

Processus de sélection d'un outil pour l'inclure dans la boîte à outils de cybersécurité

Présentation

La boîte à outils de cybersécurité de la Global Cyber Alliance (GCA) (la boîte à outils) est une ressource en ligne proposant de nombreux outils gratuits et efficaces que les entités peuvent commencer à utiliser dès maintenant pour réduire immédiatement leur cyber-risque. Les entités et les individus peuvent utiliser la boîte à outils pour évaluer leur niveau de sécurité, mettre en œuvre des outils gratuits et trouver des conseils pratiques, des ressources et des guides gratuits afin d'améliorer leur préparation et leurs défenses en matière de cybersécurité. La GCA reconnaît que les outils constituent la ressource la plus puissante de la boîte à outils. Elle s'efforce de choisir les outils gratuits les plus indispensables et les plus efficaces pour sa communauté.

Le présent document traite des spécifications et des procédures utilisées par la GCA lors de l'ajout d'un outil à une version de la boîte à outils de cybersécurité. Il fournit des détails sur l'inclusion d'un outil dans la boîte à outils ou sur la raison de son refus. Un outil actuellement inclus peut faire l'objet d'un examen pour vérifier qu'il répond toujours aux critères d'inclusion dans la version de la boîte à outils. Il peut également être supprimé par l'intermédiaire du comité de contrôle des changements de la boîte à outils si ces critères ne sont pas respectés. Ce comité prend également la décision d'ajouter des outils à la boîte à outils s'ils remplissent toutes les conditions décrites dans le présent document.

Sélection

La GCA recherche régulièrement des outils à inclure dans ses boîtes à outils et reçoit également des demandes par le biais des commentaires laissés par les parties prenantes. Une entité disposant d'un outil qu'elle souhaite ajouter à la boîte à outils peut également postuler en remplissant le formulaire de demande d'inclusion dans la boîte à outils de cybersécurité de la GCA. Ce formulaire demande des détails spécifiques sur l'outil et fait référence à certains contrôles critiques du CIS permettant la prise en charge de l'inclusion dans les boîtes à outils : une description de la fonctionnalité, le niveau de connaissances informatiques requis et la durée nécessaire à la configuration et/ou l'utilisation de l'outil. Des renseignements supplémentaires peuvent également être demandés.

L'objectif de la GCA est d'inclure des outils indispensables à la mise en œuvre d'une cyber-hygiène. Pour y parvenir, la GCA a mis en place quatre étapes par lesquelles les outils doivent passer pour être ajoutés à la boîte à outils. Les outils en lice sont évalués les uns par rapport aux autres, ce qui peut entraîner l'inclusion de plusieurs outils ayant la même utilisation, ou la suppression d'outils. Pour plus d'informations à ce sujet, consultez le diagramme ci-dessous et la section Maintenance en cours.

La durée nécessaire au processus dépend de l'utilisation et de la demande de chaque outil, qui passe par les étapes suivantes :

1. EN ATTENTE (Liste d'attente)

Les outils « en attente » sont pris en considération en vue de leur inclusion dans la boîte à outils. Les recherches sur les outils peuvent avoir commencé et doivent être terminées avant le début de l'examen. Ces recherches incluent une consultation avec la communauté (notamment nos groupes consultatifs), la prise en compte des examens et des analyses en ligne, et les examens réalisés en personne par la GCA. Par exemple, dans le cadre du processus, le comité de contrôle des changements de la boîte à outils et le personnel de la GCA déterminent si les outils sont gratuits, s'il s'avère qu'ils sont capables de satisfaire à certains contrôles critiques pour une boîte à outils, s'ils ont reçu des commentaires personnels positifs de la part de la communauté de la GCA, et s'il s'avère qu'ils peuvent recevoir des correctifs/mises à jour en temps opportun.

2. À L'ÉTUDE

Un outil est considéré comme étant « à l'étude » une fois que les vérifications requises ont été effectuées au cours de l'étape « En attente » et si l'on estime qu'il est utile de poursuivre son inclusion. D'autres vérifications préalables sont effectuées, qui peuvent intégrer les commentaires des groupes consultatifs externes (représentants externes nommés ayant une connaissance approfondie en cybersécurité/sur le secteur pour chaque boîte à outils), les discussions approfondies avec les fournisseurs, les démonstrations et les tests et analyses avec l'outil de la boîte à outils actuellement examiné. Une fois l'examen terminé, l'outil et les recommandations sont présentés en vue de leur examen au comité interne de contrôle des changements de la GCA, qui se réunit tous les mois. Si nécessaire, l'outil passe à l'étape 3 pour subir un examen externe, ou directement à l'étape 4 pour être inclus.

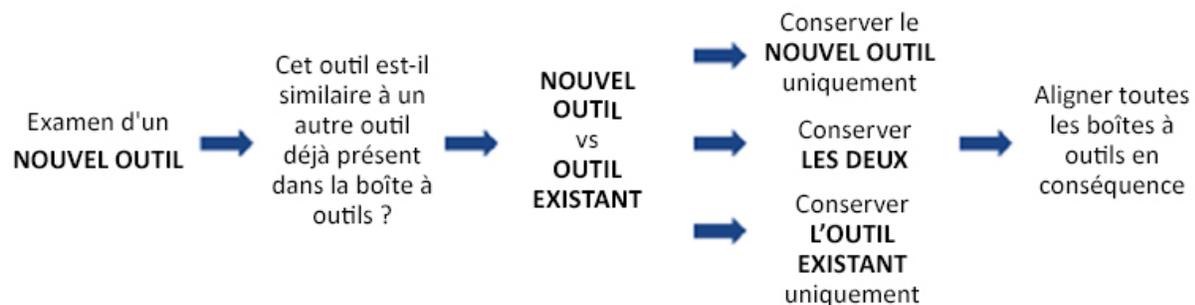
3. SOUMIS AU GROUPE CONSULTATIF EXTERNE POUR LES BOÎTES À OUTILS SPONSORISÉES

Pour les boîtes à outils sponsorisées ou co-gérées, les outils faisant l'objet d'un vote pour inclusion par le comité doivent être approuvés par des entités/individus externes à la GCA avant d'être inclus. Ces représentants externes nommés ayant des connaissances approfondies en cybersécurité/sur le secteur pour chaque boîte à outils incluent les sponsors des boîtes à outils. La GCA fournit des renseignements pertinents au groupe ainsi que toute information ou tout commentaire nécessaire, puis attend son approbation. Une fois l'approbation finale reçue, l'outil passe à l'étape finale « Approuvé ». De même, si le comité consultatif externe ne donne pas son approbation, un outil peut rester à cette étape pour pouvoir collecter des informations supplémentaires ou pour être retiré de la sélection, selon le raisonnement du groupe.

4. APPROUVÉ

Les outils qui ont fait l'objet d'un vote par le comité de contrôle des changements et le groupe consultatif externe (le cas échéant) pour être inclus dans une boîte à outils sont affectés au gestionnaire du site web pour être mis en place.

Remarque : l'outil proposé peut être rejeté à n'importe quelle étape du processus par le comité de contrôle des changements ou le groupe consultatif externe.



Sélection initiale et examen

Sélection initiale

Les outils sont sélectionnés par le comité de contrôle des changements de la boîte à outils en utilisant le processus ci-dessus et en appliquant les facteurs décrits ci-dessous.

Examen

Les boîtes à outils de la GCA évoluent continuellement en se basant sur les commentaires que nous recevons des différentes communautés, ateliers et consultants, ainsi que sur l'émergence de nouveaux outils. Un examen ultérieur peut prendre en compte d'autres éléments, notamment : les commentaires des utilisateurs et de la communauté, les conseils des fournisseurs tiers (lorsqu'une modification a été apportée à l'outil ou à ses conditions de service), et les contributions des groupes consultatifs de la GCA et du personnel de la GCA qui garantissent que l'outil est toujours pertinent dans le contexte des menaces.

Critères d'inclusion d'un outil

Le comité consultatif externe et le comité de contrôle des changements de la boîte à outils tiennent compte des critères suivants dans le processus de sélection des outils :

Coût :

Cet outil est-il gratuit ? Propose-t-il un niveau gratuit ? Est-il commercial ?

Type d'outil :

Quel est le nom de l'outil et comment sera-t-il utilisé ? Est-ce un outil pédagogique, un outil tiers, une vidéo, une politique, etc. ?

Difficulté d'utilisation :

Quel est le niveau de connaissance en informatique requis pour mettre en œuvre et exécuter correctement cet outil ? Remarque : même après l'inclusion d'un outil dans la boîte à outils, les commentaires des utilisateurs continueront de renseigner ce critère

Exigences :

Quels sont les systèmes d'exploitation et/ou extensions nécessaires à son fonctionnement ?

Durée de l'installation :

Quelle est la durée nécessaire au téléchargement et/ou à la mise en œuvre de l'outil ?

Accès :

L'utilisateur doit-il s'inscrire pour pouvoir utiliser l'outil ? L'outil est-il Plug-and-Play ?

Limitations :

Quelle est la durée de l'offre gratuite et son utilisation fait-elle l'objet de limitations ?

Contrôles et normes :

Quels sont les contrôles et les normes auxquels l'outil est conforme lorsqu'il est « prêt à l'emploi » et des étapes supplémentaires sont-elles nécessaires pour les renforcer ?

Menaces :

À quelle menace spécifique cet outil fait-il face pour la communauté en question ?

Niveau de support fourni avec l'outil :

Quel niveau de support un utilisateur obtient-il avec la version gratuite de cet outil et existe-t-il des niveaux de support supplémentaires auxquels un utilisateur peut avoir accès ?

Langues :

Dans quelles langues l'outil est-il disponible afin d'établir sa base d'utilisateurs géographique potentielle ? Plus les langues disponibles pour un outil sont nombreuses, mieux c'est. Notez toutefois que le peu de langues supplémentaires n'empêchera pas l'inclusion de l'outil. L'alignement des boîtes à outils, quel que soit le public visé ou la région, sera pris en compte.

Matériel de support :

Des guides et des vidéos de démonstration auxquels un utilisateur peut accéder pour mieux utiliser l'outil sont-ils disponibles ?



Correctifs et mises à jour :

De quelle manière les correctifs et les mises à jour de sécurité sont-ils normalement administrés et un support supplémentaire est-il nécessaire à ce titre ?

Conditions générales :

Existe-t-il des conditions générales associées à l'utilisation de l'outil ?

Confidentialité :

Comment les informations personnelles des utilisateurs de l'outil sont-elles gérées ?
L'outil est-il conforme au RGPD ?