



Managing Bug Bounty Programs: A learning journey

Cat Salangit

Application Security Specialist

Thank You to Our Sponsors and Hosts!



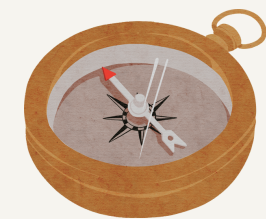
Without them, this Conference couldn't happen.

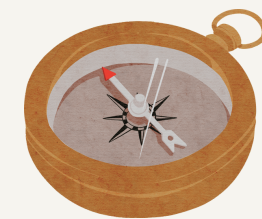
whoami

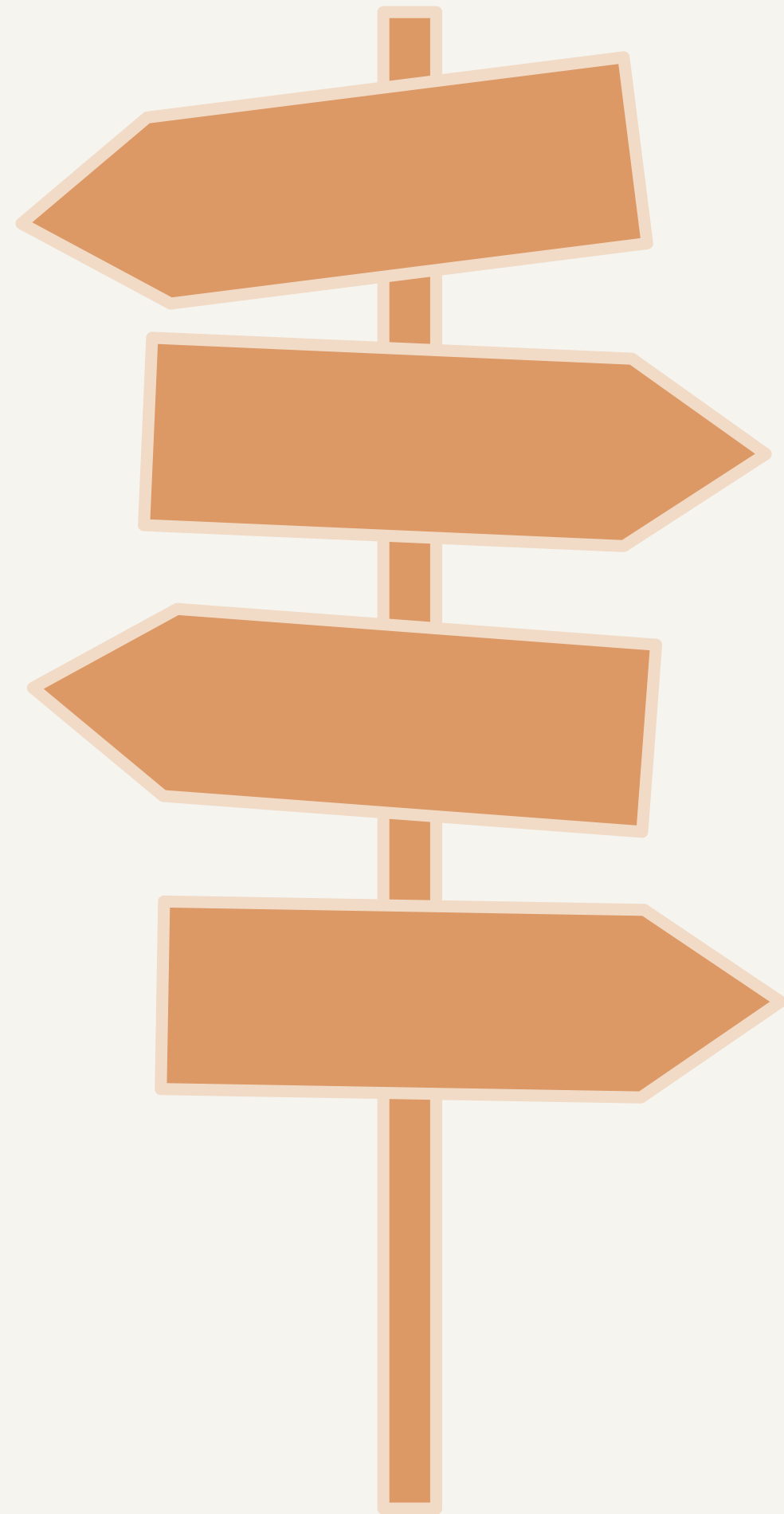
Cat Salanguit

Application Security Specialist









How It All Started

How does bug bounty programs fit in SDLC

Usefulness of managed bug bounty programs

Final thoughts



**How it
started**

Problem



- ✘ **Many are signing up for free trials to test our apps**

with no way for them to report to us

- ✘ **Dozens of reports received through email**

mainly low-hanging fruits

- ✘ **No consistent and standardised process**

to go over these reports

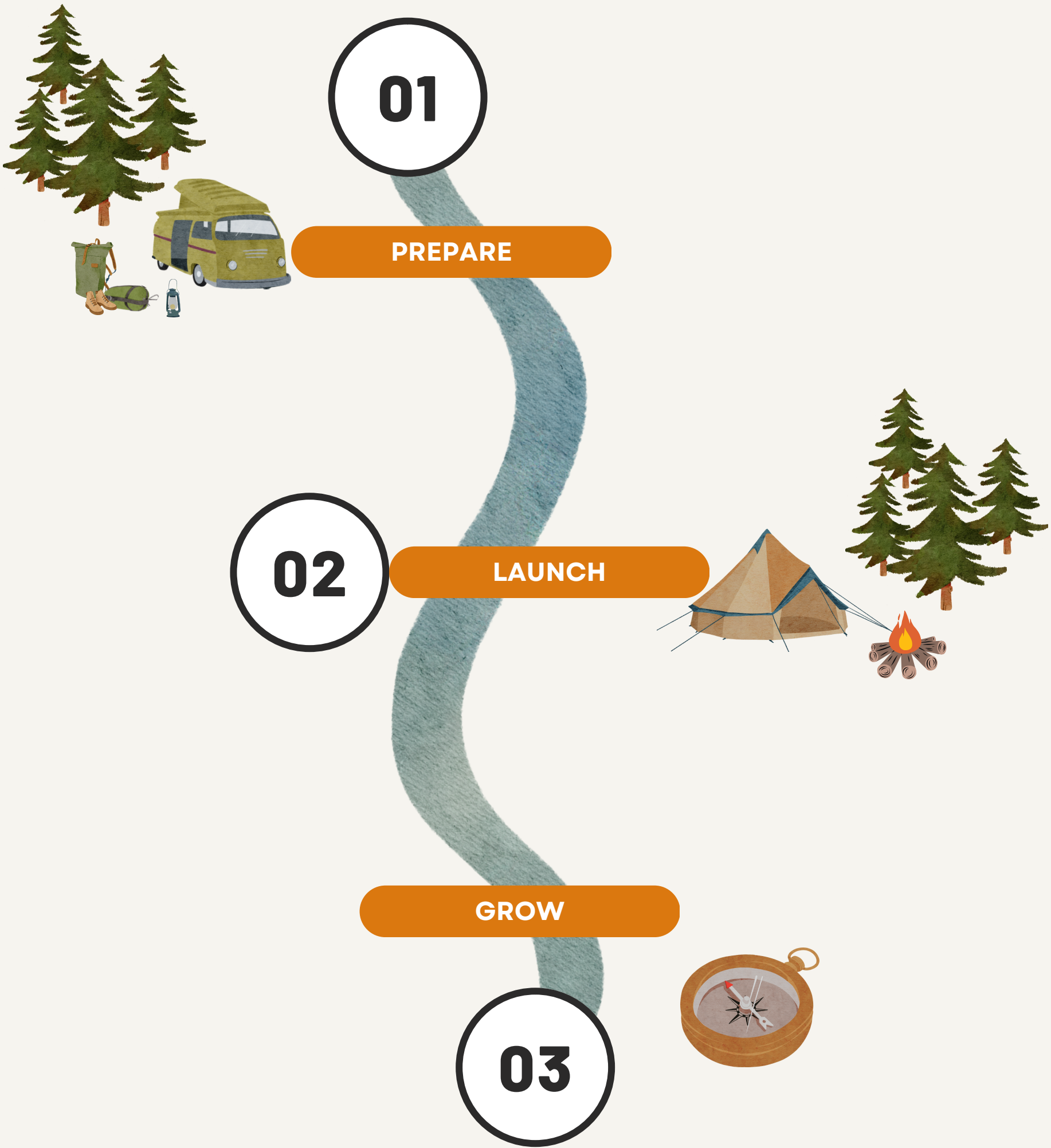
**We want to make sure we have open
channels for people to report
vulnerabilities to us.**

Bug Bounty Program

A bug bounty program offers a monetary reward given to security researchers or ethical hackers for discovering and reporting valid bsecurity vulnerabilities.



How we launch bug bounty programs



Prepare

VM PROGRAM

Setup a Vulnerability Management Program

USER GUIDE

Created a User Guide For our Engineers on How to Identify & Fix security issues

PROCESSES

Built practices and processes internally that were iterated to handle report submissions

DAST & SAST

Setup our scanning tools Dynamic Application & Static Application Security Testing

PENTESTS

Performed internal and third party penetration tests



Launch

started from private bug bounty
program first

eventually transition to public
program



Grow

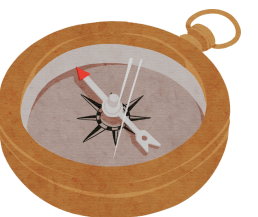
EXPANSION

PROCESS ITERATION

IMPROVE WORKFLOW

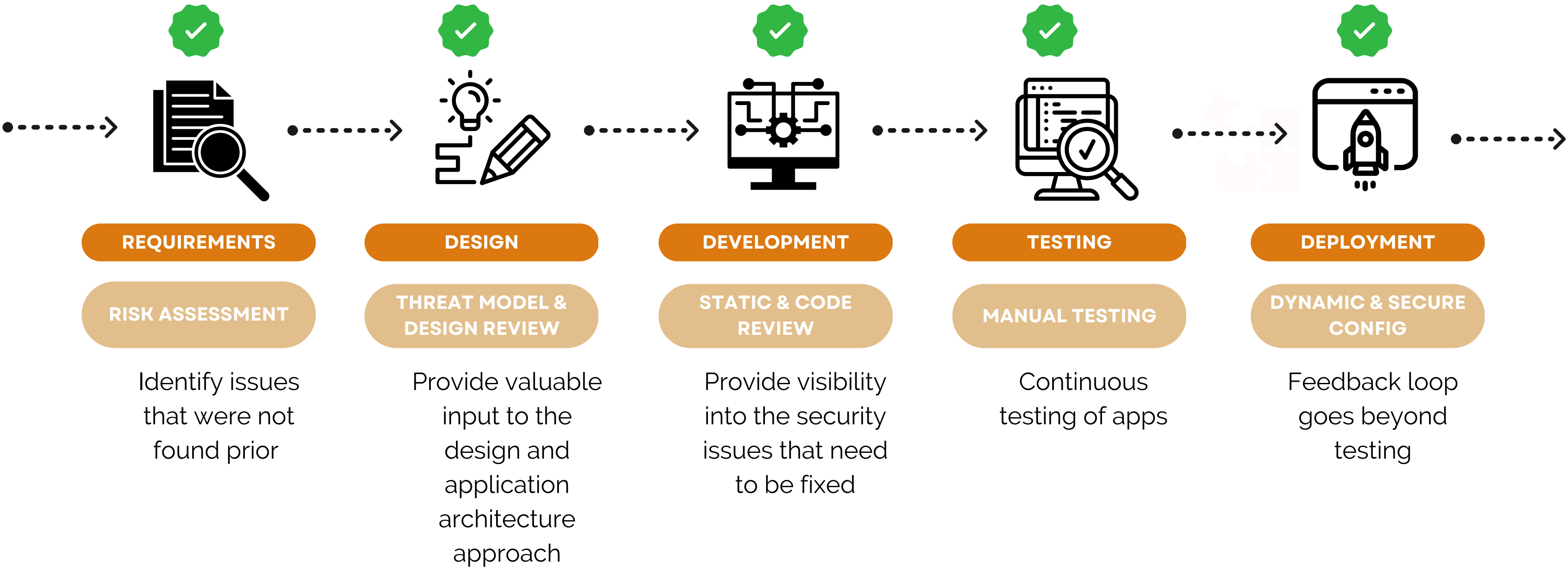
PATH TO PUBLIC

COMMUNITY AWARENESS



**Where do
Bug Bounty
Programs fit
in the SDLC?**

Where does Bug Bounty Programs fit in the SDLC?



Usefulness of managed bug bounty programs

Critical Security Vulnerability Σ Inbox x



[Redacted]

to security ▼

Hello team!

I found a critical security vulnerability on [Redacted] please tell me on which platform you have Bug bounty program, i want to report it.

Thank you, waiting for your reply

[Redacted]

Security Researcher



[Redacted]

to security ▼

Please invite me to your bug bounty program. My hackerone username is [Redacted] Vulnerability which i found is very critical.



How useful it is for us

1. Formal structure of handling external reports

Some researchers will submit report mentioning they've found critical vulnerabilities.

2. Leverage security platforms

helped our team resolve **scaling issues**, **manage duplicate** report detection, and track hacker profiles, and allow them to categorise when they submit

3. Embrace continuous testing

A bug bounty program running continuously to pick up emerging vulnerabilities

bug report

"beg bounty" report



TIMELINE



stok submitted a report

April 2, 2018(5 years ago)

Hey Team!

I love loyalty bonuses, that turns first time users into returning customers , but sometimes loyalty can be exploited, just like in this chase.

LT:DR

A firsttime loyalty customer will get x times the amount of loyalty bonus from the story by racing the loyalty link x amount of times in one go.

See POC video for full Walkthrough

<https://youtu.be/>

POC:

reported I don't get money.

Description:Please pay me some money

[Add description or summary of the vulnerability]

Please

Location/Affected Endpoints:

[Add location or endpoints of the vulnerability]

Steps To Reproduce:

[Add details for how we can reproduce the issue]

1. [add step]Bounties

1. [add step]I want bounties for my kids education please

1. [add step]I want bounties

Likelihood Analysis:

[Describe the likelihood of a threat/actor exploiting an issue.]

Impact Analysis:

[Describe the severity of the impact.]

Why get started

From the lens of a program owner

1

Collaboration across
teams and researchers

2

Cost effectiveness

3

Leverage skills from a diverse
hacker community

4

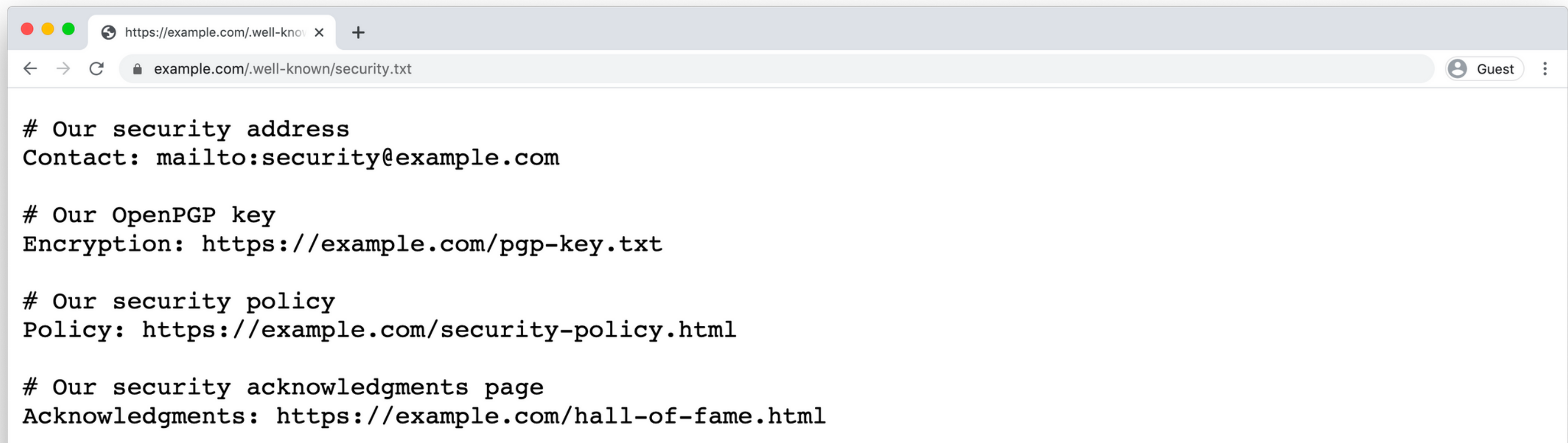
Proactive commitment to security

Where to start?

1.

Security.txt

- A standard that gives people an easy way to contact your organisation about security issues.



The screenshot shows a web browser window with the address bar displaying `https://example.com/.well-known/security.txt`. The page content is a plain text file with the following text:

```
# Our security address
Contact: mailto:security@example.com

# Our OpenPGP key
Encryption: https://example.com/pgp-key.txt

# Our security policy
Policy: https://example.com/security-policy.html

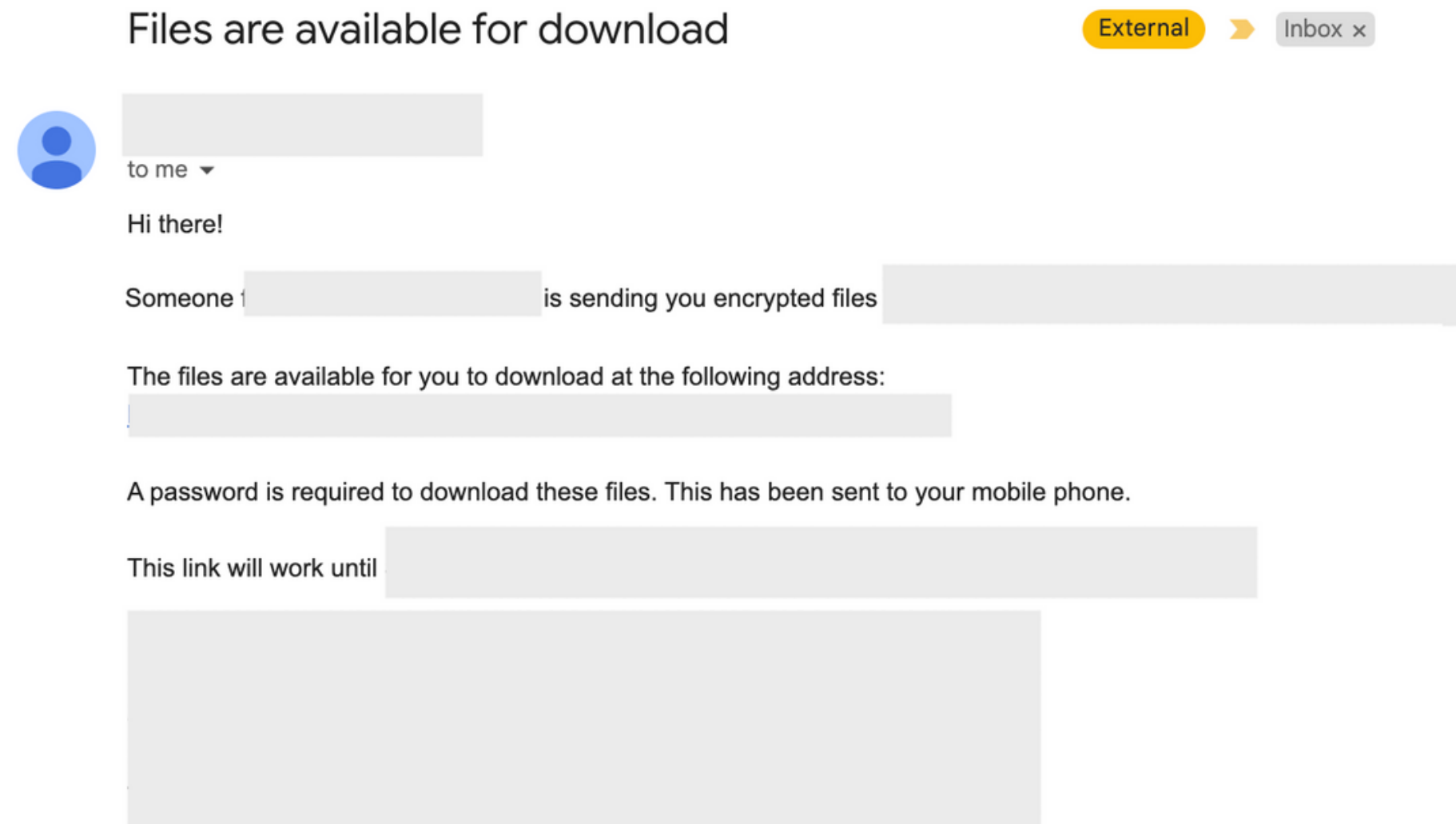
# Our security acknowledgments page
Acknowledgments: https://example.com/hall-of-fame.html
```

Where to start?

2.

Provide a secure way to send details of the vulnerability they've found

- people should be able to use PGP encryption to send a report
- receive encrypted files

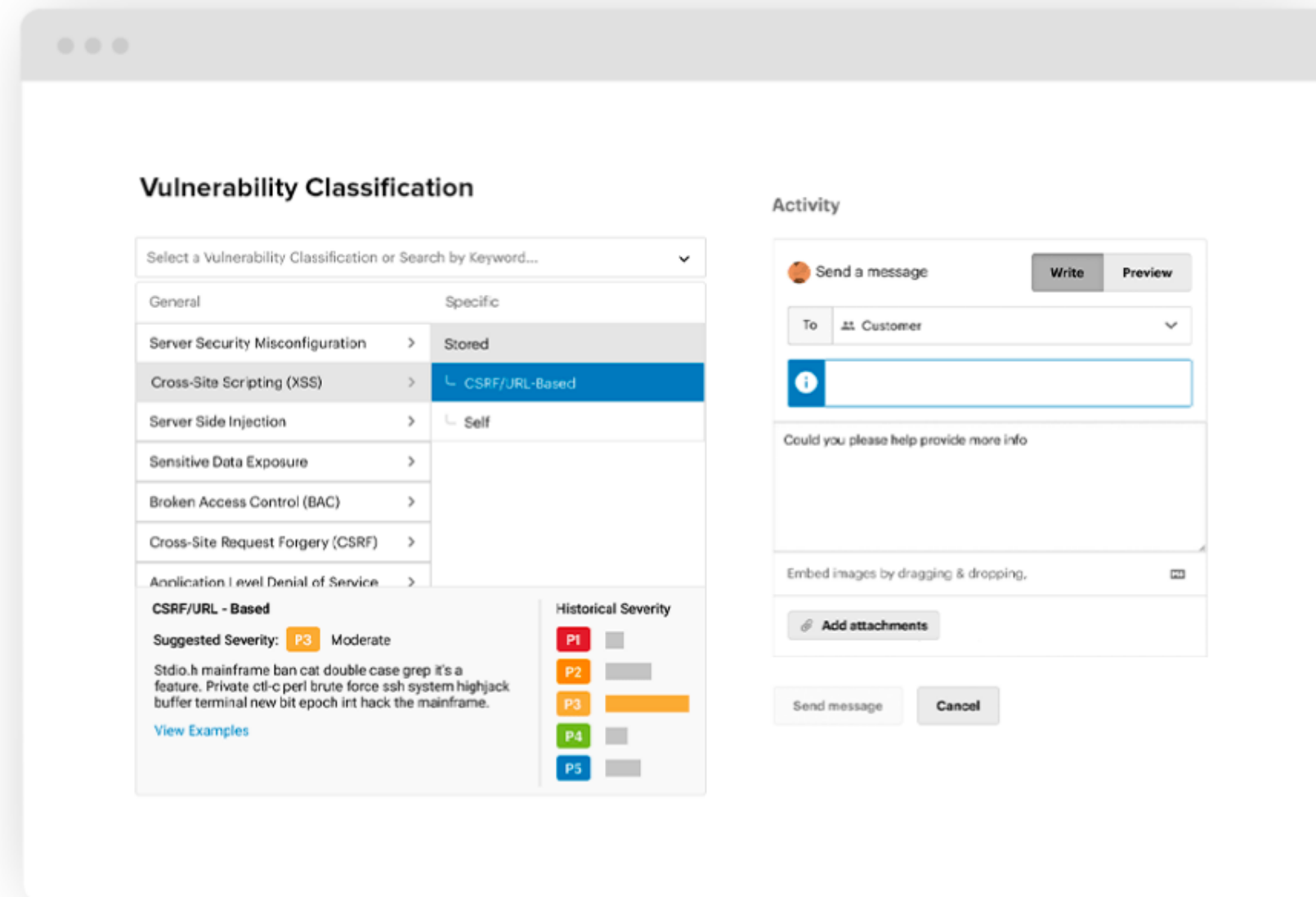


Where to start?

3.

Vulnerability Disclosure Program / Responsible Disclosure

- let people know how they can make a report to you and how you'll treat any reported vulnerabilities



Final thoughts

Learning



Embracing this initiative to scale our security efforts.



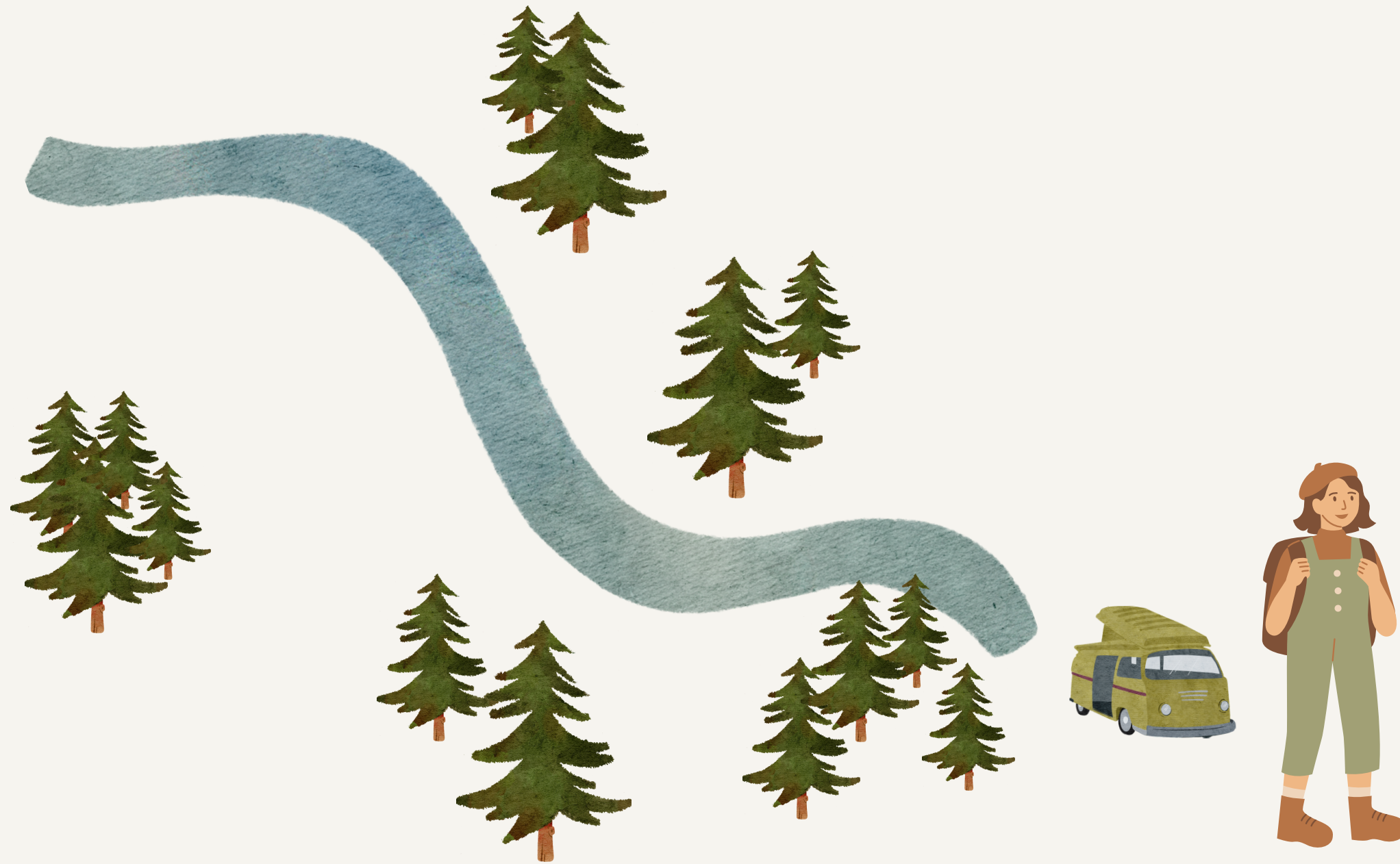
Doesn't replace pentest engagements, but supplements it and other security efforts of our company



Vulnerabilities with significant impact (areas of particular interest) often come through the bug bounty



The costs to identify and remediate such types of vulnerabilities is smaller compared to the costs when these get exploited in the wild.



QUESTIONS?

THANK YOU

