

Handling Bug Bounty from a Blue Team's Perspective

Disclaimer: This presentation is for educational purposes only. Opinions or points of view expressed in this presentation represent the view of the presenter, and does not necessarily represent the official position or policies of the Razorpay . Nothing in this presentation constitutes legal advice.

— WHO WE ARE —

1 | ABOUT RAZORPAY

2 | SETTING UP A BUG BOUNTY PROGRAM

— THE LANDSCAPE —

3 | WORKFLOW OF A BOUNTY RESEARCHER

4 | OUR SETUP

5 | QUANTIFYING THE TRAFFIC


6 | GUIDING PRINCIPLES

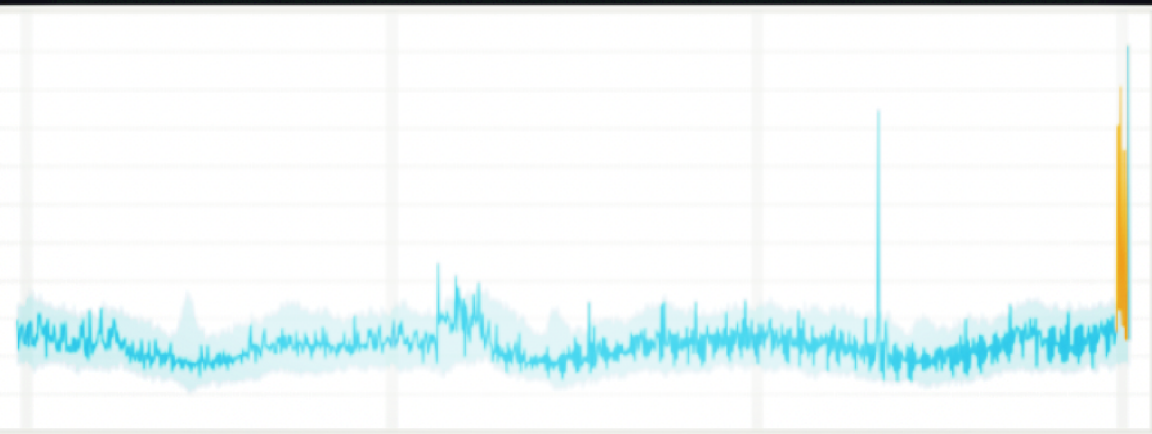
— BLUE TEAMING —

7 | OUR SOLUTION

8 | KEY TAKEAWAYS

Story Time

 Summary there is an increase in 5xx pattern on application load balancer, with an anomaly of +2133 from previous 4 days



Traefik Jam

Load balancers are overloading!

[7:00 PM]

5 app teams notify us of increased 4xx, 5xx

[10:00PM] - ERRORS INCREASE

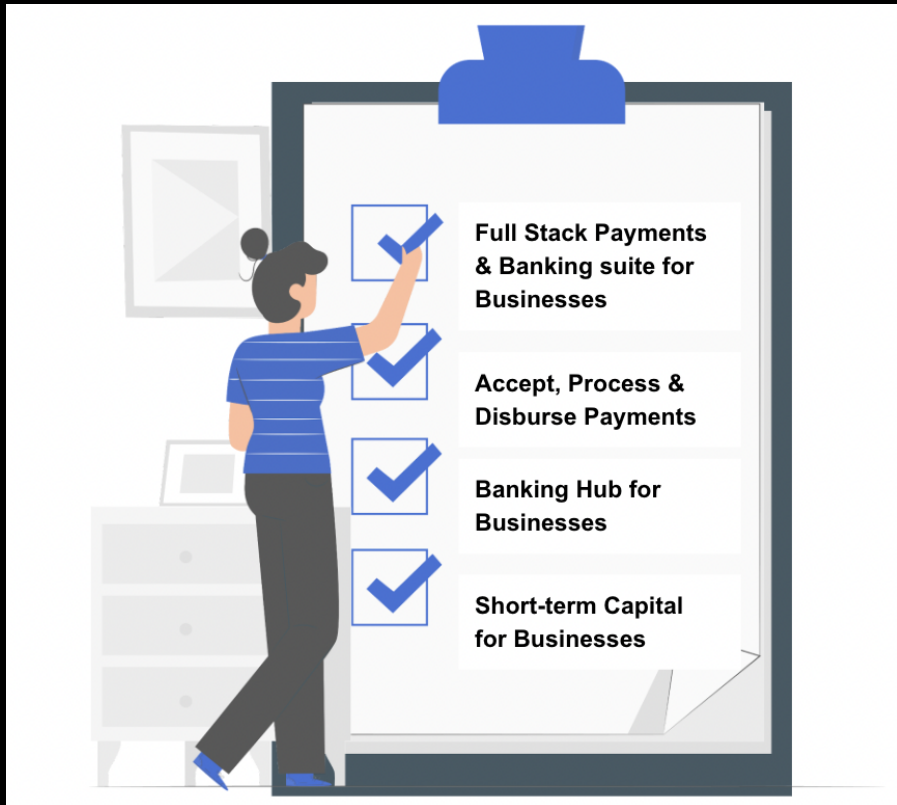
12 app teams report increased 4xx/5xx errors

[09:00 AM NEXT MORNING]

23 app teams have experienced spike in errors

About Us

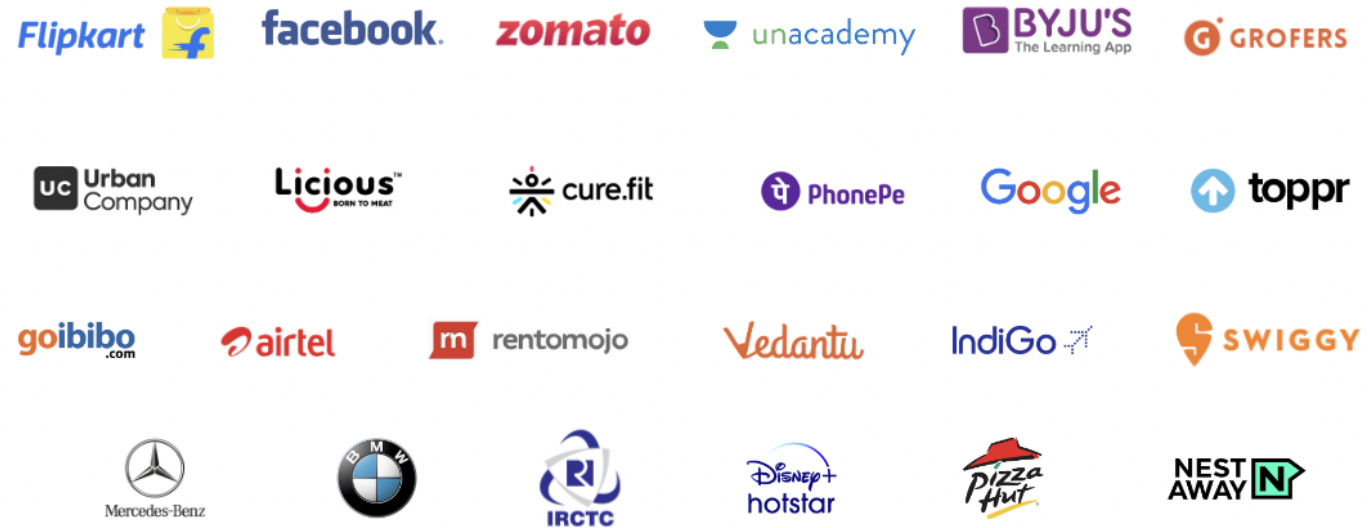
It all started with an idea...



Transforming the world of business finance
with insight, intelligence and innovation

Who uses Razorpay?

POWERING
PAYMENTS AND
BANKING FOR
OVER 10 LAKH+
BUSINESSES



Our Growth Metrics

We have 6 BUs,
over 60 pods and
800 employees in
tech.



10x Growth

10x growth in Headcount in last 4 years. ~600 engineers.



Scaling Teams

Full-Fledged Pods & BUs (4 BUs, 40+ Pods, 600+ engineers)



100+ Microservices

50+ microservices in the last 2 years and growing



5 Acquisitions

5 companies in the last 4 years.



Polyglot Stack

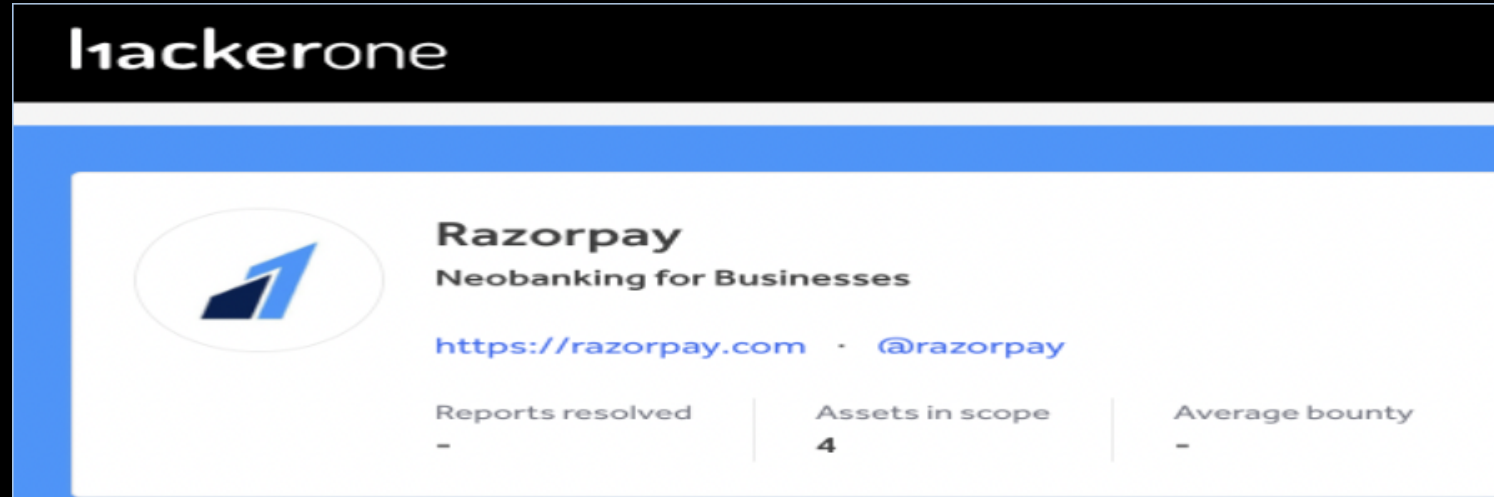
Go, PHP, Python, Java, Nodejs, Scala



Deployments

~2000 deployments per month

What happened?



Reports resolved	Assets in scope	Average bounty
-	4	-

Program Rules

- Please use your username@wearehackerone.com email address for registration where the username is your HackerOne username.
- Include a custom HTTP header in all your traffic. (Burp and other proxies allow easy automatic addition of headers to all outbound requests.) A header that includes your username: X-Bug-Bounty: HackerOne- `<username>`
- **DO NOT** use automated tools or scanners. Reports as such will be closed as N/A.

What happened?

Slack discloser
Stored X'
InVisio
Four®

@disclosedh1

Razorpay started using [@Hacker0x01](#) today:
hackerone.com/razorpay #hackerone #disclosure



hackerone.com

Razorpay - Bug Bounty Program | HackerOne

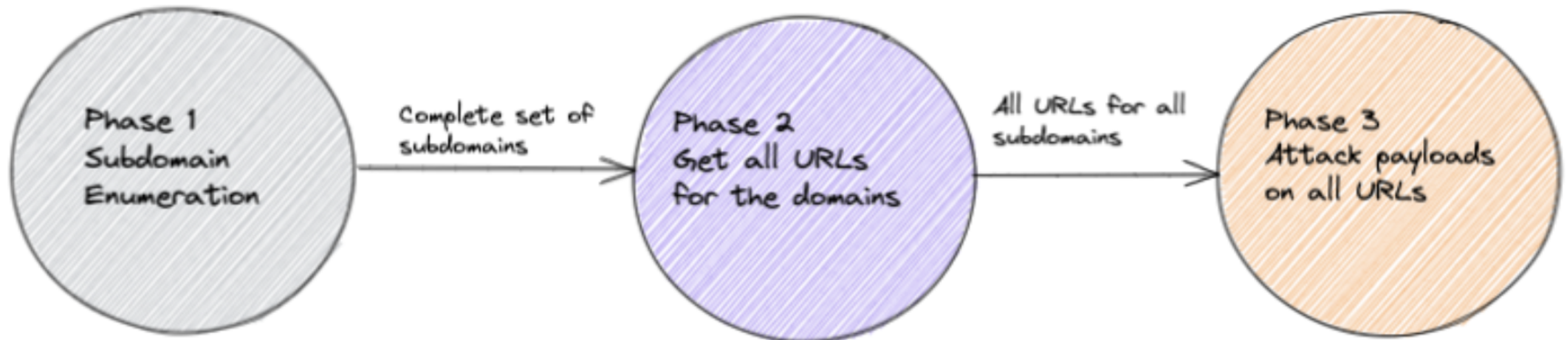
The Razorpay Bug Bounty Program enlists the help of the hacker community at HackerOne to make Razorpay more ...

But the thing about hackers is...

Typical hacker mindset : A visual guide



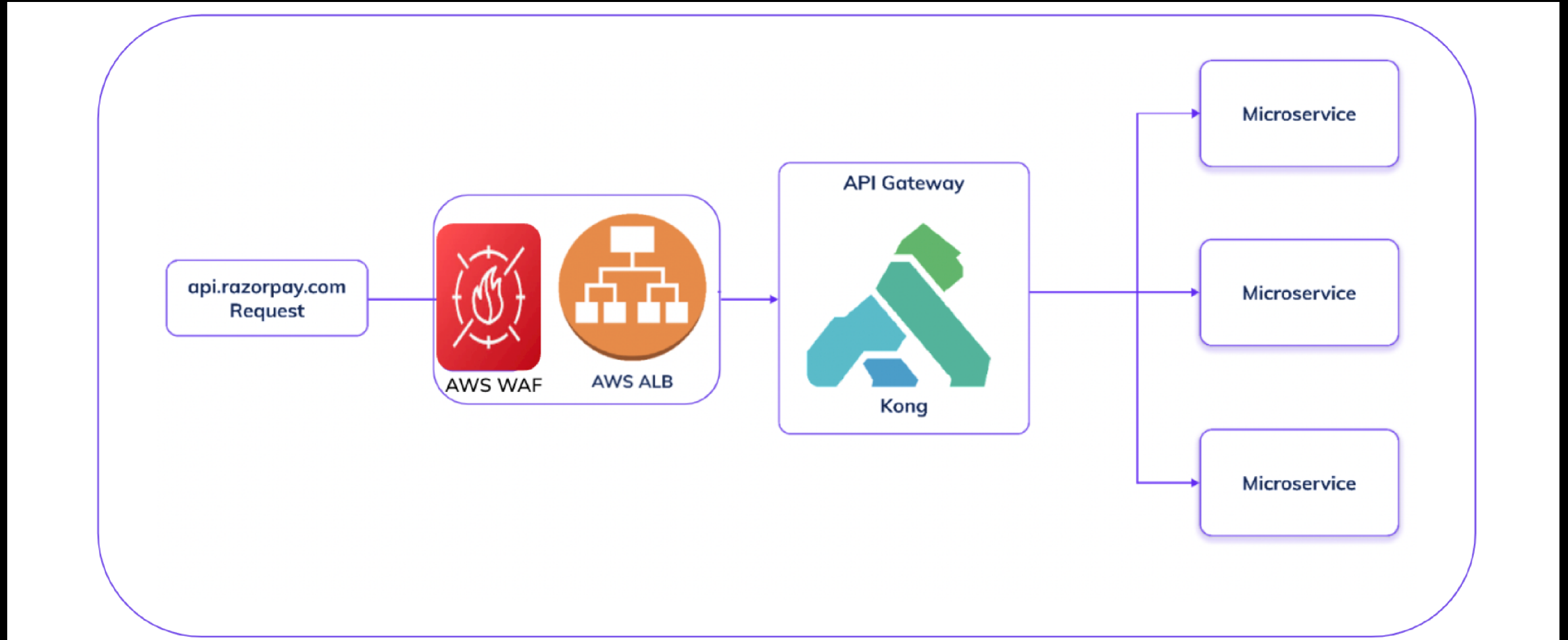
Workflow of a bug bounty hunter



Workflow of a bug bounty hunter



Our Setup



Quantifying the traffic

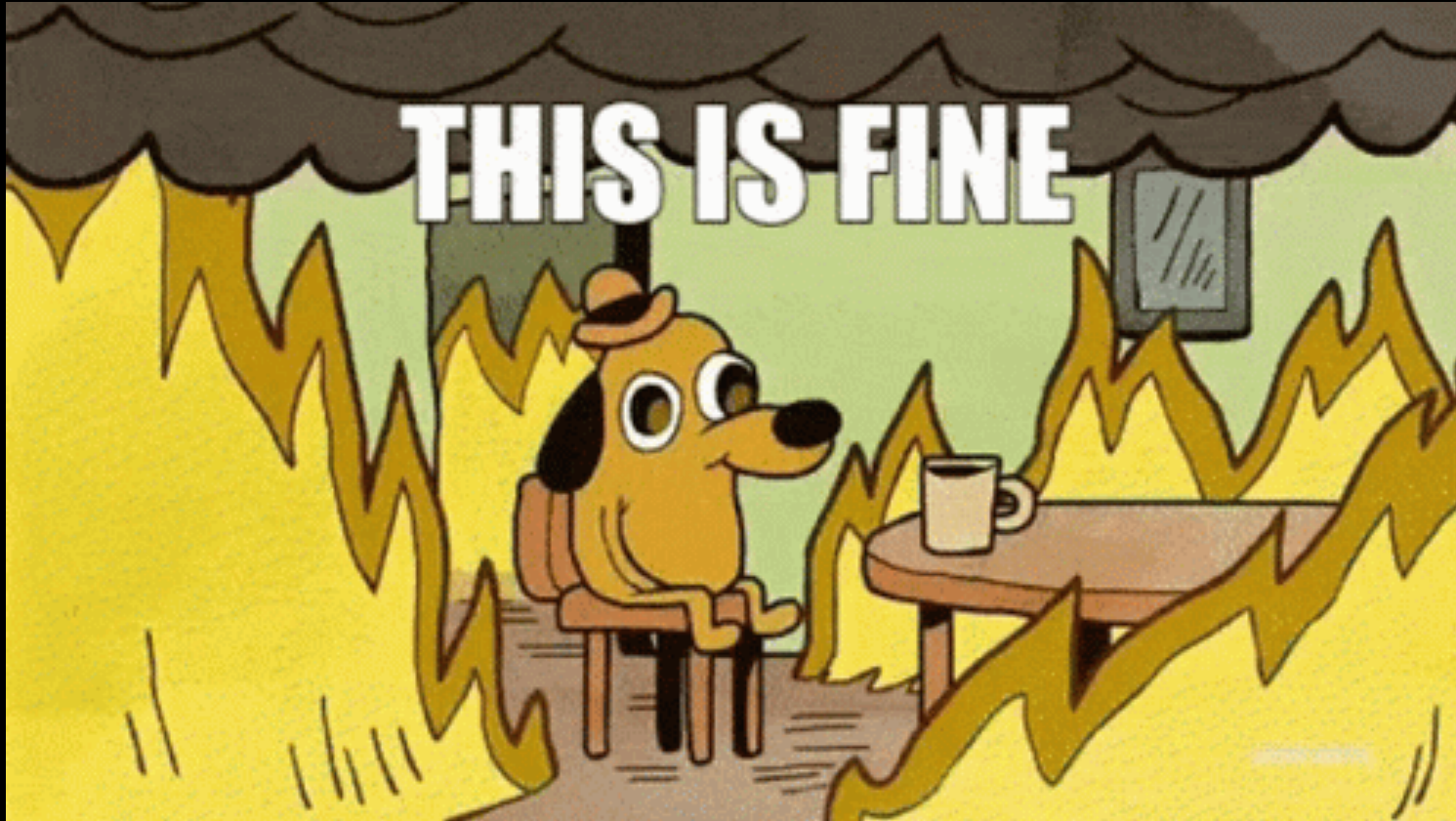


Therefore, total spike in traffic due to bug bounty alone

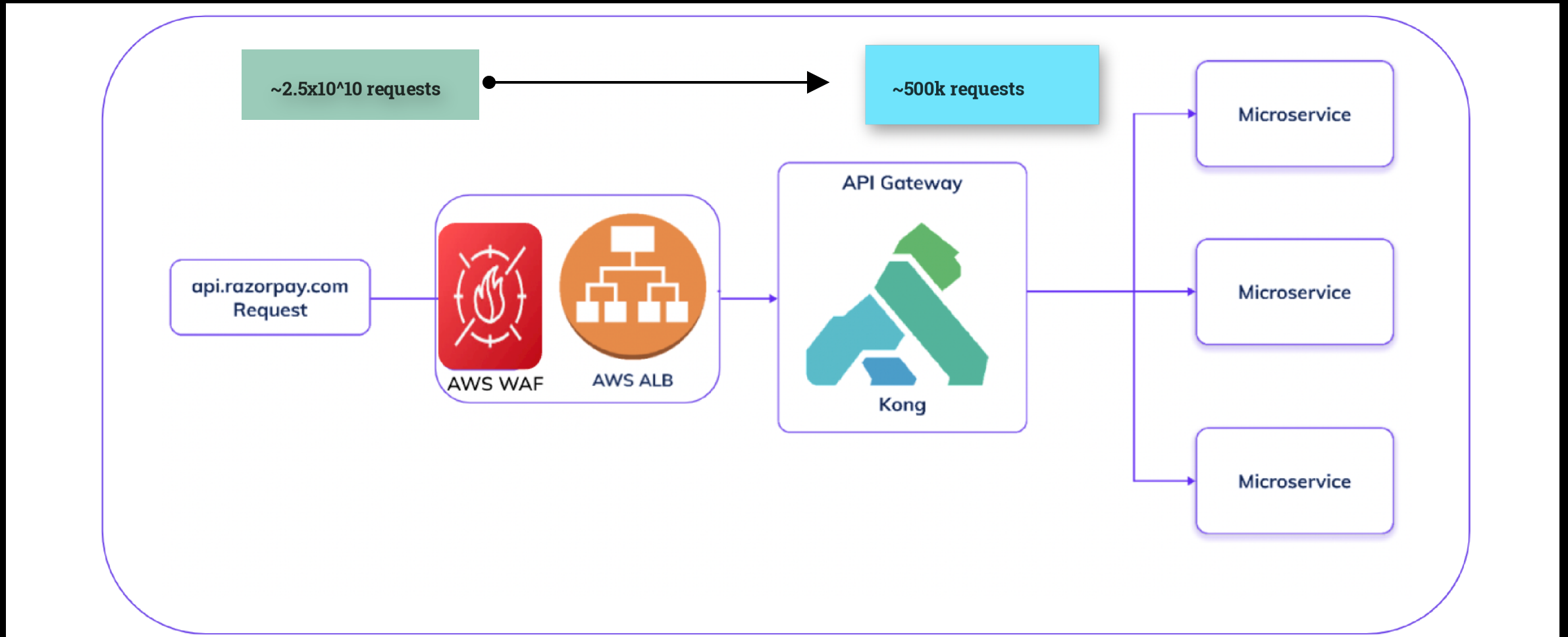
(considering all public domains are covered by the bug bounty researchers) :

$$500 * 10k * 5k = 2.5 \times 10^{10} \text{ requests}$$

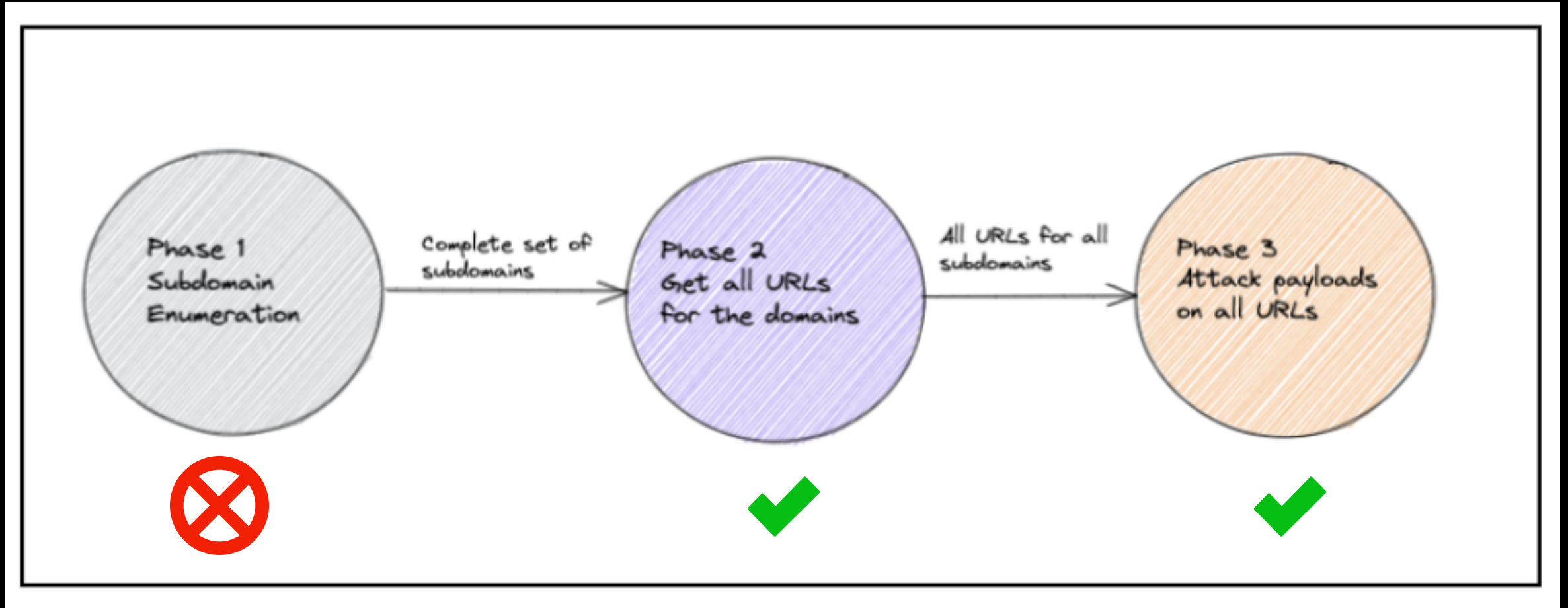
Not good news for our microservices..



Our Setup : Impact on microservices



Back to the drawing board : Controlling the controllable



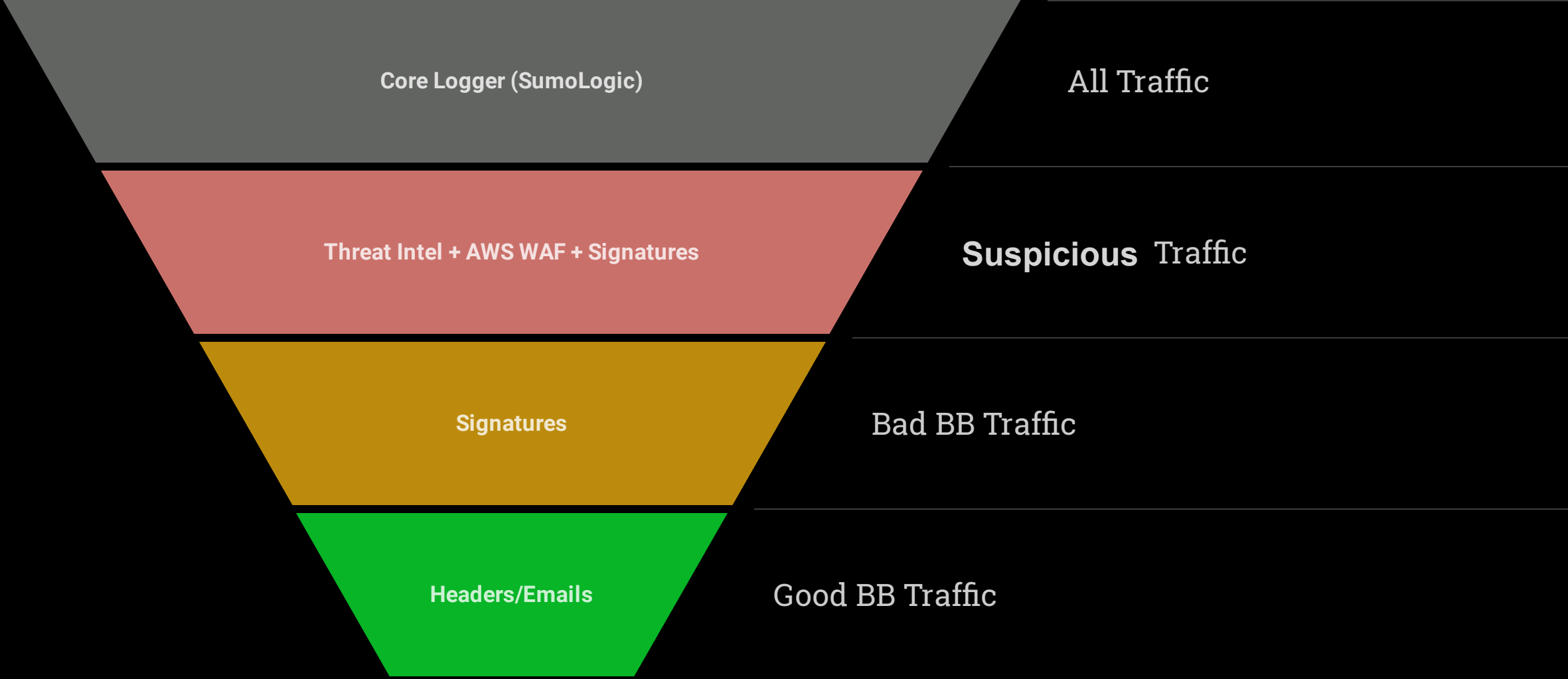
Can we do something to prevent this?

Guiding Principles

- **Availability is key**
- **Good experience for BB Hunters**
- **Ensure correct categorization of legitimate, bounty and suspicious traffic**
- **Automated framework & self-serve dashboards**



Traffic Funnel



Security Blue Team : Basics

The group responsible for defending an enterprise's use of information systems by maintaining its security posture against adversaries

1

DETECT

- a. Alert on error volume
- b. Blocking at the WAF

2

FINGERPRINT/ IDENTIFY

- a. Identify if this is BB traffic
- b. Fingerprint the actor

3

REMEDiate

- a. Throttle the attacker
- b. Block the attacker

Phase 2 & 3 - Identify & Remediate

Phase 2 : Identify

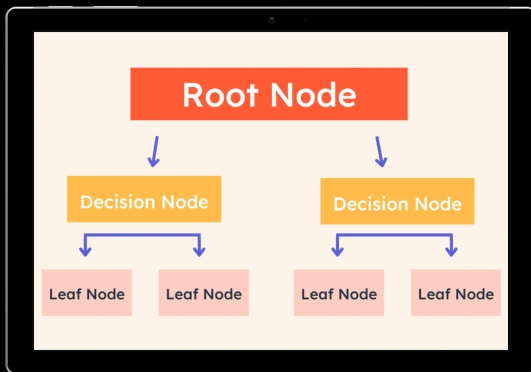
- Compliant Bounty Hunters
 - Custom Email and HTTP headers
 - Divergent Bounty Hunters
 - Attack payload based recognition
 - Database of researcher fingerprints
-

Phase 3 : Remediate

- Remediation is done at WAF
 - Compliant Bounty Hunters
 - No restriction
 - Internal communication to Incident Response team
-
- Divergent Bounty Hunters
 - Throttle/Block

Automation of Identify Phase

- Decision flow for all scenarios
- Detailed Run-books with remediation steps
- Self serve realtime dashboard of Bug Bounty Traffic



Automation of Identify Phase (Contd.)

Tool - SumoLogic

- **Microservice error traffic (upper graph)**
- **Bug Bounty traffic (bottom graph)**
 - **Based on Headers, Email**
 - **Attack payloads**
 - **IPs**
- **Superimpose the 2 graphs for a quick identification**
- **If 2 peaks are seen at same time => BB traffic**



Automation of Remediation Phase

Tool - SumoLogic, AWS WAF

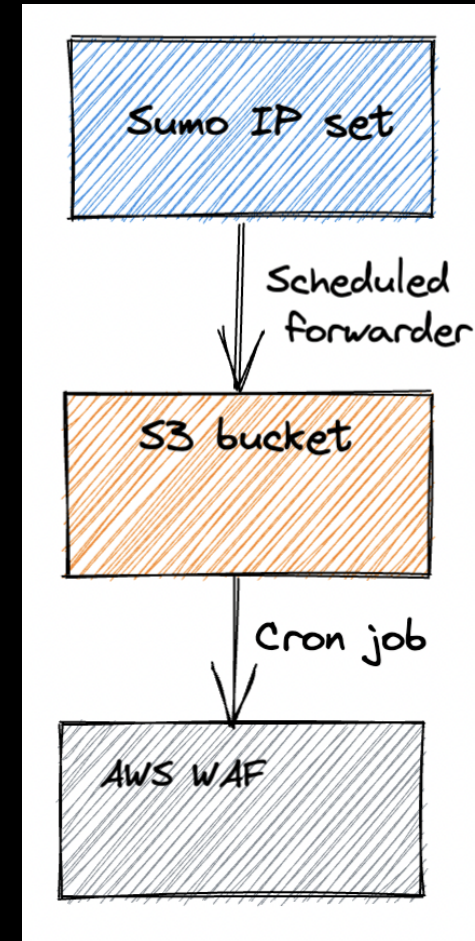
- Blue teamer analyses the BB traffic
- If attacker or bad bug bounty hunter
 - Throttle the IP
 - Block the IP
- Blue teamer adds the IP to the Sumologic Throttle or Block IP Set



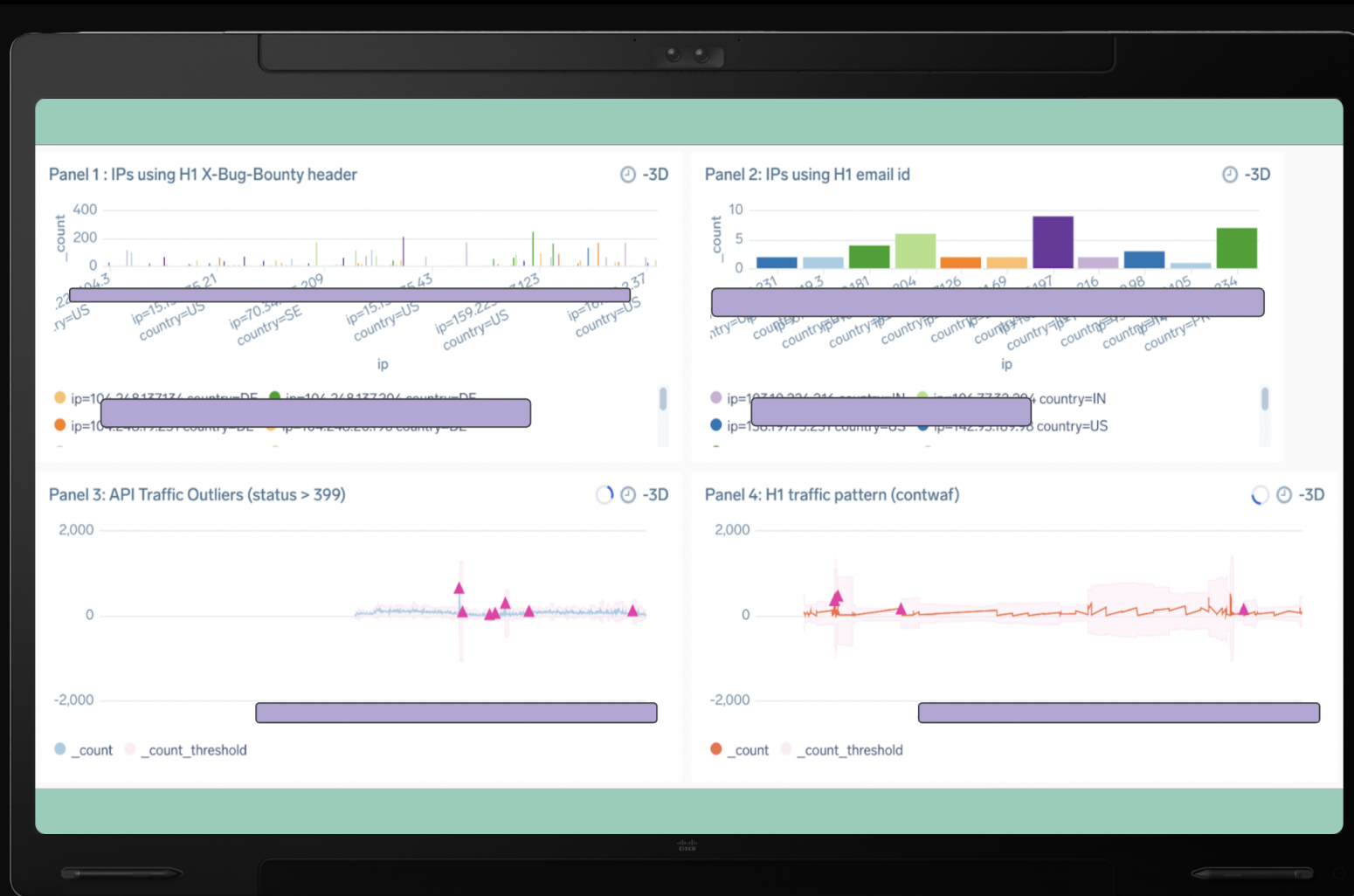
Automation of Remediation Phase (Contd.)

Tool - SumoLogic, AWS WAF

- **SumoLogic <-> AWS WAF Automation Framework**
- **Blueteamer adds/removes IPs from the Sumologic IPset**
- **Script keeps the Sumologic IP List & WAF IPset in sync**
 - **Sumologic Scheduled View pushes the IPs from Sumo -> S3 bucket**
 - **Script pushes IPs from S3 -> AWS WAF**

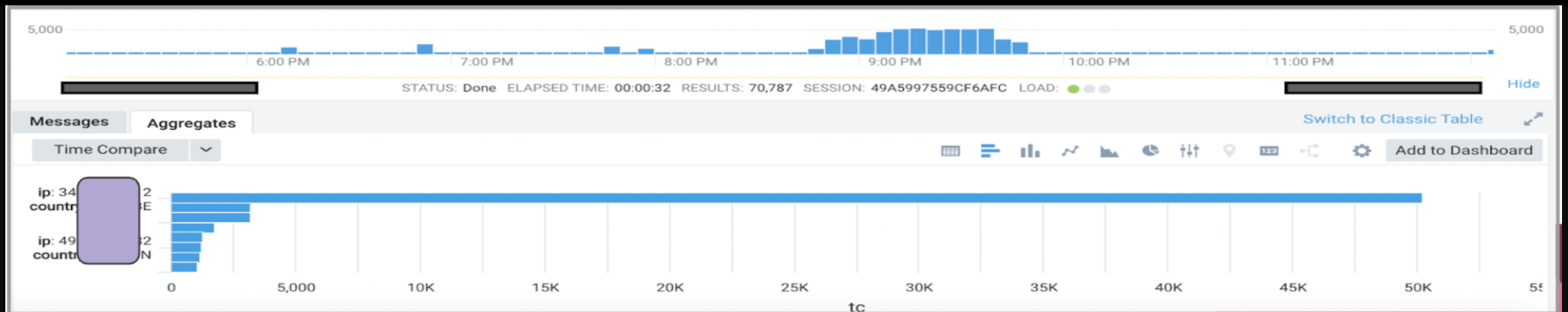


The Final Confluence



Lessons Learned

- **Continuous Feedback** - It is an ongoing process
- **Block at the outermost layer Limit** - Apply WAF rules
- **Store payload patterns & researcher fingerprints**



Key Takeaways

- **Identify your scope: What/where/how long/latency of logging**
- **Think like an attacker : A good blue team defence strategy is to look from the lens of an attacker (and possibly be one!)**
- **Focusing on automation frameworks/ self-serve dashboards**

About Us

We love to network and are always up for a chat!

Reach Out :)



ASHWATH K

Twitter : @ka3hk

LinkedIn:

<https://www.linkedin.com>

/in/

ashwath-kumar-

5a4383b/



ANKIT ANURAG

Twitter : @covertly_overt

LinkedIn:

<https://www.linkedin.com>

/in/

ankitanurag/



SUCHITH NARAYAN

Twitter:

@narayansuchith

LinkedIn:

<https://in.linkedin.com>

/in/

suchithnarayan

Thank You. Send your answers for cool swags!

