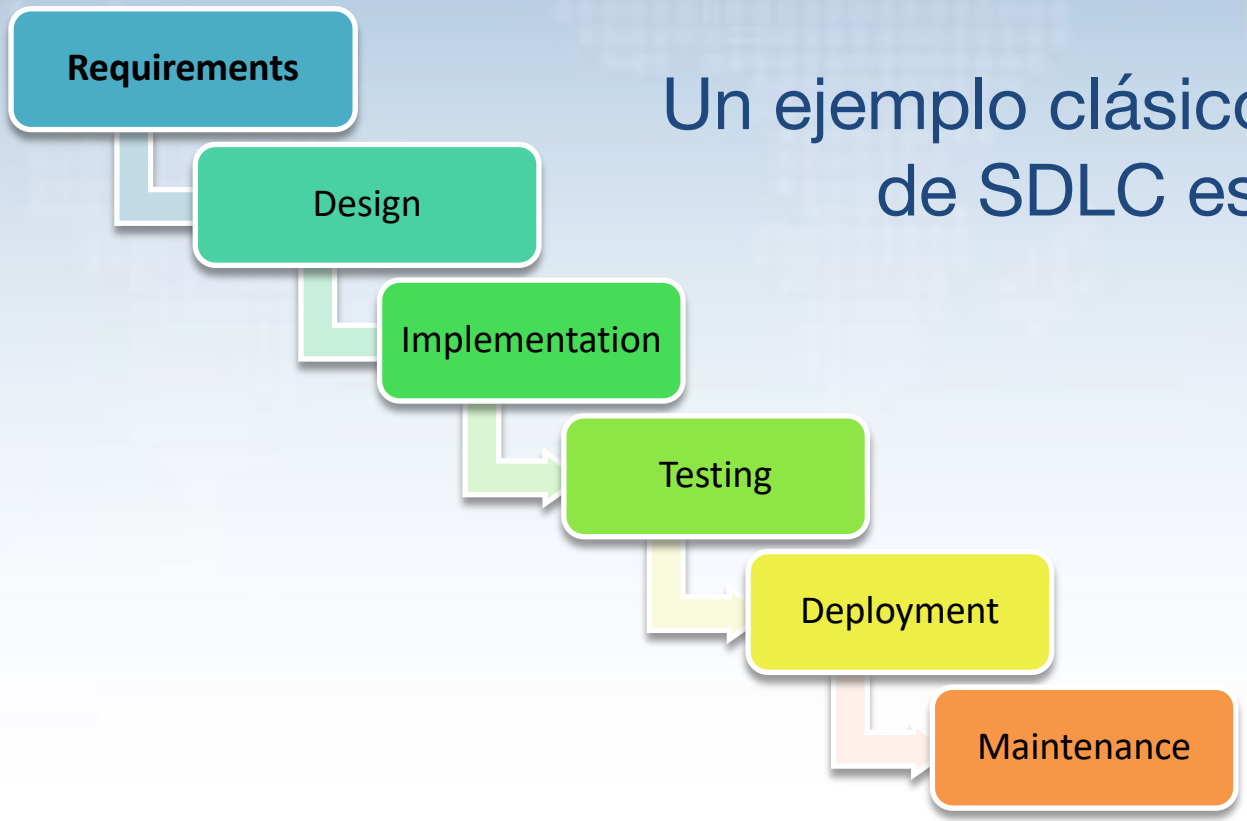
OWASP
Open Web Application Security Project

Introducción

Tradicionalmente los modelos de desarrollo han evolucionado hacia tendencias ágiles lo cual representa un reto para procesos estructurados que fueron diseñados en el pasado

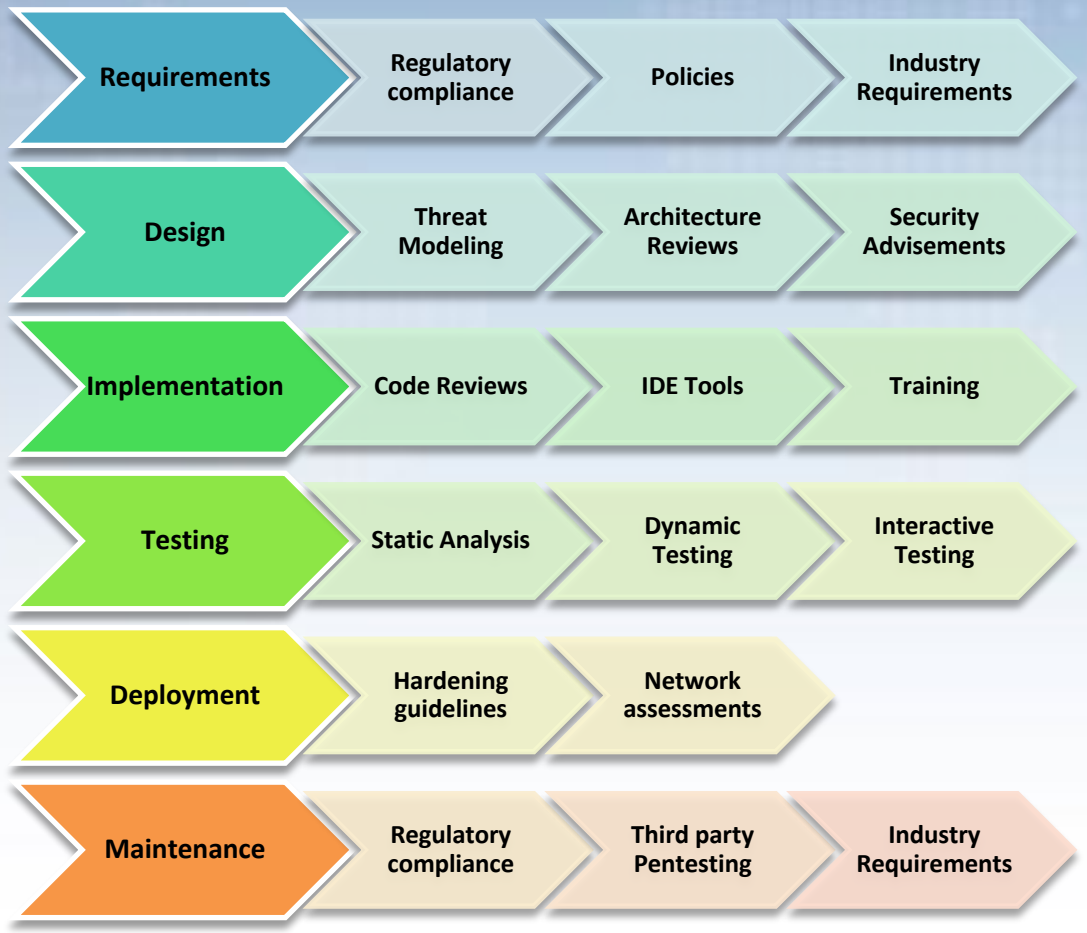
La seguridad no es la excepción

SDLC Tradicional



Un ejemplo clásico de modelo de SDLC es el Waterfall

Secure SDLC



En el Secure SDLC, se adapta la seguridad en cada fase del modelo

WHITE JAGUARS CYBER SECURITY

OWASP Open Web Application Security Project

Requerimientos

Cumplimiento Regulatorio

- FISMA
- FCRA
- HIPAA
- SOX
- PCI-DSS
- Ley de Protección de Datos 8968

Requerimientos

Políticas Internas o Externas

- Política de Seguridad Interna de la Compañía
- Estándares internos de desarrollo seguro
- Requerimientos de clientes o socios comerciales

Requerimientos

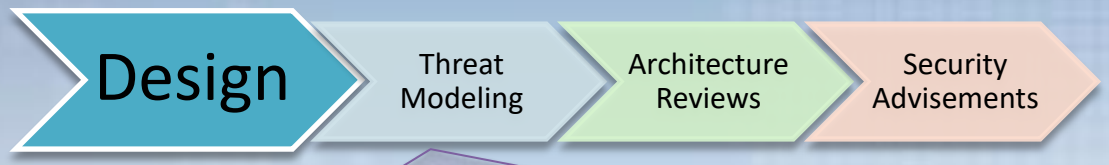
Requerimientos de la Industria

- Bancos
- Gobierno
- Comercio Electrónico

WHITE JAGUARS CYBER SECURITY

OWASP Open Web Application Security Project

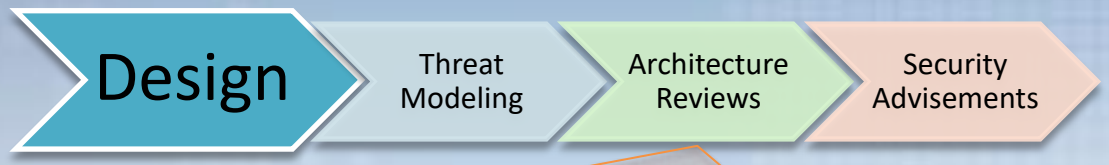
Diseño



Modelado de Amenazas

Inicia de forma macro y se amplia de forma iterativa a lo largo del ciclo de desarrollo

Diseño



Revisiones de Arquitectura

Funciona de manera menos abstracta que el modelado de amenazas

Diseño

Asesorías de Seguridad

- Equipo interno de AppSec
- Consultores externos (Third party)

Implementación

Revisiones de Código

No es muy difundido debido a que incluye trabajo manual que requiere de mucho tiempo, sin embargo puede ser requerido por clientes en algunos casos

Implementación

Herramientas en el IDE

Detección en tiempo real de malas prácticas de desarrollo incluyendo problemas de seguridad

Implementación

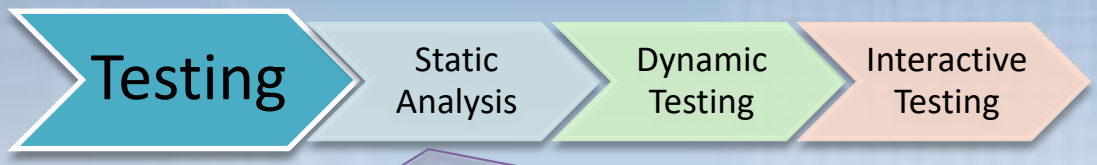
Entrenamientos

- Programas de capacitación internos
- Herramientas eLearning

WHITE JAGUARS CYBER SECURITY

OWASP Open Web Application Security Project

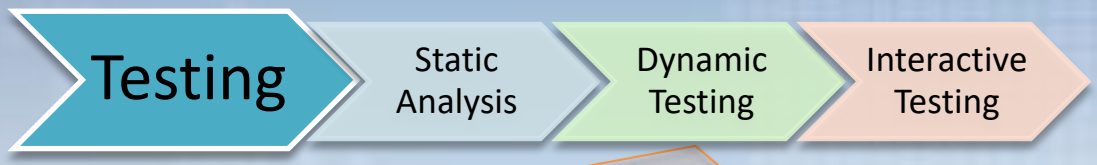
Pruebas



Static Application Security Testing (SAST)

Involucra el uso de herramientas automatizadas para el análisis tanto del código fuente como de archivos binarios compilados

Pruebas



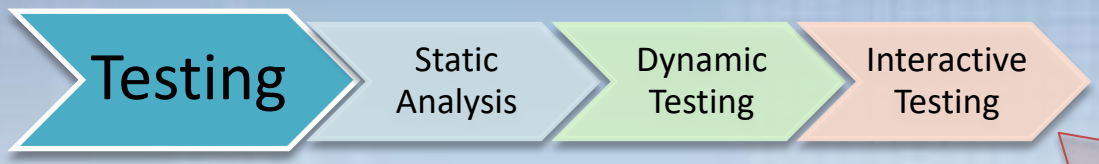
Dynamic Application Security Testing (DAST)

Herramientas automatizadas especializadas en la detección de vulnerabilidades conocidas para plataformas web

WHITE JAGUARS CYBER SECURITY

OWASP Open Web Application Security Project

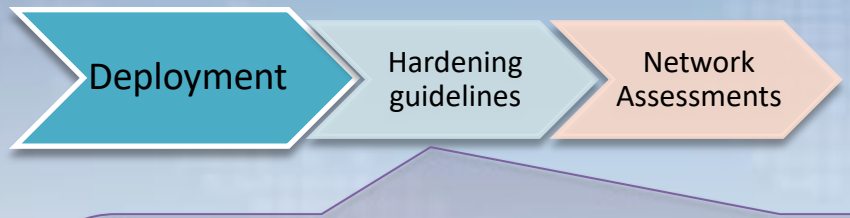
Pruebas



Interactive AppSec Testing

Nueva generación de herramientas capaces de detectar ataques directamente en el tiempo de ejecución

Deployment



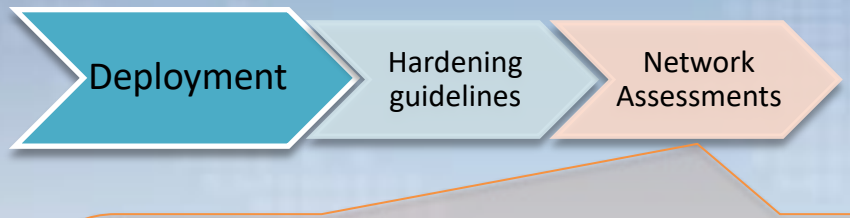
Guías de "Hardening"

Procedimientos documentados para la normalización de los procesos de implementación o instalación de entornos para las aplicaciones

WHITE JAGUARS CYBER SECURITY

OWASP Open Web Application Security Project

Deployment



Evaluaciones de Seguridad en la infraestructura

El uso de herramientas especializadas en la detección de vulnerabilidades de forma general en la infraestructura de redes previene exponer riesgos no relacionados con las aplicaciones

Mantenimiento

Cumplimiento Regulatorio

- FISMA – Acceso restringido a información federal
- FCRA – Certificación de todos los empleados
- HIPPA – Política de retención 8 años
- SOX – Política de retención 5 años
- PCI-DSS – 90 días RP, External Pentest, ASV, etc

Mantenimiento

Proveedores de Pentesting

Aún cuando muchas empresas poseen una organización interna de seguridad, en muchos casos son los clientes quienes solicitan que las evaluaciones de seguridad sean realizadas por un tercero que sea imparcial

Mantenimiento

Requerimientos de la Industria

- **Bancos**: Pentest externo cada 6 meses, reportes de herramientas SAST
- **Gobierno**: SUFEG, COBIT
- **Comercio Electrónico**: PCI-DSS
- **PCI-DSS**: Approved Scanning Vendors (ASV)

SecDevOps | DevSecOps

SecDev	¿ Secure SDLC ?
DevOps	¿ Agile model?
SecOps	¿ Blue Team, SOC ?

¿Secure DevOps o Development SecOps?

WHITE JAGUARS
CYBER SECURITY

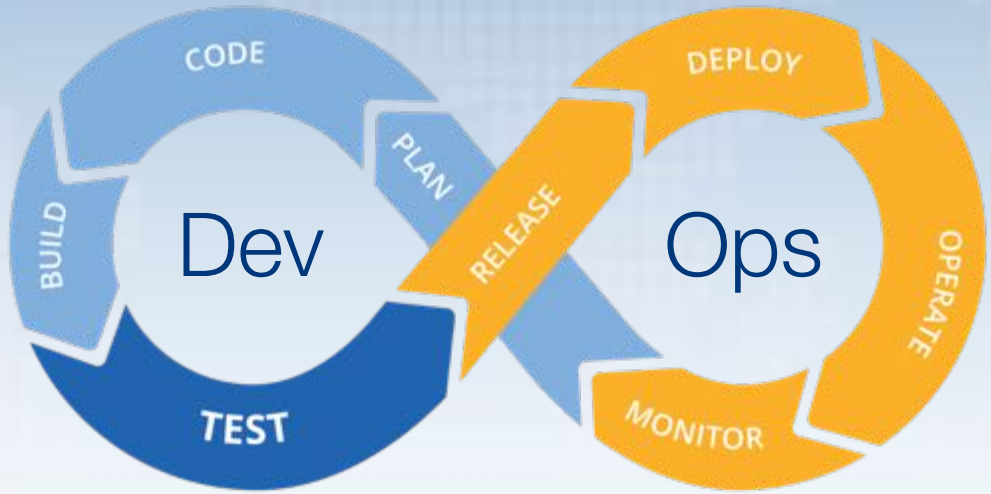
OWASP
Open Web Application Security Project

SecDevOps | DevSecOps

WHITE JAGUARS
CYBER SECURITY

OWASP
Open Web Application Security Project

SecDevOps | DevSecOps

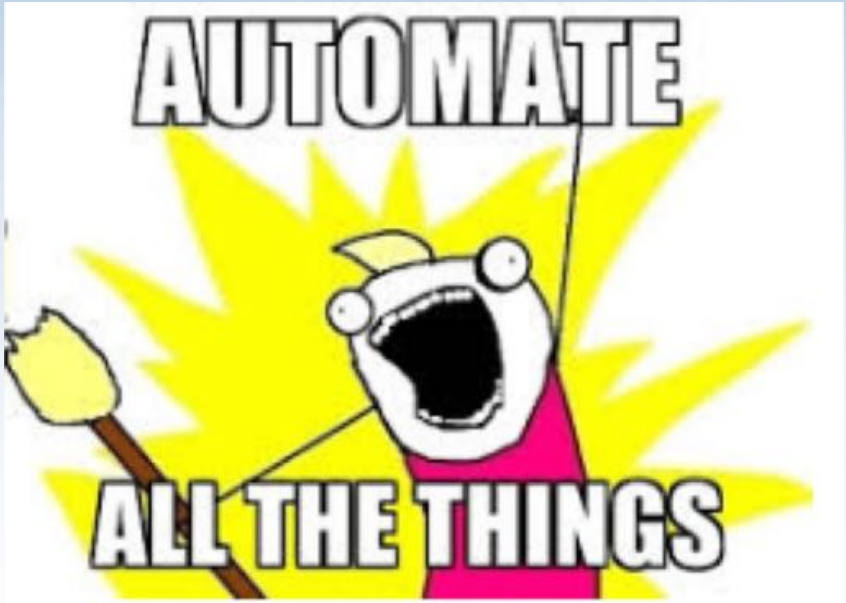


Secure SDLC	SecDevOps
División	Colaboración
Trabajo Manual	Automatización
Lento	Rápido
Estructurado	Ágil

WHITE JAGUARS CYBER SECURITY

OWASP Open Web Application Security Project

The key is automation



SecDevOps -> CI/CD

Development

- IDE Tools
- Security Guidelines

Continuous Integration

- SAST, IAST
- Security Regression Tests
- Issue Tracking

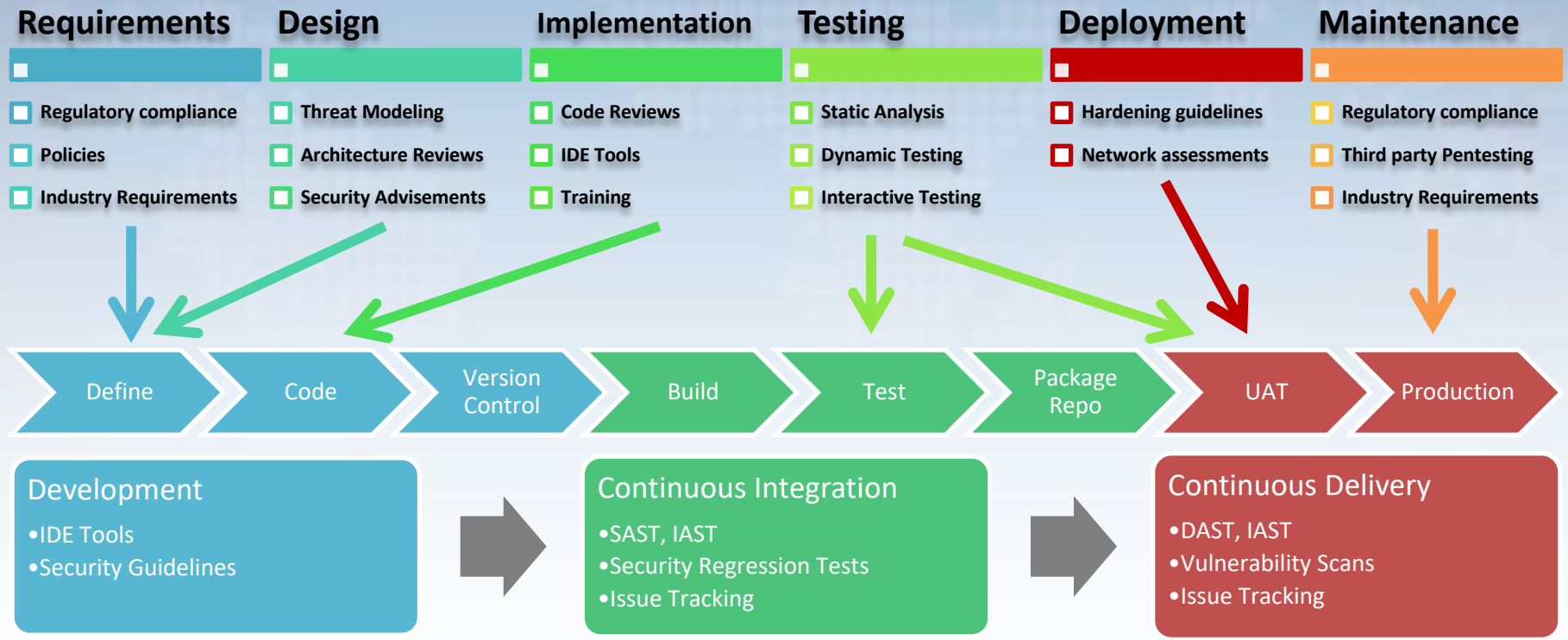
Continuous Delivery

- DAST, IAST
- Vulnerability Scans
- Issue Tracking

WHITE JAGUARS CYBER SECURITY

OWASP Open Web Application Security Project

De Secure SDLC a SecDevOps



¿Es SecDevOps el reemplazo de Secure SDLC ?

WHITE JAGUARS CYBER SECURITY

OWASP Open Web Application Security Project

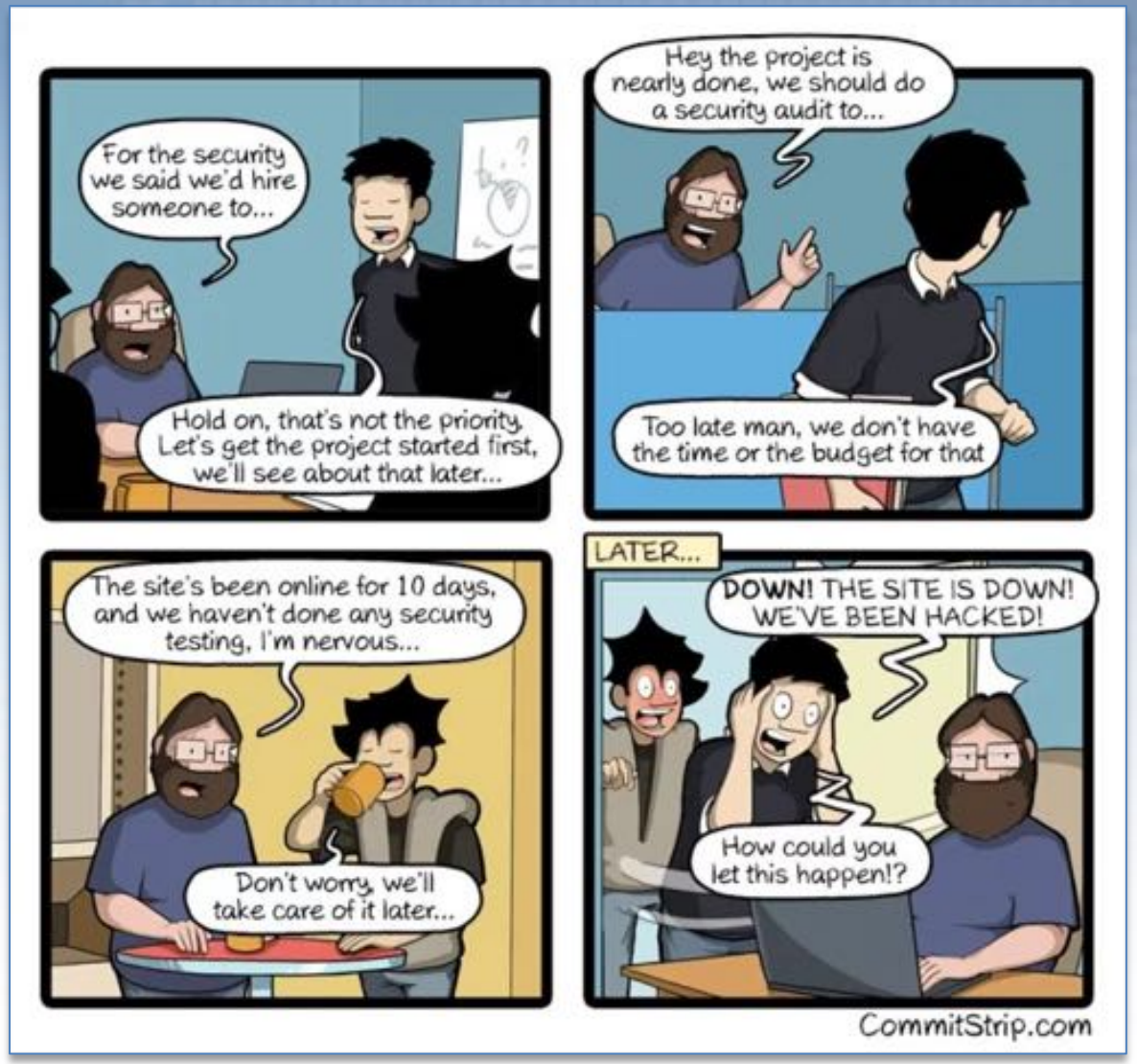
¿ Cómo iniciar desde cero ?

Al inicio la tarea puede parecer abrumadora, mi recomendación es definir un “roadmap” alineado a un modelo de madurez de aseguramiento de software y enfocarse en micro procesos

- **BSIMM** – Building Security in Maturity Model
- **OpenSAMM** – Open Software Assurance Maturity Model
- **OWASP ASVS** – AppSec Verification Standard

WHITE JAGUARS
CYBER SECURITY

OWASP
Open Web Application Security Project



WHITE JAGUARS CYBER SECURITY

mario.robles@whitejaguars.com
Móvil: +(506) 7012-8363
US +1 (732) 481-2777 | CR +(506) 2234-8596

OWASP Open Web Application Security Project

OWASP
Open Web Application Security Project

¡Muchas gracias!

mario.robles@whitejaguars.com
Móvil: +(506) 7012-8363
US +1 (732) 481-2777 | CR +(506) 2234-8596

WHITE JAGUARS
CYBER SECURITY