MMNOG 2020

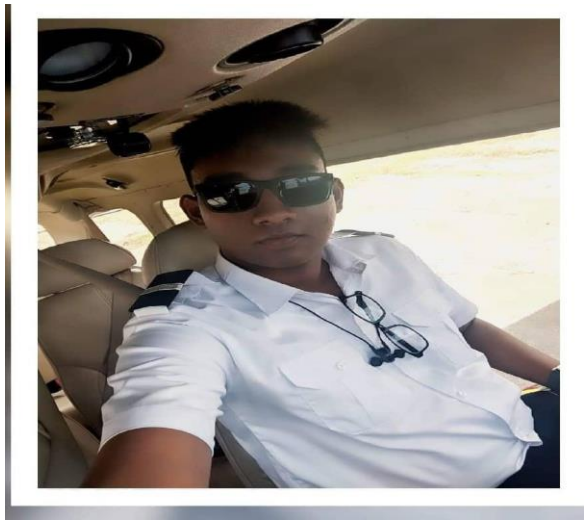
HACKERS – Internet's Immune System

HACKERS WITH DISHONEST MINDS ARE AT WORK

Your Privacy, your home, your governments and Corporates are at risk

PROTECT THYSELF TODAY

WHOAMI



I am not a hacker
I am a Bug Bounty Hunter
I break security not Heart

PASAN RAWANA LAMAHEWA

white hat

- ✓ Civil Aviation Pilot Trainee
- ✓ Undergrad in Cyber Security
- ✓ Undergrad in Biz Management
- ✓ Undergrad in IATA
- ✓ Lyricist

Security Researcher with a FACE

UNDERSANDING AND IMPLEMENTING BUG BOUNTY PROGRAMS

A G E N D A

- ✓ Understanding Bug Bounty
  - ❑ Bug Bounty Programs
  - ❑ Why Bug Bounty Programs Important in todays' Context
  - ❑ Bug Bounty Platforms
  - ❑ Bug Bounty Hunter
  - ❑ Evolution of Bug Bounty Programs
- ✓ Type of Hackers
- ✓ How to Start a Bug Bounty Program
  - ❑ Forums of Incident Response and Security Teams
  - ❑ Crowdsource platforms
  - ❑ Rewards
- ✓ My experience as a Security Researcher
- ✓ Things to Consider
- ✓ Tips to write a Good Report
- ✓ Useful Links
- ✓ Questions

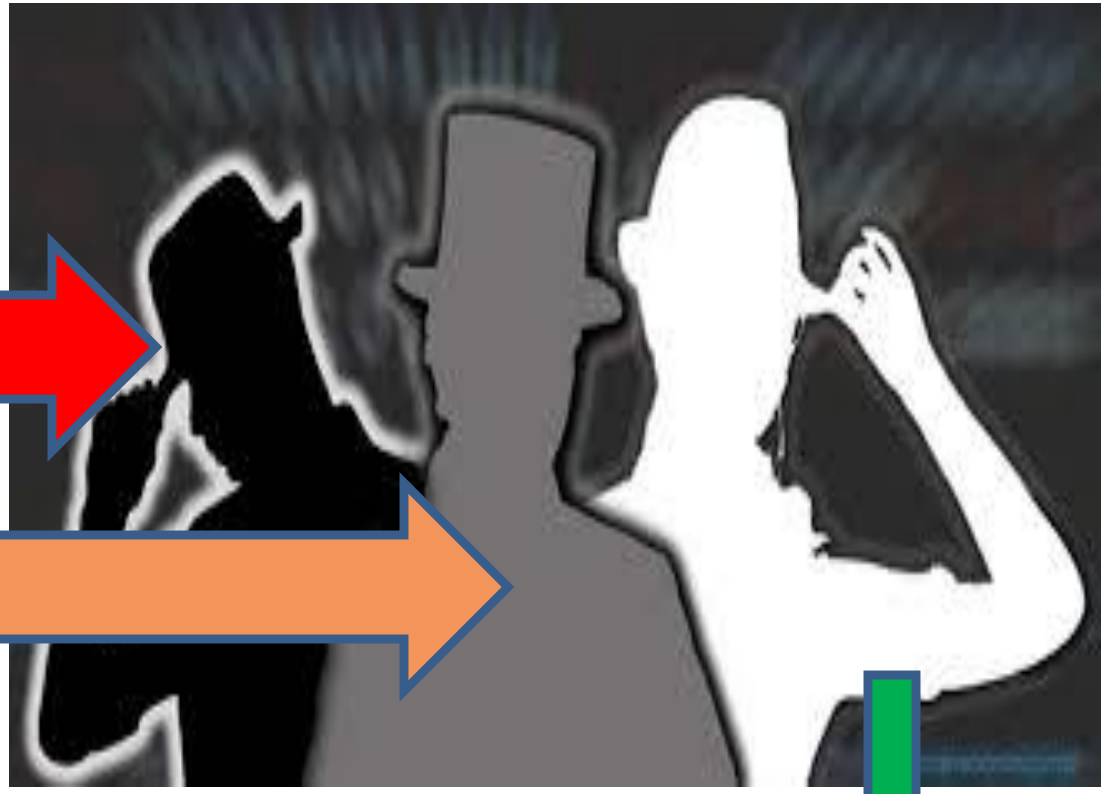
We are in the age of the hacker.
Hackers are lauded as heroes,
discussed daily in the media,
villainized at times, and portrayed by
Hollywood - anything but ignored.

"**Sometimes, you have to demo a threat to spark a solution**"

Barnaby Jack 1977 - 2013

The beauty of hackers, says cybersecurity expert Keren Elazari, is that they force us to evolve and improve. By exposing vulnerabilities, they push the Internet to become stronger and healthier, wielding their power to create a better world.

Hacking takes place in
Vicious Minds
&
Divine Minds



Black Hackers

Gray Hackers

- Divine Minds ⇔ White Hackers

A simple DEFINITION

Bug Bounty Program

Bug Bounty Program (BBP) or Vulnerability Disclosure Program (VDP) could be simply defined as an **organizational initiative** that **rewards & recognize** individual who discover flaws/loopholes in software/systems/web and **ACTING ETHICALLY** to report them to the organization.

In other words BBP/VDP is a **deal offered** by many websites, organizations and software developers by which individuals can receive recognition and rewards.

Hackers are kind of living beings with limitless potential at their figure tips. This is the rush of power they feel. **With this great power comes greater responsibility and accountability to oneself and to the society at large**. Unfortunately some hackers do not resist the temptation completely and forget responsibility ending up as Cybercriminals.

Organizations and their Security Teams need to understand this and should realize though the hackers are considered Internet Immune System, they cause miserable disruptions to the society.

WHY BUG BOUNTY PROGRAM

Bug bounty program is not Fighting the Fire with Fire, but **prevention of fire**!
It invites a White Hat Hacker to think, explore and report before a bad guy creeps in.

.

Bugs exist in any software or system, and that is a fact.
Cybercrimes are committed using a computer or computer technology
or smart phone as primary tool. Cybercriminals Love Bugs.

This is what a bug bounty program is about:
Ethical hackers help organizations to detect vulnerabilities/loopholes before the bad guys creep in.
In other words: Getting Ahead. This is all about Bug Bounty Program.

All organizations want to be tech savvy and they keep on upgrading with latest technology. The Hackers with destructive minds are also getting more and more sophisticated

Organizations and their IT professionals are aware of this impending danger, **but many believe they are satisfactorily protected, they can swiftly restore or that their organizations are too small to be observed by vicious minds**.

So organizations **'reach out to private individuals for help'.** This is called a Bug Bounty Program.

Cybercriminal activity is one of the biggest challenges that humanity will face in the next two decades(Steve Morgan, Editor-in-Chief Cybersecurity Ventures)

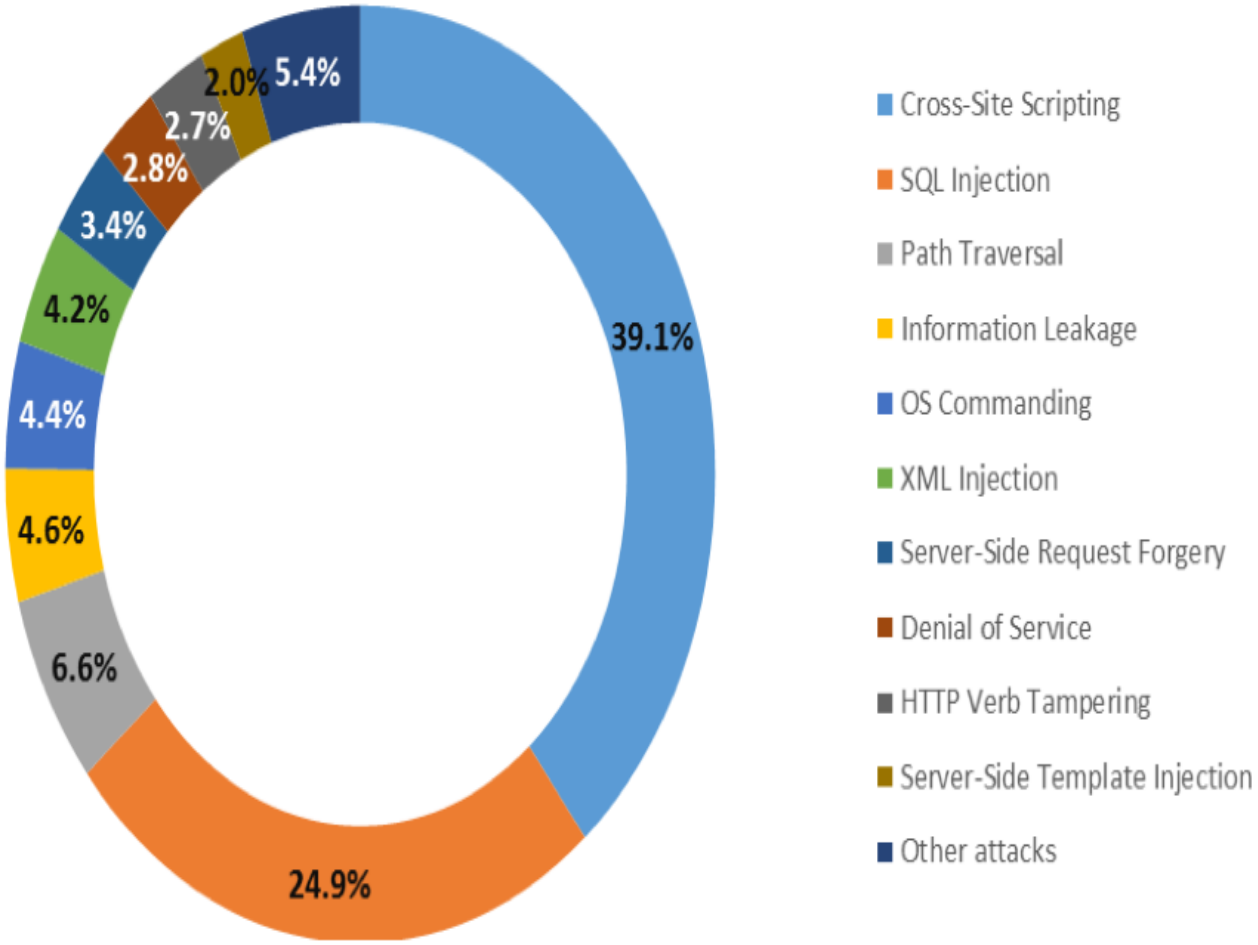
Types of Criminals

- Social Engineer - manipulates human minds
- Phisher - information / password theft
- Hacker - blocking systems
- Disgruntle Employee - information theft / blocking systems
- Ransom Artist - spread malware /demand ransom

ARE WE READY ?

Critical Vulnerabilities

Source & Information Credit to:
2019 edescan vulnerability Stats report: Eoin & The Security



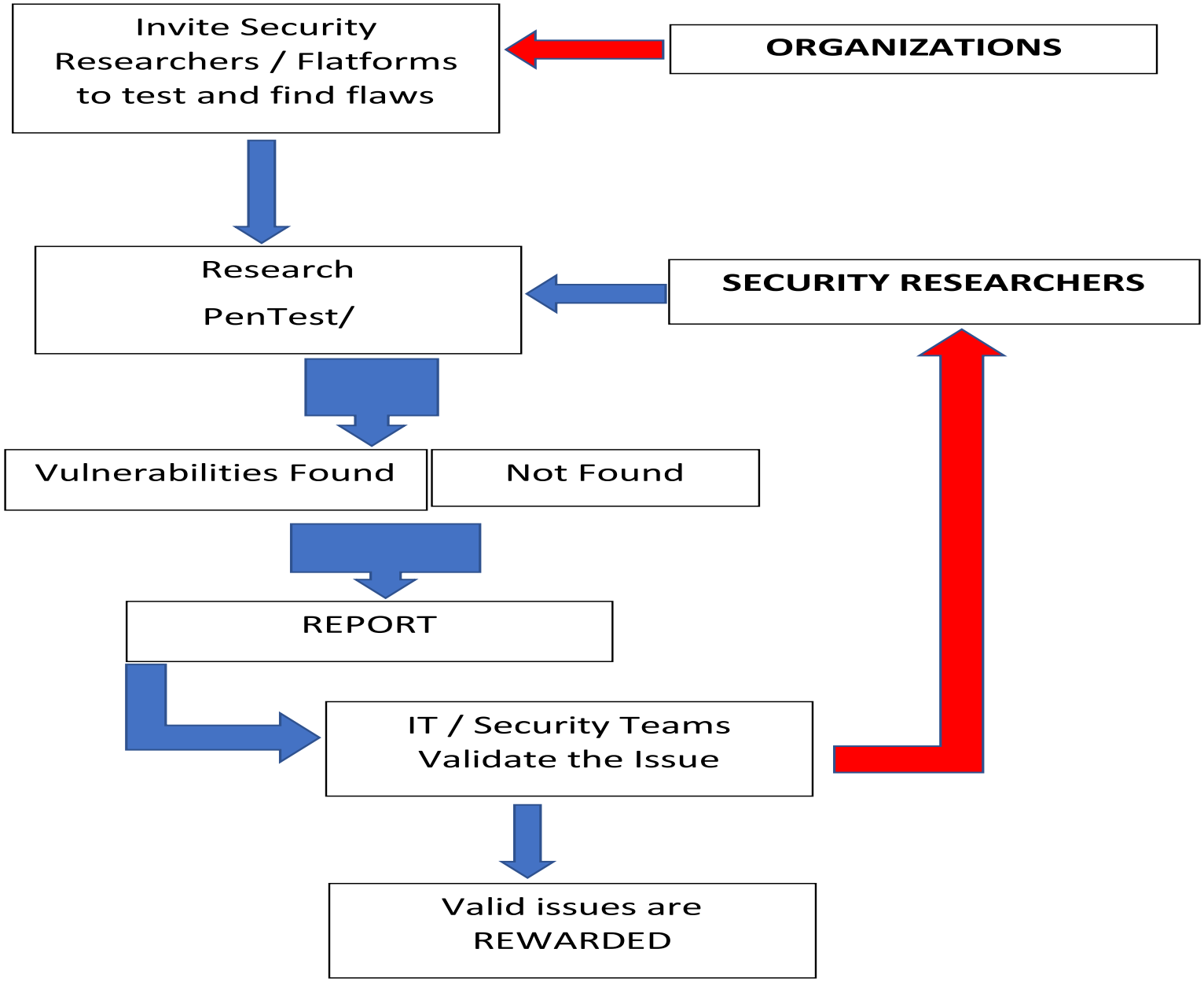
How to Start a Bug Bounty Program

- Evaluate your Organization, its Systems and IT / Security Team
- Evaluate your ICT Policy, End Users, access levels, Password protocols etc
- Evaluate and physically check your Hardware, Network, Servers and Server Rooms
- Decide on a Bug Bounty / Reward System
- Decide on a Platform / Direct approach to Security Researcher
- Prepare a draft Vulnerability Disclosure Policy
- The Rules of Engagement - define the Scope of Bug Bounty Program
- Decide on unquestionable clarity about the authorized conduct of the Security Researcher and decide what proof need to confirm a vulnerability and how both ethical hacker and organization share the findings.
- Discuss with your Team, Senior Management and agree
- Document > Validate> Authorization>Public Knowledge/Web

VERY IMPORTANT

- ✓ Select your point person very carefully
- ✓ Provide the contact details of your point person, he must be responsive and tech savvy
- ✓ Provide the clear instructions about the program, along with the specifications of the overall surface which may be IP Address, Domain name, type of test and type of reports etc. and emphasis on any exclusions

BUG BOUNTY PROGRAM – LIFECYCLE



Consider Bug Bounties Carefully

bug bounty programs are all about creating a culture of openness, transparency, responsibility and above all the **trust**.

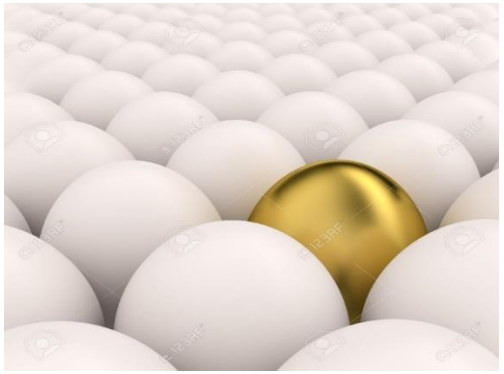
Even if an organization doesn't offer bug bounties, it is pertinent to establish a "**vulnerability disclosure policy"** or **ethical disclosure policy**: A legal statement stating that an organization will not prosecute ethical hackers who detect vulnerabilities in systems / webs and report them ethically .

- Since a bounty program is about **trust and transparency**, an organization ethically be open about how it will pay, reward or recognize for vulnerability detection.

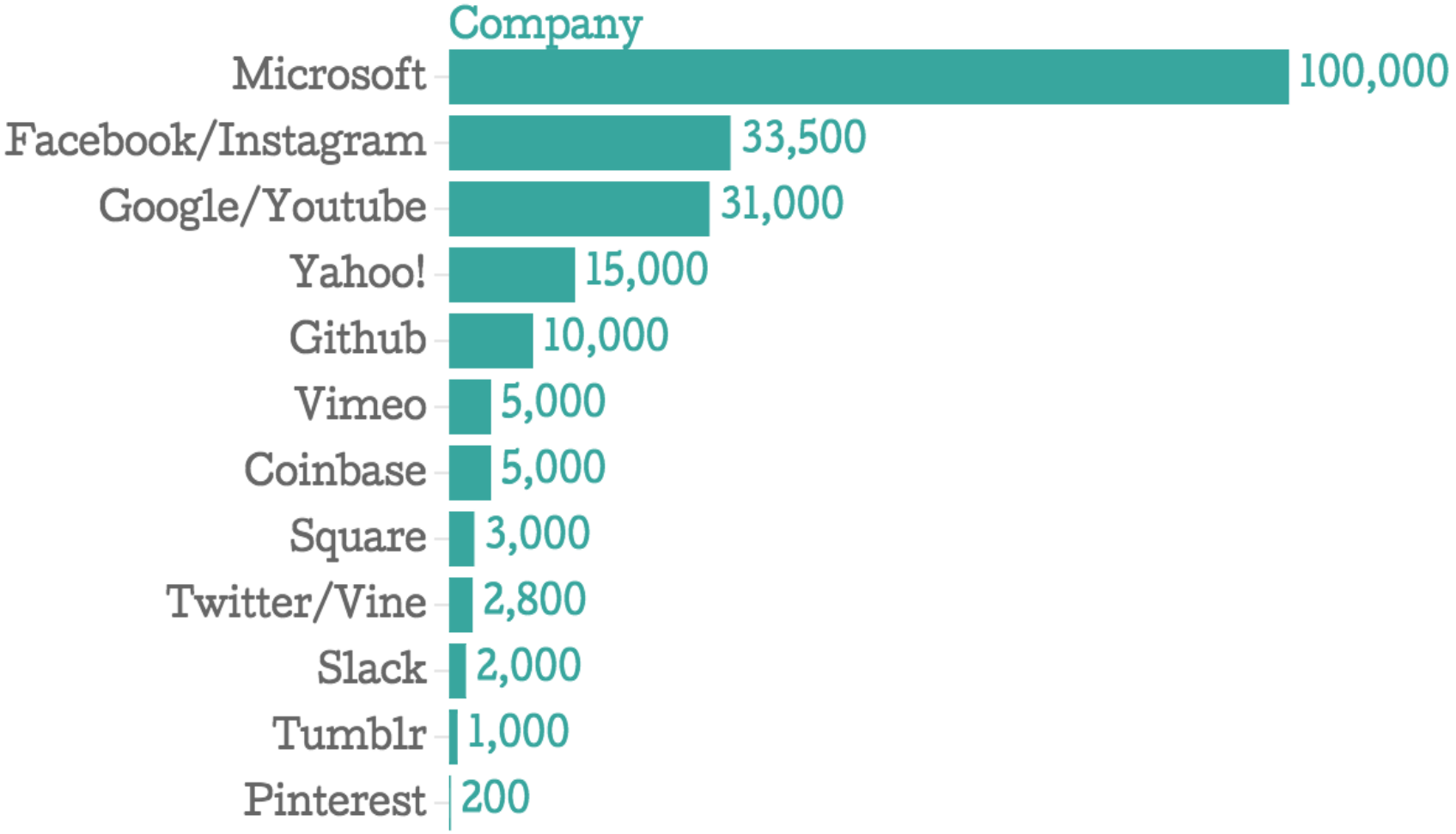
Hand Pic your Goose for Golden Egg

- ✓ Register in Good Platforms
- ✓ Research for Security Researchers
- ✓ Conversation
- ✓ Be Sure and mindful of side effects
- ✓ Vulnerability Discloser Agreements
- ✓ Connect and implement

SECLECT YOUR SECURITY RESEARCHER OR FLATFORM and/or MAKE YOUR BUG BOUNTY PROGRM OPEN TO PUBLIC



Bug Bounty Rewards by Highest Ever Paid, or Willing to Pay ($)



Observer/Jack Smith IV

Data: Bugcrowd, HackerOne, Kaspersky, Various

External Security Research

Acknowledgement of the vulnerability report

Dear Pasan Lamahewa,

Thank you for providing details on the potential identified vulnerability report provided. Intel is committed to addressing security vulnerabilities in a timely manner and mitigating such vulnerabilities. Intel appreciates the initial steps you have taken to report this concern. The next steps in the process are:

- Security Report - A report is taken that allows us to obtain sufficient details to take appropriate steps to mitigate risks.
- Evaluation - The report is evaluated to confirm potential vulnerabilities, assess the risk, determine impact, and assign priority.
- Solution - Intel develops a solution that mitigates the reported security vulnerability.

Until such time as we have evaluated this reported vulnerability and determined what mitigation is appropriate, we would appreciate if you would not publicly discuss this issue. If you have any other concerns or further information please feel contact me directly.

For your records, below we have included a certificate of acknowledgement from Intel.

For future references, Intel Corporation requires expressed written permission for any external parties conducting security testing or vulnerability assessments on Intel systems or networks. As you are aware, any testing may have adverse system impact, violate laws, and/or lead the tester to be associated with an actual incident.

Please contact us in the future and obtain our expressed written permissions prior to conducting security testing. Thank you again for bringing this to our attention.

Regards,
Intel Information Security

Certificate of Appreciation

Presented to

Pasan Lamahewa

On

December (29, 2017

For working through Intel's responsible security disclosure process

Matt Wirta
Investigations Manager
Intel Corporation

MARKTPLATZ MITTELSTAND.DE

CERTIFICATE

Marktplatz Mittelstand GmbH & Co.KG acknowledges that

Mr. Pasan Lamahewa

found a vulnerability and that he acted ethically by reporting it to us and allowing us to fix it in a timely manner.

Nuremberg/Germany | August 2019

Richard Pfadenhauer
Head of IT

MOTIVATORS FOR A SECURITY RESEARCHER

Motivator #1
Set Self Target

Motivator #2
Recognition

Motivator #3
REWARDS

Motivator #4
Self Satisfaction – "I am not a Cybercriminal wearing a Black Hat"
"I keep on Collecting and Counting my White Hats"

My Experience

Types of Organizations

- The **Genius** - take ethical reports very seriously, rewards, recognizes and partner with the security researcher.
- The **Bulletproof** – Never recognize or acknowledge and think they are Immortals. They have a mind set of building an “impenetrable wall” created mythically around their Digital Assets.
- Mr. **Know it All**– oops, we knew this before you and planning to fix it.
- The **Blind & Deaf** – Never response
- The **Neutrals** – a bug?, bug bounty program ?! News to us, anyway thank you, we’ll look into this.

Morale: two types of organizations in the world: those that know they've been hacked, and those that don't

My Experience

"The Bullet Proof ": Mythical Impenetrable Wall

"Fixed Line Telecommunication Company" in South Asia

I reported a serious flaw in their system, which can certainly expose subscribers sensitive information and many more.

It has now passed 10 months since my responsible reporting of this vulnerability to their IT Team, they live inside a impenetrable castle

This is a good example for organizations and its IT Professionals are thinking that they are "**Bullet Proof**" and act "**Mr. Know it All"**. Rather they are liabilities to their customers and to the society.

Useful Links

https://www.hackerone.com

https://www.bugcrowd.com

https://www.openbugbounty.org

HackerOne

Bugcrowd

Vulnerability Lab

Fire Bounty

Some interesting info to Ponder

Cyber Security Is in High Demand
Security specialist is one of the most promising career choices in the IT sector.

There are over 300,000 unfilled cybersecurity jobs in the United States, with the demand rising each year.
(Source: Cybint Solutions)

By 2021, the number of unfilled cybersecurity jobs is expected to balloon to 3.5 million.
(Source: The Hill)

Cybersecurity expenditures are expected to reach1 trillion dollars by 2024. So be ready with your Next Medium Term Corporate Planning
(Source: Cyber Defense Magazine) -

The annual cost of cybercrime damages is expected to hit $5 trillion by 2020.
(Source: Cyber Defense Magazine)
The rate of these crimes is only expected to increase. Criminals are finding increasingly clever and diabolical ways to get their hands on your systems. **In this context, whatever the cost of cybersecurity may be it seems like a worthy investment.**

Please feel free to contact me


pasanrlamahewa@gmail.com


https://twitter.com/Pasan_Rav

Happy to be with you all and gain knowledge in my pursue of Cyber Security Ethical Research