Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Département fédéral des finances DFF

Secrétariat général DFF
Centre national pour la cybersécurité NCSC

1er juillet 2021

Programme de primes aux bogues au sein de l'administration fédérale – projet pilote

Rapport final

Table des matières

1 Condensé

Le Centre national pour la cybersécurité (NCSC) a mené du 10 au 21 mai 2021 le premier programme de primes aux bogues *(bug bounty)* au sein de l’administration fédérale. Réalisé en collaboration avec Bug Bounty Switzerland GmbH, le Département fédéral des affaires étrangères (DFAE) et les Services du parlement (SP), ce programme a consisté à soumettre un ensemble de six systèmes informatiques du DFAE et des SP à un total de quinze pirates éthiques, chargés d’y repérer d’éventuelles failles de sécurité.

Au total, dix failles ont été détectées et signalées, dont une a été classée critique. Quatre des failles signalées ont pu être corrigées avant même que le projet s’achève. Au final, 9240 francs de primes ont été versés aux pirates. Le nombre total de failles identifiées est relativement faible pour un projet réalisé en collaboration avec des pirates éthiques et démontre que tous les systèmes informatiques testés jouissent d’une sécurité élevée.

Sur le montant mis à disposition (49 900 fr.), 27 300 francs ont été dépensés. Le solde a été mis en réserve pour financer la réalisation d’autres programmes de primes aux bogues (aussi appelés chasse aux bogues) au sein de l’administration fédérale.

Le projet pilote a montré que des programmes de chasse aux bogues s’avèrent efficaces pour détecter et éliminer les failles présentes dans des systèmes informatiques et qu’ils contribuent ainsi largement à la cybersécurité de la Confédération.

Grâce à l’expérience et aux connaissances acquises, le NCSC prévoit d’étendre sans cesse le programme de chasse aux bogues à un maximum de systèmes et d’applications informatiques de l’administration fédérale.

2 Point de départ

Les programmes de chasse aux bogues constituent un moyen efficace et financièrement avantageux pour détecter des vulnérabilités informatiques. Bien que ces programmes soient connus au niveau international depuis quelques années déjà et que des organismes étatiques y recourent également, ils ne sont pas encore très répandus en Suisse.

Ces programmes font appel au «piratage éthique», donc à des pirates informatiques qui recherchent légalement des failles dans un cadre déterminé, afin de déceler les éventuelles lacunes dans la sécurité des systèmes informatiques d'une organisation. Pour chaque bogue découvert et confirmé, le pirate reçoit une prime *(bounty),* dont le montant est fixé en fonction de la gravité de la faille détectée.

Afin de respecter la volonté du parlement de mener ce type de programmes[1] et d'engranger de premières expériences dans ce domaine, le NCSC a collaboré avec Bug Bounty Switzerland GmbH (BBS), le DFAE et les SP pour mettre sur pied et réaliser un projet pilote de chasse aux bogues.

L'administration fédérale, tout comme d'autres secteurs réglementés, applique des exigences strictes en matière de protection des données et demande que les données soient localisées en Suisse. Bug Bounty Switzerland a été le seul fournisseur connu dans notre pays qui a été en mesure de répondre à ces exigences. La plateforme créée par cette société est entièrement exploitée en Suisse. Fondée sur les dernières technologies en nuage, elle répond aux besoins de la Confédération et des autres secteurs réglementés tels que les infrastructures critiques.

Le projet pilote visait à démontrer l'utilité des programmes de chasse aux bogues pour l'administration fédérale, dans la mesure où ils permettent d'identifier des failles de sécurité, d'y remédier et de réduire ainsi les cyberrisques de manière à la fois efficace et relativement peu coûteuse. Ce projet avait également pour objectif d'engranger des expériences sur les possibilités d'intégrer un programme de chasse aux bogues dans les processus de sécurité existants.

3 Réalisation

Le projet pilote a consisté à mettre sur pied, à réaliser et à évaluer un programme de chasse aux bogues conçu sur mesure pour l'administration fédérale.

Ce programme s'est caractérisé par une durée limitée, des systèmes cibles clairement définis, un budget fixe et un nombre restreint de pirates éthiques. Les pirates sélectionnés ont été spécialement invités à participer au projet pilote.

Six systèmes informatiques du DFAE et des SP ont été choisis comme cibles. Pour ce premier test, le cercle des chasseurs de primes (et de bogues) était restreint aux pirates éthiques connus de BBS et du NCSC et ayant déjà fait leurs preuves dans d'autres projets.

Si la réalisation du programme de chasse aux bogues a été confiée à BBS, elle a été suivie de près par le NCSC de même que par des représentants du DFAE et des SP. Le projet pi-

[1] 20.4594 Po Bellaïche «Institutionnaliser le piratage éthique et améliorer la cybersécurité» (https://www.parlament.ch/fr/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20204594)

lote devait en effet servir de base de discussion pour définir un futur recours à ce type de chasse aux bogues.

Le projet a surtout mis en évidence la collaboration entre les pirates et les différents prestataires en charge des systèmes et des applications. Les pirates ayant fourni une bonne description des failles identifiées, les prestataires concernés ont pu les repérer à leur tour et lancer aussitôt les travaux pour y remédier.

Une fois la faille corrigée, le prestataire en informait le pirate, qui pouvait alors vérifier si des améliorations complémentaires s'imposaient.

Cette collaboration fructueuse et empreinte d'une grande confiance réciproque est à l'origine du succès du programme.

Déroulement du projet pilote – aperçu :

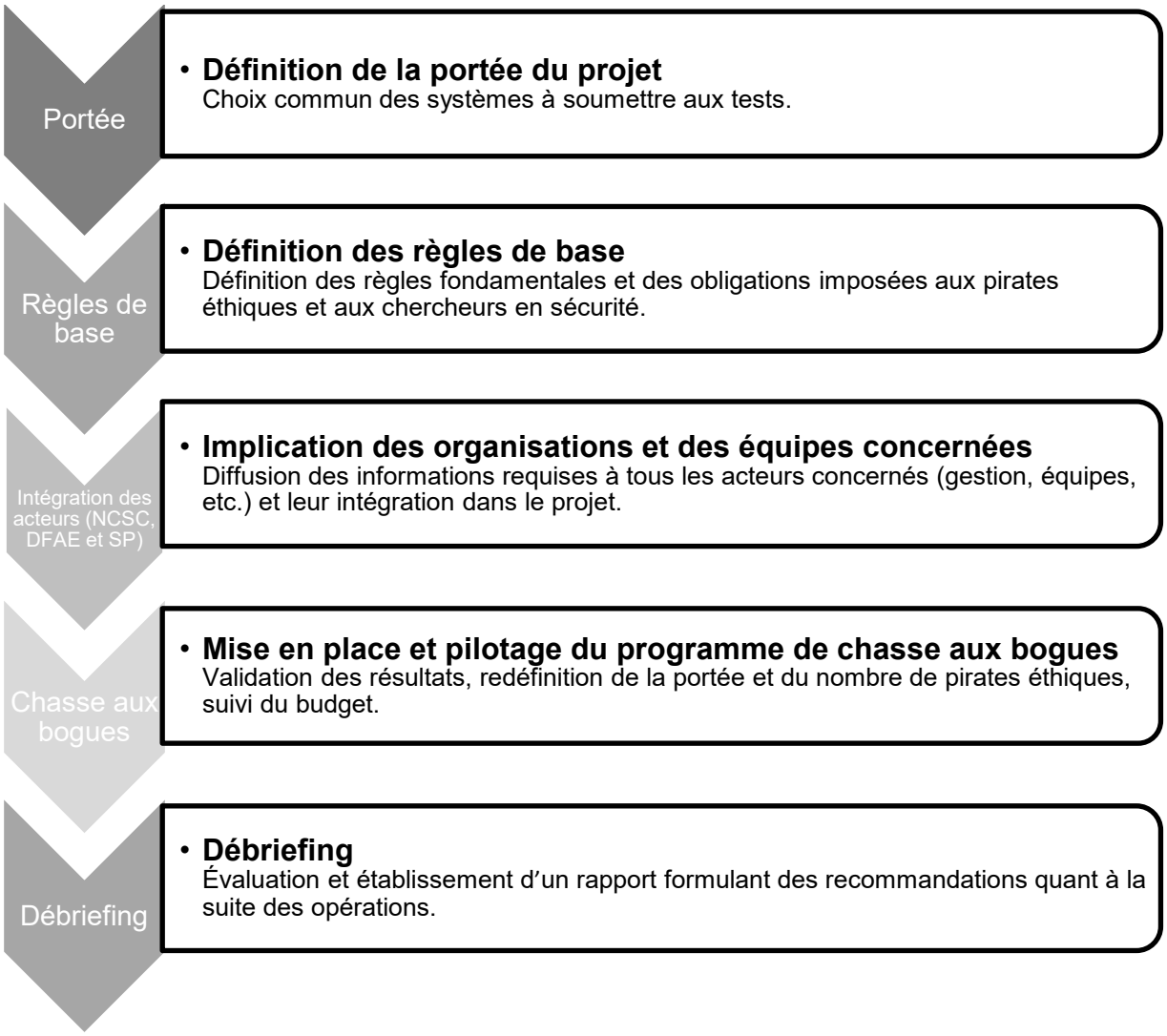

Figure 1: Déroulement du projet pilote

4 Résultats

Depuis le début du projet, le 10 mai à 00 h 01, jusqu'à sa fin, le 21 mai à 12 h 00, dix failles ont au total été signalées. Neuf d'entre elles ont été confirmées, tandis que l'un des dix rapports constituait un doublon selon les règles du programme de chasse aux bogues.

La multiplication des rapports signalant une faille au début du projet est habituelle lors de tests qui soumettent pour la première fois des systèmes à des pirates éthiques. Elle découle de la compétitivité qui régit ce type de test.

Les programmes de chasse aux bogues favorisant un fonctionnement agile et le nombre des rapports étant resté modeste, il a été possible, dès le deuxième jour, d'élargir sa portée pour y inclure des systèmes informatiques supplémentaires (de trois à l'origine, leur nombre est passé à six). Les pirates éthiques invités ont confirmé le bon niveau de sécurité des systèmes du DFAE et des SP (les qualifiant de difficiles à «craquer»).

Autre ajustement du projet, le cercle des pirates éthiques invités a été élargi afin de multiplier les tests (de 9 à l'origine, le nombre de pirates a été accru à 15).

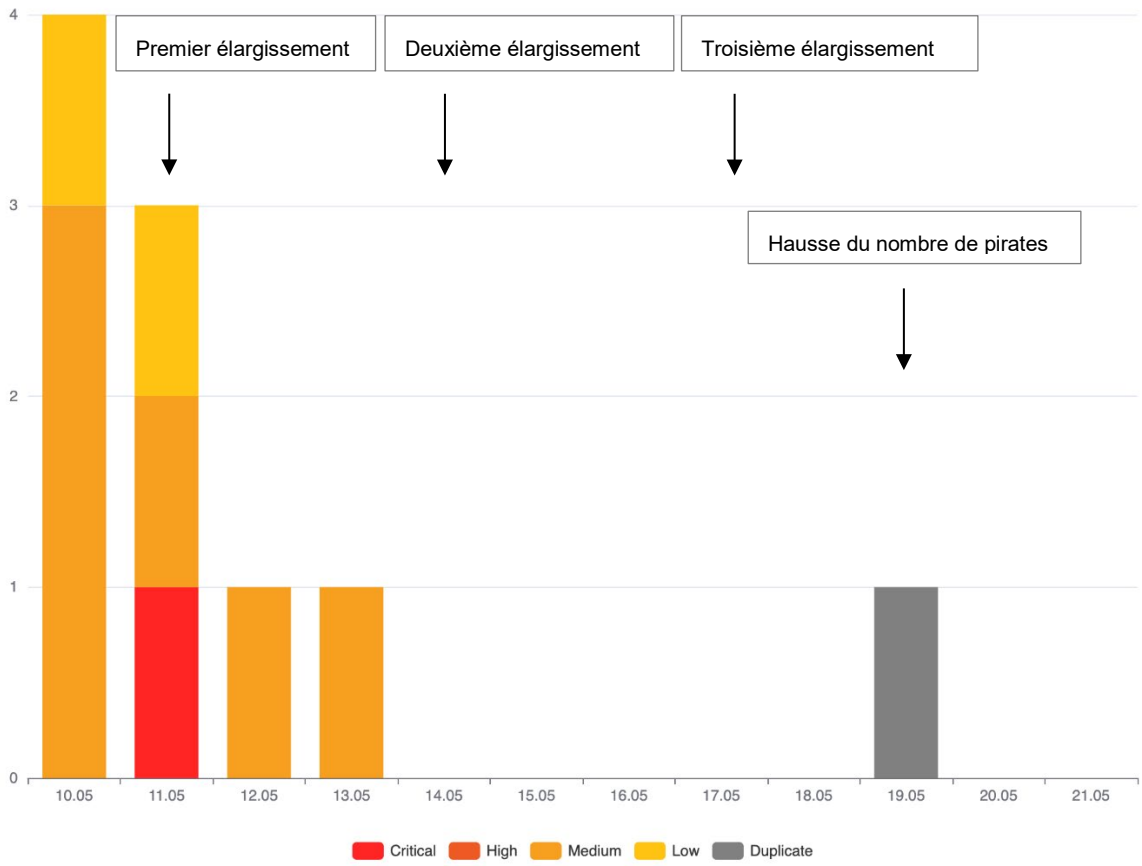

Figure 2: Rapports reçus, en fonction du niveau de risque.

Selon le niveau de risque, les failles de sécurité identifiées se répartissent comme suit.

	Cri-tique	Élevé	Moyen	Faible	Nul	Total
Système A	0	0	0	1	0	1
Système B	0	0	0	0	0	0
Système C	0	0	2	0	0	2
Système D	1	0	5	1	0	7
Total	**1**	**0**	**7**	**2**	**0**	**10**

Les systèmes informatiques soumis au programme de chasse aux bogues ne sont pas spécifiés, de sorte qu'ils sont désignés par les lettres A à D.

5 Financement

La Confédération avait plafonné le budget de ce projet pilote à 49 900 francs pour des prestations externes. Les frais engagés se répartissent comme suit :

Plafond des dépenses	CHF	49 900.00
Intégration des acteurs concernés, aspects techniques, etc.	CHF	13 375.00
Primes versées	CHF	9 240.00
Solde	**CHF**	**27 285.00**

Le solde mentionné est mis en réserve et servira à financer d'autres programmes de chasse aux bogues de l'administration fédérale, l'objectif étant de réaliser ce type de programmes pratiquement en continu.

6 Conclusion

Le projet pilote a prouvé que les programmes de primes aux bogues sont un moyen efficace d’identifier les failles dans les systèmes et applications informatiques et d’y remédier. Le retour sur investissement a été jugé élevé. La réalisation d’un tel programme par le NCSC au sein de l’administration fédérale est à même de contribuer largement à réduire les cyberrisques de la Confédération.

Tant les SP que le service informatique du DFAE ont émis des avis très positifs. Par ailleurs, différentes unités administratives requièrent des prestations comme celles qui découlent de ce type de programme. L’expérience montre en effet qu’associer la gestion et le soutien centralisés assurés par le service Gestion des vulnérabilités du NCSC, d’une part, et les solutions apportées de manière décentralisée par les prestataires responsables, d’autre part, constitue un mode de fonctionnement efficace et durable.

S’appuyant sur l’expérience tirée du projet pilote et les connaissances de tous les acteurs impliqués, le NCSC prévoit d’étendre sans cesse le programme de chasse aux bogues à un maximum de systèmes informatiques de l’administration fédérale.

Il importe dès lors de lancer la procédure d’acquisition dès que possible. En attendant son issue, il convient d’utiliser le solde du projet pilote pour poursuivre le programme de chasse aux bogues au sein de l’administration fédérale.