GLOBAL CYBER ALLIANCE

globalcyberalliance.org
New York City | London | Brussels

Cybersecurity Toolkit Tool Selection Process

Overview

The Global Cyber Alliance (GCA) Cybersecurity Toolkit (the Toolkit) is an online resource that includes a wealth of free and effective tools that entities can start using right now to make an immediate impact on reducing cyber risk. Entities and individuals can use the Toolkit to assess their security posture, implement free tools, and find practical tips, free resources, and guides that will help improve their cybersecurity readiness and response. At GCA, we recognize that the Toolkit's most powerful resource is its tools, and we strive to select the most essential and effective free tools for our community to use.

This document discusses the specifications and procedures GCA uses when adding a tool to any version(s) of the Cybersecurity Toolkit. We will outline the details here to get a tool included in the Toolkit or to understand the reason for declination. A tool that is currently included may go under review to ensure it still meets the criteria to remain in its toolkit version(s), or it may be removed via the Toolkit Change Control Board (CCB) should the criteria not be met. The Toolkit CCB is also the vehicle used for addition of tools to the Toolkit once they have met all requirements explained in this document.

Selection

GCA looks for tools to include in its toolkits often and also receives entries via feedback from stakeholders. An entity with a tool it would like to add to the Toolkit can also apply via the Application for Inclusion in the GCA Cybersecurity Toolkit. This application will ask for specific details about the tool, as well as reference to specific CIS Critical Controls to support inclusion into Toolkits to include: a description of functionality, the level of IT knowledge required, and the time required to setup and/or use. Some additional information may also be requested.

GCA's intent is to include essential tools to implement cyber hygiene. To achieve that we use the process set forth below; GCA has four stages that the tools flow through when considered for addition to the Toolkit. Competing tools will be evaluated against one another, which may result in multiple tools for similar use being included or tools being removed. More information on this can be seen in the diagram below and the ***Ongoing Maintenance*** section.

The time required for the workflow depends on the use and application for each tool(s), working through the following stages:

1. BACKLOG (Waiting List)

Tools in the 'Backlog' are being considered for inclusion in the Toolkit. Research into the tools may have started and will need to be completed before the review begins. Research includes consultation with the community (including our relevant advisory groups), consideration of online reviews and analyses, and in-person reviews by GCA. For example, as part of the process, the Toolkit CCB and GCA staff will look at whether the tools are free, are known to be able to address the specific critical controls for a toolbox, have positive personal feedback from the GCA community, and are known to receive patches/updates in a timely manner.

2. UNDER REVIEW

A tool will be considered 'Under Review' once initial background checks have been completed during the 'Backlog' stage and it is felt there is value to pursuing its inclusion. Further due diligence is conducted which may incorporate feedback from external advisory groups (appointed external representatives with cyber/sector expertise for each toolkit), detailed vendor discussions, demonstrations, and testing and analysis with the current toolkit tool set. Once the review is completed, the tool and recommendations will be put forward for consideration by the internal GCA CCB which meets on a monthly basis. If needed, the tool will move to stage 3 for external review or directly to stage 4 for inclusion.

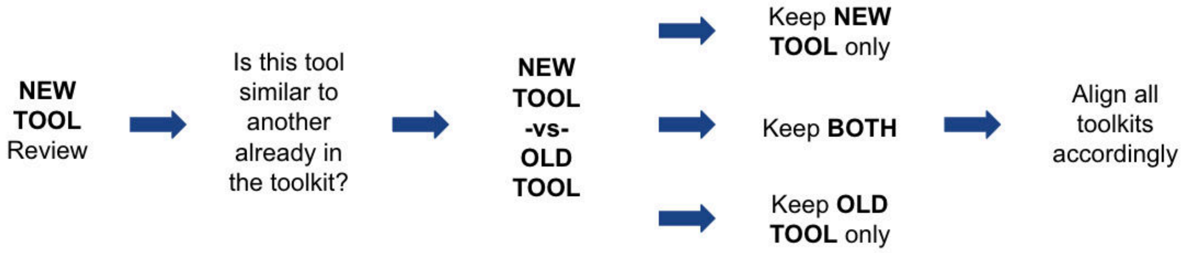
3. SUBMITTED TO EXTERNAL ADVISORY GROUP FOR SPONSORED TOOLKIT(S)

For Toolkits that are sponsored or co-managed, items voted for inclusion by the CCB must be approved and signed-off by entities/individuals external to GCA prior to being included. These are appointed external representatives with cyber/sector expertise for each toolkit, which include toolkit sponsors. GCA will provide pertinent information to the group, provide any additional feedback/information necessary, and await their approval. Once their final approval is given, it will move into the final 'Approved' stage. Likewise, if the external advisory board does not approve, a tool may stay in this stage to have more information gathered or be removed from selection altogether, depending on reasoning from the group.

4. APPROVED

Items that have been voted in by the Change Control Board and external advisory group (where applicable) to be included in a toolkit(s) will be assigned to the Website manager for execution.

Note: The proposed tool may be rejected at any stage in the process by the CCB or external advisory group.


NEW TOOL Review
Is this tool similar to another already in the toolkit?
NEW TOOL -vs- OLD TOOL
Keep NEW TOOL only
Keep BOTH
Keep OLD TOOL only
Align all toolkits accordingly

Initial Selection and Review

Initial Selection

Tools are selected by the Toolkit CCB using the above process and applying the factors described below.

Review

GCA toolkits are continuously evolving based on the feedback we receive from different communities, workshops, and advisors as well as the emergence of new tools. Additional considerations can be included during a subsequent review, including: user and community feedback; advice from third party providers (where a material change may have taken place in the tool or its terms of service); and input from GCA advisory groups and by GCA's own staff to ensure continuing appropriateness with the threat landscape.

Criteria for Tool Inclusion

The external advisory board and the Toolkit CCB consider the following criteria in the tool selection process:

Cost:
Is this tool free, does it have a free tier, is it commercial?

Tool type:
What is the tool and how will it be used? Is this instructional, a third-party tool, video, policy, etc.?

Difficulty to use:
What is the level of IT expertise required to successfully implement and operate this tool? Note: even after a tool has been included in the Toolkit, feedback from users will continue to inform this criterion.

Requirements:
What operating systems and/or extensions will be needed to operate?

Duration of installation:
What is the time needed to download and/or implement?

Access:
Does the user need to sign up for anything in order to use the tool? Is this tool plug and play?

Limitations:
What is the extent of the free offering and are there limitations on successful use?

Controls and standards:
What controls and standards does this tool conform with "out of the box" and are there additional steps needed to increase them?

Threats:
What specific threat does this tool address for the specific community?

Level of support provided with the tool:
What level of support does a user get with the free version of this tool and are there additional support levels a user may have access to?

Languages:
Which languages is the tool available in to establish its potential geographic user base? The more languages a tool is available in the better, but lack of additional languages will not prevent inclusion. Aligning Toolkits regardless of audience or region will be taken into account.

Supporting material:
Are there any how-to guides, videos, etc. that a user would have access to increase efficiency of use of the tool?

Patching and updating:
How are security patches and updates normally administered and is there any additional support needed for this?

Terms and Conditions (T&C's):
Are there any T&Cs associated with the use of the tool?

Privacy:
How is personal information of tool users handled? Is the tool GDPR compliant?