

Data Driven Bug Bounty

Arkadiy Tetelman (@arkadiyt)

Agenda

- Program logistics @ Twitter, Airbnb
- Running a data driven program
- Methodology
- Questions

Program Logistics - Twitter

- Single public program
- Soft launch (unpaid), then moved to paid
- Triage by NCC Group
- ~4-6 appsec engineers, 1 week rotation
- \$950,000 over 4 years, 850 resolved reports
- More stats:

https://blog.twitter.com/engineering/en_us/a/2016/bug-bounty-2-years-in.html

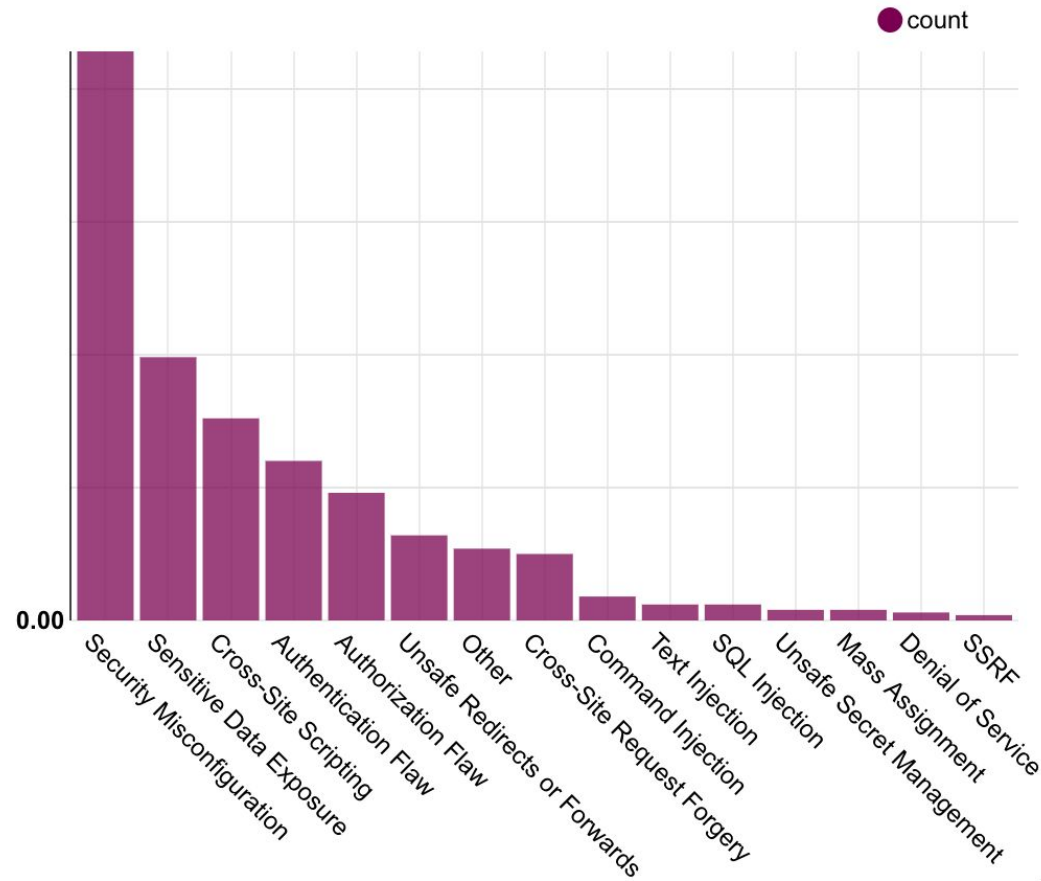
Program Logistics - Airbnb

- Started as 2 programs: public (unpaid) & private (paid)
- Merged into 1 public paid program (as of March 2018)
- Triage by Hackerone
- 4 appsec engineers, 2 week rotation
- \$430,000 over 3 years, 430 resolved reports

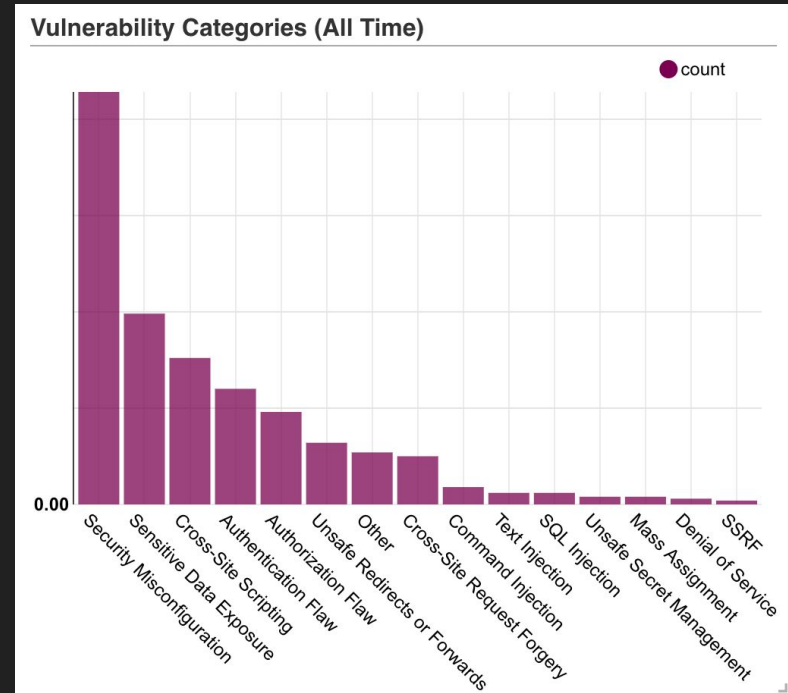
Running a data driven program

Thesis: data provides half the value

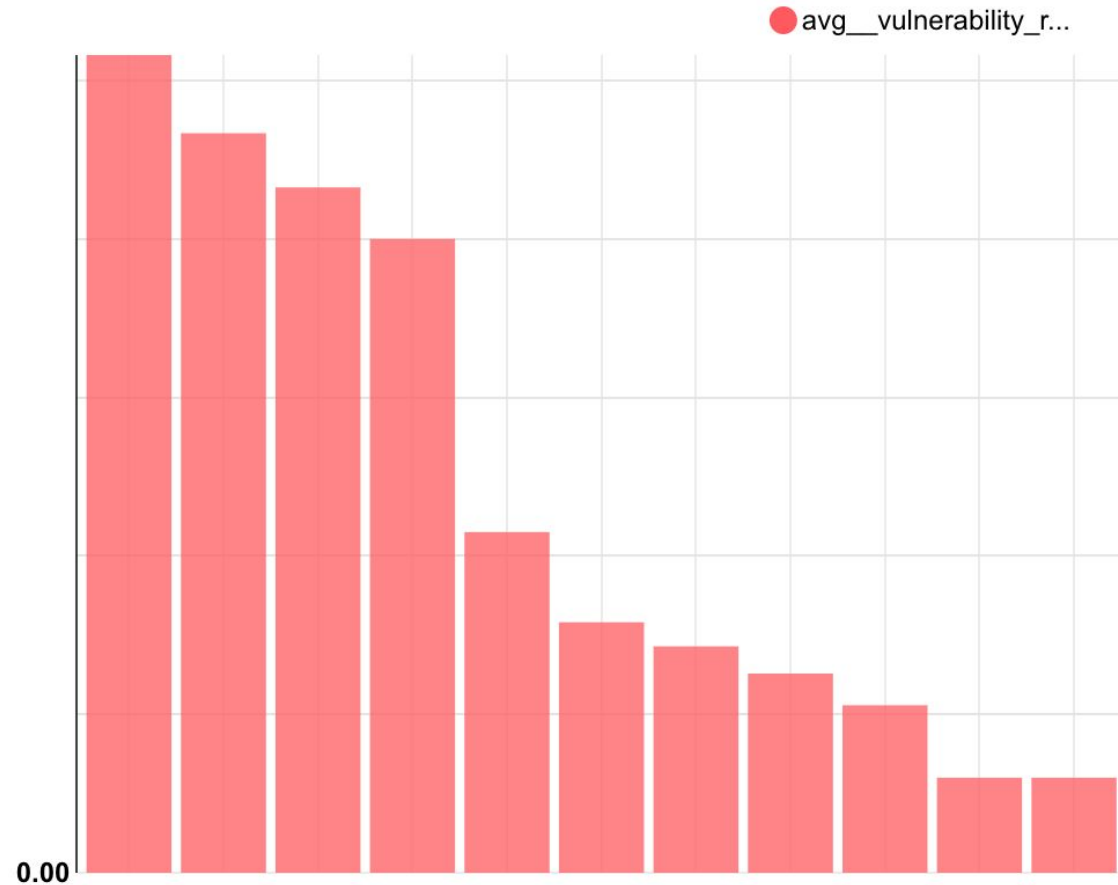
Vulnerability Categories (All Time)



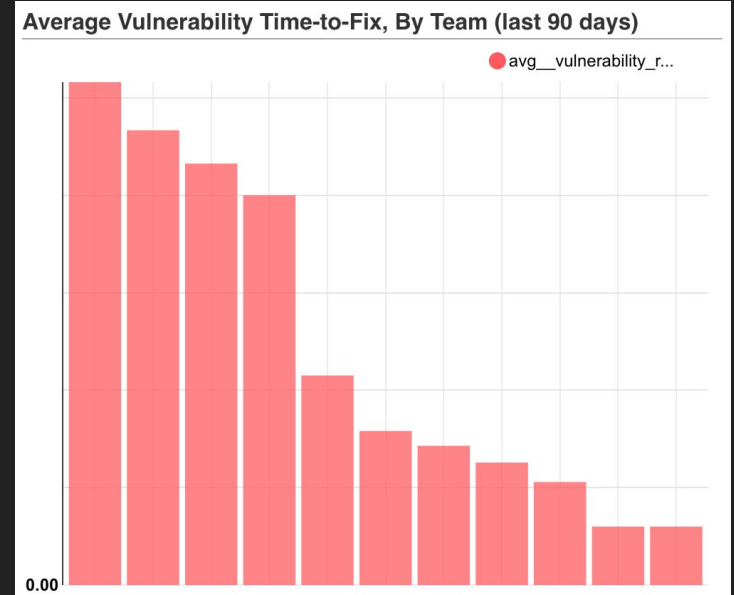
- Immediately know your risk breakdown, focus your energy there
- Feed this into quarter planning
- Measure ROI
- Requires: internal taxonomy



Average Vulnerability Time-to-Fix, By Team (last 90 days)



- 10x difference between fastest/slowest teams
- Also track SLA
- Hold teams accountable
- Give positive reinforcement



Open Vulnerabilities by Subteam and Priority



○ Grouped

● Stacked

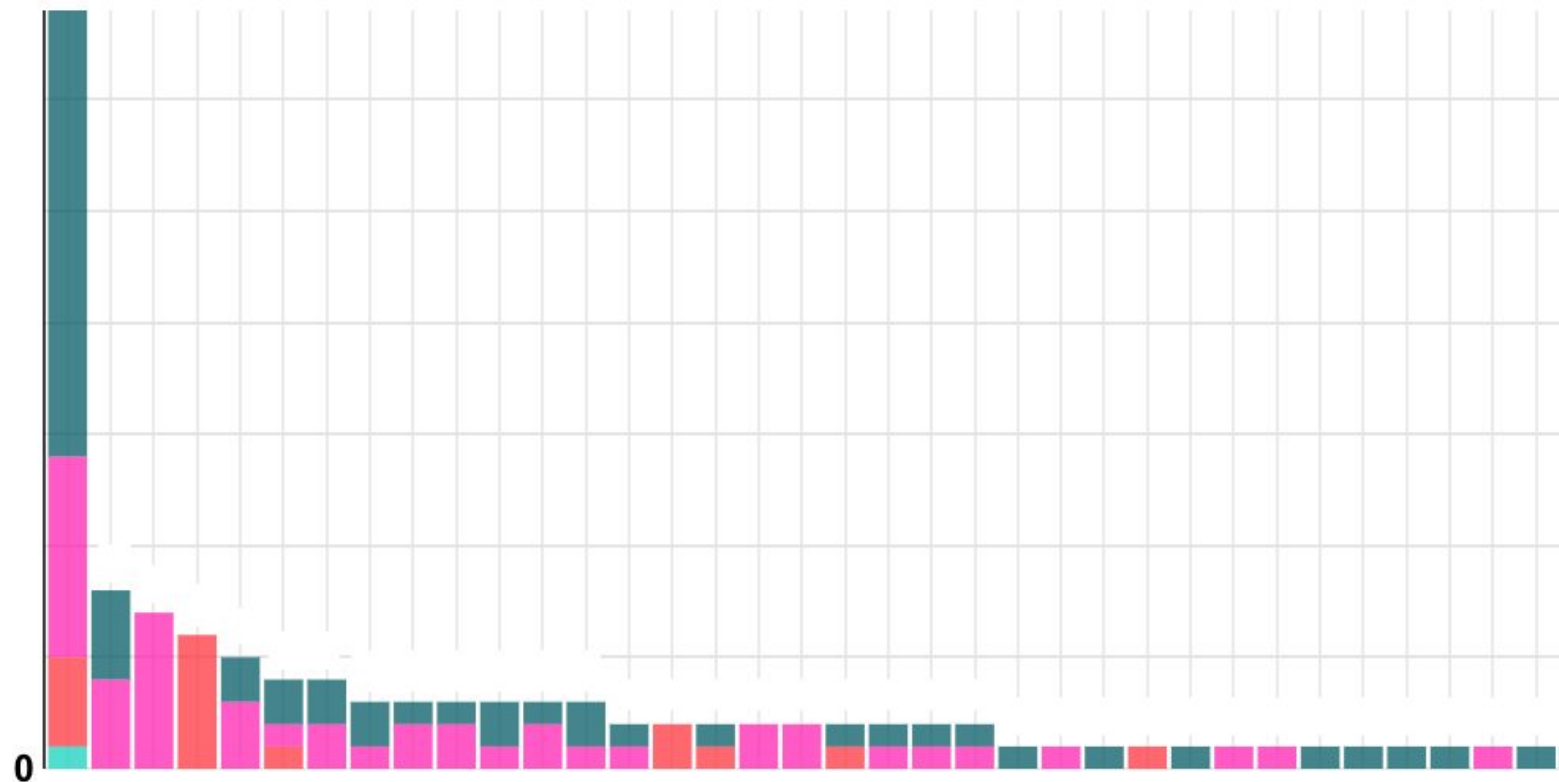
● 0

● Critical

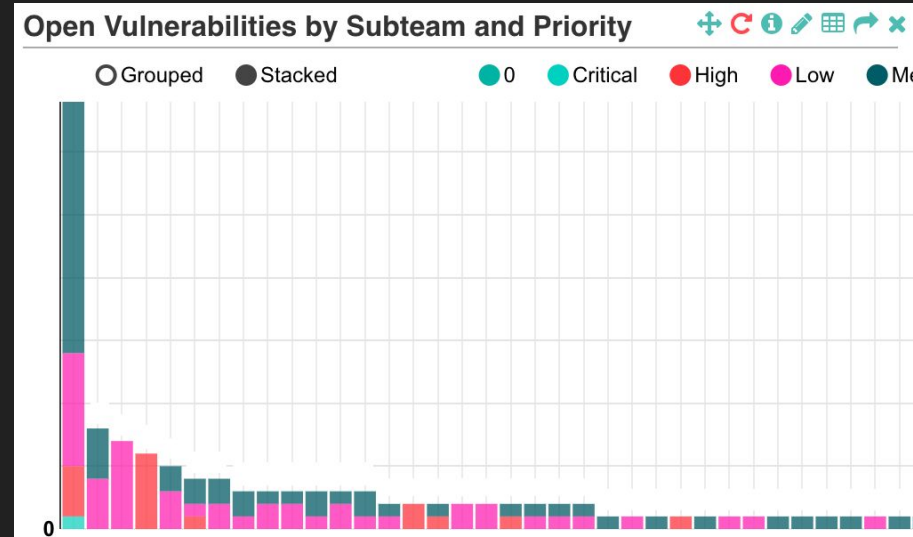
● High

● Low

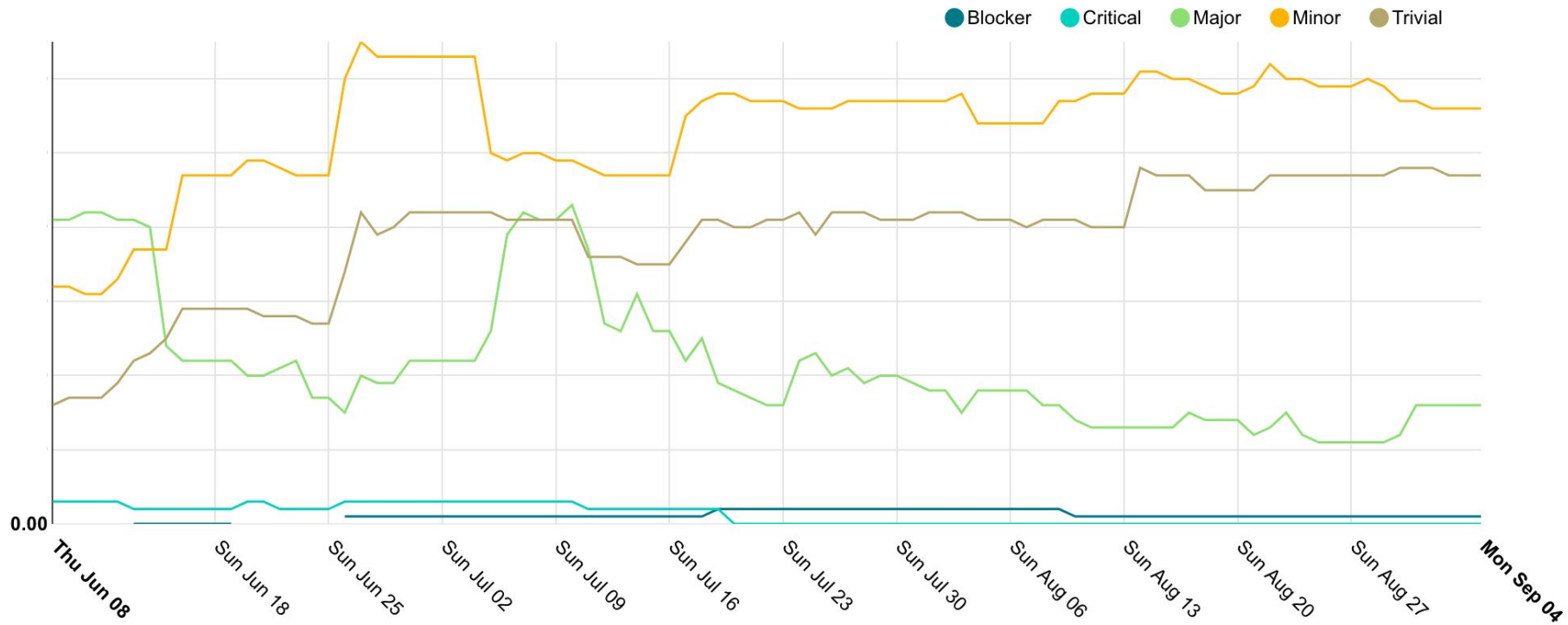
● Me



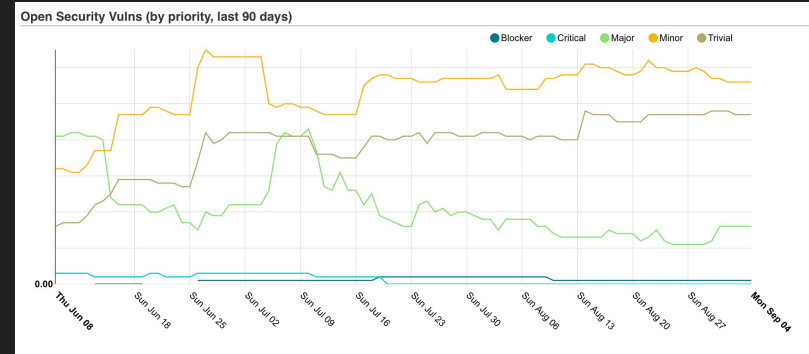
- Notice a pattern?
- Lets security engineers know good/bad teams
- Helps drive conversations forward (but be careful!)



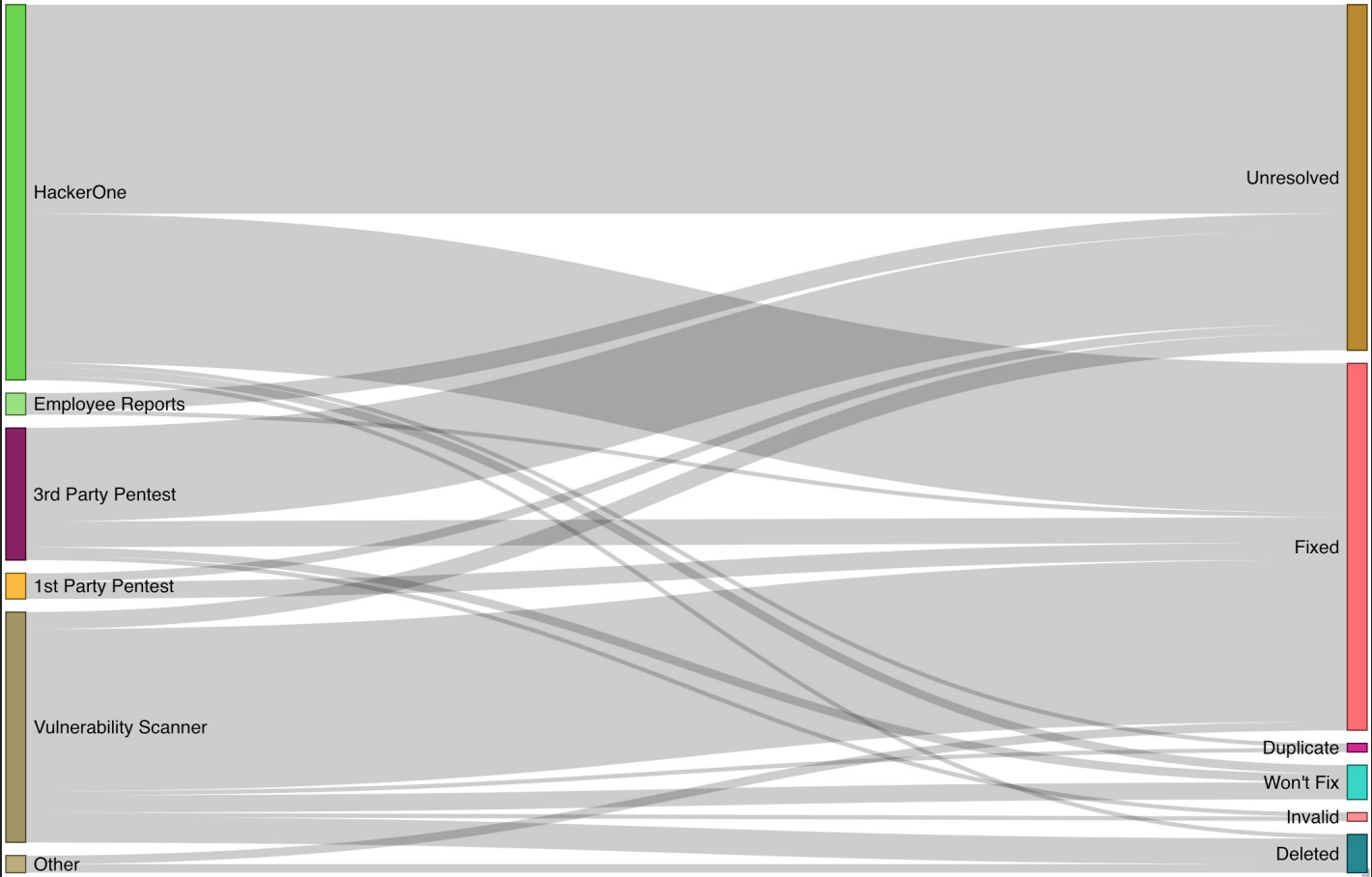
Open Security Vulns (by priority, last 90 days)



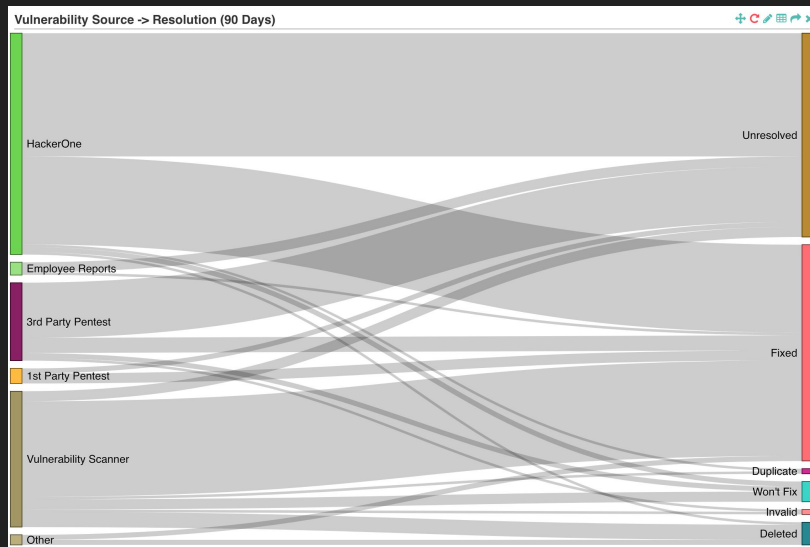
- Can be shared widely - be visible!
- Measure improvement (or lack of improvement) over time
- Use data to drive business goals



Vulnerability Source -> Resolution (90 Days)



- ~50% reports from bug bounty, ~35% of reports from scanners
- Watch for changes, i.e.:
 - ⬆ Scanner -> Invalid: tune false positives
 - ⬇ Bug bounty: is your program healthy?



● Response Efficiency

6 hrs

Time to first response *

8 hrs

Time to triage *

3 months

Time to bounty *

15 days

Time to resolution *

* Average of last 90 days

Bounty Statistics

\$242,950

Total bounties paid

\$500

Average bounty

\$1,000 - \$20,000

Top bounty range

Validation within **1 day**

75% of submissions are accepted or rejected within 1 day

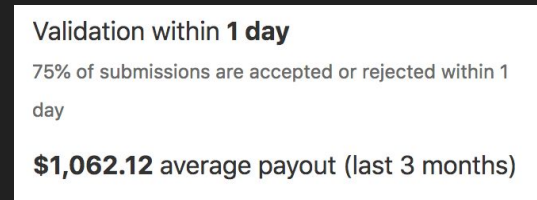
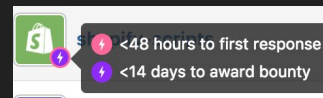
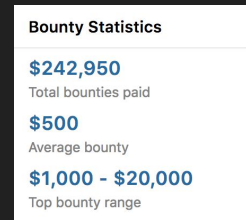
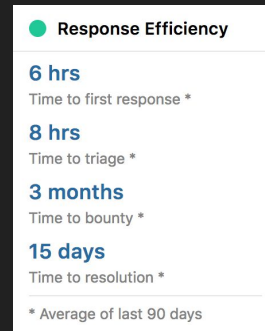
\$1,062.12 average payout (last 3 months)



<48 hours to first response

<14 days to award bounty

- Most important for program health: time to response, time to bounty
- Least important to *collect*
- Benefits:
 - More researchers, better reports
 - Researchers talk with each other
 - Get early notice/access



Methodology

- If launching a program:
 - start with a pentest, assess yourself
 - launch a private program w/ a few researchers & limited scope
 - ensure program policy gives researchers safe harbor
 - grow slowly, tune your workflow
 - go public when ready
- Starting/started a program:
 - define taxonomy, tag vulnerability class / source / team, keep track of SLA

Conclusion

- Data driven bug bounty:
 - Informs your security posture
 - Serves as input into security roadmapping
 - Drives conversations with other teams forward
 - Lets you be visible in your organization
 - Helps you run a healthier bug bounty program
- Methodology:
 - Start small & scale out

Questions

Arkadiy Tetelman (@arkadiyt)