

Tool-Auswahlprozess für das Cybersecurity Toolkit

Überblick

Das Global Cyber Alliance (GCA) Cybersecurity Toolkit (das Toolkit) ist eine Online-Ressource, die zahlreiche kostenlose und effektive Tools enthält, mit denen Unternehmen ihre Cyber-Risiken sofort reduzieren können. Organisationen und Einzelpersonen können das Toolkit verwenden, um ihre Sicherheitslage zu bewerten, kostenlose Tools zu implementieren und praktische Tipps, kostenlose Ressourcen und Anleitungen zu finden, die ihre Cybersecurity-Bereitschaft und -Reaktionsfähigkeit verbessern. Wir bei GCA wissen, dass die bedeutendste Ressource des Toolkits die enthaltenen Tools sind, und wir bemühen uns darum, die wichtigsten und effektivsten kostenlosen Tools zur Nutzung durch unsere Community auszuwählen.

In diesem Dokument werden die Spezifikationen und Verfahren erläutert, die GCA beim Hinzufügen eines Tools zu einer Version des Cybersecurity Toolkits zugrunde legt. Hier finden Sie Details dazu, wie ein Tool in das Toolkit aufgenommen werden kann oder was die Gründe für eine Ablehnung sein können. Tools, die derzeit enthalten sind, können geprüft werden, um sicherzustellen, dass sie die Kriterien für den Verbleib in den jeweiligen Toolkit-Versionen erfüllen, oder sie können über das Toolkit Change Control Board (CCB) entfernt werden, wenn die Kriterien nicht erfüllt sind. Das Toolkit CCB ist auch dafür zuständig, Tools zum Toolkit hinzuzufügen, sobald sie alle in diesem Dokument erläuterten Anforderungen erfüllt haben.

Auswahl

GCA sucht regelmäßig nach Tools, die in die Toolkits aufgenommen werden können, und erhält auch Beiträge durch Feedback von Stakeholdern. Eine Organisation mit einem Tool, das sie zum Toolkit hinzufügen möchte, kann zudem den Antrag auf Aufnahme in das GCA Cybersecurity Toolkit einreichen. In diesem Antrag werden konkrete Angaben zum Tool abgefragt sowie Verweise auf bestimmte CIS Critical Controls genannt, die die Aufnahme in Toolkits unterstützen. Folgende Informationen sind erforderlich: Beschreibung der Funktionen, erforderliche IT-Kenntnisse und Zeitaufwand für die Einrichtung und/oder Nutzung. Einige zusätzliche Informationen können ebenfalls angefordert werden.

GCA beabsichtigt, wesentliche Tools aufzunehmen, um Cyber-Sicherheit zu gewährleisten. Um dies zu erreichen, verwenden wir das unten beschriebene Verfahren; bei GCA durchlaufen Tools, die für eine Aufnahme in das Toolkit in Betracht gezogen werden, vier Phasen. Konkurrierende Tools werden miteinander verglichen, was dazu führen kann, dass mehrere Tools für eine ähnliche Verwendung einbezogen oder Tools entfernt werden. Weitere Informationen hierzu finden Sie im folgenden Diagramm und im Abschnitt „Kontinuierliche Pflege“.

Die für den Workflow benötigte Zeit hängt von der Verwendung und Anwendung der einzelnen Tools ab, die die folgenden Phasen durchlaufen:

1. BACKLOG (Warteliste)

Tools in der Phase „Backlog“ werden für eine Aufnahme in das Toolkit in Betracht gezogen. Recherchen zu den Tools wurden eingeleitet und müssen möglicherweise abgeschlossen werden, bevor die Prüfung beginnt. Recherchen umfassen die Beratung mit der Community (einschließlich relevanter Beratungsgruppen), die Berücksichtigung von Online-Bewertungen und Analysen und eigene Prüfungen durch GCA. Im Rahmen des Verfahrens sehen sich das Toolkit CCB und Mitarbeiter von GCA beispielsweise an, ob die Tools kostenlos sind, ob sie bekanntermaßen die konkreten kritischen Kontrollen für eine Toolbox einhalten, ob sie positives persönliches Feedback von der GCA Community erhalten haben und ob Patches/ Updates üblicherweise zeitnah bereitgestellt werden.

2. IN PRÜFUNG

Ein Tool ist „In Prüfung“, sobald die anfänglichen Hintergrundprüfungen der Backlog-Phase abgeschlossen sind und sofern diese ergeben haben, dass eine Weiterverfolgung der Aufnahme sinnvoll ist. Es werden weitere Due Diligence-Prüfungen durchgeführt, die Feedback von externen Beratungsgruppen (ernannte externe Vertreter mit Cyber-/Branchenkenntnissen für jedes Toolkit), eingehende Gespräche mit dem Anbieter, Demonstrationen sowie Tests und Analysen mit den aktuellen Toolkit-Tools umfassen können. Sobald die Prüfung abgeschlossen ist, werden das Tool und die Empfehlungen dem internen GCA CCB, das monatlich zusammentritt, zur Berücksichtigung vorgelegt. Je nach Bedarf durchläuft das Tool dann Phase 3 zur externen Prüfung oder Phase 4 zur Aufnahme.

3. AN EXTERNE BERATUNGSGRUPPE FÜR GESPONSERTE TOOLKITS EINGEREICHT

Bei Toolkits, die gesponsert oder gemeinsam verwaltet werden, müssen die Elemente, deren Aufnahme das CCB beschlossen hat, vor der Aufnahme von externen Organisationen/ Einzelpersonen außerhalb von GCA genehmigt und abgesegnet werden. Dabei handelt es sich um externe Vertreter mit Cyber-/Branchenkenntnissen für jedes Toolkit, zu denen auch Toolkit-Sponsoren gehören. GCA legt der Gruppe relevante Informationen vor, stellt zusätzlich notwendiges Feedback/Informationen bereit und wartet die Zustimmung ab. Sobald die endgültige Zustimmung erteilt wurde, geht das Tool in die final Phase „Genehmigt“ über. Wenn die externe Beratungsgruppe jedoch nicht zustimmt, kann ein Tool je nach Argumentation der Gruppe in dieser Phase verbleiben, bis weitere Informationen zusammengetragen werden, oder vollständig aus dem Auswahlverfahren entfernt werden.

4. GENEHMIGT

Elemente, die vom Change Control Board und der externen Beratungsgruppe (sofern zutreffend) für die Aufnahme in ein Toolkit ausgewählt wurden, werden dem Website-Manager zur Ausführung zugewiesen.

Hinweis: Das vorgeschlagene Tool kann in jeder Phase des Verfahrens vom CCB oder der externen Beratungsgruppe abgelehnt werden.



Vorauswahl und Prüfung

Vorauswahl

Tools werden anhand des oben dargelegten Verfahrens und unter Anwendung der unten beschriebenen Faktoren vom Toolkit CCB ausgewählt.

Prüfung

GCA-Toolkits entwickeln sich ständig weiter, basierend auf dem Feedback, das wir von verschiedenen Communities, Workshops und Beratern erhalten, sowie durch die Einführung neuer Tools. Weitere Überlegungen können bei einer anschließenden Prüfung berücksichtigt werden, darunter: Benutzer- und Community-Feedback, Informationen von Drittanbietern (wenn eine wesentliche Änderung am Tool oder den zugehörigen Nutzungsbedingungen stattgefunden hat) und Input von GCA-Beratungsgruppen und von GCA-Mitarbeitern, um die weitere Eignung innerhalb der Bedrohungslandschaft zu gewährleisten.

Kriterien für die Toolaufnahme

Die externe Beratungsgruppe und das Toolkit CCB berücksichtigen die folgenden Kriterien bei der Toolauswahl:

Kosten:

Ist dieses Tool kostenlos, gibt es eine kostenlose Version, ist es kommerziell?

Art des Tools:

Was ist das Tool und wie wird es verwendet? Handelt es sich um eine Anleitung, ein Drittanbieter-Tool, ein Video, eine Richtlinie usw.?

Benutzerfreundlichkeit:

Welche IT-Kenntnisse sind erforderlich, um dieses Tool erfolgreich zu implementieren und zu betreiben? Hinweis: Auch nachdem ein Tool in das Toolkit aufgenommen wurde, wird dieses Kriterium weiterhin anhand von Feedback von Benutzern bewertet.

Anforderungen:

Welche Betriebssysteme und/oder Erweiterungen werden für den Betrieb benötigt?

Dauer der Installation:

Wie lange dauert der Download und/oder die Implementierung?

Zugriff:

Muss sich der Benutzer anmelden, um das Tool verwenden zu können? Handelt es sich um ein Plug & Play-Tool?

Einschränkungen:

Was umfasst das kostenlose Angebot und gibt es Einschränkungen für eine erfolgreiche Verwendung?

Kontrollen und Standards:

Welche Kontrollen und Standards erfüllt dieses Tool standardmäßig und sind zusätzliche Schritte erforderlich, um die Standards zu erhöhen?

Bedrohungen:

Welche konkrete Bedrohung wehrt dieses Tool für die jeweilige Community ab?

Mit dem Tool bereitgestellter Support:

Welche Art von Support erhält der Benutzer mit der kostenlosen Version dieses Tools und gibt es zusätzlichen Support, auf den ein Benutzer möglicherweise Zugriff erhalten kann?

Sprachen:

In welchen Sprachen steht das Tool zur Verfügung, um die potenzielle geografische Basis an Benutzern zu ermitteln? In je mehr Sprachen ein Tool verfügbar ist, desto besser, aber weniger verfügbare Sprachen wirken sich nicht negativ auf eine Aufnahme aus. Ausrichtungs-Toolkits unabhängig von Zielgruppe oder Region werden berücksichtigt.

Begleitmaterial:

Gibt es Anleitungen, Videos usw., auf die ein Benutzer Zugriff erhält, um die Effizienz der Nutzung des Tools zu erhöhen?

Patching und Updates:

Wie werden Sicherheitspatches und Updates normalerweise verwaltet und ist dafür zusätzlicher Support erforderlich?

Allgemeine Geschäftsbedingungen (AGB):

Sind mit der Nutzung des Tools AGB verbunden?

Datenschutz:

Wie werden personenbezogene Informationen von Benutzern des Tools verarbeitet? Ist das Tool DSGVO-konform?