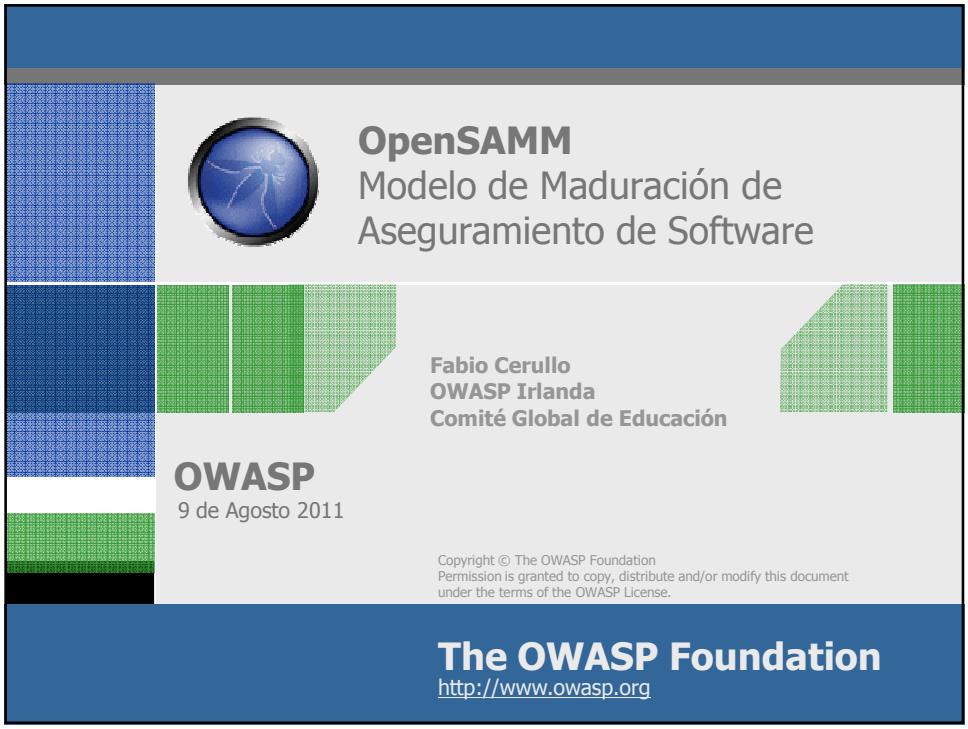


Agenda

- Iniciativas Existentes
- El modelo SAMM
- Aplicación de SAMM
- Niveles y Actividades SAMM
- SAMM en el mundo real
- Proyecto OpenSAMM
- AppSec Latam 2011

OWASP

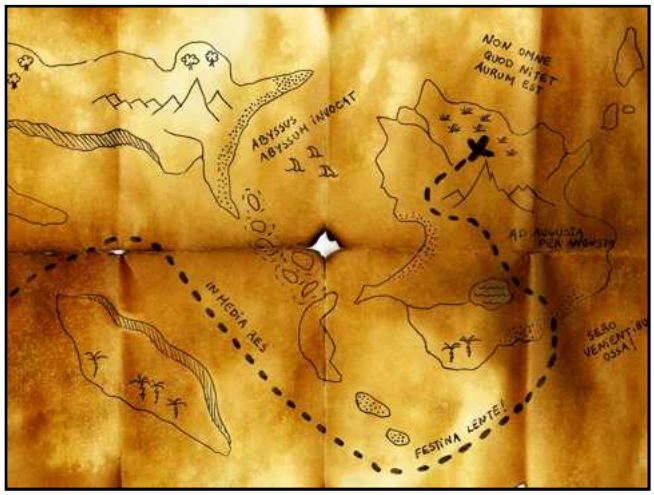
Objetivos de Presentación

Aprender a:

- Evaluar las prácticas de seguridad existentes en una organización.
- Construir un plan de aseguramiento de calidad de software en etapas bien definidas.
- Demostrar las mejoras concretas del plan de calidad en la seguridad del software.
- Definir y medir actividades relacionadas con la seguridad en el conjunto de la organización.

OWASP

Iniciativas Existentes



OWASP

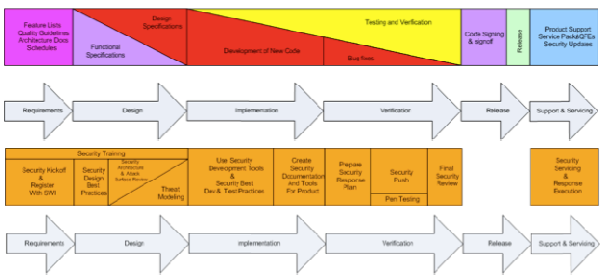
CLASP

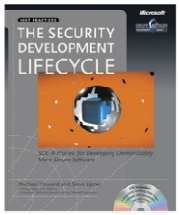
- Comprehensive, Lightweight Application Security Process
  - Centrado en 7 buenas prácticas de desarrollo de aplicaciones seguras
  - Cubre al completo el ciclo de vida del software (no únicamente la fase de desarrollo)
- Adaptable a cualquier proceso de desarrollo
  - Define roles en todo el SDLC
  - 24 procesos basados en definición de roles
  - Comienzo simple y adaptable según necesidades

OWASP

Microsoft SDL

- SDL= Security Development Lifecicle
- Construido internamente para software MS
- Extendido y hecho público para otros

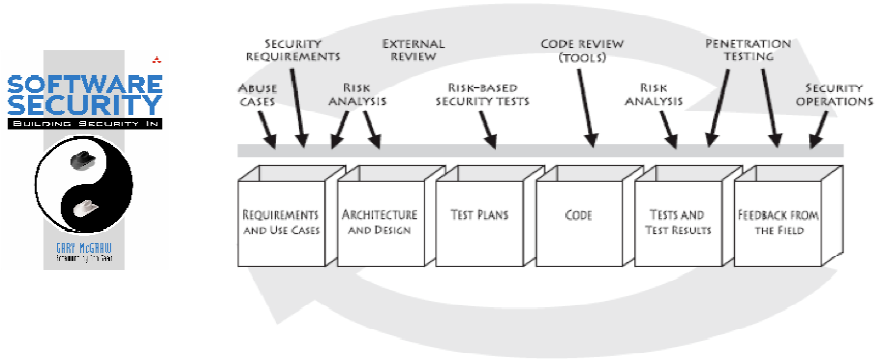




OWASP 6

Touchpoints

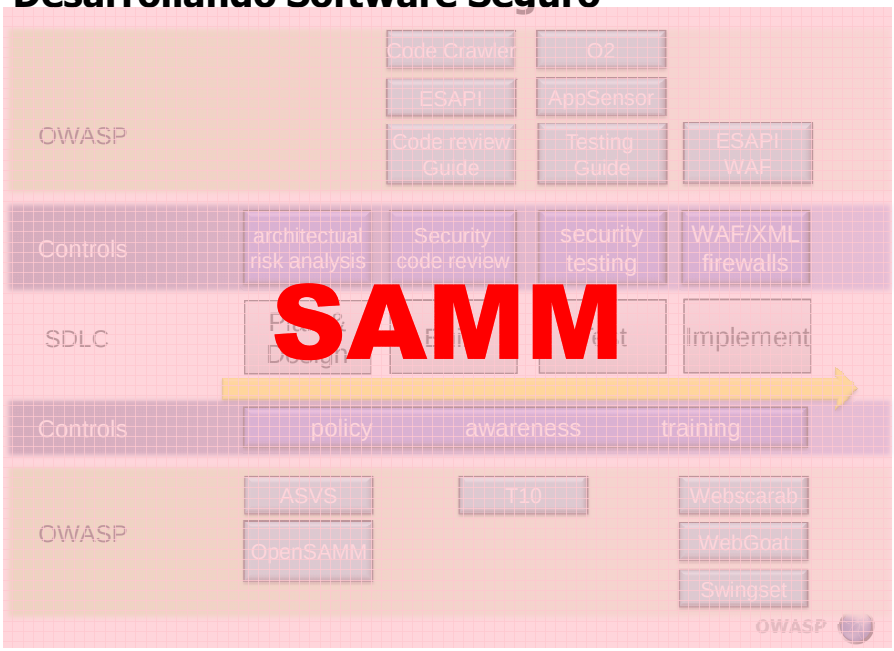
- El modelo de Gary McGraw y Cigital



Conclusiones de Modelos Existentes

- Microsoft SDL
  - Muy pesado, bueno para grandes ISVs
- Touchpoints
  - De alto nivel, no es lo suficientemente detallado desde un punto de vista operativo
- CLASP
  - Amplia colección de actividades, pero sin asignación de prioridades
- TODOS: Buenos para que expertos puedan usarlos como referencia, pero complicado para que gente sin conocimientos de seguridad lo usen como guía

Desarrollando Software Seguro



Premisas para un Modelo de Maduración

- El entorno de una organización cambia lentamente en el tiempo.
  - Los cambios deben ser secuenciales persiguiendo un objetivo concreto a largo plazo
- No hay una única solución que funcione para todas las organizaciones
  - Flexibilidad de acuerdo al riesgo de la organización
- La orientación de las actividades relacionadas con la seguridad deben ser prescriptivas
  - Su comprensión debe ser posible para personas que no formen parte del equipo de seguridad.
- Solución SENCILLA, BIEN DEFINIDA y MESURABLE.

OWASP 10

El Modelo de Madurez debe…

- Definir los componentes básicos de un proceso de mejora de seguridad
  - Diseñar todas las funciones con una estructura organizativa que pueda ser mejorada con el tiempo
- Definir cómo deben relacionarse los componentes básicos
  - Hacer que los cambios en cada iteración sean asimilables sin esfuerzo
- Definir los detalles de cada componente básico claramente
  - Aclarar las partes relevantes a la seguridad de la manera más genérica posible

El Modelo SAMM

• Metodología que sirve para evaluar las practicas actuales de desarrollo seguro en una organización.

• Puede ser utilizado para implementar un programa de seguridad de aplicaciones en forma iterativa.

• Demuestra mejoras concretas en un programa de aseguramiento de seguridad de aplicaciones.

• Define y mide actividades relacionadas a la seguridad en su organización.

Historia de SAMM

- Versión Beta liberada en Agosto de 2008
  - 1.0 publicada en Marzo 2009
- Fundada originalmente por Fortify (ahora HP)
  - Todavía permanece involucrada activamente y haciendo uso de este modelo
- Publicada bajo licencia Creative Commons Attribution Share-Alike
- Donada al proyecto OWASP, actualmente es un proyecto propio de OWASP
- Versión en español lanzada en Julio 2011

El Modelo SAMM

Funciones de Negocio SAMM

- Se comienza con el núcleo de actividades presentes en cualquier organización que realiza desarrollo de software
- El nombre asignado es genérico, pero deberían ser identificables por cualquier desarrollador o gestor

Prácticas de Seguridad SAMM

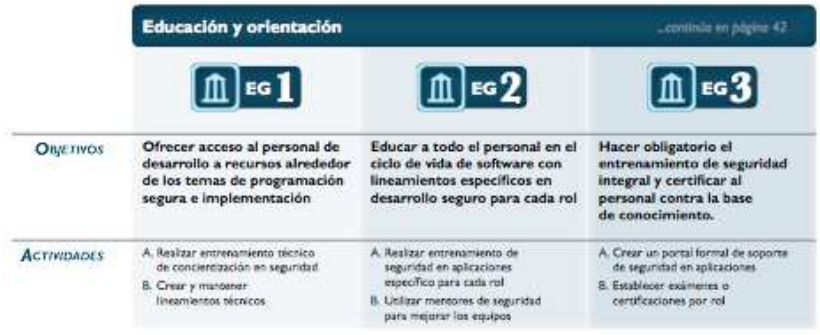
- Por cada una de las Funciones de Negocio se definen 3 Prácticas de Seguridad.
- Dichas prácticas cubren las áreas relevantes al aseguramiento de calidad en el software.
- Cada una de ellas en un 'nicho' de mejora.

Prácticas de Seguridad SAMM

- Cada Práctica tiene objetivos específicos que definen cómo ir mejorando a lo largo del tiempo.
  - Esto establece el concepto de **Nivel** en el que una organización se encuentra al cumplir una determinada Práctica.
- Los distintos niveles son:
  - (0: Punto de partida implícito cuando la Práctica es incumplida)
  - 1: Comprensión inicial y disposición específica para adoptar la Practica
  - 2: Incrementar la eficacia y/o eficiencia de la Práctica
  - 3: Dominio completo de la Práctica

Prácticas de Seguridad SAMM

EJEMPLO



Educación y orientación	EG 1	EG 2	EG 3
Objetivos	Ofrecer acceso al personal de desarrollo a recursos alrededor de los temas de programación segura e implementación	Educar a todo el personal en el ciclo de vida de software con lineamientos específicos en desarrollo seguro para cada rol	Hacer obligatorio el entrenamiento de seguridad integral y certificar al personal contra la base de conocimiento.
Actividades	A. Realizar entrenamiento técnico de concientización en seguridad B. Crear y mantener lineamientos técnicos	A. Realizar entrenamiento de seguridad en aplicaciones específico para cada rol B. Utilizar mentores de seguridad para mejorar los equipos	A. Crear un portal formal de soporte de seguridad en aplicaciones B. Establecer exámenes o certificaciones por rol

Por cada Nivel se definen…

Educación y orientación EG 1

Ofrecer acceso al personal de desarrollo a recursos alrededor de los temas de programación segura e implementación

Actividades

A. Realizar entrenamiento técnico de concientización en seguridad

Ya sea interna o externamente, lleve a cabo entrenamiento en seguridad para el personal técnico que cubra los principios básicos de seguridad en aplicaciones. Generalmente, esto se puede lograr vía instructor en 1 o 2 días o con entrenamiento basado en computadora con módulos teniendo la misma cantidad de tiempo por desarrollador. El contenido del curso debe cubrir información tanto conceptual como técnica. Temas apropiados incluyen mejores prácticas de alto nivel para la validación de entradas, codificación de salida, manejo de errores, registro, autenticación, autorización. La cobertura adicional de vulnerabilidades de software comunes también es deseable como una lista de los 10 problemas mayores relacionados al software que está siendo desarrollado (aplicaciones Web, dispositivos embebidos, aplicaciones cliente-servidor, etc.). Cuando sea posible, usar muestras de código y ejercicios de laboratorio en el lenguaje de programación específico aplicable a la compañía. Para desplegar dicho entrenamiento, es recomendado exigir entrenamiento de seguridad anual y después tener cursos (ya sea por instructor o computadora) con la frecuencia necesaria basándose en el número de desarrolladores.

B. Crear y mantener lineamientos técnicos

Para el personal de desarrollo, reúna una lista de documentos aprobados, sitios Web, y notas técnicas que proporcionen consejos de seguridad específicos a la tecnología. Estas referencias pueden ser reunidas de muchos recursos públicos en Internet. En casos donde las tecnologías sean muy especializadas o propietarias estén presentes, utilice personal experto en seguridad para crear notas a lo largo del tiempo para crear una base de conocimientos. Asegúrese que la administración esté consciente de los recursos e informe al personal acerca del uso esperado. Trate de mantener los lineamientos ligeros y actualizados para evitar desorden e irrelevancia. Una vez que se ha establecido un nivel de confort, pueden ser usados como una lista de verificación cualitativa para asegurar que los lineamientos han sido leídos, entendidos y seguidos en el proceso de desarrollo.

Evaluación

- ¿La mayoría de los desarrolladores han recibido entrenamiento de alto nivel sobre concientización de seguridad?
- ¿Cada equipo tiene acceso a mejores prácticas y orientación para desarrollo seguro?

Resultados

- Mejor concientización de los desarrolladores sobre los problemas más comunes a nivel código
- Mantener software con mejores prácticas de seguridad elementales
- Establecer lineamientos base para saber como llevar a cabo la seguridad entre el personal técnico
- Habilitar verificaciones de seguridad cualitativas para una base de datos de conocimiento de seguridad

Métricas de Éxito

- >50% de los desarrolladores informados en problemas de seguridad el último año
- >75% de los desarrolladores expertos/ arquitectos informados en problemas de seguridad el último año
- Lanzar orientación técnica dentro de los 3 meses del primer entrenamiento

Costos

- Construcción del curso o licencia
- Mantenimiento continuo de la orientación técnica

Personal

- Desarrolladores (1-2 días/año)
- Arquitectos (1-2 días/año)

Niveles Relacionados

- Política y cumplimiento - 2
- Requisitos de seguridad - 1
- Arquitectura de seguridad - 1

- Objetivo
- Actividades
- Resultados
- Umbrales de satisfacción
- Coste
- Personal
- Niveles relacionados

La Mejora Iterativa

- Dado que cada una de las 12 Prácticas es un área de madurez, los objetivos sucesivos representan los componentes básicos para cualquier programa de mejora de la seguridad en el desarrollo.
- En pocas palabras, la idea es definir un plan de mejora de la seguridad en el desarrollo de la siguiente forma:
  1. Seleccionar **Prácticas** de seguridad a potenciar en la siguiente fase del plan de mejora.
  2. Lograr el siguiente **Objetivo** en cada Práctica mediante la realización de las **Actividades** asociadas a los **Umbrales de Satisfacción**

Aplicando el Modelo SAMM

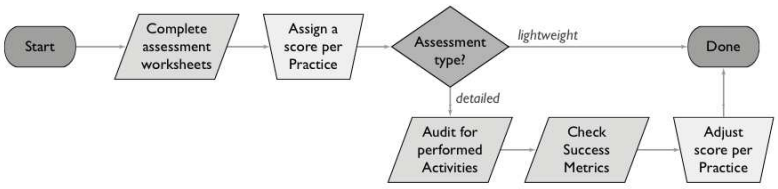
Realizacion de Evaluaciones

- SAMM incluye documentos de evaluación para cada **Práctica** de seguridad

Education & Guidance	Yes/No	
Have most developers been given high-level security awareness training?		
Does each project team have access to secure development best practices and guidance?		EG 1
Are most roles in the development process given role-specific training and guidance?		
Are most stakeholders able to pull in security coaches for use on projects?		EG 2
Is security-related guidance centrally controlled and consistently distributed throughout the organization?		
Are most people tested to ensure a baseline skill-set for secure development practices?		EG 3

Proceso de Evaluación

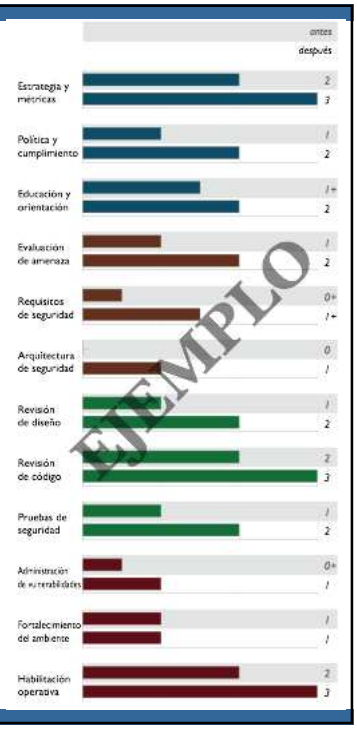
- Se permite tanto evaluaciones superficiales como detalladas
- Es posible que las organizaciones se encuentren en niveles intermedios (+)



OWASP 23

Cuadros de Mando

- Análisis diferencial
  - Capturando las puntuaciones de evaluaciones detalladas versus niveles de rendimiento esperados.
- Seguimiento de mejoras
  - Comparando las puntuaciones acumuladas de antes y despues de una iteración del programa de mejora
- Medida contínua
  - Capturando puntuaciones en períodos de tiempo constantes para planes de mejora que ya estén en marcha



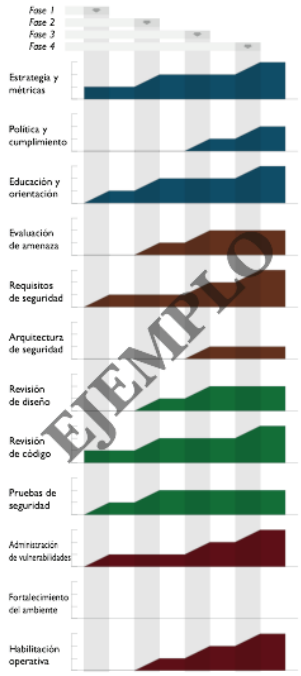
Plantillas de Mejora

Para hacer los "componentes básicos" del modelo utilizables, SAMM define Plantillas de Planes de mejora (Roadmaps) para diferentes Organizaciones Tipo.

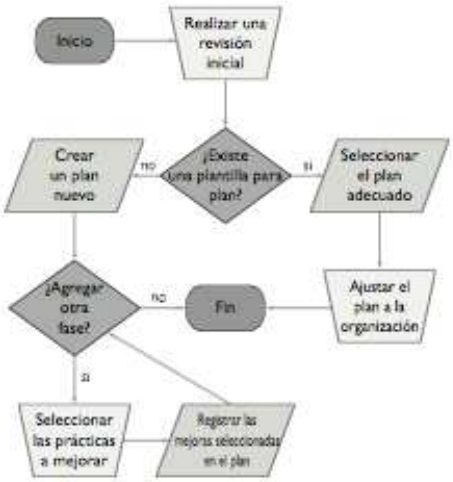
- Desarrolladores de Software Independientes
- Proveedores de servicios Online
- Organizaciones de servicios financieros
- Administraciones Públicas

Las Organizaciones tipo se han elegido porque:

- Representan los casos de uso más comunes
- Los riesgos típicos del software son distintos en función del tipo de organización
- La definición de un plan de mejor de la seguridad óptimo es diferente en cada caso.



Programa de Mejora de la Seguridad



Casos de Estudio: VirtualWare

- Un tutorial completo con explicaciones concisas acerca de cómo afectan a la mejora de la organización las decisiones que se han tomado.
- Fases descritas en detalle
  - Restricciones de la Organización
  - La elección de construir o adquirir
  - Al día de hoy existe un caso de estudio, y hay varios en proceso a través de socios de la industria

SAMM en el Mundo Real

Contribuciones de Expertos

- Definida en base a la experiencia recogida con cientos de organizaciones.
- Incluye expertos en seguridad, desarrolladores, arquitectos, gestores de desarrollo y gestores de Tecnologías de la Información.

Author & Project Lead

Pravir Chandra

Contributors/Reviewers

Fabio Arciniegas	Brian Chess	Matteo Meucci	John Steven
Matt Bartoldus	Dinis Cruz	Jeff Payne	Chad Thunberg
Sebastien Deleersnyder	Justin Derry	Gunnar Peterson	Colin Watson
Jonathan Carter	Bart De Win	Jeff Piper	Jeff Williams
Darren Challey	James McGovern	Andy Steingruebl	

Apoyo de la Industria

- SAMM siendo utilizado por:

FORTIFY · OWASP The Open Web Application Security Project · ASPECT SECURITY · coveros · DENIM GROUP · GOTHAM DIGITAL SCIENCE · leviathan security group · Minded security · Security Compass · WhiteHat SECURITY

El Proyecto OpenSAMM

- http://www.opensamm.org
- Dedicado a definir, mejorar y probar el marco de referencia de SAMM.
- Siempre tecnológicamente independiente, pero con amplia participación de la industria
  - Abierto y conducido por la comunidad
- Objetivo de publicación de nuevas versiones cada 6-12 meses
- Proceso de gestión de cambios
  - Propuestas de mejoras en SAMM (*SAMM Enhancement Proposals - SEP)*

Planes a Futuro

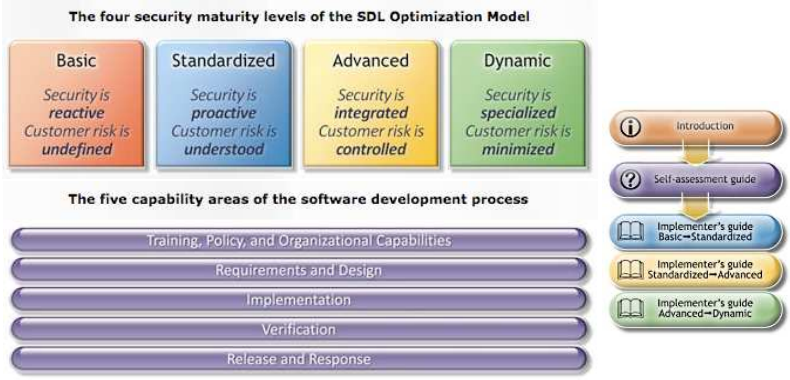
- Relacionarlo a regulaciones y estándares existentes (muchos en proceso actualmente)
  - PCI, COBIT, ISO-17799/27002, ISM3, etc.
- Planes de actuación adicionales donde se identifiquen necesidades.
- Incorporación de casos de estudio adicionales
- *Feedback* para refinamiendo del modelo
- Traducciones a otros lenguajes

Otros acercamientos 'modernos'

- Microsoft SDL Optimization Model
- Fortify/Cigital Building Security In Maturity Model (BSIMM)

SDL Optimization Model

- Hecho por MS para hacer la adopción de SDL más sencilla



BSIMM

- Framework derivado de la versión Beta de SAMM
- Basado en los datos recopilados de 9 grandes corporaciones

Governance	Intelligence	SSDL Touchpoints	Deployment
Strategy and Metrics	Attack Models	Architecture Analysis	Penetration Testing
Compliance and Policy	Security Features and Design	Code Review	Software Environment
Training	Standards and Requirements	Security Testing	Configuration Management and Vulnerability Manage-ment

Repaso sobre uso de SAMM

- Evaluar las prácticas de seguridad en el desarrollo de software existentes en una compañía.
- Definir un plan adaptado de mejora en la seguridad del software basado en iteraciones bien definidas.
- Cuantificar mejoras concretas durante la aplicación del plan de mejora en la seguridad.
- Definir y medir actividades relacionadas con la seguridad en una organización.

Involucrate!

- Utiliza SAMM y cuéntalo
  - Blog, email, etc.
- Las últimas novedades en http://www.opensamm.org
  - Inscríbete en la lista de correo
    - samm@lists.owasp.org

AppSec Latam 2011

- Dias de Entrenamiento 4 y 5 Octubre 2011
- Dias de Conferencia 6 y 7 Octubre 2011

SORPRESA
Sorteo de una entrada!!!

Preguntas y Respuestas

Queres contribuir o proveer feedback?

FCERULLO@OWASP.ORG

Gracias!

OWASP