Proses Pemilihan Alat Toolkit Keamanan

Ikhtisar

Toolkit Keamanan Siber Global Cyber Alliance (GCA) adalah sumber daya daring yang terdiri dari bermacam alat gratis dan efektif yang saat ini juga dapat mulai digunakan oleh setiap entitas untuk membuat dampak langsung terhadap pengurangan risiko siber. Entitas dan individu dapat menggunakan Toolkit untuk menilai postur keamanan sistem mereka, menerapkan alat gratis, dan menemukan tips praktis, sumber daya gratis, dan panduan yang akan membantu meningkatkan kesiapan dan respons keamanan siber mereka. Di GCA, kami menyadari bahwa sumber daya Toolkit yang paling andal adalah setiap alat yang tersedia, dan kami berusaha untuk memilihkan alat gratis yang paling penting dan efektif untuk digunakan oleh komunitas kami.

Dokumen ini membahas spesifikasi dan prosedur yang digunakan GCA saat menambahkan alat pada setiap versi Toolkit Keamanan Siber. Di sini, kami akan uraikan secara mendetail cara mendapatkan alat yang tersedia dalam Toolkit maupun untuk memahami alasan untuk menolaknya. Setiap alat yang saat ini tersedia mungkin perlu ditinjau untuk memastikannya masih memenuhi kriteria untuk tetap disertakan dalam versi toolkit-nya, atau dapat dihapus melalui Toolkit Change Control Board (CCB) jika kriteria sudah tidak terpenuhi. CCB Toolkit juga merupakan sarana yang digunakan untuk menambahkan alat pada Toolkit setelah alat dinilai memenuhi semua persyaratan yang dijelaskan dalam dokumen ini.

Pilihan

GCA secara rutin mencari alat untuk disertakan dalam toolkit-nya dan juga menerima masukan melalui umpan balik dari para pemangku kepentingan. Entitas yang alatnya ingin ditambahkan ke Toolkit juga dapat mendaftar melalui Aplikasi untuk Disertakan dalam Toolkit Keamanan Siber GCA. Aplikasi ini akan meminta detail yang spesifik mengenai alat, serta rujukan ke CIS Critical Controls yang spesifik untuk mendukung penyertaan alat ke dalam Toolkit yang mencakup: deskripsi fungsionalitas, tingkat pengetahuan TI yang diperlukan, dan waktu yang diperlukan untuk mengatur dan/atau menggunakannya. Beberapa informasi tambahan mungkin juga akan diminta.

Tujuan GCA adalah menyertakan alat penting untuk menerapkan higiene siber. Untuk mencapai tujuan tersebut, kami menggunakan proses yang ditetapkan di bawah ini; GCA memiliki empat tahap yang dilalui alat ketika dipertimbangkan untuk ditambahkan pada Toolkit. Alat yang bersaing akan dievaluasi satu sama lain, sehingga alat dengan fungsi yang mirip akan berpeluang untuk disertakan atau dihapus. Informasi lebih lanjut tentang hal ini dapat dilihat dalam diagram di bawah ini dan di bagian **Pemeliharaan Berjalan.**

Waktu yang dibutuhkan untuk alur kerja akan tergantung pada penggunaan dan aplikasi masing-masing alat, dengan melalui tahapan berikut:

1. BACKLOG (Daftar Tunggu)

Alat dalam ‘Backlog’ sedang dipertimbangkan untuk disertakan dalam Toolkit. Penelitian menyeluruh pada alat mungkin telah dimulai dan perlu diselesaikan sebelum peninjauan dimulai. Penelitian mencakup konsultasi dengan komunitas (termasuk grup penasihat kami yang relevan), pertimbangan ulasan dan analisis daring, dan ulasan langsung oleh GCA. Misalnya, sebagai bagian dari proses, Toolkit CCB dan staf GCA akan meninjau apakah alat tersedia gratis, diketahui dapat menangani kontrol vital yang spesifik untuk kotak peralatan, mendapat umpan balik personal yang positif dari komunitas GCA, dan diketahui menerima tambalan/pembaruan secara tepat waktu.

2. DALAM PENINJAUAN

Alat akan dianggap 'Dalam Peninjauan' setelah pemeriksaan latar belakang awal selesai selama tahap 'Backlog' dan dirasakan ada nilai untuk mengejar inklusinya. Uji tuntas lebih lanjut dilakukan yang dapat menyertakan masukan dari grup penasihat eksternal (perwakilan eksternal yang ditunjuk dengan keahlian siber/sektor untuk setiap toolkit), diskusi vendor terperinci, demonstrasi, serta pengujian dan analisis dengan set alat toolkit saat ini. Setelah peninjauan selesai, alat dan rekomendasi akan diajukan untuk dipertimbangkan oleh GCA CCB internal yang bertemu setiap bulan. Jika diperlukan, alat ini akan beralih ke tahap 3 untuk ditinjau secara eksternal atau langsung ke tahap 4 untuk dimasukkan.

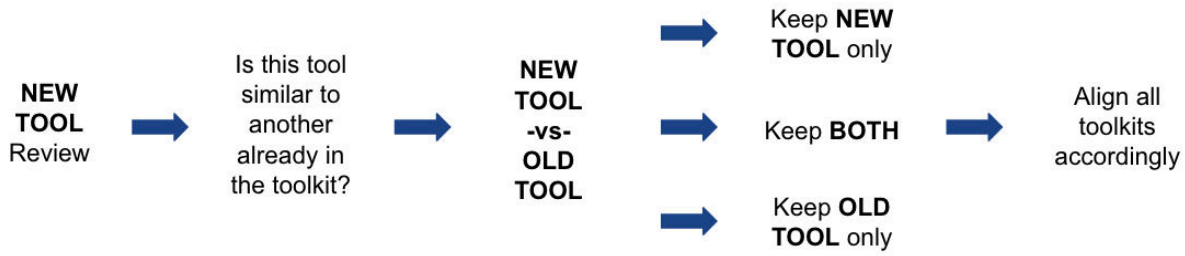
3. DIKIRIM KE GRUP PENASIHAT EKSTERNAL UNTUK TOOLKIT BERSPONSOR

Untuk Toolkit yang disponsori atau dikelola bersama, item yang dipilih untuk dimasukkan oleh CCB harus disetujui dan ditandatangani oleh entitas/individu di luar GCA sebelum disertakan. Entitas/individu ini merupakan perwakilan eksternal yang ditunjuk dengan keahlian siber/sektor untuk masing-masing toolkit, yang mencakup sponsor toolkit. GCA akan memberikan informasi yang bersangkutan kepada grup, memberikan masukan/ informasi tambahan yang diperlukan, dan menunggu persetujuan mereka. Setelah persetujuan akhir mereka diberikan, alat akan beralih ke tahap akhir 'Disetujui'. Demikian juga, jika dewan penasihat eksternal tidak menyetujui, alat mungkin tetap dalam tahap ini untuk mengumpulkan lebih banyak informasi atau dihapus dari seleksi sama sekali, tergantung alasan grup.

4. DISETUJUI

Item yang telah dipilih oleh Change Control Board dan grup penasihat eksternal (jika berlaku) untuk dimasukkan dalam toolkit akan ditetapkan ke manajer Situs Web untuk dilaksanakan.

Catatan: Alat yang diusulkan dapat ditolak pada tahap apa pun dalam proses oleh CCB atau grup penasihat eksternal.



Seleksi Awal dan Peninjauan

Seleksi Awal

Alat dipilih oleh Toolkit CCB menggunakan proses di atas dan menerapkan faktor-faktor yang dijelaskan di bawah ini.

Peninjauan

Toolkit GCA terus berkembang berdasarkan masukan yang kami terima dari berbagai komunitas, lokakarya, dan penasihat serta munculnya alat baru. Pertimbangan tambahan dapat disertakan selama peninjauan berikutnya, termasuk: masukan pengguna dan komunitas; saran dari penyedia pihak ketiga (di mana perubahan material mungkin telah terjadi di alat atau ketentuan layanannya); dan masukan dari grup penasihat GCA dan oleh staf GCA sendiri untuk memastikan kesesuaian yang berkelanjutan dengan lanskap ancaman.

Kriteria untuk Penyertaan Alat

Dewan penasihat eksternal dan Toolkit CCB mempertimbangkan kriteria berikut dalam proses pemilihan alat:

Biaya:
Apakah alat ini gratis, apakah memiliki tingkat gratis, apakah alat ini bersifat komersial?

Jenis alat:
Apa yang dimaksud dengan alat dan bagaimana alat tersebut akan digunakan? Apakah ini bersifat instruksional, alat pihak ketiga, video, kebijakan, dll.?

Kesulitan penggunaan:
Apa tingkat keahlian TI yang diperlukan agar berhasil menerapkan dan mengoperasikan alat ini? Catatan: bahkan setelah alat disertakan dalam Toolkit, masukan dari pengguna akan terus menginformasikan kriteria ini.

Persyaratan:
Sistem operasi dan/atau ekstensi apa yang diperlukan untuk beroperasi?

Durasi pemasangan:
Berapa lama waktu yang diperlukan untuk mengunduh dan/atau menerapkan?

Akses:
Apakah pengguna harus mendaftar untuk menggunakan alat ini? Apakah alat ini memiliki metode plug and play?

Batasan:
Seberapa jauh tingkat gratis yang ditawarkan dan apakah ada batasan untuk penggunaan yang berhasil?

Kontrol dan standar:
Kontrol dan standar apa yang sesuai dengan "penerapan langsung" alat ini dan apakah ada langkah tambahan yang diperlukan untuk meningkatkannya?

Ancaman:
Apa ancaman spesifik yang ditangani oleh alat ini untuk komunitas tertentu?

Tingkat dukungan yang diberikan dengan alat:
Apa tingkat dukungan yang diperoleh pengguna dengan versi gratis alat ini dan apakah ada tingkat dukungan tambahan yang mungkin dapat diakses pengguna?

Bahasa:
Apa saja bahasa yang tersedia pada alat untuk membangun basis pengguna geografis potensialnya? Suatu alat akan semakin baik jika tersedia dalam banyak bahasa, tetapi ketiadaan bahasa tambahan tidak akan membatasi penyertaan alat tersebut. Menyelaraskan Toolkit tanpa memandang audiens maupun wilayahnya akan diperhitungkan.

Materi pendukung:
Apakah ada panduan cara penggunaan, video, dll. yang dapat diakses pengguna untuk meningkatkan efisiensi penggunaan alat?

Menambal dan memperbarui:
Bagaimana tambalan dan pembaruan keamanan biasa diberikan dan apakah ada dukungan tambahan yang diperlukan untuk itu?

Syarat dan Ketentuan (S&K):
Apakah ada S&K yang berlaku untuk penggunaan alat ini?

Privasi:
Bagaimana penanganan informasi pribadi pengguna alat dilakukan? Apakah alat tersebut mematuhi GDPR?