Reconocimiento-CompartirIgual 3.0
España (CC BY-SA 3.0 ES)

Análisis y gestión del riesgo

Caso práctico 1: Nivel de madurez de un equipo de desarrollo

Marta Beltrán Pardo

©2023 Marta Beltrán URJC (marta.beltran@urjc.es)
Algunos derechos reservados.
Este documento se distribuye bajo la licencia "Reconocimiento-CompartirIgual 3.0 España" de Creative Commons, disponible en
https://creativecommons.org/licenses/by-sa/3.0/es/

Contenidos

©2023 Marta Beltrán URJC (marta.beltran@urjc.es)
Algunos derechos reservados.
Este documento se distribuye bajo la licencia "Reconocimiento-CompartirIgual 3.0 España" de Creative Commons, disponible en
https://creativecommons.org/licenses/by-sa/3.0/es/

1. Introducción

Para la realización de este caso práctico todos los miembros del equipo vais a asumir el mismo rol: responsable de seguridad de producto.

Hace poco tiempo que habéis comenzado a trabajar en la empresa ChaseMyCash y, de momento, habéis decidido intentar que el desarrollo del producto siga prácticas de DevSecOps.

Para estandarizar el trabajo del equipo de desarrollo os han pedido que tracéis un plan para los primeros 6 meses que comience por 15 prácticas o controles de seguridad, ya que hasta el momento no se había realizado ninguna actividad explícita en relación con la seguridad de la aplicación ChaseMyCash.

Vuestra idea es proponer un modelo de madurez del equipo de desarrollo que permita reducir el número de vulnerabilidades de la aplicación ChaseMyCash y por lo tanto, el ciberriesgo asociado al producto.

©2023 Marta Beltrán URJC (marta.beltran@urjc.es)
Algunos derechos reservados.
Este documento se distribuye bajo la licencia "Reconocimiento-CompartirIgual 3.0 España" de Creative Commons, disponible en
https://creativecommons.org/licenses/by-sa/3.0/es/

2. Material para la realización del caso

A continuación, se enumeran los materiales necesarios para la realización de esta práctica, que pueden descargarse desde el Aula Virtual:

- **Caso1_Guion.pdf**: este documento.
- **Dossier ChaseMyCash.pdf**: información sobre la empresa con la que vamos a trabajar en los casos y las prácticas.
- **Material sobre el OWASP DSOMM (os puede servir de ejemplo)**: https://owasp.org/www-project-devsecops-maturity-model/

©2023 Marta Beltrán URJC (marta.beltran@urjc.es)
Algunos derechos reservados.
Este documento se distribuye bajo la licencia "Reconocimiento-CompartirIgual 3.0 España" de Creative Commons, disponible en
https://creativecommons.org/licenses/by-sa/3.0/es/

3. Normativa y evaluación

En este apartado se detalla el formato de entrega del caso y la forma en la que se evaluará la misma:

- El porcentaje de la nota final de la asignatura al que corresponde esta práctica puede consultarse en la Guía docente de la propia asignatura.

- El caso deberá realizarse, de forma obligatoria en el aula el día indicado en el calendario de la asignatura en Aula Virtual, en grupos de cuatro personas. Para la asignación de los grupos se deberán seguir las indicaciones del profesor. Será necesario trabajar fuera del aula para terminar las tareas propuestas.

- Cada grupo deberá entregar una única memoria en formato pdf a través de Aula Virtual. La fecha límite para la entrega se avisará con tiempo suficiente.

- Esta memoria debe incluir, como mínimo, los entregables propuestos en el siguiente apartado.

©2023 Marta Beltrán URJC (marta.beltran@urjc.es)
Algunos derechos reservados.
Este documento se distribuye bajo la licencia "Reconocimiento-CompartirIgual 3.0 España" de Creative Commons, disponible en
https://creativecommons.org/licenses/by-sa/3.0/es/

4. Tareas y entregables

1. Debéis comprender bien el producto y cómo se desarrolla. También buscar prácticas o controles relacionados con DevSecOps y con ciclo de desarrollo seguro. A partir de ese momento, deberíais escoger las 15 prácticas o controles por los que pensáis que es mejor comenzar el proyecto de seguridad de producto e integrar en el CI/CD.

Entregable 1: Listado de 15 prácticas o controles y justificación de su elección.

2. Como el equipo de desarrollo todavía no está muy experimentado en temas de seguridad, les vais a preparar un modelo de madurez al estilo del C2M2, en el que para cada control de los 15 seleccionados propongáis una tabla con las actividades concretas que deben realizar para llegar al nivel 1, 2 ó 3 de madurez. Es decir, son necesarias explicaciones de manera que para cada control los desarrolladores comprendan cuándo cumplen y cuándo no, qué cambios tienen que hacer en su manera de trabajar para cumplir, cómo pueden comprobar si cumplen. Cuanto más específicas y concretas, más sencillo será para el equipo de desarrollo trabajar con este modelo de madurez.

Entregable 2: Modelo de madurez con las tablas explicativas para los 15 controles.

3. Para orientar al equipo de desarrollo en su trabajo, debéis indicar el punto de partida para cada control (en qué nivel de madurez está el equipo al comenzar el proyecto en relación con ese control) y el objetivo (a qué nivel de madurez se debería llegar pasados los primeros 6 meses).

Entregable 3: Punto de partida y nivel de madurez objetivo para cada control (junto con su justificación).

Sugerencia de organización. Se puede dedicar la sesión de 2 horas en el aula a escoger los 15 controles que incluirá vuestro CI/CD y a decidir los criterios para escogerlos. También para determinar el punto de partida y el nivel de madurez objetivo. Fuera del aula, se puede repartir el trabajo con los controles entre los miembros del grupo de manera que sólo sea necesario integrar las aportaciones de todos y revisar, unificar el lenguaje, etc.

©2023 Marta Beltrán URJC (marta.beltran@urjc.es)
Algunos derechos reservados.
Este documento se distribuye bajo la licencia "Reconocimiento-CompartirIgual 3.0 España" de Creative Commons, disponible en
https://creativecommons.org/licenses/by-sa/3.0/es/