Vulnerability Management Process

Maria Mora
@RiaMariaDotCom
riamaria.com

whoami

Staff Security and Compliance Engineer at crunchyroll®

this presentation and my opinions are my own and do not reflect the views of my company

HEAD: Security and Compliance Team

- Application Security, Compliance Management, Incident Response, Bug Bounty Triaging, Software Engineering

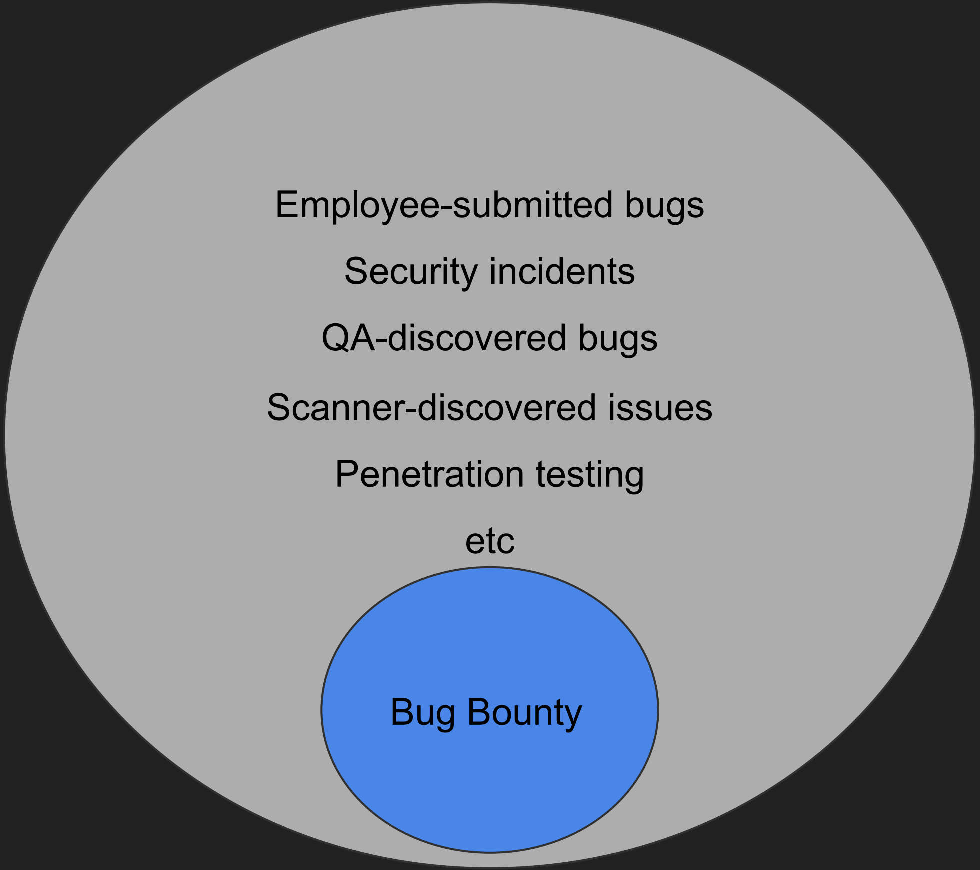
HEAD~1: Payments and Subscriptions Software Engineer

- Software Engineering, Product Development

goal

Raise awareness and visibility of the entire bug bounty lifecycle

Panel: Let’s Get 360 With Bug Bounty (BSides SF 2020)
L-R: Jeff Boothby, Maria Mora, Chloé Messdaghi
Out of frame: cache-money, nahamsec



Employee-submitted bugs

Security incidents

QA-discovered bugs

Scanner-discovered issues

Penetration testing

etc

Bug Bounty

scope

bug bounty program

1. Reports come in
2. We determine severity
3. Give the $
4. Fix the bug

bug bounty program

1. Reports come in
2. We determine severity
   a. Try and replicate (back and forth)
   b. See if QA or engineering teams can help
   c. A lot of communication here
3. Give the $
4. Fix the bug

bug bounty program

1. Reports come in
2. We determine severity
   a. Try and replicate (back and forth)
   b. See if QA or engineering teams can help
   c. A lot of communication here
3. Give the $
   a. Figure out how to get them the money
   b. Ensure money gets to them
   c. Work with other departments to disburse funds
4. Fix the bug

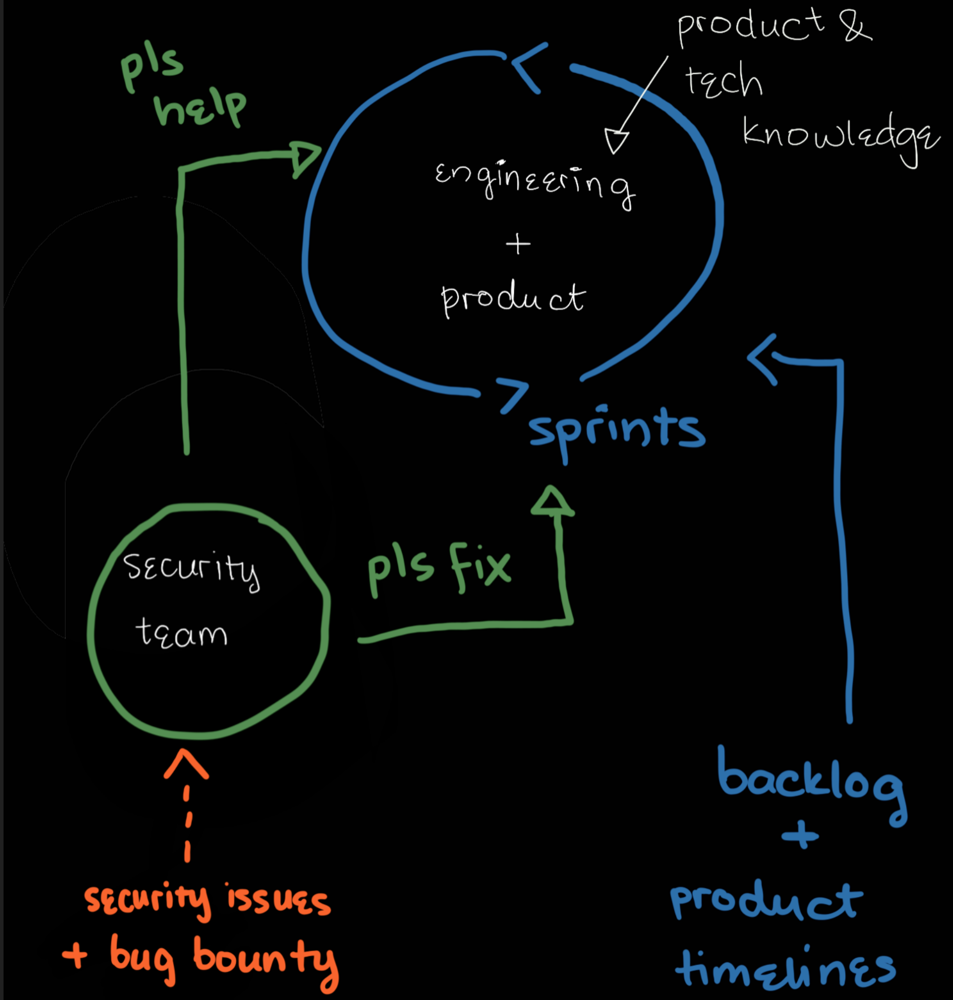
bug bounty program

1. Reports come in
2. We determine severity
   a. Try and replicate (back and forth)
   b. See if QA or engineering teams can help
   c. A lot of communication here
3. Give the $
   a. Figure out how to get them the money
   b. Ensure money gets to them
   c. Work with other departments to disburse funds

~~4. Fix the bug~~ Get others to fix

consider

it takes a village



company A

↓

Legacy Code

company B

↓

no dedicated security team

company C

↓

don't have their ★★★★ together

triagers, bug bounty hunters, product and engineering teams, students, newbies, companies, engineering leadership, company leadership

that's just **part** of the story