YogOsha

Ebook

11 questions

that everyone asks us

about Bug Bounty

The concept of Bug Bounty was born at Netscape, one of the first start-ups of the 90s. Over the past two decades, it has progressively conquered Silicon Valley before moving onto American companies with global networks and finally reaching Europe.

The idea is very simple and has proven to be extremely efficient: rather than having to pay for a penetration test or “pentest”, in which a cyber-security expert attempts to identify and exploit vulnerabilities within a cyber-space over a specific time frame before reporting his findings, you can work with an organisation of “researchers” and pay for their findings.

We therefore move from a resource-based view to a results-based view, from a singular diagnostic to a continuous audit, from a contracted task in a formal environment to a service that can be interrupted and restarted at any time, where we can alter the research parameter at will.

Why is it so efficient?

Increased Resources

A Bug Bounty program leads to a considerable increase in the potential number of researchers compared to the more traditional approach of pentesting, therefore increasing the odds of finding, at any time, vulnerabilities in the security system.

Having such a broad community of bug hunters and experts in cyber-security continuously auditing your technology can be compared to having a permanent IT Security audit.

A hotbed of creativity

A broad community, in permanent expansion, obviously involves a multitude of talented profiles coming from different backgrounds, each possessing unique abilities and mindsets.

Some security researchers have extensive skills and areas of expertise whereas others have become particularly efficient in specific fields.

Therefore, when assembled, their collective creativity contributes to the discovery of extremely varied vulnerabilities during a Bug Bounty program.

Better Results

Automated scanners are highly limited and are only capable of detecting what they have been programmed to recognise. As for Pentesters, they are restricted by their specific ability and knowledge, therefore producing results that are limited to the small number of security consultant involved in an audit.
Crowdsourcing by nature, is not subjected to these limitations. More researchers and more variety lead to better results.

A better return on investment

During a Bug Bounty program, you only pay if a vulnerability is found, not for the research. This means that you are not paying for work-days but for tangible vulnerabilities.

Contrary to traditional methods where companies pay for the time spent testing their applications independently of the results obtained, with a Bug Bounty they only pay for proven and impactful vulnerabilities. We are moving from a resource-based view to a results-based view.

Yet, due to its novelty, Bug Bounty faces numerous apprehensions. In this guide, we are going to attempt to explain certain aspects of Bug Bounty which still need clarification.

YogOsha

Public, private

Why is the difference?

There are three types of Bug Bounty depending on the manner in which the multitude of researchers are assembled for a Bug Bounty. Originally, Bug Bounties were “public”, which means that they were open to everyone, professionals as well as amateurs in cybersecurity, anyone could offer report a vulnerability in a system that they had found within the parameters set by the company organising the Bug Bounty. Nowadays, Google and Facebook, are among those who still offer public Bug Bounties.

The advantage of these types of Bug Bounties is that they enable the organisers to develop virtuous relationships with cybersecurity researchers, as well as integrating various hacker communities into their ecosystems...

This can be an important objective for companies such as Google, who look to value their “employer branding” within the hacker community. The inconvenience is that they generate a large number of false-positives (only 5% of vulnerability reports sent to Facebook are valid) which leads to sizeable management costs (according to a report done by Cobalt, for every 1€ spent on rewarding a flaw in the system, 1,80€ in management costs is generated for each public Bug Bounty) and requires an important mobilization of a large pool of workers from the company that is organising it.

Public Bug Bounties are much more efficient at identifying vulnerabilities, up to four times quicker according to HackerOne’s latest report. However, this is not very useful as very few companies have the capacity to fix these flaws within such a short timeframe, therefore leading to an increasing amount of “duplicates” which only weakens the signal-to-noise ratio of a Bug Bounty.

It is with private Bug Bounties in 2015 that the market really took off and that an increasing number of companies adopted this new approach to cybersecurity. A private Bug Bounty consists of reserving access to a selection of cybersecurity researchers who have been selected for their professionalism and experience. The results from this type of approach are much easier to manage, the number of false-positives is much lower and the interaction with the researchers is made much easier due to their experience and customer-relations know-how.

In 2016, according to the latest report from HackerOne, 92% of Bug Bounties were private, which clearly indicates the stance taken by the market. In reality, apart from the Technology sector and in some rare cases the banking sector, no other sectors look to use public Bug Bounties.

Finally, there has been the emergence of “Customised” Bug Bounties, where the pool of researchers assembled for a Bug Bounty is chosen on request, depending on the objectives of the company which is organising the Bug Bounty and the technology that is being audited.

This type of Bug Bounty has once again improved the efficiency of the procedure and has prompted the major corporations in France to start implementing Bug Bounty.

Bug Bounty's Signal/Noise ratio

Sources : BugCrowd, HackerOne, Facebook, Cobalt, Kyos, Yogosh

Public Private Tailor-made

YogOsha

Which communities are united by Bug Bounty Plateforms?

Today, thousands of companies of all sizes, from start-ups to industrial giants and covering almost the entire Silicon Valley, have supplemented their cybersecurity systems by using Bug Bounty. In France, the take-off has been explosive. Introduced on the market at the end of 2015, Bug Bounty has seduced multiple CAC40s to the extent that the “non Technological” sector will soon be more advanced on the subject in France than in the United States.

In 2014, Yogosha’s founders worked from the basis that American Bug Bounty platforms would have to deal with various cultural disparities in order to establish themselves in Europe. After studying the European cybersecurity market and holding meetings with multiple managers in this sector, the Yogosha team, supported at all times by carefully recruited members, adapted the American Bug Bounty concept to respond to the demands and pressures of the European market.

In order to join the Yogosha community, a security researcher must complete an examination that is approximately three days long. This is an evaluation of their technical ability, their professionalism, and their willingness to share their findings through vulnerability reports with the individuals in charge of fixing these flaws.

Their identities are checked and details are available for our clients to see, a background check is also completed on every profile.

The community is structured by a network of Yogosha ambassadors who are recognised figures in the cybersecurity sector, they are responsible for ensuring the activity of the community, for collecting feedback which enables product improvement and also for recruiting new members.

Yogosha has moulded their Bug Bounty offer based on this closed community. This entry level selection policy is very different to the one implemented by American platforms, which started with an offer of public Bug Bounties. They progressively moved towards private Bug Bounties, by retaining only the most efficient researchers. Platforms were also created by building on a pre-existing community made up of amateurs and professionals and of course platforms which depended on joint contracts from service companies with little motivation to come up with results.

What kind of companies call on Bug Bounty?

Emerging in the United States over twenty years ago, Bug Bounty programs were exclusive to Information Technology companies. In the United States, most companies with a Bug Bounty program are based in Silicon Valley, even if they have now been adopted by companies from a wide range of fields, such as Western Union or United Airlines.

In Europe, where there are fewer Technology giants, the Bug Bounty trend started with more traditional companies such as those in the CAC40, who are specialized in a wider array of fields and seek to be more discreet. The fact that companies in economic sectors which usually struggle to find new ways to be innovative are taking this approach, is the result of the undeniable effort made by companies from the “old economy” to benefit not only themselves but also support the new generation of start-ups, which provide out of the box innovative ideas.

The difference between the two continents is also a result of the pressure being exerted by Europe. Particularly through the General Data Protection Regulation, which is allowing companies operating in this continent a few more months to reinforce the protection of personal data that they are using before they reach the phase in which any mistake could prove costly, both in terms of the company’s finances but also their reputation, which could be tarnished by one simple mistake.

Private and customised programs have also played a sizeable role in encouraging traditional corporations to start using Bug Bounty. More secure, because restricted to using only pre-qualified researchers and professionals, private Bug Bounties are attracting an increasing number of major corporations across Europe whilst also enticing start-ups which have reached a stage of maturity where cybersecurity has become an important factor, particularly in B2B. apollo

Most of the time businesses start with a customised Bug Bounty, by assembling an ensemble of researchers with specific skills and expertise whilst also keeping in mind the primary objective of a Bug Bounty, such as the improvement in infosec standards within the customer's Development team.

What are the risks of lauching a Bug Bounty Program?

The idea of inviting anyone and everyone to audit your technology can seem daunting at first, and if Google and Facebook can handle these sorts of projects, the reality is that most companies cannot. Only a select few have the capacity to orchestrate programs of that size, and most are not overly enthusiastic about the prospect of sub-contracting the management of their Bug Bounty to a third party,
which could increase risks as well as adding legal and operational complications.

Managing relationships with multiple researchers with varying abilities, from high-end professionals to script kiddies on a day-to-day basis requires a very specific know-how. It also represents an undeniable source of stress, especially when it comes to negotiating the price of a system vulnerability with a stranger, which could potentially be detrimental to your Information System and have a negative impact on your reputation.

Working with a Bug Bounty platform which is based on a trusted community, where the Bug Hunter selection criteria is radical, gets to the heart of the problem. You will only be working alongside professional bug hunters, whose identities, available for all to see, have been confirmed by a trusted third party and whose profiles have been verified and validated by the platform.

The risk associated with this type of operation is similar to a traditional pentesting campaign: particularly weak. Moreover, by publicly announcing a private Bug Bounty, you are not increasing the odds of attracting individuals who would automatically be excluded from it any more than if you were to announce a traditional pentesting campaign. Multiple American companies publicly announce their private Bug Bounty, with Apple being the most recognisable. The Pentagon, whose private Bug Bounty shaped the history of this innovative approach in cybersecurity, even supported their private Bug Bounty with an international communication campaign.

If the idea of having your technology audited by the entirety of the bug hunters involved in a private Bug Bounty is daunting, you can adopt the same approach as many large corporations, which is to launch a “customised” Bug Bounty by assembling an exclusive group of bug hunters, chosen specifically for this task, before gradually increasing its size, opening it up to a community as a whole, or for the more audacious companies, to the public.

How to attract the best researchers?

Many of our researchers are among the most talented in the world and some are employed full-time in the cybersecurity sector. They often work across multiple Bug Bounty platforms as there is no exclusivity in this sector, something that would not be accepted by top level bug hunters. Maintaining a high level of appeal in order to attract the best bug hunters on the Bug Bounties that we organise relies primarily on the balance between the number of bug hunters signed up to the platform and the number of Bug Bounties that are offered to them.

Yogosha's approach, based on a carefully selected, exclusive community, works off this principle and its primary objective is to attract the most efficient workers in the sector. We pride ourselves in keeping the right balance between having enough researchers to be able to benefit from the effects of a broad array of talent and ideas but always ensuring that their expected return is not affected.

Who Are They?

On our platform we have assembled some of the most internationally acclaimed bug hunters, whom most companies would struggle to hire. And with reason; a talented researcher who devotes himself to Bug Bounty can expect a far more lucrative income than if he were to pursue regular salary-based employment. With unemployment being an unknown in this sector, the promise of job security is of little value in their eyes. In addition to the high income, this form of employment enables them to structure their work schedule in a way that no company can match.

What motivates them?

As the Bug Bounty market evolves and expands, it is more complicated to determine precisely what motivates each bug hunter to join the community. The opportunity to organise one's work schedule and to be able to work from anywhere remain two of the biggest advantages in this line of work, but there is also the challenge and thrill of working on an everchanging subject, with new problems to solve every day – this plays a big role in people wanting to work in this field. Of course, the lucrative revenue that this job ensures is very appealing, whether it be for people who are looking to supplement another income or for those who see an enviable alternative to salary-based employment.

How to budget a Bug Bounty?

It is not very complicated, but at first glance this approach can appear disconcerting compared to a traditional pentesting campaign.
If you plan a pentesting campaign, you will have to estimate the timeframe the pentester in charge of the campaign will need in order to find the flaws in your systems. This task can prove to be particularly challenging, especially as there is no guarantee of results at the end of your campaign, the security consultants may not have found as many vulnerabilities as they could have, had they had more time.

With Bug Bounties, rather than purchasing man-hours, the organisers will offer a community of bug hunters a pre-determined price for any flaws that can be found within their systems, with the price-range varying depending on how critical any vulnerability is deemed to be.

We therefore go from a resource-based approach to a results-based approach, we do not pay for the time it takes to do the research but the results of that research instead, rectifying one of the shortcomings of pentesting.

The audit offered by Bug Bounty is permanent and continuous, the wide array of bug hunters involved thereby ensures a level of creativity and diversity that cannot be matched by traditional pentesting. The speed with which a Bug Bounty program can be launched means that it is perfectly compatible with the demands of software development cycles.

From an economic standpoint, the return on investment from this type of audit is far more straightforward: each flaw acquired by an organisation during their Bug Bounty enables them to reinforce their security systems. The budget is also easier to manage as a Bug Bounty can be capped in advance by a limit which cannot be surpassed. If the maximum budget is reached, the Bug Bounty is paused.
Pentesting requires conjecture, predicting how long it will take to find vulnerabilities, this kind of audit is usually performed by a sole expert, whose standards of performance remain undetermined as they are based more on creativity than on qualifications and achievements.

YogOsha

How to budget a Bug Bounty?

You are no longer required to predict the ability of an auditor to find flaws within a certain timeframe, you can simply attribute a specific budget to reward the findings of faults present in your system. If this budget proves to be too large, you can just retrieve the remaining balance. If it is insufficient, it will rapidly be depleted which is an indication that there may still remain multiple flaws to be found in the system. The next step is then to re-credit the account and resume the campaign.

As long as the balance of your funds is positive, your Bug Bounty remains operational and constantly attracts bug hunters present on the platform (or the ones you have invited if it is a customised Bug Bounty), once your budget is spent, your Bug Bounty is simply paused and awaits your instructions.

Pricing IT security flaws

Determining the price for your own flaws is a delicate matter. Too high and it represents unnecessary spending for the company, too low and you will struggle to attract researchers and will make your Bug Bounty less efficient. Yogosha relies on the CVSS standard (Common Vulnerability - Scoring System) to determine and justify the economic approach to security flaws. This standard which is widely recognised in the cybersecurity sector, enables the calculation of the criticality of a vulnerability found in a system.

A reward system is then made up of four levels of payment, determined by the CVSS score of the flaw in question: Low, Medium, High and Critical. Yogosha designed a pragmatic approach to determine a price-range for security flaws that takes three things into account: the maturity of the security perimeter, the degree of necessity and its scope. This system also allows you to project the predicted price evolution over the duration of a Bug Bounty program, depending on specific goals. These prices are, of course, only a reflection of the market at any given time and you are free to charge what you like. With the Yogosha community being made up of high-quality professionals, the minimum charge for a system flaw is €50.

How to manage a Bug Bounty program?

Building a network of researchers has never been easier

Yogosha relies on a community built around trust, made up of carefully recruited cybersecurity researchers. In order to join the community, a researcher must complete a three days entry examination which will test their technical ability, their efficiency with customer-relations and their ability to transfer information to the teams in charge of fixing any faults they find in a system. Let us not forget that each researcher must also be approved by at least two members of the community and, following a background check, their identities are confirmed and remain available for customers to see.

Yogosha has also recorded the specific abilities of each of the bug hunters which allows us to assemble the most efficient pool of researchers for each individual Bug Bounty. They are selected based on the objective of the Bug Bounty as well as the type of system that is being audited.

Each report that is submitted leads to a rating by the client and every interaction with a researcher leads to a rating of the company by the researcher. This two-way rating system, which is common in the world of the “sharing-economy”, allows us to keep track of and maintain a high level of service and also to respond to any frustrations as promptly as possible.

Managing a Bug Bounty through a customer friendly interface

The Yogosha platform provides a general control panel which allows you to oversee all of the Bug Bounties in an account or to take an in-depth look at one particular Bug Bounty in order to monitor specific results. The different key performance indicators displayed on these dashboards allow you not only to monitor all the different tasks that make up a Bug Bounty program but also to get useful feedback regarding the flaws that have been found. This enables you to benchmark service providers as well as internal teams with regard to securing developments, redefining training programs or updating your work methods.

It is of course possible to filter any reports you receive during the Bug Bounty according to their severity or their status (incoming report, awaiting payment, corrected) or according to the types of flaws that have been found.

How to keep calm when negociating the price of a flaw?

Yogosha relies upon the CVSS standard which allows you to determine the severity of a security flaw in order to establish a reasonable economic approach to security flaws. Yogosha designed a method which, alongside the CVSS score, determines the price of flaws that bug hunters put up for sale. For this, Yogosha used a “widget” that enables researchers to calculate criticality. Once this is done, the value is determined according to the price-range previously set by the client. Thanks to the CVSS scoring, clients can then evaluate this offer, taking into consideration their field of work and the urgency of the problem.

Yogosha has therefore eliminated the issues surrounding the price negotiation process which is a common source of tension across Bug Bounty platforms. Since its introduction by Yogosha, multiple platforms across the USA and France have started using CVSS, without however using the double-validation process that is unique to Yogosha.

Until Yogosha introduced the CVSS system onto the Bug Bounty market in 2015, it was usual for the negotiation process to be based simply around an exchange between the bug hunter and the company on a Bug Bounty platform. This process not only generates a considerable amount of stress but also leaves both parties susceptible to not getting the best deal possible, whether that be the understanding of the flaw or the transfer of information to the developers in charge of rectifying it.

How to involve the IT team?

It is important to prepare every branch within your business that is going to be impacted by a Bug Bounty, from the departments in charge of security within the company, to the specific divisions that are being audited, all the way to the communication and marketing branches or PR service (without necessarily providing specific details regarding the Bug Bounty but at least warning them about an upcoming operation).

A Bug Bounty, will affect numerous departments within your company, especially if it is auditing multiple applications. It is a great opportunity for the various branches within your company to expand their knowledge with regard to cybersecurity and its implications.

The launch of a Bug Bounty requires a considerable amount of manpower and it is common for dozens of critical vulnerabilities to be found within the first few weeks, a pace that will slow down considerably once the “cybersecurity debt” has been cleared.

In order to manage the Bug Bounty, it is important to determine the relevant key performance indicators that enable you to determine the cybersecurity issues that your company will face: the amount and the severity of the flaws discovered throughout a Bug Bounty, the time it will take to fix them depending on their severity and typology, and the improvement in the different teams’ infosec skills. All of these KPIs can be accessed through the control panel provided by Yogosha.

When multiple areas and applications managed by different teams are audited and affected during a Bug Bounty, it is preferable to run multiple Bug Bounties one after the other, building specific teams for each and involving the development teams that will be impacted by the alterations that will be made. The team management functions that can be found on a platform such as Yogosha’s optimise the relationship between researchers and the client which in turn maximises the transfer of information.

Can a Bug Bounty be a one-off intervention?

Bug Bounty is designed to be a continuous audit and it is under this format that it is the most efficient. But many people saw this advantage as restrictive so therefore it was necessary once again to adapt an American concept to the European market.

Yogosha was inspired by a concept that first appeared in the automobile industry known as “Stop and Start”, where the engine in a car shuts down when the car stops. Yogosha was inspired by this concept and by totally rethinking the interaction that takes place between the platform and the researchers working on a given project they designed a function whereby a client can pause a Bug Bounty at any moment and the message will be transferred to researchers immediately.

When a company decides to pause an ongoing Bug Bounty, the bug hunters involved in the process are immediately warned and they stop their investigations.

It is just as easy for the company to then restart the Bug Bounty and in one click on the Yogosha platform the message is sent to researchers to resume their work.

This function enables companies to cope with the first wave of flaws that are detected during the first sequence of a Bug Bounty, it means that the process of fixing the vulnerabilities does not become too chaotic and impossible to manage. It allows companies, who for the most part are experiencing their first Bug Bounty, to adapt to this new approach to cybersecurity. Some businesses need to pause their programs multiple times in order to control the workload within the company. Others use Bug Bounty as a one-off intervention. In both cases this flexible approach to Bug Bounty is greatly appreciated compared to the traditional American approach.

About Yogosha

During its year and a half of existence, Yogosha has amassed multiple awards and plaudits. Identified from the off by Hewlett-Packard Entreprise, who coached them as part of the “Promo Startup 2016”, the young company acquired the Frenchtech grant in March 2016.

The business then benefited form the mentoring of Schientipôle, which allowed the directors to obtain grants allocated by “l’accélérateur francilien” designed to finance their development. In the spring of 2016, Yogosha earned the Maroc Numeric Cluster label, recognising its innovation which was a stepping stone onto the Moroccan market, a genuine hub towards the African market. They also integrated Axeleo, the first B2B “accelerateur” of FrenchTech. The startup rapidly became a member of the Syntec Numérique and ended the year by winning the “Grand Prix de l’Innovation de la Ville de Paris”, in the category of Business Service Provider.

A few months later, in May 2017, Yogosha picked up the Scientistar award organised by Scientipôle, this time in the “Business Digital Tansformation” category. During this period,Yogosha was also selected to be a member of the first group in the Founders Program, and was invited to join Station F, the largest start-up incubator in the world, at its launch by Xavier Niels in Paris. In October 2017, Yogosha was selected by Tahles to join the incubator dedicated to cybersecurity inaugurated by the cybersecurity giant Station F.

Come and meet us !