Proceso de selección del contenido de la caja de herramientas de ciberseguridad

Descripción

La caja de herramientas de ciberseguridad de Global Cyber Alliance (GCA) es un recurso en línea que contiene multitud de herramientas gratuitas y eficaces que las organizaciones pueden empezar a utilizar hoy mismo para actuar de inmediato y reducir el ciberriesgo. Las organizaciones y los particulares pueden utilizar la caja de herramientas para evaluar su estrategia de seguridad, implementar herramientas gratuitas, encontrar consejos prácticos y acceder a recursos y guías gratuitos que les ayuden a mejorar la preparación y la respuesta en relación con la ciberseguridad. En GCA, sabemos que el recurso más eficaz de la caja de herramientas son las aplicaciones que contiene y nos esforzamos por seleccionar herramientas gratuitas esenciales y eficaces para ponerlas a disposición de nuestra comunidad.

En este documento se abordan las especificaciones y procedimientos que la GCA aplica a la hora de agregar una herramienta a cualquier versión de la caja de herramientas de ciberseguridad. También se incluye información sobre los factores que se tienen en cuenta a la hora de incluir una aplicación en la caja de herramientas o que establecen el motivo de su desestimación. El comité de control de cambios (CCB por sus siglas en inglés) puede revisar cualquier aplicación que ya forme parte de la caja de herramientas para determinar si sigue cumpliendo los criterios necesarios para permanecer en esa versión o si debe eliminarse no cumplir dichos criterios. El CCB también es el mecanismo que se utiliza para incorporar aplicaciones a la caja de herramientas cuando estas cumplen todos los requisitos que se indican en este documento.

Selección

De forma habitual, la GCA busca herramientas para incluirlas en sus cajas de herramientas, aunque también puede recibir sugerencias de las partes interesadas. Si una organización dispone de una aplicación que le gustaría que se incluyera en la caja de herramientas, puede enviar una solicitud para que la incorporemos. En esta solicitud, se le pedirán detalles concretos sobre la herramienta, además de referencias a controles críticos de CIS específicos que respalden su inclusión en las cajas de herramientas, como una descripción de su funcionalidad, el nivel de conocimientos de TI necesario y el tiempo requerido para configurarla y utilizarla. También puede solicitarse otro tipo de información adicional.

El objetivo de la GCA es incluir herramientas esenciales para implantar una buena "higiene informática". Para ello, seguimos el proceso que se describe más abajo. La GCA ha establecido cuatro fases que las herramientas deben pasar cuando se evalúa su incorporación a la caja de herramientas. Las herramientas semejantes se evaluarán comparando unas con otras, lo que puede provocar que se agreguen o eliminen varias herramientas con usos similares. En el diagrama siguiente y en la sección Mantenimiento continuo encontrará más información.

El tiempo necesario para el flujo de trabajo depende del uso y la aplicación de cada herramienta, que debe pasar por las siguientes fases:

1. PENDIENTE (lista de espera)

En la fase "Pendiente", comienza la fase de evaluación de las herramientas para determinar si se incluyen en la caja de herramientas. Es posible que estas herramientas ya hayan comenzado a analizarse, pero este estudio debe completarse antes de pasar a la fase de revisión. Para realizar este estudio, la GCA consultará a la comunidad (incluidos los grupos de asesoramiento), tendrá en cuenta las revisiones y análisis en línea, y realizará entrevistas en persona. Por ejemplo, durante este proceso, el personal del CCB de la caja de herramientas y la GCA comprobarán si las herramientas son gratuitas, si pueden abordar controles críticos específicos de la caja de herramientas, si tienen una valoración positiva en la comunidad de la GCA y si reciben actualizaciones o parches en los plazos indicados.

2. EN REVISIÓN

Una herramienta se considera "En revisión" una vez que se han realizado las comprobaciones iniciales de la fase "Pendiente" y se ha determinado que merece la pena valorar su inclusión. Se llevarán a cabo todas las diligencias necesarias, que pueden incluir la valoración de grupos de asesoramiento externos (representantes externos designados que tengan experiencia en el sector o en el campo informático de la caja de herramientas), conversaciones pormenorizadas con los proveedores y demostraciones, así como pruebas y análisis con el conjunto de aplicaciones actuales de la caja de herramientas. Una vez completada la revisión, la herramienta y las recomendaciones se presentarán al CCB interno de la GCA, que se reúne mensualmente, para su consideración. A continuación, si es necesario, la herramienta pasará a la etapa 3, que es una revisión externa, o directamente a la etapa 4 para su inclusión.

3. ENVIADO A UN GRUPO DE ASESORAMIENTO EXTERNO DE CAJAS DE HERRAMIENTAS PATROCINADAS

En el caso de las cajas de herramientas patrocinadas o coadministradas, es necesario que organizaciones y particulares externos aprueben y refrenden los productos votados por el CCB antes de su inclusión. Estas organizaciones y particulares serán representantes externos designados con experiencia en el sector o en el campo informático de cada caja de herramientas, y pueden incluir a los patrocinadores de la caja de herramientas. La GCA proporcionará información relevante al grupo, así como cualquier consideración o dato adicional que resulte necesario, y esperará a su aprobación. Una vez que se tenga su aprobación, la herramienta pasará a la fase final "Aprobada". Del mismo modo, si el comité de asesoramiento externo decide no aprobar la herramienta, esta puede permanecer en esta fase mientras se recopila más información o desestimarse de la selección, en función de los argumentos aportados por el grupo.

4. APROBADO

Aquellos productos que reciban el voto del comité de control de cambios y del grupo de asesoramiento externo para incluirse en la caja de herramientas se asignarán al administrador del sitio web para su ejecución.

Nota: el CCB y el grupo de asesoramiento externo pueden rechazar la herramienta propuesta en cualquier fase.

Selección inicial y revisión

Selección inicial

El CCB de la caja de herramientas selecciona las herramientas aplicando el proceso anterior y los factores que se describen a continuación.

Revisión

Las cajas de herramientas de la GCA están sujetas a continuas modificaciones en función de los comentarios que recibimos de diferentes comunidades, talleres y asesores, así como de la aparición de nuevas herramientas. Durante la fase de revisión, pueden tenerse en cuenta otras consideraciones, como los comentarios de los usuarios y la comunidad, el asesoramiento de proveedores externos (dado que pueden haberse producido cambios sustanciales en la herramienta o en sus términos) y la opinión de los grupos de asesoramiento y el propio personal de la GCA para garantizar en todo momento la idoneidad de estos recursos a la hora de combatir las amenazas.

Criterios para la inclusión de herramientas

El comité de asesoramiento externo y el CCB de la caja de herramientas tendrán en cuenta los siguientes criterios en el proceso de selección de herramientas:

Costo:
¿Esta herramienta es gratis? ¿Tiene alguna modalidad gratuita? ¿Se comercializa?

Tipo de herramienta:
¿Qué tipo de herramienta es y cómo se utiliza? ¿Es una herramienta de aprendizaje, una herramienta de terceros, un vídeo, una política, etc.?

Dificultad de uso:
¿Cuál es el nivel de experiencia en TI necesario para implementar y utilizar con éxito esta herramienta?
Nota: los comentarios de los usuarios seguirán teniéndose en cuenta en este criterio incluso después de incorporar una herramienta

Requisitos:
¿Qué sistemas operativos y/o extensiones son necesarios para que la herramienta funcione?

Duración de la instalación:
¿Cuánto tiempo se requiere para descargar e implementar la herramienta?

Acceso:
¿El usuario tiene que registrarse en algún momento para poder utilizar la herramienta? ¿Es una herramienta "plug and play"?

Limitaciones:
¿Cuál es el alcance de la oferta gratuita y existen limitaciones en el uso de la herramienta?

Controles y estándares:
¿Qué controles y estándares cumple esta herramienta tal y como está y qué medidas adicionales son necesarias para mejorarlos?

Amenazas:
¿Qué amenaza concreta aborda esta herramienta en la comunidad a la que está destinada?

Nivel de soporte que se proporciona con la herramienta:
¿Qué nivel de soporte obtiene el usuario con la versión gratuita de esta herramienta? ¿Existen otros niveles a los que puede tener acceso?

Idiomas:
¿En qué idiomas está disponible la herramienta para establecer el potencial geográfico de la base de usuarios? Cuantos más idiomas estén disponibles en la herramienta, mejor; sin embargo, la ausencia de otros idiomas no impedirá su inclusión. La idoneidad para las cajas de herramientas se valorará con independencia de la región o el público de destino.

Material de apoyo:
¿Hay alguna guía, vídeo, etc. que los usuarios puedan consultar para aumentar la eficiencia del uso de la herramienta?

Parches y actualizaciones:
¿Cómo se administran normalmente los parches de seguridad y las actualizaciones?
¿Requiere soporte técnico adicional?

Términos y condiciones (T&C):
¿Hay términos y condiciones asociados al uso de la herramienta?

Privacidad:
¿Cómo trata la herramienta los datos personales? ¿Cumple el RGPD?