

UNIVERSIDAD NACIONAL DE LA MATANZA



***Departamento de Ingeniería e Investigaciones
Tecnológicas***

Seguridad y Calidad en Aplicaciones Web

Unidad N° 6: Anexo SAMM

Fuente: OWASP Software Assurance Maturity Model
1.0, “Resumen ejecutivo” y “Entendiendo el modelo”



Creative Commons(CC) Attribution Share-Alike

Free version at <http://www.owasp.org>

Resumen Ejecutivo

El modelo de madurez para el aseguramiento de software (SAMM por sus siglas en inglés) es un marco de trabajo abierto para ayudar a las organizaciones a formular e implementar una estrategia de seguridad para Software que sea adecuada a las necesidades específicas que está enfrentando la organización. Los recursos proveídos por el SAMM ayudarán a:

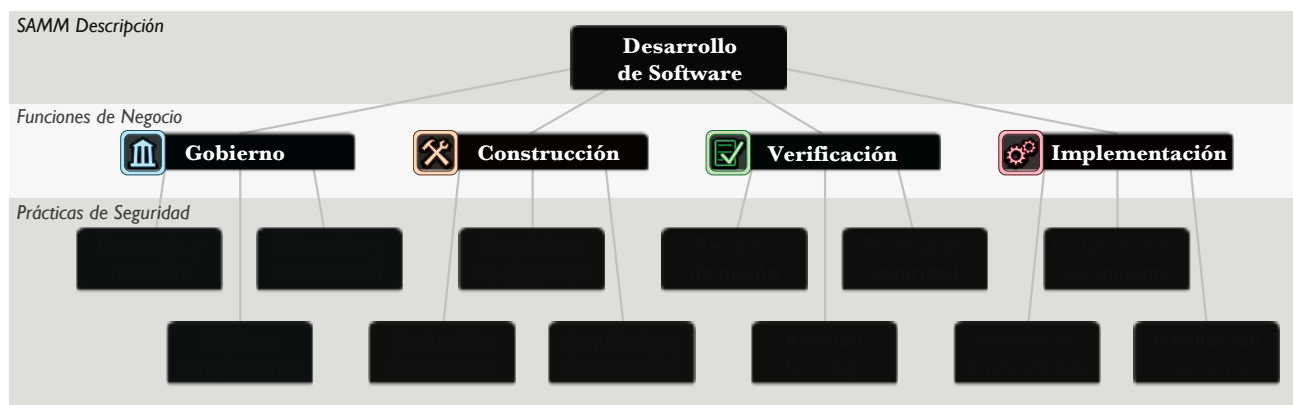
- ♦ *Evaluar las prácticas de seguridad en Software existentes en la organización*
- ♦ *Construir un programa de seguridad en Software balanceado en iteraciones bien definidas*
- ♦ *Demostrar mejoras concretas en el programa de aseguramiento de Software*
- ♦ *Definir y medir las actividades relacionadas con seguridad en la organización*

SAMM fue definido para ser flexible de manera que pueda ser utilizado por organizaciones pequeñas, medianas o grandes que utilicen cualquier estilo de desarrollo. Además, este modelo puede ser aplicado en toda la organización, en una sola línea de negocio o incluso en un proyecto en particular. Además de estos elementos, SAMM fue construido sobre los siguientes principios:

- ♦ *Cambios de comportamiento de una organización a través del tiempo.* Un programa de seguridad para Software exitoso debería ser creado en pequeños ciclos que entreguen ganancias tangibles en el aseguramiento de Software, al mismo tiempo, debe trabajar incrementalmente hacia metas de largo plazo.
- ♦ *No hay una sola receta que funcione para todas las organizaciones.* Un marco de seguridad en Software debe ser flexible y permitir a las organizaciones personalizar sus opciones basándose en su tolerancia a riesgo y la manera en la cual construye y usa el Software.
- ♦ *Los lineamientos relacionados a las actividades de seguridad deben ser específicos.* Todos los pasos en la construcción y medición del programa de aseguramiento deben ser simples, bien definidos y medibles. Este modelo también provee plantillas de planes de implementación para tipos comunes de organizaciones.

Las bases de este modelo están construidas alrededor de las funciones de negocio relacionadas al desarrollo de Software, se incluyen una serie de prácticas relacionadas a cada función (vea el diagrama abajo). Los bloques de construcción del modelo son los tres niveles de madurez definidos para cada una de las doce prácticas de seguridad. Estas definen una amplia variedad de actividades a las que una organización se puede adherir para reducir los riesgos de seguridad e incrementar el aseguramiento del Software. Se incluyen detalles adicionales para medir el desempeño exitoso de las actividades, entender los beneficios del aseguramiento asociado, estimar los costos de personal y otros costos.

Dado que SAMM es un proyecto abierto, el contenido se puede mantener siempre independiente de los vendedores y disponible libremente para que todo mundo lo use.



Funciones de Negocio

Al nivel más alto, SAMM define cuatro funciones de negocio importantes. Cada función de negocio (listada abajo) es una categoría de actividades relacionadas a las tareas específicas del desarrollo de software, dicho de otra manera, cualquier organización involucrada en el desarrollo de Software debe cumplir con cada una de esas funciones en cierto grado.

Para cada función de negocio, SAMM define tres prácticas de seguridad. Cada práctica de seguridad (listada al opuesto) es un área de actividades de seguridad que construyen las actividades de aseguramiento para las funciones de negocio relacionadas. Así que, en términos generales hay doce prácticas de seguridad que son las áreas de oportunidad a mejorar y comparar contra la funciones de desarrollo de Software del negocio.

Para cada práctica de seguridad, SAMM define tres niveles de madurez como objetivos. Cada nivel en las prácticas de seguridad esta caracterizado por un objetivo sucesivamente más sofisticado, definido por actividades específicas y mayores y mas exigente métricas de éxito que en el nivel anterior. Así mismo, cada práctica de seguridad puede ser mejorada independientemente, a través de actividades relacionadas que lleven a optimizaciones.



Gobierno

El gobierno de TI está enfocado en los procesos y actividades relacionadas a como una organización gestiona las actividades de desarrollo de software global. Más específicamente, esto incluye preocupaciones que atraviesan los grupos implicados en el desarrollo, así como procesos de negocio que son establecidos a nivel de organización.

...continúa en página 10



Construcción

Construcción se refiere a los procesos y actividades relacionados a como una organización define metas y crea software dentro de proyectos de desarrollo. En general, esto incluir la gestión de producto, reunión de requisitos de seguridad, especificación de arquitectura de alto nivel, diseño detallado e implementación.

...continúa en página 12



Verificación

La verificación está enfocada en los procesos y actividades relacionadas a como una organización verifica y prueba artefactos producidos a través del desarrollo de Software. Esto típicamente incluye un trabajo de aseguramiento de calidad como lo son las pruebas, pero esto puede también incluir otras revisiones y actividades de evaluación.

...continúa en página 14



Implementación

La implementación abarca los procesos y actividades relacionadas con la forma en que una organización administra la liberación de sistemas que han sido creados. Esto puede incluir el envío de productos a los usuarios finales, la instalación de los productos en ambientes internos o externos, y las operaciones normales de los sistemas en un ambiente de ejecución.

...continúa en página 16

Estrategia y métricas involucra la dirección estratégica global del programa de aseguramiento de software e instrumentación de procesos y actividades para recolectar métricas acerca de la postura de seguridad de una organización.

Política y cumplimiento involucra establecer una estructura de control y auditoría para seguridad y cumplimiento de regulaciones a lo largo de una organización para alcanzar un aseguramiento superior en software bajo construcción y en operación.

Educación y orientación involucra incrementar el conocimiento de seguridad entre el personal de desarrollo de software a través de entrenamiento y orientación en temas de seguridad pertinentes a funciones del trabajo individual.

Evaluación de amenazas involucra identificar y caracterizar con precisión los ataques potenciales contra el software de una organización, con el fin de comprender mejor los riesgos y facilitar su gestión.

Requisitos de seguridad involucra promover la inclusión de las necesidades de seguridad durante el proceso de desarrollo de software a fin de especificar la funcionalidad correcta desde el principio.

Arquitectura de seguridad implica el fortalecimiento del proceso de diseño con actividades para promover diseños con seguridad en mente y los marcos de trabajo en que se basa el software.

Revisión de diseño involucra la inspección de artefactos creados a partir del proceso de diseño para asegurar la provisión de mecanismos de seguridad adecuados y apegados a las expectativas de seguridad de la organización

Revisión de código involucra la evaluación del código fuente de una organización para ayudar en el descubrimiento de vulnerabilidades y actividades relacionadas a la mitigación como es el establecimiento de bases para las expectativas de la seguridad en programación.

Pruebas de seguridad involucra probar el software de la organización en su ambiente de ejecución para descubrir vulnerabilidades y establecer un estándar mínimo para la liberación del software.

Administración de vulnerabilidades involucra establecer procesos consistentes para administrar reportes internos o externos de vulnerabilidades para limitar la exposición, recopilar datos y así mejorar el programa de aseguramiento.

Fortalecimiento de ambientes implica la implementación de controles para el ambiente operativo que rodea a los programas de una organización para reforzar la postura de seguridad de las aplicaciones que han sido implementadas.

Habilitación operativa implica identificar y capturar información relevante a la seguridad que necesita un operador para configurar, instalar y correr los programas de una organización.

Niveles de Madurez

Cada una de las prácticas de seguridad tiene tres niveles de madurez bien definidos y un nivel inicial (cero) implícito. Los detalles de cada nivel difieren entre las prácticas pero generalmente representan:

- 0** Punto de inicio implícito, las actividades en la práctica no se han realizado
- 1** Entendimiento inicial y provisión ad hoc de la práctica de seguridad
- 2** Incremento en la eficiencia y/o efectividad de la práctica de seguridad
- 3** Dominio amplio de la práctica de seguridad

Notación

A través de este documento, los siguientes términos en mayúsculas se utilizarán como palabras reservadas que se refieren a los componentes del SAMM definidos en esta sesión. Si los términos aparecen sin mayúsculas, deben ser interpretados de acuerdo a el contexto en el que se encuentren:

- ◆ Función de Negocio también nombrado Función
- ◆ Práctica de Seguridad también nombrada Práctica
- ◆ Nivel de Madurez también nombrado como Nivel u Objetivo

Gobierno

Descripción de prácticas de seguridad



Estrategia y métricas

La práctica de estrategia y métricas (SM por sus siglas en Inglés) está enfocada en establecer la estructura dentro de una organización para un programa de aseguramiento de software. Este es el paso más fundamental en la definición de objetivos de seguridad de una forma que sea medible y alineada con los riesgos de negocio reales de la organización. Al iniciar con perfiles de riesgo sencillos, una organización aumenta con el tiempo sus esquemas de clasificación de riesgos para aplicación y activos de datos. Con una perspectiva adicional sobre las medidas de riesgo relativo, una organización puede ajustar sus objetivos de seguridad a nivel de proyecto y elaborar planes de implementación granulares para que el programa de seguridad sea más eficiente. En los niveles más avanzados en esta práctica, una organización se basa en muchas fuentes de datos, tanto internos como externos, para recolectar métricas y retroalimentación cualitativa acerca del programa de seguridad. Esto permite un ajuste fino de la relación costo-beneficio a nivel del programa.



Política y cumplimiento

La práctica de Política y Cumplimiento (PC por sus siglas en Inglés) está enfocada en comprender y cumplir con requisitos externos legales y regulatorios, además de implementar estándares de seguridad internos para asegurar el cumplimiento regulatorio de una manera que está alineada con los objetivos de negocio de la organización. Un tema importante a mejorar dentro de esta práctica es enfocarse en auditorías a nivel proyecto que reúnan información acerca del comportamiento de la organización para comprobar que las expectativas se están cumpliendo. Al introducir auditorías de rutina que comiencen sencillamente y crezcan en profundidad con el tiempo, el cambio organizacional es alcanzado de forma iterativa. De una forma sofisticada, la prestación de esta práctica implica entendimiento organizacional de estándares internos y cumplimientos externos y al mismo tiempo mantiene las aprobaciones de baja latencia con equipos de proyecto para asegurar que ningún proyecto esté operando fuera de las expectativas y sin visibilidad.



Educación y orientación

La práctica de educación y orientación (EG por sus siglas en Inglés) está enfocada en el personal involucrado en el ciclo de vida de software con conocimiento y recursos para diseñar, desarrollar e implementar software seguro. Con acceso mejorado a la información, los equipos de proyecto estarán en mejores condiciones de para identificar proactivamente y mitigar los riesgos de seguridad específicos que apliquen para su organización. Un tema importante para la mejora a través de los objetivos es proporcionar entrenamiento para los empleados, ya sea con sesiones basadas en instructores o módulos basados en computadora. Conforme una organización progresa, una gran cantidad de entrenamiento es construido al empezar con los desarrolladores y moverse a otros roles en la organización, culminando con la adición de certificación basada en roles para asegurar la comprensión del material. Además del entrenamiento, esta práctica también requiere convertir información relevante a seguridad en lineamientos que sirvan como información de referencia para el personal. Esto construye un cimiento para establecer una expectativa base para las prácticas de seguridad en la organización, y después permite la mejora incremental una vez que el uso de los lineamientos ha sido adoptado.

Gobierno

Resumen de actividades

Estrategia y métricas

...continúa en página 34



OBJETIVOS

Establecer un plan estratégico unificado para la seguridad del software dentro de la organización

Medir el valor relativo de los datos y bienes, y elegir la tolerancia al riesgo

Alinear los gastos de seguridad con indicadores de negocio pertinentes y el valor de los activos

ACTIVIDADES

- A. Estimar el perfil global de riesgo del negocio
- B. Crear y mantener un plan de implementación para el programa de aseguramiento

- A. Clasificar datos y aplicaciones basado en riesgo de negocio
- B. Establecer y medir los objetivos de seguridad por cada clasificación

- A. Realizar comparaciones de costo periódicas a nivel industria
- B. Recolectar métricas históricas de gastos de seguridad

Política y cumplimiento

...continúa en página 38



OBJETIVOS

Entender los motivos relevantes para el gobierno de TI y cumplimiento de regulaciones para la organización

Establecer base de seguridad y cumplimiento, y entender los riesgos por proyecto

Exigir cumplimiento de regulaciones y medir a los proyectos conforme a las políticas y estándares de la organización

ACTIVIDADES

- A. Identificar y monitorear los indicadores externos de cumplimiento
- B. Crear y mantener lineamientos de cumplimiento

- A. Crear políticas y estándares para seguridad y cumplimiento
- B. Establecer la práctica de auditoría de proyecto

- A. Crear puntos de control de cumplimiento para proyectos
- B. Adoptar una solución para la recolección de datos de auditoría

Educación y orientación

...continúa en página 42



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

Construcción

Descripción de prácticas de seguridad



Evaluación de amenaza

La Práctica de Evaluación de Amenazas (TA por sus siglas en inglés) se centra en la identificación y comprensión de los riesgos a nivel de proyecto, basándose en la funcionalidad del software a desarrollar y las características del entorno de ejecución. Desde los detalles de cada amenaza y los probables ataques contra cada proyecto, la organización en su conjunto opera más eficazmente por medio de mejores decisiones en la priorización de las iniciativas para la seguridad. Además, las decisiones de aceptación de riesgo son más informadas, y por lo tanto, mejor alineadas con el negocio. Al comenzar con modelados simples de amenaza y moverse a la creación de métodos más detallados de análisis de las amenazas y ponderación, la organización mejora con el tiempo. En última instancia, una organización sofisticada mantendría esta información estrechamente unida a los factores de compensación y de paso a los riesgos de las entidades externas. Esto proporciona una mayor amplitud de comprensión para los potenciales impactos debido a problemas de seguridad, mientras mantiene una estrecha vigilancia sobre el desempeño actual de la organización contra las amenazas conocidas.



Requisitos de seguridad

La Práctica de Requisitos de Seguridad (SR por sus siglas en inglés) se centra en especificar proactivamente el comportamiento esperado del software con respecto a la seguridad. A través de la adición de las actividades de análisis a nivel de proyecto, los requisitos de seguridad se reúnen inicialmente basándose en el objetivo comercial del software. Conforme avanza una organización, se utilizan técnicas más avanzadas como las especificaciones de control de acceso para descubrir nuevos requisitos de seguridad que pueden no haber sido evidentes inicialmente para el desarrollo. En una forma sofisticada, la prestación de esta Práctica implica meter los requisitos de seguridad de la organización dentro de sus relaciones con los proveedores y luego auditar los proyectos para asegurar que todos se adhieren a las expectativas, respecto a la especificación de los requisitos de seguridad.



Arquitectura de seguridad




La Práctica de Arquitectura de Seguridad (SA por sus siglas en inglés) se centra en medidas proactivas para una organización para diseñar y construir software seguro por defecto. Al mejorar el proceso de diseño de software con servicios y componentes reutilizables, el riesgo de seguridad global de desarrollo de software puede ser dramáticamente reducido. A partir de simples recomendaciones sobre los marcos de software y la consideración explícita de los principios de diseño seguro, una organización que evoluciona hacia el uso consistente de patrones de diseño para la funcionalidad de seguridad. Además, las actividades animan a los equipos de proyecto a una mayor utilización de los servicios de seguridad centralizados y de infraestructura. Como una organización que evoluciona con el tiempo, el suministro sofisticado de esta Práctica implica organizaciones construyendo plataformas de referencia para cubrir los tipos genéricos de software que construyen. Estos sirven como marcos en los que los desarrolladores pueden crear software a medida con menor riesgo de vulnerabilidad.

Construcción

Resumen de actividades




Evaluación de amenaza

...continúa en página 46

	 TA 1	 TA 2	 TA 3
OBJETIVOS	Identificar y comprender las amenazas de alto nivel para la organización y los proyectos individuales	Aumentar la precisión de la evaluación de amenazas y mejorar la granularidad de la comprensión por proyecto	Comparar concretamente controles de compensación a cada amenaza contra el software interno y de terceros
ACTIVIDADES	<p>A. Desarrollar y mantener modelos de amenaza específicos a cada aplicación</p> <p>B. Elabore perfil de atacante desde la arquitectura de software</p>	<p>A. Desarrollar y mantener modelos de casos de abuso por proyecto</p> <p>B. Adoptar un sistema de ponderación para la medición de las amenazas</p>	<p>A. Evaluar explícitamente el riesgo de los componentes de terceros</p> <p>B. Elaboración de modelos de amenaza con controles de compensación</p>




Requisitos de seguridad

...continúa en página 50

	 SR 1	 SR 2	 SR 3
OBJETIVOS	Considerar explícitamente la seguridad durante el procesamiento de captura de requisitos de software	Aumentar la granularidad de los requisitos de seguridad derivados de la lógica de negocio y riesgos conocidos	Exigir que se siga el proceso de requisitos de seguridad para todos los proyectos de software y dependencias de terceros
ACTIVIDADES	<p>A. Deducir los requisitos de seguridad a partir de la funcionalidad de negocios</p> <p>B. Evaluar la seguridad y los lineamientos de cumplimiento para regulaciones de los requisitos</p>	<p>A. Generar una matriz de control de acceso a los recursos y capacidades</p> <p>B. Especificar los requisitos de seguridad en base a los riesgos conocidos</p>	<p>A. Incorporar los requisitos de seguridad a acuerdos con proveedores</p> <p>B. Ampliar el programa de auditoría para los requisitos de seguridad</p>

Arquitectura de seguridad

...continúa en página 54

	 SA 1	 SA 2	 SA 3
OBJETIVOS	Insertar consideraciones para lineamientos proactivos de seguridad en el proceso de diseño de software	Dirija el proceso de diseño de software hacia servicios seguros conocidos y diseños seguros desde la concepción	Controlar formalmente el proceso de diseño de software y validar la utilización de componentes de seguridad
ACTIVIDADES	<p>A. Mantener una lista de los marcos de trabajo de software recomendados</p> <p>B. Aplicar explícitamente los principios de seguridad para el diseño</p>	<p>A. Identificar y promover los servicios de seguridad e infraestructura</p> <p>B. Identificar los patrones de diseño de seguridad desde la arquitectura</p>	<p>A. Establecer arquitecturas y plataformas formales de referencia</p> <p>B. Validar el uso de marcos de trabajo, patrones, y plataformas</p>

Verificación

Descripción de prácticas de seguridad



Revisión de diseño

La Práctica de Revisión de Diseño (DR por sus siglas en inglés) está enfocada en evaluar el diseño de software y arquitectura en busca de problemas relacionados a la seguridad. Esto permite a una organización el detectar problemas de arquitectura a principios del desarrollo de software, de esta manera, evitar grandes costos potenciales de re-trabajar después por cuestiones de seguridad. Comenzando con las actividades ligeras para construir un entendimiento de los detalles relevantes de la seguridad de una arquitectura, una organización evoluciona hacia una inspección más formal de los métodos que verifiquen la integridad en la provisión de mecanismos de seguridad. A nivel organización, los servicios de revisión de diseño son construidos y ofrecidos a los interesados. En una forma sofisticada, proveer esta práctica involucra una inspección de diseños detallada, a nivel de datos y la aplicación de las bases esperadas para conducir una evaluación de diseño y revisión de fallos antes de que el código sean aceptado.



Revisión de código

La Práctica de revisión de código (CR por sus siglas en inglés) está enfocada en inspeccionar software al nivel de código fuente para encontrar vulnerabilidades de seguridad. Las vulnerabilidades a nivel de código son generalmente sencillas de entender. Pero incluso desarrolladores informados pueden fácilmente cometer errores que dejan el software abierto a un compromiso potencial. Para empezar, una organización usa listas de verificación sencillas y, por eficiencia, solo inspecciona los módulos más críticos del software. Sin embargo, conforme una organización evoluciona, utiliza la tecnología de automatización para mejorar dramáticamente la cobertura y la eficacia de las actividades de revisión de código. Una sofisticada disposición de esta Práctica involucra una integración más profunda de la revisión de código en el proceso de desarrollo para permitir equipos de proyecto encontrar problemas antes. Esto también permite a las organizaciones una mejor auditoria y conjunto de expectativas para los resultados de la revisión de código antes de que pueda hacerse la liberación del código.



Pruebas de seguridad

La Práctica de Prueba de Seguridad (ST por sus siglas en inglés) está enfocada en la inspección de software en el ambiente de ejecución con el fin de encontrar problemas de seguridad. Estas actividades de pruebas refuerzan los casos de seguro para software verificándolo en el mismo contexto en el cual se espera será ejecutado, así hace visible las malas configuraciones operacionales o errores en la lógica de negocio que son difíciles de encontrar de otra manera. Empezando con una prueba de intrusión y casos de prueba a alto nivel basados en la funcionalidad del software, una organización evoluciona hacia el uso de pruebas de seguridad automatizadas para cubrir la amplia variedad de casos de prueba que podrían demostrar una vulnerabilidad en el sistema. En una forma avanzada, el ofrecer esta Práctica implica la personalización de las pruebas automatizadas para construir una serie de pruebas de seguridad que cubran a detalle las preocupaciones específicas sobre la aplicación. Con una visibilidad adicional a nivel organización, las pruebas de seguridad permiten a las organizaciones establecer las expectativas mínimas para los resultados de las pruebas de seguridad antes que la liberación de un proyecto sea aceptada.

Verificación

Resumen de actividades

Revisión de diseño

...continúa en página 58



OBJETIVOS

Apoyar en las revisiones de diseño de software para asegurarse que existan los lineamientos de mitigación para riesgos conocidos

Ofrecer evaluaciones de servicios para revisar el diseño del software contra buenas prácticas integrales de seguridad

Exija evaluar y valide los artefactos para desarrollar un entendimiento detallado de mecanismos de protección

ACTIVIDADES

A. Identificar superficies de ataques de software
B. Analizar el diseño contra requisitos de seguridad conocidos

A. Inspeccionar por completo la provisión de los mecanismos de seguridad
B. Implementar el servicio de revisión de diseño para los equipos de proyecto

A. Desarrollar diagrama de flujo de datos para recursos sensible
B. Establecer puntos de liberación para la revisión de diseño

Revisión de código

...continúa en página 62



OBJETIVOS

Encontrar oportunamente vulnerabilidades básicas a nivel de código y otros problemas de seguridad de alto riesgo

Hacer revisiones de código más precisas y eficientes durante el desarrollo a través de la automatización

Exigir un proceso de revisión de código integral para descubrir riesgos específicos de la aplicación y a nivel del lenguaje

ACTIVIDADES

A. Crear listas de verificación para la revisión de los requisitos de seguridad conocidos
B. Realizar revisiones en código de puntos de alto riesgo

A. Utilizar herramientas automatizadas de análisis de código
B. Integrar análisis de código en el proceso de desarrollo

A. Personalizar el análisis de código para las preocupaciones específicas de la aplicación
B. Establecer puntos de control para la liberación de las revisiones de código

Pruebas de seguridad

...continúa en página 66



OBJETIVOS

Establecer el proceso para realizar pruebas de seguridad basándose en la implementación y los requisitos del software

Hacer pruebas de seguridad durante el desarrollo, más completas y eficientes a través de la automatización

Exigir pruebas de seguridad específicas a la aplicación para asegurarse que los lineamientos de seguridad están implementados antes de la publicación

ACTIVIDADES

A. Deducir casos de prueba desde los requisitos de seguridad conocidos
B. Conducir pruebas de intrusión en cada publicación del software

A. Utilizar herramientas automatizadas para pruebas de seguridad
B. Integrar pruebas de seguridad en el proceso de desarrollo

A. Emplear automatización de pruebas de seguridad específicas de la aplicación
B. Establecer puntos de control para la liberación de las revisiones de código

Implementación

Descripción de prácticas de seguridad



Administración de vulnerabilidades

La práctica de administración de vulnerabilidades (AV por sus siglas en Inglés) está enfocada en los procesos de una organización con respecto al manejo de reportes de vulnerabilidades e incidentes operativos. Al tener estos procesos establecidos, los proyectos de una organización tendrán expectativas consistentes y una mayor eficiencia para manejar estos eventos, en lugar de respuestas caóticas y sin uniformidad. Empezando con la asignación de roles en caso de un incidente, una organización genera un proceso de respuesta a incidentes más formal, que asegura la visibilidad y el seguimiento de los problemas que ocurran. Las comunicaciones también se mejoran para mejorar el entendimiento global de los procesos.

De forma avanzada, la administración de vulnerabilidades implica una disección completa de los incidentes y los reportes de vulnerabilidades para obtener métricas detalladas e información sobre las causas raíz para proveer retroalimentación al comportamiento de la organización.



Fortalecimiento del ambiente

La práctica de reforzamiento de ambientes (EA por sus siglas en Inglés) se enfoca en construir el aseguramiento del ambiente de ejecución que alberga los programas de la organización. Debido a que la operación segura de una aplicación se puede deteriorar por problemas en componentes externos, asegurar esta infraestructura base directamente mejora la postura de seguridad general del programa. Empezando con un simple seguimiento y distribución de información sobre el ambiente operativo para mantener mejor informados a los equipos de desarrollo, una organización evoluciona a métodos escalables para administrar la instalación de parches de seguridad y equipar el ambiente operativo con detectores tempranos de potenciales problemas de seguridad antes de que el daño se materialice. Conforme una organización avanza, el ambiente operativo se revisa y se refuerza con la instalación de herramientas de producción para agregar capas de defensa y redes de seguridad para limitar el daño en caso de que alguna vulnerabilidad sea explotada.



Habilitación operativa

La práctica de habilitación de operativa (HO por sus siglas en Inglés) se enfoca en la recolección de información crítica de seguridad de los equipos de proyectos que construyen programas y en comunicar esta información a los usuarios y operadores del programa. Sin esta información, aún el programa diseñado más seguramente corre riesgos no planeados, ya que algunas características importantes y opciones de seguridad no serán conocidas en el sitio de publicación. Empezando con documentación preliminar para capturar los detalles más impactantes para los usuarios y operadores, una organización evoluciona hacia la construcción de guías completas de seguridad de operaciones que se entregan con cada distribución.




De forma avanzada, la habilitación de las operaciones también comprende pruebas a nivel organización para cada uno de los equipos de proyecto, esto, para asegurar que la información sea capturada y compartida de acuerdo a las expectativas.

Implementación

Resumen de actividades




Administración de vulnerabilidades

...continúa en página 70

	 VM 1	 VM 2	 VM 3
OBJETIVOS	Entender el plan de alto nivel para responder a los reportes o incidentes de vulnerabilidades	Elaborar expectativas para prácticas de respuesta para mejorar la consistencia y las comunicaciones	Mejorar en análisis y la colección de datos en el proceso de respuesta para retroalimentación en la planeación proactiva
ACTIVIDADES	<ul style="list-style-type: none"> A. Identificar un punto de contacto para problemas de seguridad B. Crear equipo(s) informal(es) de respuesta de seguridad 	<ul style="list-style-type: none"> A. Establecer un proceso consistente de respuesta a incidentes B. Adoptar un proceso de divulgación de problemas de seguridad 	<ul style="list-style-type: none"> A. Conducir análisis de causa raíz para incidentes B. Recolectar métricas por incidente




Fortalecimiento del ambiente

...continúa en página 74

	 EH 1	 EH 2	 EH 3
OBJETIVOS	Entender el ambiente operativo base para aplicaciones y componentes de sistemas	Mejorar la confianza en las operaciones de aplicaciones al reforzar el ambiente operativo.	Validar la salud de las aplicaciones y el estado de los ambientes operativos contra las mejores prácticas conocidas.
ACTIVIDADES	<ul style="list-style-type: none"> A. Mantener una especificación de ambiente operativo B. Identificar e instalar actualizaciones y parches críticos de seguridad 	<ul style="list-style-type: none"> A. Establecer un proceso rutinario de administración de parches B. Monitoreo del estado de configuración básico del ambiente 	<ul style="list-style-type: none"> A. Identificar e implementar herramientas de protección relevantes para las operaciones B. Expandir el programa de auditoría hacia la configuración de ambientes

Habilitación operativa

...continúa en página 78

	 OE 1	 OE 2	 OE 3
OBJETIVOS	Habilitar las comunicaciones entre los equipos de desarrollo y los operadores para datos críticos relevantes a seguridad	Mejorar las expectativas de operaciones seguras y continuas al proveer procedimientos detallados	Exigir la comunicación de información sobre seguridad y validar que los artefactos estén completos
ACTIVIDADES	<ul style="list-style-type: none"> A. Capturar la información de seguridad crítica para el ambiente de publicación B. Documentar procedimientos para alertas de aplicación típicas 	<ul style="list-style-type: none"> A. Crear procedimientos de administración de cambio por distribución B. Mantener guías formales de seguridad de operaciones 	<ul style="list-style-type: none"> A. Expandir el programa de auditoría para información operativa B. Realizar firma de código para componentes de aplicaciones