LES ESSENTIELS

BUG BOUNTY

FAQ

Novembre 2023

CLUSIF

.

Table des matières

Remerciements

Le Clusif tient à mettre ici à l'honneur les personnes qui ont rendu possible la réalisation de ce document, tout particulièrement :

Les responsables du groupe de travail :

Yassir	KAZAR	YOGOSHA
Rayna	STAMBOLIYSKA	YES WE HACK

Les contributeurs :

Louise	BAUTISTA	SISTECH
Aïmad	BERADY	YES WE HACK
Guillaume	BON	ARKHINEO
Benjamin	BROSSARD	DEVOTEAM
Cédric	CAILLEAUX	AXIANS
Geoffroy	CECILE	SOPRA STERIA GROUP
Sylvain	CORREIA PRAZERES	DÉPARTEMENT DE L'EURE
Etienne	COTASSON	ACOSS
Antoine	COUTANT	SYNETIS SAS
Michel	DUBOIS	GROUPE LA POSTE
Rodolphe	HARAND	YES WE HACK
Selim	JAAFAR	YES WE HACK
Bertrand	LE PIOLOT	LA FRANÇAISE DES JEUX
Maxly	MADLON	C2S BOUYGUES
Garance	MATHIAS	MATHIAS AVOCATS
Laure	PACITTO	ASSEMBLÉE NATIONALE
Sébastien	PALAIS	YOGOSHA
Philippe	PUYOU-LASCASSIES	TEREGA
Laurent	SARRAZIN	CAISSE DES DEPOTS ET CONSIGNATIONS
Guillaume	VASSAULT-HOULIERE	YES WE HACK

Le Clusif remercie également les adhérents ayant participé à la relecture.

1. DÉFINITIONS

1.1 Qu'est-ce que le bug bounty ?

Le **bug bounty**, littéralement traduit par « prime à la faille », est une pratique ayant émergé dans les années 1990. Ce terme a officiellement fait son entrée dans le vocabulaire de la défense[1] où il est défini comme une *« rémunération octroyée par une organisation à un expert informatique indépendant qui découvre une faille de sécurité au sein d'un système informatique utilisé par cette organisation. »*

Il s'agit d'une démarche de recherches de vulnérabilités informatiques réalisées par des experts indépendants, appelés « **hackers éthiques », « hunters » « chasseurs de primes » ou « chercheurs »**, aucune terminologie officielle n'étant retenue pour les désigner[2]. Par souci de simplicité, nous utiliserons dans ce document le terme « hunters ».

Ces hunters reçoivent **une récompense monétaire pour chaque vulnérabilité** qu'ils découvrent. Le montant de la récompense est calculé en fonction de la criticité de la vulnérabilité détectée et de son impact sur l'activité de l'organisation. La grille des récompenses est quant à elle définie à l'avance par le client en relation avec la plateforme, et communiquée via un programme de bug bounty.

1.2 Qu'est-ce qu'un programme de bug bounty ?

Un programme de bug bounty définit les règles qui encadrent la collaboration avec les hunters, telles que le périmètre à tester (site web, application, etc.), les récompenses, les types de vulnérabilités attendues et exclues, les restrictions, les obligations de confidentialité à respecter, etc. Il existe actuellement **deux types de programmes** de bug bounty :

- **Les programmes publics,** qui sont ouverts à tout le monde. Tous les hunters sont libres d'y participer en recherchant des vulnérabilités dans les périmètres ciblés.
- **Les programmes de bug bounty privés, ou sur invitation,** qui sont quant à eux confidentiels et accessibles aux seuls chercheurs expressément invités à y participer.

Les programmes se déroulent en général sur plusieurs mois ou de manière continue, mais il existe aussi des « live events programs » (sur site ou en ligne) où les experts sont libres de participer au programme de bug bounty en répondant présents au moment et au lieu où se tient l'événement. Cette version est souvent bien plus intensive. Tous ces programmes, qu'ils soient publics ou privés, sont publiés sur des plateformes de bug bounty.

---

[1] Commission d'enrichissement de la langue française, Vocabulaire de la défense (liste des termes, expressions et définitions adoptés, JORF n° 0299 du 11 décembre 2020 : https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000042649361

[2] https://dl.acm.org/doi/10.1145/3586180

1.3 Qu'est-ce qu'une plateforme de bug bounty ?

Une plateforme de bug bounty[3] est un service développé en interne (grands acteurs de l'industrie) ou proposé par une entreprise spécialisée dans le domaine. Elle facilite la collaboration entre les organisations et les chercheurs en sécurité dans le cadre d'un programme de bug bounty, et agit comme un intermédiaire entre les deux parties. La plateforme bug bounty offre notamment un espace sécurisé où les chercheurs peuvent signaler les vulnérabilités découvertes et où les entreprises peuvent gérer ces remontées[4].

La pratique du hacking éthique est antérieure aux plateformes de bug bounty, mais ces dernières sont venues encadrer l'exercice et la relation. Il est également possible d'opérer un programme de bug bounty en interne, sans passer par une plateforme, à l'image de Google ou Facebook, mais c'est une pratique extrêmement rare tant les moyens humains, techniques et financiers requis sont importants.

Il existe deux types de plateformes de bug bounty :

- **Les plateformes publiques :** les inscriptions sont libres, et tous les chercheurs peuvent créer un compte sur ces plateformes. Une sélection des hunters peut s'appliquer dans le cadre des programmes sur invitation.
- **Les plateformes privées :** les inscriptions sont sur demande, et l'accès à la plateforme et ses programmes sont conditionnés par la réussite de tests techniques.

Il existe cependant des plateformes sauvages n'ayant pas contractualisé avec les clients.

Un programme de bug bounty peut être **« managé »**, qu'il soit public ou privé. Dans ce contexte, le client délègue la mise en œuvre et le suivi du programme à une plateforme qui propose ce service ou à un prestataire spécialisé en sécurité informatique. Ce prestataire agit alors en tant que tiers de confiance. Il joue le rôle d'intermédiaire entre les hackers et le client, et accompagne dans différentes tâches comme le triage des rapports de vulnérabilités, la sélection des hunters, la détermination des paramètres liés aux primes ou l'animation du programme.

[3] Liste non exhaustive de plateformes de bug bounty : https://github.com/disclose/bug-bounty-platforms

1.4 Qu’est-ce qu’un hunter ? Quelle sélection ? Quelles obligations ?

Les hunters sont des hackers éthiques. Ce sont des chercheurs en sécurité indépendants qui identifient et signalent les vulnérabilités dans les systèmes informatiques, les réseaux ou les applications, dans le but d'aider à renforcer leur sécurité.

La pratique du hacking éthique repose sur des principes de légalité, d'éthique et de responsabilité. Les hackers éthiques doivent respecter les lois et les réglementations en vigueur, obtenir des autorisations appropriées, protéger la confidentialité des données sensibles découvertes pendant leurs tests et s'engager à ne pas exploiter les vulnérabilités qu'ils découvrent à des fins malveillantes.

Les plateformes de bug bounty publiques ont une politique d’inscription libre. Une sélection peut être ensuite faite par les organisations au sein de panel d'experts pour engager sur certains de leurs programmes des compétences spécifiques. Dans le cas des plateformes privées, la sélection des chercheurs obéit à des règles bien définies. Il s'agit d'un cercle restreint où l'acceptation d’un hunter est conditionnée par la réussite de tests de type CTF *(Capture the Flag*), qui permettent d’évaluer ses compétences techniques et pédagogiques. Le hunter doit être capable de décrire précisément les vulnérabilités qu'il a découvertes et d'orienter l'entreprise dans son travail de remédiation.

Le contrat entre les hunters et les plateformes peut spécifier des exigences en termes de forme et de qualité des rapports, y compris la langue de rédaction et le contenu du rapport.

Quel que soit le modèle de plateforme, la sélection des hunters dépend également du type de programme : public ou privé (cf. section 1.2).

Grâce à un programme privé, une organisation qui débute dans le bug bounty peut restreindre volontairement l’accès à quelques hunters plutôt qu'à toute la communauté de la plateforme. Cette sélection des hunters peut également tenir compte de leurs compétences vis-à-vis du périmètre du programme. Après tout, les hunters peuvent avoir une expertise dans des domaines spécifiques (mobile, réseaux, rétro-ingénierie, etc.), voire des attaques ou des typologies de vulnérabilités qu’ils maîtrisent plus que d’autres.

Les hunters prennent en considération plusieurs critères lorsqu'ils décident de participer activement ou non à un programme de bug bounty, comme :

- **l'étendue du périmètre à tester,** un facteur déterminant qui influe directement sur les chances d’identifier une faille. Plus le périmètre est grand, plus les probabilités d'identifier une vulnérabilité sont élevées ;
- **le montant des récompenses.** La rémunération proposée pour chaque vulnérabilité joue un rôle crucial et doit être équitable par rapport à sa sévérité, qui reflète souvent l'expertise et les efforts investis par le hunter ;
- **le type de vulnérabilités valides.** Les hunters ont tendance à se spécialiser ou à avoir des appétences particulières pour la recherche et l’exploitation de certaines vulnérabilités ;

- **la clarté des attendus et des prérequis**. Cela permet au hunter de mieux comprendre le cadre technique et les limitations du programme. Une ambigüité pourrait créer de la frustration et démotiver le hunter ;
- **les cycles de vie des applications testées.** Une application qui évolue et qui communique sur ses mises à jour a tendance à stimuler les hunters. Cela leur permet de suivre sur le long terme les applications et leurs nouvelles fonctionnalités ;
- **les performances des équipes en termes de délais de traitement** (réponse, gratification, remédiation et la qualité des échanges). Le hunter qui remonte une vulnérabilité apprécie avoir un suivi sur sa découverte et, au-delà de la gratification offerte, voir la vulnérabilité corrigée est la finalité de sa démarche.

La rémunération proposée joue un rôle crucial, car elle doit être équitable par rapport à l'effort investi par le hunter. C'est un travailleur indépendant, qui adopte le plus souvent une logique de retour sur investissement. L'important n'est pas tant de viser les primes les plus conséquentes, mais plutôt de trouver un juste équilibre entre le temps passé à rechercher des vulnérabilités et le montant des primes ainsi gagnées.

Les modalités de paiement des hunters doivent être établies préalablement au lancement du bug bounty, et indiquées clairement dans le programme. Cela inclut la grille des récompenses, les délais de paiement, la devise utilisée et le taux de change le cas échéant. En France, les plateformes ont obligation de passer par des prestataires de comptes séquestres[5].

1.5 Quelles différences avec d'autres approches du test de sécurité ?

Les approches du test de sécurité sont nombreuses, tant et si bien qu'il serait difficile de les comparer toutes ici avec le bug bounty. Mais on peut distinguer deux méthodes communément utilisées par les organisations :

- **le scanner de vulnérabilités**, qui est une approche automatisée du test de sécurité.
- **le test d'intrusion, ou pentest**, qui est une approche humaine et méthodologique du test de sécurité.

1.5.1 Les scanners de vulnérabilités

Les scanners de vulnérabilités sont adaptés pour effectuer des **scans de surface**, identifiant des erreurs de configuration, des vulnérabilités courantes de l'OWASP[6] Top 10 ou des vulnérabilités annoncées par les éditeurs (CVE).

[5] Obligation amenée par la Directive (UE) 2015/2366 concernant les services de paiement dans l'ensemble de l'UE, dite Directive sur les services de paiement (DSP2), accessible sur EUR-Lex

[6] L'Open Web Application Security Project, ou OWASP, est une organisation internationale à but non lucratif qui se consacre à la sécurité des applications web

Ils peuvent être configurés pour des **exécutions régulières et exhaustives** sur l'ensemble des systèmes et applications d'un périmètre donné, permettant une détection rapide des vulnérabilités.

Ils sont néanmoins limités dans leur capacité à détecter les vulnérabilités complexes ou des failles de logique métier, celles qui résultent d'enchaînements d'actions ou de combinaisons de vulnérabilités individuelles. L'absence de qualification humaine peut également engendrer de faux positifs, ce qui nécessite l'implication de ressources supplémentaires afin de traiter ces remontées.

1.5.2 Les tests d'intrusion

Les tests d'intrusion, ou pentests, sont effectués par des consultants spécialisés en cybersécurité. Ils adoptent **une approche structurée** du test de sécurité, qui combine des outils automatisés, comme les scanners, et des opérations manuelles pour des examens plus avancés.

Ces tests sont réalisés sur **une période déterminée et encadrés par un budget préétabli**, selon l'étendue et la complexité des tests requis. Les tests d'intrusion sont parfois réalisés en équipe, favorisant la collaboration dans la découverte de vulnérabilités et de méthodes d'exploitation potentielles.

Les tests d'intrusion offrent **une vision globale et précise du niveau de sécurité d'un actif à un instant précis**. Ils sont particulièrement pertinents pour valider la sécurité avant la mise en production d'un projet ou pour tester des systèmes et des applications en interne. De plus, les tests d'intrusion sont souvent **privilégiés lors d'une évaluation initiale**, notamment lors du lancement d'une nouvelle application ou d'une version majeure. **Il est également recommandé de soumettre les actifs à des tests d'intrusion avant d'envisager le bug bounty**, afin d'avoir une première idée du niveau de sécurité des environnements.

Les tests d'intrusion ont un rapport coût-efficacité maîtrisé dans le contexte d'une évaluation initiale des actifs. Ils permettent aux organisations de défricher les vulnérabilités les plus nombreuses et évidentes pour un prix fixe, là où chaque vulnérabilité amènerait une récompense individuelle avec un bug bounty.

1.5.3 Le bug bounty

Le bug bounty a pour lui la force du nombre, de quelques dizaines sur des programmes privés à plusieurs dizaines de milliers sur des programmes publics. Il permet d'évaluer la sécurité d'un périmètre en faisant appel à un grand nombre de hunters provenant de différents horizons. Multiplier les regards sur un actif, c'est aussi multiplier les chances d'y identifier une vulnérabilité.

Chaque hunter vient également avec ses propres compétences et expériences professionnelles. Au-delà du nombre brut de chercheurs, le bug bounty permet donc de diversifier les angles d'attaque et la couverture technique des tests. Rappelons ici que les programmes de bug bounty privés (cf. section 1.2) permettent de sélectionner les hunters

selon leurs domaines d'expertise, leur disponibilité, leur nationalité, leur expérience sur la plateforme en fonction des besoins du client ou des spécificités du périmètre à éprouver.

Par ailleurs, le bug bounty est **un programme de sécurité continu, qui permet une veille de sécurité permanente** des actifs. Les vulnérabilités sont remontées tout au long de l'année, et le programme reste pertinent tout au long du cycle de vie des applicatifs visés. Le bug bounty offre en cela une plus grande **agilité** que les pentests, car les hunters peuvent travailler sur les nouvelles fonctionnalités dès leur sortie. Il suffit de les prévenir en mettant à jour le programme, ce qui orientera leurs recherches.

Corollaire du précédent : **le bug bounty n'étant pas limité dans le temps, il permet de révéler les vulnérabilités complexes et chronophages à identifier**. Il est évident qu'un hunter qui peut travailler sur la durée sera capable d'échafauder des attaques plus complexes qu'un pentester n'ayant que deux semaines devant lui. Les hunters ont d'ailleurs eux-mêmes intérêt à remonter les vulnérabilités les plus critiques : leur récompense sera bien plus importante avec une attaque construite de bout en bout. Dans le jargon du bug bounty, c'est ce qu'on appelle le *chainbug* – un enchaînement des vulnérabilités qui permet de maximiser l'impact final et, pour le hacker, le montant de la récompense.

En définitive, le **bug bounty ne remplace ni n'annule les autres tests de sécurité** : il les complète. Une bonne cybersécurité doit s'agencer autour de plusieurs approches : **les scanners, les pentests et le bug bounty sont complémentaires.** Ils viennent chacun avec leurs propres forces et faiblesses. C'est en combinant ces méthodes qu'on peut obtenir une couverture plus complète et une meilleure compréhension des vulnérabilités d'un système.

	Scanner	**Pentest**	**Bug Bounty**
Fréquence d'exécution	Ponctuel, à intervalle régulier	Campagnes limitées dans le temps	Continu
Diversité d'expertise	Sur la base des signatures	Limitée à l'équipe engagée	Large communauté
Faux positifs	Taux élevé	Peu fréquent	Rare
Coût d'une vulnérabilité	Gratuit	Paiement à la campagne, quel que soit le nombre de vulnérabilités remontées	Paiement à la prime quelle que soit la durée du programme
Délai de mise en œuvre	Immédiat	En fonction de la disponibilité des équipes	Quelques heures

2. MISE EN PLACE

2.1 Juridique

2.1.1 Quid des engagements de confidentialité et des aspects juridiques ?

D'une manière générale, la mise en place d'un programme de bug bounty nécessite un cadre contractuel approprié, donnant lieu à une **relation tripartite** entre les parties concernées :

- un contrat entre la plateforme et son client ;
- un contrat entre la plateforme et les hunters ;
- des conditions générales d'utilisation (CGU) de la plateforme, acceptées préalablement par le client et les hunters.

Il va de soi que selon les cas d'usage et/ou les plateformes, des solutions juridiques spécifiques peuvent être négociées entre les parties ou donner lieu à d'autres relations contractuelles.

À l'instar d'autres stipulations contractuelles comme les éventuelles limitations de responsabilité de la plateforme ou des hunters, et/ou les garanties exigées par le client, ces dernières doivent faire l'objet d'une négociation et être conformes aux enjeux de la prestation et aux risques associés par le client. Il convient de rappeler que l'éventuelle limitation de responsabilité ne doit pas être dérisoire.

En outre, d'autres documents peuvent être annexés aux contrats, comme un code de bonne conduite (conformité) ou une charte éthique regroupant les règles et principes sur lesquels le hunter s'engage à se conformer lors de la réalisation de sa mission.

Il est essentiel de déterminer le périmètre d'intervention autorisé pour les contrats entre la plateforme et le client, ainsi qu'entre la plateforme et les hunters. Ce périmètre est souvent défini par un mandat juridique, adapté en fonction de la prestation, comprenant le nombre de participants au programme, leurs profils, les types de vulnérabilités recherchées, les techniques utilisées, etc.

Il convient de rappeler que tout dépassement du périmètre contractuel autorisé peut engager la responsabilité contractuelle, voire pénale, notamment en cas d'accès non autorisé à un système de traitement automatisé de données.[7]

De plus, il est crucial de prévoir des **garanties de sécurité et de confidentialité** lors du déploiement d'un programme de bug bounty. Cela concerne tant la plateforme du prestataire où les solutions informatiques sont publiées, y compris l'hébergement, que le traitement des données, y compris les données à caractère personnel. En effet, le traitement de ces données requiert la mise en place de mesures techniques et organisationnelles appropriées pour

[7] Article 323-1 du code pénal

répondre aux risques, conformément à l'article 32 du Règlement UE 2016/679 relatif à la protection des données à caractère personnel – le RGPD.

La **confidentialité des vulnérabilités** découvertes doit également faire l'objet d'une attention particulière afin d'éviter toute divulgation non autorisée. Les hunters ne doivent remonter les vulnérabilités qu'à travers la plateforme de bug bounty et sont soumis à une obligation de confidentialité concernant les informations auxquelles ils ont eu accès lors de leur intervention. Il leur est strictement interdit de partager des informations sur les vulnérabilités, les applications ou tout autre élément relevant du périmètre d'intervention, que ce soit avec des tiers ou au sein de la communauté des hunters, sur d'autres sites tels que des forums ou réseaux sociaux.

Ainsi, la confidentialité des échanges sera susceptible de faire l'objet soit d'un accord de confidentialité spécifique, soit d'une clause renforcée.

En complément, **l'organisation peut prévoir un contrat cadre pour tester plusieurs services ou applications non définis dans le périmètre initial, ou ajouter des conditions particulières** pour chaque programme qu'elle lance, afin de refléter ses propres exigences et obligations. Ces conditions particulières doivent être acceptées par les chercheurs avant leur participation au programme. Il est ainsi possible d'inclure des clauses spécifiques de confidentialité propres à l'organisation, et de rappeler les dispositions liées au RGPD.

2.1.2 Le bug bounty dans le cadre de la conformité juridique

Comme tout acteur économique, le prestataire mettant en œuvre un programme de bug bounty est soumis aux réglementations relatives à la conformité, notamment en matière de lutte anticorruption, anti-blanchiment ou RSE (responsabilité sociétale des entreprises). La conformité de l'activité du prestataire aux réglementations applicables doit faire l'objet d'une organisation interne efficace et d'une veille continue en la matière.

En outre, en présence d'éléments d'extranéité dans l'exécution de la prestation de Bug Bounty hors du territoire français, voire hors de l'Union européenne, l'application des réglementations relatives à l'export et aux sanctions économiques doit être interrogée. Dans cette hypothèse, un programme et une politique de conformité robustes devraient être mis en place afin d'assurer le respect des réglementations applicables et d'éviter tout risque de sanction.

Le processus de sélection des hunters doit également être examiné à la lumière des obligations de conformité réglementaire, notamment en ce qui concerne les modalités de vérification de leur identité. De plus, le pays de résidence des hunters peut avoir des conséquences sur la protection des secrets commerciaux et des données à caractère personnel, y compris en ce qui concerne les transferts de ces données en dehors de l'Union européenne, qui sont soumis à des exigences réglementaires spécifiques.

2.2 Budget & Finance

2.2.1 Le business model

Le modèle économique du bug bounty se compose généralement de trois éléments principaux :

1. **l'abonnement à la plateforme** de bug bounty ;
2. **les récompenses** versées aux chercheurs en sécurité ;
3. **le coût de pilotage** du programme par le client.

Le support est généralement inclus dans le prix de l'abonnement à la plateforme ou dans les coûts de gestion du programme. Le coût de l'**abonnement** n'est pas anodin : il couvre la maintenance, l'hébergement, et le développement initial d'une plateforme où la sécurité et la souveraineté des données sont des sujets cruciaux puisque les rapports de vulnérabilités vont y transiter.

Les primes versées aux hunters représentent également un coût à prendre en compte, puisqu'un programme qui rétribue mal les chercheurs n'attirera jamais les meilleurs experts.

Il est également recommandé de disposer de ressources internes compétentes en matière de **remédiation**, ou d'envisager l'externalisation de ces tâches – ce qui peut représenter un coût annexe. Il peut y avoir quelque chose de décourageant à voir qu'une vulnérabilité remontée plusieurs mois auparavant n'a toujours pas été corrigée. Les meilleurs hunters pourraient se décourager, et ne plus participer au programme. Une remédiation rapide est donc essentielle pour **maintenir la motivation des chercheurs**, et la qualité du bug bounty.

2.2.2 Un ROI transversal

La cybersécurité est un sujet majeur pour les entreprises et institutions, et améliorer la sécurité d'un système d'information (SI) passe nécessairement par l'allocation d'**un budget adéquat**. Néanmoins, l'une des principales problématiques reste **la réticence des dirigeants à accorder des budgets conséquents** sur des prestations intellectuelles/produits qui sont difficilement quantifiables en matière de ROI.

Le bug bounty a l'avantage de pouvoir être présenté comme un projet rentable, projections et chiffres à l'appui. Le succès d'un bug bounty peut être « chiffré », et un responsable sécurité des systèmes d'information (RSSI) peut tout à fait avancer à son Comex (comité exécutif) : « *Cette année nous avons payé tant de primes pour tant de vulnérabilités ; qui avaient tels scores de criticité CVSS*[8]*. Elles auraient pu coûter tant à l'entreprise, sans compter le montant des potentielles rançons, la perte d'activité et les retombées négatives sur les activités business.* »

[8] https://www.first.org/cvss/

En cela, le bug bounty offre plusieurs avantages en matière de retour sur investissement :

- **la possibilité de quantifier le succès du programme** grâce aux récompenses versées et aux vulnérabilités identifiées ;
- **l'opportunité de valoriser la sécurité du SI** en présentant des chiffres concrets à la direction ;
- un retour sur investissement en termes de **communication et marketing** – cf. section 3. Acteurs & Rôles ;
- un ROI en matière de **formation passive et continue des équipes de développement**, qui peuvent monter en compétences sur des sujets de cybersécurité au contact direct des hackers éthiques.

2.2.3 Grille indicative du montant des primes dans un programme de bug bounty

Voici une grille indicative des récompenses pratiquées lors d'un bug bounty, selon les scores CVSS (*Common Vulnerability* ***Scoring*** *System*) des vulnérabilités découvertes, le niveau de sécurité requis pour l'application visée mis en perspective avec le niveau de maturité de l'organisation :

	Sécurité +	**Sécurité ++**	**Sécurité +++**
LOW (CVSS 0-3.9)	50 €	100 €	250 €
MEDIUM (CVSS 4-6.9)	200 €	350 €	750 €
HIGH (CVSS 7-8.9)	500 €	1 000 €	2 500 €
CRITICAL (CVSS 9-10)	1 000 €	3 000 €	10 000 €

2.3 Organisation

Un programme de bug bounty se décline en plusieurs étapes :

- **une étape de prélancement,** où la communication interne et la coordination des équipes de l'organisation cliente sont cruciales ;
- **le lancement** lui-même ;
- et enfin, la **« vitesse de croisière »**.

Une phase de préparation soignée est essentielle pour assurer la coordination interne et la communication efficace entre les équipes de l'organisation cliente. Il est primordial de définir clairement les processus de gestion. Cela inclut la **répartition des rôles et des responsabilités** : qui sera chargé du triage des vulnérabilités, de leur qualification, de leur résolution et de leur validation ? Une coordination en amont permet d'optimiser l'efficacité du programme une fois qu'il est lancé.

Le client met à disposition au travers de la plateforme toutes les ressources nécessaires aux hunters (environnement, comptes, code source, documentation, etc.).

Ensuite vient le lancement effectif du programme, où il est crucial d'informer et d'impliquer toutes les parties prenantes concernées quant au périmètre à tester – les équipes de sécurité internes par exemple.

Après quelques semaines, le programme atteint une vitesse de croisière. L'activité des hunters peut décroître, et les détections se faire moins nombreuses. Là, il devient essentiel d'animer le programme via des actions régulières, comme :

- **inviter de nouveaux hunters** à rejoindre un programme qui serait privé, ou le rendre public pour élargir la communauté et mobiliser davantage d'experts ;
- **ajouter de nouveaux périmètres** de recherche au programme, afin d'agrandir le terrain de jeu des hunters ;
- **annoncer rapidement les nouvelles fonctionnalités ou les versions majeures à tester**, afin de susciter l'intérêt des chercheurs ;
- **augmenter le montant des récompenses au fur et à mesure** de la vie du programme. Les actifs visés gagnent normalement en sécurité, et il devient donc plus difficile pour les chercheurs de trouver des vulnérabilités. Il semble logique d'indexer les primes sur ce niveau de difficulté croissant, ce qui peut inciter les meilleurs éléments à investir du temps dans le programme.

2.4 Communication

La communication joue un rôle crucial dans la pratique du bug bounty, tant au niveau interne qu'externe. Lorsque l'organisation décide de lancer un programme, il est essentiel de mettre en place une **communication claire et efficace** pour assurer la compréhension et l'adhésion de toutes les parties prenantes et notamment la **direction générale**.

En interne, la communication est le plus souvent assurée par le/la **RSSI** et un **représentant sécurité de la direction des systèmes d'information (DSI)**. Leur rôle est de garantir une compréhension partagée des objectifs et des modalités du bug bounty. Par ailleurs, le soutien du service juridique est nécessaire pour rassurer et contractualiser les engagements de la plateforme et des chercheurs.

Une communication fluide et rapide avec la **DSI** est primordiale pour le succès du bug bounty. Il est essentiel d'informer immédiatement les équipes responsables des applicatifs de toute vulnérabilité identifiée par les hunters.

Pour les entreprises qui ont des **développeurs** internes, l'interaction avec leurs équipes de sécurité est essentielle. Il convient donc de mettre en place un processus de communication efficace pour partager les résultats des recherches de vulnérabilités, favorisant ainsi les échanges entre toutes les parties concernées.

La remontée des vulnérabilités aux directions métiers peut également stimuler une **émulation saine** entre elles. Chacun peut suivre des indicateurs clés, tels que le nombre de vulnérabilités détectées, le nombre de failles corrigées, le temps moyen de détection et de remédiation, etc.

Ces critères permettent de sensibiliser les équipes internes à la sécurité, et d'évaluer l'amélioration de leur capacité à gérer les vulnérabilités.

Enfin, pour les entreprises concernées, une bonne communication avec les **équipes SOC** (*Security Operations Center*) leur permet également d'améliorer leur posture de sécurité ; en élargissant par exemple le périmètre de détection des attaques et en ajoutant des règles de sécurité (virtual patching du Web Application Firewall – WAF, par exemple).

La communication externe se concentre principalement sur les **hackers éthiques**. Il est essentiel de les tenir informés des mises à jour, des corrections apportées et de l'évolution des récompenses afin de maintenir leur motivation. Cette communication avec les hunters doit être à la fois professionnelle et agréable, pour **maintenir une relation saine et positive** avec ces acteurs clés du programme.

3. ACTEURS ET RÔLES DU BUG BOUNTY

Un programme de bug bounty implique plusieurs acteurs au sein de l'organisation cliente, chacun ayant un rôle spécifique :

3.1 Le responsable de la sécurité des systèmes d'information (RSSI)

Le RSSI est généralement à l'origine et responsable de la mise en place du programme de bug bounty. Il doit convaincre en interne de l'approche, valider le besoin avec les équipes opérationnelles et métiers, et identifier un premier périmètre pour le premier exercice. Il coordonne également l'évaluation des différentes plateformes afin de sélectionner celle qui répond le mieux aux besoins de l'organisation.

3.2 La direction juridique ou l'avocat

Ces acteurs interviennent dans la négociation et la rédaction des contrats entre la plateforme, l'organisation cliente et les hunters. Ils collaborent étroitement avec les équipes métiers pour définir le périmètre d'intervention des hunters, en tenant compte des exigences légales. Ils s'assurent de la conformité juridique du projet, en anticipant les risques et en veillant à la rédaction et à la négociation des contrats.

3.3 Les équipes de conformité

Les équipes de conformité sont chargées de vérifier si des conditions spécifiques doivent être ajoutées pour respecter les réglementations applicables à l'organisation. Elles référencent également les tests de bug bounty dans les mesures de sécurité de l'entreprise. Le délégué à la protection des données (DPO) est informé des modalités de déploiement du programme et s'assure de la conformité des prestations aux règles de protection des données. Il qualifie les intervenants conformément au RGPD, met à jour le registre des activités de traitement et participe à la contractualisation en définissant les obligations de chaque partie.

3.4 Les équipes métiers

Les équipes métiers doivent être informées de la mise en place des tests de bug bounty. Une collaboration préalable avec ces équipes est nécessaire avant le lancement de nouveaux programmes. Il est essentiel d'identifier les contraintes spécifiques liées à la réalisation de ces tests en production.

3.5 La direction des systèmes d'information (DSI)

Le ou la DSI joue un rôle clé dans la définition des processus nécessaires pour traiter rapidement les vulnérabilités identifiées grâce au bug bounty. Il ou elle participe à la mise en

place des règles de déclaration des vulnérabilités, à l'identification des « security champions » chargés de l'analyse et de la priorisation, ainsi qu'au suivi des vulnérabilités identifiées. Si des développements sont sous-traités, le ou la DSI veille à ce que les équipes de production intègrent les correctifs dans leurs activités habituelles. Une capitalisation des retours d'expérience (REX) peut permettre ensuite de faire monter en compétence les équipes internes afin que certaines des « erreurs » commises ne soient plus refaites dans de prochains développements ou mises en production.

3.6 Les équipes de production informatique

Les équipes de production contribuent à définir les processus nécessaires à la réalisation des programmes de bug bounty. Elles sont impliquées dans la définition des conditions de réalisation des tests, la déclaration des incidents et la communication avec les équipes internes chargées de la gestion des programmes. Elles sont responsables de l'ouverture des plateformes aux hunters, de la création de comptes de tests et des actions liées à la mise en production des correctifs. Elles doivent être tenues informées du lancement, des pauses et des arrêts des programmes de bug bounty.

3.7 Le Security Operation Center (SOC)

Le SOC est informé de la mise en place des programmes et des modalités des tests afin de pouvoir traiter les alertes de manière appropriée. Il doit pouvoir distinguer ces tests des activités malveillantes réelles, tout en analysant et en traitant les alertes provenant des tests. La supervision du SOC est essentielle pour veiller au respect des conditions des programmes, notamment en ce qui concerne le périmètre des activités des hunters.

Tour Eria – 5, rue Bellini
92821 Puteaux Cedex
France
✆ +33 1 53 25 08 80
clusif@clusif.fr

clusif.fr