Qu'est ce que le Bug Bounty ?

Un livre blanc rédigé par

YogOsha COLLABORATIVE CYBERSECURITY

Table des matières

Seconde édition - avril 2018

Le concept

En cybersécurité comme en médecine, tout commence par un diagnostic destiné à identifier un problème qui pourrait avoir une issue malheureuse s'il n'était pas traité à temps. Dans le cyber, ce problème est une faille de sécurité qui pourrait être exploitée à des fins malveillantes.

Jusqu'ici, il existait deux approches pour réaliser un tel diagnostic. La première consiste à utiliser des "scans automatiques", qui vont scruter les technologies en usage dans une organisation à la recherche de vulnérabilités, et produire un rapport imposant. Utile pour identifier des erreurs basiques, cette approche produit beaucoup de faux-positifs, n'est pas en mesure de détecter des failles fonctionnelles, et ne peut anticiper la créativité propre à la cybercriminalité et à l'esprit humain en général.

La seconde approche consiste à faire appel à un service de "pentesting" (de l'anglais "penetration testing"). On acquiert alors auprès d'une société spécialisée des "jours/homme" d'un "chercheur en cybersécurité" (un terme politiquement correct pour désigner un hacker éthique). Au bout du temps imparti, ce dernier dresse un inventaire des failles découvertes sur le système ainsi audité. Cette approche présente elle aussi des inconvénients : très lourde en ce qui concerne sa gestion, elle ne repose que sur la créativité d'un ou deux auditeurs, au plus, qui disposent d'un temps limité. Qui plus est, c'est une opération ponctuelle. Ce dernier point est un handicap en tant que tel, à l'heure où la plupart des organisations ont adopté un mode de développement informatique dit "agile", qui consiste à mettre en ligne régulièrement de nouvelles versions de leurs applicatifs, et donc d'y introduire de nouvelles failles. Car la production de nouveau code est nécessairement accompagnée de nouvelles failles - l'erreur est humaine, même chez les développeurs informatiques.

Le Bug Bounty complète ces deux approches de la cybersécurité, et renverse la logique économique du "pentesting", en lui appliquant les principes de l'économie collaborative.

Plutôt que d'acheter du temps de recherche en jours/homme, les organisations vont, à travers une plateforme de Bug Bounty, proposer à une communauté de chercheurs en cybersécurité d'acquérir les failles qu'ils pourraient trouver sur leurs systèmes, en indexant le prix de ces failles sur leur criticité, sur la base d'une fourchette de prix convenue d'avance.

On passe ainsi d'une logique de moyens à une logique de résultats, on n'achète plus du temps de recherche mais le résultat de cette recherche, et on comble ainsi les lacunes du pentesting. L'audit proposé par le Bug Bounty est permanent et continu, la multitude des chercheurs ainsi mobilisés offre une diversité en termes de créativité que le pentesting est incapable de proposer. La rapidité de mise en œuvre d'un Bug Bounty fait que cette approche est parfaitement compatible avec les cycles cadencés du développement agile.

D'un point de vue économique, le ROI d'un tel audit est bien plus évident : chaque faille acquise par une organisation lors d'un Bug Bounty lui permet de renforcer sa sécurité. Le budget est également bien plus simple à déterminer, car un Bug Bounty peut être capé par un budget maximal. Une fois le budget atteint, le Bug Bounty se met en pause. Le pentesting, lui, demande à "deviner" le temps nécessaire à la découverte de failles jusqu'ici inconnues, et cet audit n'est réalisé que par un unique expert la plupart du temps, dont on ne sait pas grand chose des performances, celle-ci ayant plus à faire avec sa créativité qu'à ses diplômes ou ses certifications.

Histoire du Bug Bounty

Etymologiquement, le terme 'bug' désigne depuis le XIXe siècle une erreur de conception dans un dispositif technique; il était fréquemment utilisé par Thomas Edison. Le Bounty est la prime, offerte au temps des cowboys aux chasseurs de primes, auxiliaires zélés de la justice de l'époque.

Le concept de Bug Bounty est apparu en 1995, imaginé par Netscape, l'une des toutes premières startups de l'ère de l'internet grand public. A l'époque les prix offerts aux chercheurs en sécurité qui participaient à la découverte de "bugs" techniques sur le navigateur Netscape étaient constitués de "goodies".

Mais c'est que quinze ans plus tard, en 2010, que Google, puis Facebook, appliquent le concept non plus aux bugs techniques mais aux failles de sécurité, lançant la vague du Bug Bounty. Ils ouvrent alors la voie à une multitude d'entreprises qui leur emboîteront le pas, issues pour la plupart du secteur des nouvelles technologies. Entre temps les « goodies » ont laissé place à des récompenses en cash.

Pourtant, si Google ou Facebook peuvent gérer eux-mêmes un Bug Bounty, ce n'est pas le cas de la plupart des entreprises, qui préfèrent passer par une plateforme de Bug Bounty leur assurant son organisation, sa promotion, l'accès à une communauté de chercheurs dédiée, ainsi que sa gestion.

C'est en 2012 qu'apparaissent aux Etats-Unis les premières plateformes de Bug Bounty telles que BugCrowd, HackerOne et Synack. Celles-ci vont populariser le concept au sein de la Silicon Valley et rapidement convertir la plupart des acteurs des NTIC américains à cette nouvelle approche collaborative de la cybersécurité. Le dernier géant californien à se convertir au Bug Bounty sera Apple, convaincu de cette nécessité après son affrontement malheureux face au FBI lors des dernières présidentielles américaines, où le FBI s'était finalement porté acquéreur d'une faille de sécurité lui permettant, face au refus d'Apple, d'accéder à l'iPhone verrouillé de l'auteur d'une attaque terroriste.

Aujourd'hui, l'essentiel des grands noms de la Silicon Valley pratique le Bug Bounty, et les primes offertes pour une faille critique par des acteurs tels que Google peuvent atteindre 200.000$, bien que le prix moyen d'une faille soit de l'ordre de 500$, toutes plateformes confondues. En 2016, c'est l'armée américaine qui a donné ses lettres de noblesse au Bug Bounty en lançant le sien en partenariat avec Synack et HackerOne, pour, par la suite, généraliser cette démarche et l'étendre à une multitude de systèmes informatiques sous sa supervision.

C'est en 2015 qu'apparaissent les premières plateformes de Bug Bounty en Europe. Avec Yogosha en France et Zerocopter aux Pays Bas, puis l'année suivante BountyFactory et BugBountyZone en France. En 2017 enfin apparaissait Intigriti en Belgique et FindBug au Kosovo. Chacune de ces plateformes propose une approche spécifique du Bug Bounty.

Un Bug Bounty, comment ça marche ?

Mettre en place un Bug Bounty est plutôt simple. La première étape consiste à délimiter un périmètre pour l'audit que l'on souhaite réaliser à travers une telle opération, et à rédiger une mission à l'intention de la communauté que l'on souhaite convier à son Bug Bounty. La plupart des plateformes proposent un accompagnement pour cela.

Il faut ensuite déterminer le budget qu'on est prêt à investir dans son Bug Bounty. C'est là encore particulièrement simple. Le paiement à la faille rationalise l'approche qui consiste à constituer une cagnotte qui, au fur et à mesure que l'on acquiert auprès des chercheurs de nouvelles failles, vient à diminuer. Une fois cette cagnotte épuisée, le Bug Bounty s'interrompt. On peut alors marquer une pause, le temps de corriger les failles identifiées, le mettre à l'arrêt, ou continuer en alimentant la cagnotte.

Il faut également déterminer une fourchette de prix pour les failles que les chercheurs d'une communauté seraient appelés à identifier et proposer à la vente dans le cadre d'un Bug Bounty. Différentes approches existent pour établir cette fourchette, certaines plateformes proposent une approche plus aboutie que d'autres, basée sur l'observation du marché et une multitude de paramètres qui peuvent impacter les dynamiques au sein de la communauté des chercheurs, tout en prenant en compte le contexte et la réalité de l'entreprise qui lance ainsi son Bug Bounty.

Enfin, une fois le Bug Bounty lancé, il s'agit de collecter les rapports de faille proposés par les chercheurs, de les valider en interagissant avec eux au besoin, et d'acquérir chaque rapport pour ensuite les faire suivre aux équipes techniques en charge de les corriger. Certaines plateformes proposent une gestion avancée des utilisateurs, permettant de convier différents interlocuteurs à un Bug Bounty afin de multiplier les échanges et les transferts de compétences entre la communauté de chercheurs en cybersécurité rassemblée sur la plateforme et une multitude de participants du coté de l'entreprise qui organise son Bug Bounty : responsables sécurité, analystes, développeurs, partenaires, sous traitants…

Le marché du Bug Bounty

Les récentes cyberattaques qui ont paralysé hôpitaux comme industriels annoncent un temps où la cybersécurité devient un enjeu vital pour toute organisation. La disruption de l'environnement législatif du cyber, annoncé par le Règlement Général sur la Protection des Données, ajoute au risque cyber un risque financier et réputationnel considérable.

Selon Gartner, le marché de la protection informatique a augmenté de 7,9% entre 2015 et 2016 pour atteindre 81,6 milliards de dollars. Selon CyberSecurityVentures, il pourrait atteindre 120 milliards de dollars en 2017, contre 3,5 milliards en 2004, soit un chiffre multiplié par 35 en 13 ans. Dans les 5 prochaines années, les entreprises devraient dépenser plus de 1.000 milliards de dollars en cybersécurité.

Le Bug Bounty s'inscrit dans ce marché global de la cybersécurité en croissance forte, et y prend une place appelée à être conséquente.

Un marché américain du Bug Bounty qui arrive à maturité

Aux USA, où les plateformes de Bug Bounty sont installées depuis 2012, trois acteurs majeurs se dégagent du lot : BugCrowd, HackerOne et Synack, faisant mentir l'adage qui veut que dans l'économie des plateformes, un seul acteur finisse par dominer le marché. Il est vrai que le marché de la cybersécurité est un peu particulier et n'obéit pas nécessairement aux mêmes règles que l'eCommerce ou le Search.

Alors que sur le continent américain la quasi-totalité du monde des technologies a adopté la pratique du Bug Bounty, les autres secteurs sont plus lents à faire évoluer leur panoplie en matière de cybersécurité. On trouve néanmoins des acteurs tels que United Airlines, General Electric ou Western Union parmi les adeptes du Bug Bounty.

Un marché européen naissant qui s'annonce très différent

En Europe, où il n'existe pas une telle concentration de géants des technologies, la mode du Bug Bounty a pris dans des entreprises bien plus traditionnelles, des figures du CAC40 qui font contraste avec les pratiquants américains, mais qui souhaitent rester discrètes, tout comme elles restent discrètes en général sur leur arsenal en matière de cybersécurité. Cette adoption par des acteurs économiques, habituellement en difficulté face à l'innovation, est incontestablement le fruit des efforts considérables que font les acteurs français de l'ancienne économie pour établir des relations mutuellement bénéfiques avec le monde des startups, afin de profiter d'une innovation née hors les murs.

La différence entre les deux côtés de l'Atlantique tient également à la pression exercée par l'Europe, notamment à travers le Règlement Général sur la Protection des Données, qui impose aux entreprises exerçant une activité sur le continent de renforcer la protection des données personnelles qu'elles manipulent, et annonce une époque où la moindre erreur se paiera au prix fort, tant en ce qui concerne les sanctions financières pour les contrevenants que les conséquences réputationnelles futures de la moindre fuite d'informations personnelles.

Les deux marchés évoluent très différemment, et il est à parier que l'Afrique, l'Asie et le Moyen-Orient évolueront également d'une façon qui leur est propre pour ce qui est d'adopter cette nouvelle approche de la cybersécurité.

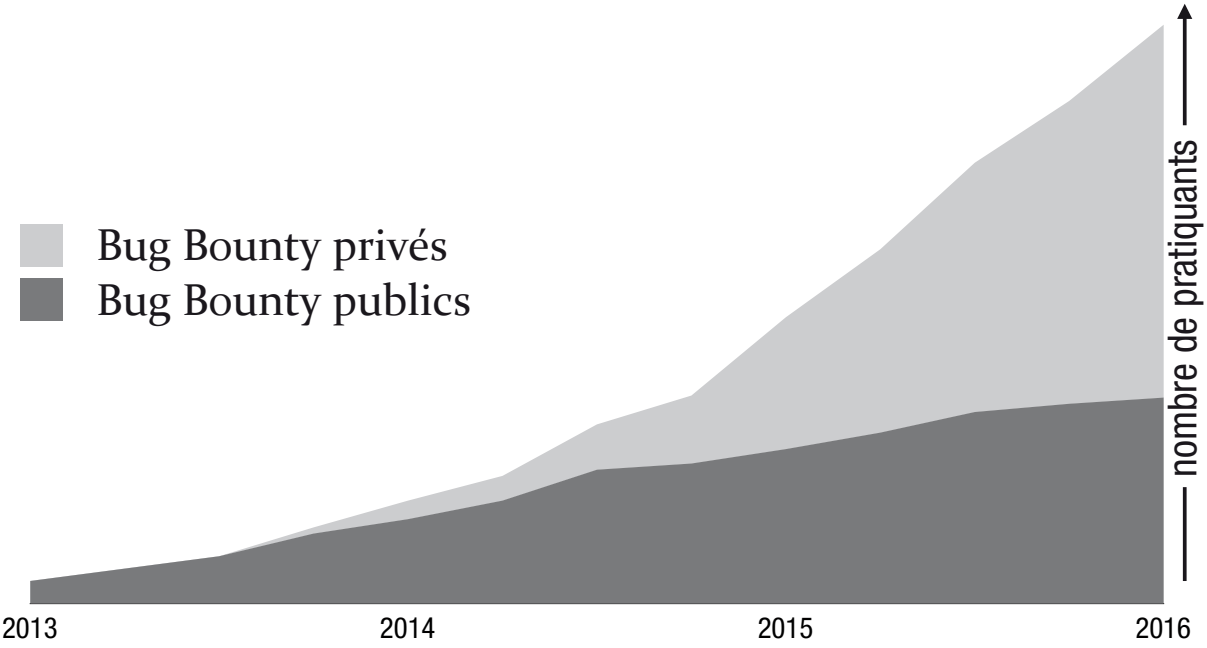
Yogosha, qui a déjà investi énormément de réflexion préalablement à son lancement en France afin d'adapter le concept du Bug Bounty au continent européen, a dans son viseur l'Afrique et le Moyen-Orient. Les tout premiers pas de la startup sur le continent africain se sont traduits par l'obtention du label Maroc Numeric Cluster, et l'entreprise compte bien faire du Maroc sa base avancée sur le continent africain.

L'évolution du Bug Bounty

Il existe trois types de Bug Bounty selon la façon d'assembler la "multitude" qui sera mobilisée sur un Bug Bounty.

A l'origine, les Bug Bounties étaient "publics", c'est-à-dire qu'ils étaient ouverts à tous, amateurs comme professionnels de la cybersécurité, n'importe qui pouvait proposer à la vente une faille qu'il avait découverte sur un périmètre défini par l'entreprise organisatrice. Aujourd'hui, Google, Facebook ainsi que quelques autres proposent encore des Bug Bounties publics. Ils ont pour avantage de permettre à leurs organisateurs de mettre en place des relations vertueuses avec le monde des chercheurs en cybersécurité et d'intégrer à leur écosystème différentes communautés hackers. Cela peut être un objectif important pour des entreprises telles que Google, qui cherchent à valoriser leur "marque employeur" auprès de communautés hackers. Ils ont pour inconvénient de générer énormément de faux positifs (seuls 5% des rapports de faille ainsi envoyés à Facebook sont valides), d'entraîner des frais de gestion très conséquents, et de mobiliser d'importantes ressources humaines du côté de l'entreprise qui l'organise.

Du public au privé



C'est avec les Bug Bounties privés que le marché a véritablement décollé à partir de 2015, et qu'un nombre croissant d'entreprises ont adopté cette nouvelle approche de la cybersécurité. Un Bug Bounty privé consiste à en réserver l'accès à une sélection de chercheurs en cybersécurité, choisis pour leur professionnalisme et leur expérience. Les résultats d'une telle approche sont en effet bien plus simples à gérer, le nombre de faux positifs bien plus faible, et l'interaction avec les chercheurs facilitée du fait de leur expérience de la relation clientèle.

C'est cette approche du Bug Bounty "on demand" qui a convaincu les premiers clients "CAC40" français de se mettre au Bug Bounty.

Puis sont apparus les Bug Bounties "on demand", où le pool de chercheurs assemblé à l'occasion d'un Bug Bounty est constitué sur mesure, en fonction des objectifs de l'entreprise qui organise son Bug Bounty et des technologies auditées à cette occasion. Ce type de Bug Bounty a encore amélioré l'efficacité de la démarche.

Qui pratique le Bug Bounty ?

Aujourd'hui, des milliers d'entreprises de toutes tailles, de la startup au géant industriel en passant par la quasi-totalité de la Silicon Valley, ont complété leurs dispositifs cybersécurité par du Bug Bounty. En France, le départ est assez fulgurant. Introduit sur le marché à la fin de l'année 2015, le Bug Bounty a séduit plusieurs CAC40 au point que le secteur "non technologique" sera bientôt plus avancé sur le sujet en France qu'aux Etats-Unis.

Un problème de souveraineté numérique

A l'heure où les grandes plateformes internet américaines dominent le monde et s'accaparent toutes les parts de marché, le monde du Bug Bounty est bien parti pour faire mentir l'adage du "winner takes it all".

Yogosha vise à offrir à ses clients une véritable indépendance, en leur offrant, de par sa conception dite de "privacy by design", une parfaite souveraineté, quels qu'ils soient et où qu'ils soient. Ségrégation des données, chiffrement, tout a été mis en œuvre pour assurer une sécurité maximale et une confidentialité absolue aux utilisateurs de la plateforme, y compris, bien sûr, un Bug Bounty.

Si la domination des GAFA a réveillé beaucoup de consciences en Europe, qui y voient une perte de souveraineté, l'arrivée des plateformes de Bug Bounty pose le problème sous un angle autrement plus critique, puisqu'il s'agit désormais de souveraineté en matière de défense. A l'heure où la cybercriminalité a montré sa capacité à paralyser une partie du secteur hospitalier britannique et plusieurs acteurs industriels en exploitant une arme dérobée à la NSA, tout le monde s'accorde à dire qu'il est stratégique de disposer, sur le sol européen, de startups dans le secteur de la cyberdéfense aptes à relever le défi et à proposer une alternative sérieuse aux plateformes américaines.

La question de la propriété intellectuelle des failles découvertes

Deux approches opposées de la propriété intellectuelle des failles découvertes par les chercheurs lors d'un Bug Bounty s'opposent. La plus répandue est celle qui a accompagné la naissance du Bug Bounty, elle s'appelle le « coordinated disclosure ». Elle fait suite au « full disclosure », une pratique qui date d'avant l'apparition du Bug Bounty tel que défini par Google et Facebook en 2012. Cette pratique du « full disclosure » consistait, pour un chercheur qui découvrait une faille sur un système, d'en avertir l'administrateur et, si l'entreprise ne corrigeait pas la faille signalée, à la révéler publiquement, poussant ainsi l'entreprise à la corriger. Une pratique en tout point illégale, mais qui avait le mérite de forcer les entreprises à se sécuriser, à une époque où le corpus législatif n'était pas particulièrement contraignant.

Le « coordinated disclosure », qui se pose en alternative, si ce n'est en évolution du « full discosure », consiste, une fois une faille signalée et payée sur une plateforme de Bug Bounty et corrigée par l'entreprise, à la révéler publiquement, par le biais de la plateforme, ce qui permet au chercheur l'ayant découverte de montrer aux yeux de tous son expertise et sa valeur.

La plupart des grandes plateformes de Bug Bounty en sont restées au principe du « coordinated disclosure », seul deux plateformes ont adopté une pratique différente : l'américain Synack et le français Yogosha. L'approche de ces dernières consiste à considérer une faille de sécurité comme une information confidentielle, qui, lors de sa vente sur une plateforme de Bug Bounty, voit sa propriété transférée à l'entreprise qui organise son Bug Bounty et reste sa propriété pleine et entière. Ces deux plateformes ont pour point commun de rassembler des communautés bien plus limitées en nombre que les autres, mais constituées de chercheurs sélectionnés pour leur professionnalisme et leur experience, qui n'ont, du coup, pas besoin de faire valoir publiquement leurs exploits et leurs découvertes pour se constituer un curriculum.

L'écosystème des chercheurs en cybersécurité

Un marché du travail tendu

Le marché du travail pour les professionnels de la cybersécurité est caractérisé par une "tension" exceptionnelle. Selon l'Agence Nationale de la Sécurité des Systèmes d'Information, sur quatre offres d'emploi publiées en France, une seule trouve un candidat. La situation ne peut qu'empirer au vu d'une étude publiée par la Commission européenne, qui estime qu'il manquera d'ici à cinq ans plus de 750.000 talents en matière de cybersécurité sur le continent européen pour faire face aux problèmes à venir.

Face à une problématique qui ne peut trouver de réponse immédiate, et qui va demander des efforts considérables en matière d'éducation et de formation professionnelle, le Bug Bounty apporte une solution pragmatique.

D'une part, le Bug Bounty abolit en quelque sorte les frontières. Les chercheurs en sécurité de la communauté Yogosha viennent des quatre coins du monde, et sont mobilisables à tout instant. Sur les plateformes américaines, les chercheurs vivant sur le continent indien sont ainsi très nombreux, compensant ainsi l'incapacité du continent nord-américain, comme de l'Europe, à disposer sur son sol de ressources humaines en nombre suffisant. Certains Bug Bounties peuvent cependant n'être accessibles qu'à des nationaux, comme le Bug Bounty du Pentagone aux USA ou ceux de certains OIV en France.

D'autre part, la productivité d'une foule assemblée avec soin est bien supérieure à ce que le travail salarié est capable de produire. Trouver une faille dans un système informatique complexe peut s'imaginer comme une victoire dans une partie d'échecs. Kasparov à lui seul est capable de mener avec succès plusieurs dizaines de parties en même temps, et cette productivité incroyable

se retrouve chez les meilleurs chercheurs en sécurité, comme ceux que Yogosha rassemble petit à petit au sein de sa communauté.

Les chercheurs, de leur côté, y gagnent des revenus nettement supérieurs à ce que leur propose un emploi salarié, pour ceux qui consacrent l'essentiel de leur temps de travail au Bug Bounty. Quant à ceux qui font du Bug Bounty une activité annexe, ils y trouvent un complément de revenu souvent très confortable. Le Bug Bounty offre également des perspectives très appréciées dans le monde des hackers : une maîtrise totale de son temps, et une liberté de mouvement totale. Car on peut travailler sur une plateforme de Bug Bounty de n'importe où sur terre, pour peu que l'on dispose d'une connexion internet, ou même, comme le font certains, en voyageant sans cesse d'une conférence à l'autre, à la façon d'un globe-trotteur.

Au final, un groupe de chercheurs en sécurité de haut niveau fédéré par une plateforme de Bug Bounty peut rivaliser en terme d'expertise avec les meilleures équipes de R&D du secteur, voir avec certaines petites agences gouvernementales, et c'est ce type de compétences que le Bug Bounty peut mettre au service des entreprises, car ces mêmes entreprises font face à ce même type d'expertises du côté de la cybercriminalité.

Noir, gris et blanc, trois nuances de marchés

Les plateformes de Bug Bounty s'inscrivent dans le commerce plus large des failles de sécurité. Un marché - ou plutôt des marchés - où s'achètent et se vendent des failles de sécurité qui peuvent, selon l'usage qu'on en fait, être utilisées à des fins défensives ou offensives. Ces trois marchés, noir, gris et blanc, ont des acteurs et des usages spécifiques, et constituent ensemble un marché global pour les failles de sécurité, les plateformes de Bug Bounty sont les derniers acteurs à entrer dans cet écosystème avec la ferme intention de le disrupter.

Le marché noir

Les acheteurs sur le marché noir des failles de sécurité sont pour l'essentiel des organisations criminelles, mais on y trouve également des agences de renseignement ou des officines pratiquant l'intelligence économique. Les transactions y sont bien plus lentes que sur les marchés blanc et gris, mais les prix bien plus élevés. Les failles qui y sont acquises sont systématiquement utilisées à des fins offensives, le plus souvent criminelles.

Les "places de marché" qui structurent le marché noir des failles de sécurité se trouvent pour la plupart sur le fameux "darknet", et bien sûr aucune forme de régulation ne s'applique à ce marché, ce qui ne l'empêche pas d'avoir ses règles et ses usages.

Le marché gris

Les acheteurs du marché gris sont des gouvernements, des forces de l'ordre ou des agences de renseignement. Les failles qui y sont achetées seront, selon toutes vraisemblances, utilisées à des fins offensives, mais de façon responsable. Certains gouvernements utilisent cependant ces failles pour espionner leur opposition politique ou les médias, ou bien encore faire de l'espionnage industriel au profit de leurs industries nationales. Comme toujours quand il s'agit du bien et du mal, il existe une zone grise, occupée ici par le marché éponyme.

Le marché gris constitué par ces acteurs est, contrairement au marché noir, régulé, notamment à travers les arrangements de Wassenaar, qui touchent au commerce des armes et englobent celui des armes numériques.

Le marché blanc

Dernier arrivé, le marché blanc est constitué par l'ensemble des plateformes de Bug Bounty, ainsi que par les entreprises qui les utilisent pour acheter leurs propres failles de sécurité. Le fait que, contrairement aux marchés gris et noir, sur ce marché blanc, les propriétaires des failles soient les seuls à pouvoir les acquérir, fait que ces failles ne peuvent être utilisées qu'à des fins défensives.

D'un point de vue macro-économique, l'objectif de ce marché blanc est de disrupter les marchés gris et noir en étant plus fluide, plus rapide et plus simple.

Rappelons qu'une faille, une fois corrigée, n'a plus la moindre valeur sur quelque marché que ce soit. C'est pour cette raison du reste que les prix proposés par des entreprises telles que Google pour leurs Bug Bounty peuvent atteindre des sommes dépassant les centaines de milliers de dollars : ces mêmes failles ont également une valeur très élevée sur le marché noir.

La plateforme Yogosha

Une startup reconnue comme faisant parti des plus prometteuses

En un an et demi d'existence, Yogosha a accumulé les prix et les réussites. Repérée dès le début par Hewlett-Packard Entreprise, qui l'a coachée dans le cadre de sa "Promo Startup 2016", la jeune pousse a obtenu la bourse Frenchtech en mars 2016. Elle a ensuite bénéficié de l'accompagnement de Scientipôle destiné à financer son développement. Au printemps 2016, Yogosha obtient le label Maroc Numeric Cluster, reconnaissant son innovation et l'invitant à mettre pied sur le marché marocain, véritable hub vers le marché africain, et intègre Axeleo, le premier accélérateur B2B de la FrenchTech. La startup devient rapidement membre du Syntec Numérique et termine l'année en remportant le Grand Prix de l'Innovation de la Ville de Paris, dans la catégorie Service aux entreprises. Quelques mois plus tard, en mai 2017, Yogosha remporte le prix Scientistar organisé par Scientipôle, dans la catégorie Transformation Numérique de l'Entreprise. Au même moment, Yogosha est sélectionnée pour faire partie de la première promotion du Founders Program, l'invitant à rejoindre dès son ouverture Station F, le plus grand campus de startups du monde, lancé par Xavier Niels à Paris. En juin 2017, Yogosha boucle sa première levée de fonds, quatre mois plus tard, la startup intègre l'incubateur cybersécurité de Thales.

L'importation d'un concept américain

Yogosha est parti du constat, fait par ses fondateurs dès 2014, que les plateformes américaines de Bug Bounty auraient à affronter un écart culturel important pour arriver à s'implanter en Europe. C'est après avoir finement étudié le marché européen de la cybersécurité que l'équipe de Yogosha a commencé par proposer des Bug Bounties "on demand", puis des Bug Bounties privés, en prenant

appui sur une communauté recrutée avec soin : une formule plus à même de séduire une clientèle européenne, et bien plus rassurante que les Bug Bounties publics.

Les mentalités en Europe en matière de cybersécurité sont très différentes, à l'image du rapport au risque qui culturellement n'est pas le même, sans que cela ne traduise de retard particulier. Alors qu'aux USA la pratique du Bug Bounty est revendiquée et fait l'objet de campagnes de communication, les pratiquants français sont pour l'instant plus timides, et ne souhaitent pas à ce stade s'afficher comme des utilisateurs de cette approche innovante de la cybersécurité. Seules les startups de l'univers B2B affichent fièrement leur adoption du Bug Bounty, et l'utilisent comme un gage de sérieux vis-à-vis de leurs clients.

Plateforme et communauté, les deux piliers de l'offre de Yogosha

Yogosha propose une plateforme de cybersécurité collaborative dédiée à la détection de failles de sécurité. Cette plateforme permet de mettre en place une dynamique collaborative au sein d'une équipe de pentesteurs, son management et l'entreprise qu'ils auditent, ainsi qu'avec la communauté de chercheurs en cybersécurité sélectionnée et assemblée par Yogosha.

Les avantages sont multiples : standardisation des rapports de failles, suivit en temps réel d'une équipe lors d'une mission de pentesting, classification et évaluation de la criticité des failles découvertes au fil de l'eau, agilité à appréhender la globalité d'une mission, dispensant ainsi de bien des réunions inutiles, et relation directe et continue avec le client final chez qui l'audit est réalisé.

Cette plateforme permet de centraliser les travaux d'une équipe de pentesteurs, ainsi que de leur adjoindre les service d'une communauté riche et diversifiée.

Parallèlement, Yogosha assemble et constitue une communauté d'élite de chercheurs en cybersécurité, pensée pour être une réserve de main d'œuvre de haut niveau disponible à tout moment et mobilisable à la demande. La communauté Yogosha se distingue par le mode de sélection particulièrement rigoureux des chercheurs, qui outre un véritable examen d'entrée permettant de s'assurer de leur expertise, de leur professionnalisme et de leur capacités pédagogiques, doivent être cooptés par deux membres de la communauté s'engageant sur leur probité.

La constitution d'une communauté d'élite

Officiellement lancée fin 2015, Yogosha s'appuie aujourd'hui sur une communauté de confiance de chercheurs en sécurité dont l'état civil et le curriculum sont parfaitement connus de la startup comme de ses utilisateurs. Ils ont été recrutés de façon méticuleuse, en prenant soin de sélectionner des talents diversifiés, qui ont tous en commun un véritable professionnalisme dans la relation clientèle, une créativité hors du commun dans leur approche des technologies, et une véritable envie de partager leurs connaissances avec les utilisateurs de la plateforme Yogosha.

Les chercheurs en sécurité seniors de la communauté Yogosha, professionnels, créatifs et pédagogues, sont recrutés à travers un processus rigoureux et une sélection drastique à l'entrée.

Cette logique de sélection à l'entrée est très différente de celle des plateformes américaines, qui ont commencé par proposer une offre de Bug Bounty public et ont par la suite fait évoluer leur

offre vers du Bug Bounty privé, en ne retenant que les chercheurs les plus performants, ou bien encore des plateformes qui se sont montées en prenant appui sur une communauté existante, faite d'amateurs comme de professionnels.

La plateforme Yogosha a en effet comme objectif de favoriser des échanges de qualité et un véritable transfert de connaissances entre le chercheur ayant découvert une faille et l'équipe cybersécurité ainsi que les développeurs qui utilisent la plateforme. Le but est de permettre une utilisation du Bug Bounty en continu, de façon synchrone avec les cycles propres au développement agile, en cours dans la plupart des entreprises et dans la quasi totalité des startups, ainsi que de favoriser les transferts de compétences entre chercheurs et utilisateurs de la plateforme.

Des standards de marché pour une économie de marché déroutante

Dans cette inversion de la logique économique propre au Bug Bounty, où c'est l'organisateur d'un Bug Bounty qui fixe le prix de ses propres failles appelées à être découvertes par une communauté de chercheurs, il a fallu innover pour faciliter la prise en main d'une offre qui peut apparaître comme déroutante.

Pour cela, Yogosha a mis au point une approche rationnelle à l'intention de ses utilisateurs, destinée à déterminer une fourchette de prix pour leurs propres failles. La startup a imaginé une matrice de calcul prenant en compte aussi bien l'existant en matière de cybersécurité, l'appréciation du risque par le client sur le périmètre audité, la taille de ce dernier, ainsi qu'une dizaine d'autres critères permettant de fixer le juste prix pour chaque criticité de faille découverte, ainsi que pour chaque itération d'un même Bug Bounty.

Une fois cette fourchette de prix établie, il s'agit de régler cette même problématique du côté des chercheurs, afin de leur offrir une méthode destinée à déterminer le prix - corrélé à la criticité - d'une faille qu'ils proposent à la vente. Pour cela, Yogosha a été la première plateforme au monde à se baser sur le standard de marché CVSS, largement reconnu dans le monde de la cybersécurité. En proposant aux chercheurs de saisir les éléments permettant de calculer la criticité de la faille qu'ils ont découverte, tout en laissant la possibilité à l'acheteur, au besoin, de réviser ce calcul destiné à déterminer le prix d'une faille, Yogosha a éliminé la friction liée à la négociation du prix, un point d'achoppement courant dans l'expérience client des utilisateurs de plateformes de Bug Bounty. Yogosha a ainsi fluidifié les échanges pour les focaliser sur le transfert de compétences, tout en valorisant la relation clientèle.

Car le marché établi par une plateforme de Bug Bounty est quelque peu biaisé, au sens économique du terme, par le fait qu'il ne peut y avoir qu'un seul acheteur. Le "widget CVSS" mis au

point par Yogosha élimine ce qui constituait un obstacle à une relation sereine entre chercheurs et clients sur une plateforme de Bug Bounty.

Depuis son introduction par Yogosha en février 2016, plusieurs autres plateformes, tant aux USA qu'en France, ont adopté l'usage du CVSS, sans pour autant proposer le processus de double validation propre à Yogosha.

Privacy by design

Afin de se mettre en conformité avec le droit Européen, mais surtout dans le but d'offrir une garantie de confidentialité à ses utilisateurs sur des données particulièrement critiques, la plateforme Yogosha a été conçu dès le départ dans une logique de "privacy by design". Les données déposées sur la plateforme sont systématiquement chiffrées, seuls le chercheur ayant rapporté une faille et le client organisant son Bug Bounty via la plateforme y ont accès. Le client peut, s'il le désire, inviter des membres de ses équipes, ou un partenaire extérieur sur son environnement de Bug Bounty, en utilisant les fonctionnalités de gestion d'équipe de la plateforme, mais il reste seul maître à bord.

Une plateforme co-construite avec ses utilisateurs

Deux an après son lancement, la plateforme dispose de nombreuses fonctionnalités dont beaucoup ont été co-construites avec ses clients et les chercheurs qui y travaillent.

Elle a su s'adapter aux différents besoins exprimés par ses utilisateurs, startups comme Grands Comptes, qui utilisent le Bug Bounty aussi bien pour monitorer une solution existante et en faire un bilan en matière de sécurité, que pour benchmarker la qualité des développements de leurs prestataires. Certains ont commencé à intégrer le Bug Bounty dans leurs cycles de développement agile, ouvrant la voie à une nouvelle approche de la cybersécurité, le DevOpsSec.

Vers le DevOpsSec

Si les scans automatiques peuvent aisément s'intégrer à une approche agile de type DevOps, ce n'était pas le cas jusqu'ici de l'approche humaine de la détection de faille qu'est le "pentesting", dont le temps de mise en œuvre ne permettait pas de se synchroniser avec les "sprints" qui rythment les développements informatiques de nos jours.

Le Bug Bounty, qui donne des résultats dans les premières vingt-quatre heures qui suivent son lancement, et qui peut se lancer en moins d'une heure, pallie à cet inconvénient et ouvre la voie à l'intégration d'une véritable taskforce crowsourcée de cybersécurité au cœur d'une démarche DevOps. C'est l'un des objectifs de Yogosha, mis en œuvre avec succès par plusieurs startups avec lesquelles Yogosha travaille en étroite collaboration.

C'est une petite révolution copernicienne dans le monde de la cybersécurité, qui jusqu'ici arrivait après coup, une fois les développements finalisés. En insérant la détection de faille en amont, le délai qui sépare la création du code qui recèle une faille et sa détection se raccourcit considérablement, offrant une chance à celui qui a développé un code contenant une faille de la corriger dans la foulée; ce qui abaisse très significativement le coût d'un tel correctif, et permet aux déve-

loppeurs d'apprendre des éléments de cybersécurité sur la base d'un code qu'ils ont eux même produit. Le transfert de compétences et l'apprentissage sont ainsi maximisés.

Evangéliser l'entreprise

Mais les bénéfices d'un Bug Bounty pour une entreprise ne s'arrêtent pas là. Avec des rapports de faille clairs et immédiatement activables, accompagnés d'un "proof of concept" qui illustre la façon dont la faille pourrait être exploitée à des fins malveillantes, il devient aisé pour quiconque dans l'entreprise de réaliser ce que peut être concrètement une attaque informatique à travers un exemple concret, qu'ils peuvent même parfois reproduire par eux-mêmes.

C'est ce qu'a constaté Yogosha lors des retours d'expérience réalisés auprès de ses clients, en particulier chez les startups au sein desquels les équipes sécurité sont proches du reste de l'entreprise, et ont saisi cette occasion d'évangéliser la cybersécurité au sein de leur startup. Les anecdotes sont nombreuses, du "product owner" qui réalise qu'il est préférable de retarder la sortie d'une nouvelle fonctionnalité pour donner la priorité à la cybersécurité, aux commerciaux qui abordent désormais la cybersécurité sous un angle plus concret, et en parlent d'autant mieux à leurs clients et prospects en utilisant les résultats d'un Bug Bounty lors de leurs échanges.

Q&R

Pourquoi est-ce si efficace ?

Plus de ressources

Un programme de Bug Bounty permet d'augmenter considérablement les effectifs potentiels par rapport à l'approche traditionnelle du pentesting, démultipliant ainsi les chances de trouver, à tout moment, de nouvelles failles de sécurité.

Avoir à disposition une telle communauté de chercheurs en sécurité auditant votre technologie à tout moment s'apparente à un audit de sécurité permanent.

Une multitude de créativités

Une vaste communauté, en perpétuelle expansion, se traduit logiquement par une multitude de profils talentueux venant d'horizons différents et possédant des compétences et des points de vue uniques.

Certains chercheurs en sécurité ont des capacités et des champs d'expertise très vastes tandis que d'autres sont devenus particulièrement pointus dans des domaines spécifiques.

Ainsi assemblées, leurs créativités combinées contribuent à la découverte de failles extrêmement variées lors d'un programme de Bug Bounty.

De meilleurs résultats

Les scanners automatiques sont extrêmement limités, et ne sont en mesure de détecter que ce qu'ils ont été programmés à reconnaître. Les pentesteurs, quant à eux, sont restreints par les connaissances et les capacités spécifiques, et produisent des résultats limités au peu de chercheurs impliqués dans un audit.

Le crowdsourcing, par nature, n'est pas soumis à ces contraintes. Plus de chercheurs, et plus de variété, produisent de meilleurs résultats.

Un meilleur retour sur investissement

Lors d'un Bug Bounty, vous ne payez que pour une faille découverte, pas pour sa recherche. Vous ne rémunérez donc plus des jours-homme, mais des failles tangibles.

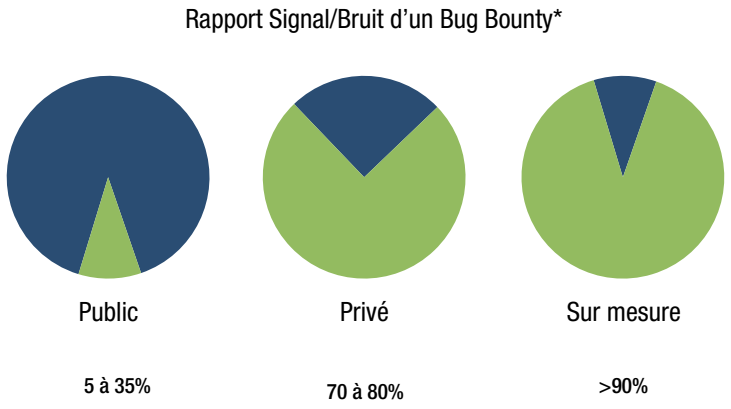
Contrairement aux méthodes traditionnelles où les entreprises payaient pour le temps passé à tester leurs applications indépendamment des résultats obtenus, on ne paie ici que pour des failles avérées. On passe d'une logique de moyens à une logique de résultats.

Pourtant, du fait de sa nouveauté, le Bug Bounty se heurte à de nombreuses appréhensions. Dans ce guide, nous allons tenter de mettre au clair certains aspects du Bug Bounty qui ne sont pas toujours limpides.

Public, privé, quelle différence ?

Il existe trois types de Bug Bounty selon la façon d'assembler la "multitude" qui sera mobilisée sur un Bug Bounty.

A l'origine, les Bug Bounties étaient "publics", c'est-à-dire qu'ils étaient ouverts à tous, amateurs comme professionnels de la cybersécurité, n'importe qui pouvait proposer à la vente une faille qu'il avait découverte sur un périmètre défini par l'entreprise organisatrice. Aujourd'hui,



Google, Facebook ainsi que quelques autres proposent encore des Bug Bounties publics.

Ils ont pour avantage de permettre à leurs organisateurs de mettre en place des relations vertueuses avec le monde des chercheurs en cybersécurité et d'intégrer à leur écosystème différentes communautés hackers. Cela peut être un objectif important pour des entreprises telles que Google, qui cherchent à valoriser leur "marque employeur" auprès des communautés hackers.

Ils ont pour inconvénient de générer énormément de faux positifs (seuls 5% des rapports de faille ainsi envoyés à Facebook sont valides), d'entraîner des frais de gestion très conséquents (selon une étude de Cobalt, pour 1€ dépensé en achat de faille, il faut compter 1,80€ pour la gestion d'un Bug Bounty public), et de mobiliser d'importantes ressources humaines du côté de l'entreprise qui l'organise.

Les Bug Bounties publics remontent des failles bien plus rapidement cependant, jusqu'à quatre fois plus vite selon le dernier rapport de HackerOne, ce qui n'a pas grand intérêt cependant, car peu d'entreprises sont en mesure de corriger leurs failles à une telle vitesse, et ne fait guère qu'augmenter le nombre de « duplicates », contribuant ainsi à affaiblir le rapport signal/bruit d'un Bug Bounty.

C'est avec les Bug Bounties privés que le marché a véritablement décollé à partir de 2015, et qu'un nombre croissant d'entreprises a adopté cette nouvelle approche de la cybersécurité.

Un Bug Bounty privé consiste à en réserver l'accès à une sélection de chercheurs en cybersécurité, choisis pour leur professionnalisme et leur expérience. Les résultats d'une telle approche sont en effet bien plus simples à gérer, le nombre de faux positifs bien plus faible, et l'interaction avec les chercheurs facilitée du fait de leur expérience de la relation client.

En 2016, selon le dernier rapport de HackerOne, 92% des Bug Bounties étaient privés, ce qui indique clairement la direction prise par le marché. En pratique, en dehors du secteurs des technologies, et dans une bien moindre mesure du secteur bancaire, aucun secteur ne lance de Bug Bounty publics.

Puis sont apparus les Bug Bounties "sur mesure", où le pool de chercheurs assemblé à l'occasion d'un Bug Bounty est constitué à la demande, en fonction des objectifs de l'entreprise qui organise son Bug Bounty et des technologies auditées.

Ce type de Bug Bounty a encore amélioré l'efficacité de la démarche, et a incité les Grands Comptes en France à se lancer dans le Bug Bounty.

Quelles sont ces communautés fédérées par les plateformes de Bug Bounty ?

Aujourd'hui, des milliers d'entreprises de toutes tailles, de la startup au géant industriel en passant par la quasi-totalité de la Silicon Valley, ont complété leurs dispositifs cybersécurité par du Bug Bounty. En France, le départ est assez fulgurant. Introduit sur le marché à la fin de l'année 2015, le Bug Bounty a séduit plusieurs CAC40 au point que le secteur "non technologique" sera bientôt plus avancé sur le sujet en France qu'aux Etats-Unis.

Yogosha est parti du constat, fait par ses fondateurs dès 2014, que les plateformes américaines de Bug Bounty auraient à affronter un écart culturel important pour arriver à s'implanter en Europe. C'est après avoir étudié le marché européen de la cybersécurité et s'être entretenu avec de nombreux responsables du secteur, que l'équipe de Yogosha a adapté le concept américain du Bug Bounty aux besoins et aux contraintes du marché européen, en prenant appui sur une communauté recrutée avec soin.

Pour intégrer la communauté Yogosha, un chercheur en sécurité doit passer un examen d'une durée de trois heures environ, permettant d'évaluer ses compétences techniques, ses capacités en termes de relation client, et son appétence à partager, à travers des rapports de failles, ses connaissances auprès de ceux qui seront en charge de réparer les failles identifiées. Chaque chercheur doit par ailleurs avoir été coopté par deux membres de la communauté. Leurs identités sont vérifiées, et sont visibles de nos clients, par ailleurs, un "background check" est effectué sur chaque profil. La communauté est structurée par un réseau d'ambassadeurs Yogosha, personnalités reconnues du monde de la cybersécurité, en charge de l'animation de la communauté, de la collecte de feedbacks permettant d'améliorer le produit, et du recrutement de nouveaux membres.

C'est sur la base de cette communauté fermée que Yogosha a construit son offre de Bug Bounty. Cette logique de sélection à l'entrée est très différente de celle des plateformes américaines, qui ont commencé par proposer une offre de Bug Bounty public, et ont par la suite fait évoluer leur offre vers du Bug Bounty privé, en ne retenant que les chercheurs les plus performants, ou bien encore des plateformes qui se sont montées en prenant appui sur une communauté existante,

faite d'amateurs comme de professionnels, et bien sûr des plateformes qui prennent appui sur les inter-contrats d'une société de service, peu ou pas incentivés pour leur découvertes.

Quels types d'entreprises font appel au Bug Bounty ?

Apparus il y a plus de vingt ans aux USA, les programmes de Bug Bounty ont longtemps été l'apanage des entreprises issues du monde des technologies. Aux Etats-Unis, la majorité des entreprises ayant un programme de Bug Bounty sont issues de la Silicon Valley, même s'ils sont désormais adoptés par des entreprises venues d'horizons très différents, tels Western Union ou United Airlines.

En Europe, où il n'existe pas une telle concentration de géants des technologies, la mode du Bug Bounty a pris dans des entreprises bien plus traditionnelles, des figures du CAC40 qui font contraste avec les pratiquants américains, mais qui souhaitent rester discrètes, tout comme elles restent discrètes en général sur leur arsenal en matière de cybersécurité. Cette adoption par des acteurs économiques, habituellement en difficulté face à l'innovation, est incontestablement le fruit des efforts considérables que font les acteurs français de l'ancienne économie pour établir des relations mutuellement bénéfiques avec le monde des startups, afin de profiter d'une innovation née hors les murs.

La différence entre les deux côtés de l'Atlantique tient également à la pression exercée par l'Europe, notamment à travers le Règlement Général sur la Protection des Données, qui donne encore quelques mois aux entreprises exerçant sur le continent pour renforcer la protection des données personnelles qu'elles manipulent, avant de passer à une phase où la moindre erreur se paiera au prix fort, tant en ce qui concerne les sanctions financières pour les contrevenants que les conséquences réputationnelles futures de la moindre fuite d'informations personnelles.

Les programmes privés et "sur mesure" ont également largement contribué à entraîner des acteurs traditionnels à adopter l'usage du Bug Bounty. Plus sécurisant, car limité à des chercheurs pré-qualifiés et professionnels, les Bug Bounty privés séduisent un nombre croissant de Grands Comptes en Europe tout en attirant à eux les startups ayant atteint un stade de maturité où la cybersécurité est devenu un enjeu central, en particulier dans le B2B.

La plupart du temps, les entreprises commencent par un programme de Bug Bounty "sur mesure", en assemblant un pool composé de compétences particulières ou d'expertises spécifiques, tout en prenant en compte les objectifs spécifiques d'un Bug Bounty, comme la montée en compétences infosec des équipes Dev côté client.

Faire un Bug bounty, quels sont les risques ?

L'idée d'inviter la terre entière à auditer ses technologies semble à première vue effrayante, et si Google ou Facebook sont capables de gérer de tels programmes, il en est tout autrement de la plupart des entreprises.

Peu d'entre elles ont la capacité à orchestrer de tels programmes, et elles ne sont pas nécessairement enthousiastes à l'idée de sous traiter à un tiers la gestion de leur Bug Bounty, ce qui peut également représenter un risque et ajoute une complexité juridique et opérationnelle.

Gérer au quotidien des relations avec une multitude de chercheurs ayant des compétences très disparates, du professionnel de haut niveau au script kiddy, demande un savoir faire certain, et représente un stress indéniable, surtout quand il s'agit de négocier le prix d'une faille avec un inconnu qui peut potentiellement être très nuisible pour votre SI et porter gravement atteinte à votre réputation.

S'adresser à une plateforme basée sur une communauté de confiance, aux conditions d'accès drastiques, résout l'essentiel du problème. Vous n'avez plus à faire qu'à des chercheurs professionnels, dont l'identité, visible de tous, a été certifiée par un tiers de confiance, et dont le profil a été vérifié et validé par la plateforme. Le risque lié à une telle opération est tout à fait similaire à une campagne de pentesting traditionnelle : particulièrement faible. Du reste, annoncer publiquement votre Bug Bounty privé n'attirera pas plus les farfelus qui en seraient d'office exclus que le fait d'officialiser la mise en œuvre d'une campagne de pentesting. De nombreuses entreprises américaines annoncent publiquement leur Bug Bounty privé, Apple étant certainement la plus célèbre. Le Pentagone, dont le Bug Bounty privé a marqué l'histoire de cette approche innovante de la détection de vulnérabilités, a même accompagné son Bug Bounty privé d'une vaste campagne de communication à l'international.

Si pour autant l'idée de faire auditer vos technologies par l'ensemble des chercheurs de la plateforme dans un Bug Bounty "privé" vous effraie, vous pouvez adopter l'approche qu'ont de nombreux Grands Comptes, qui consiste à initier un Bug Bounty "sur mesure" en assemblant un pool limité de chercheurs choisis explicitement, pour l'augmenter petit à petit avant, dans un second temps, de l'ouvrir à l'ensemble d'une communauté, voir, pour les plus téméraires, à tout public.

Comment faites-vous pour attirer les meilleurs chercheurs ?

Beaucoup de nos chercheurs sont parmi les plus talentueux au monde, et certains sont employés à plein temps dans le secteur de la cybersécurité. Nombre d'entre eux sont par ailleurs inscrits sur plusieurs plateformes de Bug Bounty différentes, car il n'existe pas d'exclusivité, ce que les chercheurs de haut niveau n'accepteraient pas. Maintenir une attractivité forte, en mesure d'attirer les meilleurs chercheurs sur les Bug Bounties que nous organisons, repose en large partie sur un juste équilibre entre le nombre de chercheurs inscrits sur la plateforme et le nombre de Bug Bounties qui leur est proposé.

L'approche de Yogosha, basé sur une communauté fermée sélectionnée avec soin, repose sur ce principe et a pour objectif d'attirer les compétences les plus pointues du secteur, en nombre suffisant pour bénéficier de l'effet de la multitude, mais pas dans des proportions où leur espérance de gain s'en trouve affectée. C'est un équilibre que nous nous efforçons de conserver.

Qui sont-ils?

Nous avons réuni sur notre plateforme des chercheurs parmi les plus reconnus à l'international, que la plupart des entreprises auraient bien du mal à engager. Et pour cause, un chercheur de talent qui s'adonne au Bug Bounty peut espérer des gains dépassant de très loin ce qu'un emploi salarié peut lui offrir. La profession ne connaissant pas le chômage, la promesse d'échapper à une forme de précarité n'a pas grand intérêt à leurs yeux. Cette façon de travailler leur apporte, outre des gains élevés, une liberté dans la gestion de leur temps et une mobilité qu'aucune entreprise n'est en mesure de proposer aujourd'hui.

Par quoi sont-ils motivés ?

Au fur et à mesure de l'expansion et de l'évolution du marché du Bug Bounty, celui-ci devient plus nuancé et la motivation est très variable d'un chercheur à l'autre. La liberté de disposer de son temps et la possibilité de travailler de n'importe où restent des motivations fortes, mais il ne faut pas négliger l'intérêt que présente à leurs yeux la possibilité de travailler sur une multitude de problématiques sans cesse renouvelée, qui compte pour beaucoup dans la motivation des chercheurs pratiquant le Bug Bounty, sans oublier bien sûr les espérances de gains élevés, qui représentent pour certain un confortable complément de revenus ou pour d'autres une alternative enviable à un emploi salarié.

Comment budgétiser un Bug Bounty ?

Ce n'est pas si compliqué que cela, mais l'approche par rapport à une campagne de pentesting traditionnelle peut sembler à première vue déroutante.

Si vous planifiez une campagne de pentesting, il vous faudra évaluer le temps nécessaire, pour les auditeurs en charge de la campagne, à trouver les failles de sécurité présentes sur vos technologies. Cela peut s'avérer particulièrement compliqué, et vous n'avez nulle assurance qu'au bout du temps imparti, les auditeurs auront trouvé tout ce qu'ils auraient pu trouver s'ils disposaient de plus de temps pour leurs recherches.

Avec les Bug Bounties, plutôt que d'acheter du temps de recherche en jours/homme, les organisations vont proposer à une communauté de chercheurs en cybersécurité d'acquérir les failles qu'ils pourraient trouver sur leurs systèmes, en indexant le prix de ces failles sur leur criticité, sur la base d'une fourchette de prix convenue d'avance.

On passe ainsi d'une logique de moyens à une logique de résultats, on n'achète plus du temps de recherche mais le résultat de cette recherche, et on comble ainsi les lacunes du pentesting. L'audit proposé par le Bug Bounty est permanent et continu, la multitude des chercheurs ainsi mobilisés

offre une diversité en termes de créativité que le pentesting est incapable de proposer. La rapidité de mise en œuvre d'un Bug Bounty fait que cette approche est parfaitement compatible avec les cycles cadencés du développement agile.

D'un point de vue économique, le ROI d'un tel audit est bien plus évident : chaque faille acquise par une organisation lors d'un Bug Bounty lui permet de renforcer sa sécurité. Le budget est également bien plus simple à déterminer, car un Bug Bounty peut être capé par un budget maximal. Une fois le budget atteint, le Bug Bounty se met en pause. Le pentesting, lui, demande à "deviner" le temps nécessaire à la découverte de failles jusqu'ici inconnues, et cet audit n'est réalisé que par un unique expert la plupart du temps, dont on ne sait pas grand chose des performances, celle-ci ayant plus à faire avec sa créativité qu'à ses diplômes ou ses certifications.

Vous n'avez plus à deviner la capacité d'un auditeur à trouver des failles en un temps imparti, vous pouvez simplement attribuer un budget à l'achat de failles présentes sur vos technologies. Si ce budget s'avère trop important et qu'il n'est pas consommé, vous pouvez en récupérer le solde, s'il est insuffisant, il sera épuisé rapidement ce qui vous indiquera clairement qu'il reste des failles à découvrir. Il vous suffira alors de re-créditer votre compte pour reprendre les recherches.

Tant que le solde de votre cagnotte est positif, votre Bug Bounty reste ouvert et attire constamment l'attention des chercheurs présents sur la plateforme (ou de ceux que vous avez invités s'il s'agit d'un Bug Bounty "sur mesure"), une fois votre cagnotte épuisée, il se met en pause et attend vos instructions.

Mettre à prix ses failles de sécurité

Déterminer le prix de ses propres failles est un exercice délicat. Trop élevé, il représenterait une dépense inutile pour l'entreprise, trop faible, il échouerait à attirer les meilleurs profils et rendrait votre Bug Bounty moins efficace. Yogosha s'appuie sur le standard CVSS pour rationaliser l'approche économique des failles de sécurité. Ce standard de marché, largement reconnu dans le secteur de la cybersécurité, permet de calculer la criticité d'une vulnérabilité.

Une grille de récompense est composée de quatre niveaux de rémunération, indexés sur le score CVSS de la faille proposée à la vente : Low, Medium, High et Critical. Yogosha a mis au point une approche pragmatique destinée à déterminer une fourchette de prix pour les failles de sécurité : une matrice de calcul, qui prend en compte la maturité du périmètre de sécurité, l'urgence du besoin et l'étendue du scope. Cette matrice de calcul permet également de simuler l'évolution des prix dans le temps pour un même programme de Bug Bounty, en fonction d'objectifs particuliers. Ces prix sont bien sûr indicatifs, et sont le reflet des bonnes pratiques observées sur le marché, vous restez libre de les fixer. La communauté Yogosha étant composée de profils de haut niveau, le prix plancher est de 50€.

Comment gérer un programme de Bug Bounty ?

Constituer un pool de chercheur n'a jamais été aussi simple

Yogosha s'appuie sur une communauté de confiance, composée de chercheurs en sécurité recrutés avec le plus grand soin. Pour intégrer la communauté, un chercheur doit préalablement passer un examen d'une durée de trois heures environ, qui permet de valider ses compétences techniques, sa capacité à établir une relation clientèle productive et efficace, et son appétence à partager ses connaissances avec les équipes en charge de la correction des failles qu'il est amené à découvrir. Rappelons que chaque chercheur doit par ailleurs avoir été coopté par deux membres de la communauté. L'identité des chercheurs a été vérifiée, et elle est visible par nos clients, ils ont par ailleurs fait l'objet d'un "background check".

Yogosha a également référencé les compétences spécifiques de chacun d'entre eux, ce qui nous permet d'assembler des pools de chercheurs adaptés à chaque Bug Bounty, sélectionnés en fonction d'objectifs spécifiques, ainsi qu'en prenant en compte les technologies auditées à l'occasion.

Chaque rapport déposé donne lieu à une notation de la part du client qui l'acquière, et chaque interaction avec un chercheur donne lieu à une notation de l'entreprise par le chercheur. Ce double système de notation, courant dans le monde de l'économie collaborative, nous permet de nous assurer en continu d'une réelle qualité de service, et d'identifier au plus vite les frustrations afin d'y remédier dans les meilleurs délais.

Gérer un Bug Bounty à travers une interface intuitive

La plateforme Yogosha propose un tableau de bord complet permettant de suivre l'ensemble des Bug Bounty d'un même compte et d'en avoir une vue synthétique, ou bien de se focaliser sur un Bug Bounty en particulier afin de monitorer ses résultats spécifiques. Les différents KPI remontés dans ces dashboards permettent de monitorer aussi bien l'avancement des différentes missions composant un programme des Bug Bounties, que des feedbacks utiles quant aux failles découvertes. Cela permet aussi bien un benchmark des prestataires ou des équipes internes en matière de développements sécurisés, que la mise au point de plans de formation ou bien encore à la mise à jour de méthodes de travail.

Il est bien sûr possible de filtrer les rapports récoltés à l'occasion d'un Bug Bounty en les classant selon leur criticité, leur statut (rapport entrant, en attente de paiement, corrigé, etc) ou la typologie des failles identifiées.

Comment négocier de façon sereine le prix d'une faille ?

Yogosha s'appuie sur le standard CVSS, qui permet d'évaluer la criticité d'une faille de sécurité, afin de rationaliser l'approche économique des failles de sécurité. Yogosha a imaginé une méthode destinée à déterminer le prix - corrélé à la criticité CVSS - des failles que les chercheurs proposent à la vente. Pour cela, Yogosha utilise un "widget" permettant aux chercheurs d'en calculer la criticité. Une fois celle-ci établie, un prix est fixé selon la fourchette préalablement définie par le client. Ce dernier peut alors réévaluer au besoin la criticité CVSS, en prenant notamment en compte son contexte métier, ce qui peut aboutir à réviser le prix de la faille.

Yogosha a ainsi éliminé la friction liée à la négociation du prix, un point de tension courant dans l'expérience client sur les plateformes de Bug Bounty. Depuis son introduction par Yogosha, de nombreuses plateformes, tant aux USA qu'en France, ont adopté l'usage du CVSS, sans pour autant proposer ce processus de double validation propre à Yogosha.

Jusqu'à ce que Yogosha introduise l'approche CVSS sur le marché du Bug Bounty, en 2015, il était d'usage de négocier le prix d'une faille dans le cadre de l'échange entre un chercheur et une entreprise sur une plateforme de Bug Bounty, ce qui non seulement générait une forme de stress de part et d'autre, mais était susceptible de nuire à un échange de qualité centré sur la bonne compréhension de la faille, sa remédiation et la transmission de connaissance du chercheur vers le développeur en charge de la corriger. C'est pour optimiser cet aspect de l'échange que Yogosha a introduit, dès sa version Beta, cette approche par le CVSS, en partie reprise par différents acteurs du marché.

Comment impliquer les équipes IT ?

Il est important de préparer les ressources humaines qui sont appelées à être impactées par un Bug Bounty, qu'il s'agisse du département sécurité de l'entreprise, des équipes en charge des applicatifs audités à l'occasion d'un Bug Bounty, mais également des services marketing et communication, ou du service RP (ceci que vous choisissiez de communiquer ou pas à propos de votre Bug Bounty, il convient à minima de les avertir d'une opération à venir, et de les briefer quant à sa nature).

Un Bug Bounty, surtout s'il audite plusieurs applications différentes, va affecter de nombreux départements au sein de votre organisation. C'est une opportunité pour faire monter en compétence vos équipes de développement, pour peu qu'elles aient été préparées et mises au courant des objectifs. C'est également une opportunité pour sensibiliser d'autres départements de l'entreprise aux enjeux de la cybersécurité.

Le démarrage d'un Bug Bounty nécessite la mobilisation d'importantes ressources humaines, il est courant que les failles critiques se comptent par dizaines durant les premières semaines, pour ensuite être découvertes à un rythme bien moins soutenu, une fois la "dette" en matière de cybersécurité épongée.

Afin de suivre cela, il convient de déterminer les KPI permettant de cerner les problématiques de cybersécurité auxquels votre entreprise fait face : nombre et criticité des failles découvertes au fil d'un Bug Bounty, temps mis pour les corriger selon leur criticité, typologie des failles découvertes, et montée en compétences infosec des équipes. Tous ces éléments peuvent s'appréhender à travers les KPI réunis dans les dashboards mis au point par Yogosha.

Quand un Bug Bounty touche à plusieurs périmètres et audites différentes applications gérées par différentes équipes, il est souhaitable de mener de front ou de façon séquentielle plusieurs Bug Bounties et de constituer des équipes spécifiques pour chacun, en y impliquant les équipes Dev qui seront impactées par les correctifs à apporter. Les fonctionnalités de gestion d'équipe avancées que l'on retrouve sur une plateforme telle que Yogosha permettent cela, et focalisent sur les échanges entre chercheurs et équipes côté clients afin de maximiser les transferts de compétences.

Un Bug Bounty peut-il être une opération ponctuelle ?

Le Bug Bounty est conçu pour être un audit permanent, et c'est dans une telle configuration qu'il est le plus efficace. Mais cet atout est vécu comme une contrainte par beaucoup, et il a fallu, là encore, adapter un concept américain aux réalités du marché européen.

Yogosha s'est inspiré d'un concept apparu dans l'automobile, le "Stop and Start", qui permet au moteur d'une voiture de s'éteindre quand celle-ci marque un arrêt. En repensant intégralement les interactions entre la plateforme et les chercheurs en sécurité qui y travaillent, Yogosha a mis

au point une fonctionnalité de type “Stop and Start”, qui permet de mettre en pause en un clic n’importe quel Bug Bounty.

Lors de son déclenchement par l’organisateur d’un Bug Bounty, les chercheurs qui s’y sont impliqués sont immédiatement prévenus et stoppent aussitôt leurs investigations. De la même façon, l’organisateur peut relancer son Bug Bounty en un clic et remettre au travail la multitude tout aussi facilement.

Cette fonctionnalité permet d’absorber bien plus facilement le nombre important de failles détectées lors des premiers temps d’un Bug Bounty de façon à ne pas créer de goulot d’étranglement dans le processus de correction des vulnérabilités, afin de permettre à l’entreprise dont c’est, la plupart du temps, le premier Bug Bounty, d’adapter son organisation à cette nouvelle approche de la cybersécurité. Certains, qui sont contraints par leur organisation interne, marquent plusieurs arrêts afin d’absorber la surcharge de travail générée par leur Bug Bounty, d’autres encore font du Bug Bounty une opération ponctuelle, tous apprécient cette souplesse par rapport aux approches américaines du Bug Bounty.

A propos de Yogosha

En deux années d’existence, Yogosha a accumulé les prix et les réussites. Repérée dès le début par Hewlett-Packard Entreprise, qui l’a coachée dans le cadre de sa “Promo Startup 2016”, la jeune pousse a obtenu la bourse Frenchtech en mars 2016. Elle a ensuite bénéficié de l’accompagnement de Scientipôle, qui a permis à ses dirigeants de souscrire à des prêts d’honneur octroyés par l’accélérateur francilien destinés à financer son développement. Au printemps 2016, Yogosha obtient le label Maroc Numeric Cluster, reconnaissant son innovation et l’invitant à mettre pied sur le marché marocain, véritable hub vers le marché africain, et intègre Axeleo, le premier accélérateur B2B de la FrenchTech.

La startup devient rapidement membre du Syntec Numérique et termine l’année en remportant le Grand Prix de l’Innovation de la Ville de Paris, dans la catégorie Service aux entreprises. Quelques mois plus tard, en mai 2017, Yogosha remporte le prix Scientistar organisé par Scientipôle, dans la catégorie Transformation Numérique de l’Entreprise. Au même moment, Yogosha est sélectionnée pour faire partie de la première promotion du Founders Program, l’invitant à rejoindre dès son ouverture Station F, le plus grand incubateur de startups du monde, lancé par Xavier Niels à Paris. Quelques mois plus tard, la startup boucle sa première levée de fonds, et peu de temps après, Yogosha est choisie par Thales pour intégrer l’incubateur dédié à la cybersécurité inauguré par le géant de la cybersécurité à Station F.

Des questions ? Envie d’assister à une démonstration ?

Prenez contact avec nous sur contact@yogosha.com
ou à travers le formulaire situé sur www.yogosha.com