RSAConference2018
San Francisco | April 16–20 | Moscone Center

SESSION ID: TV-R11

BUILDING A BUG BOUNTY PROGRAM: FROM THE TRENCHES

Yogesh Badwe

Director of Security
Okta, Inc.

Planning Cycle

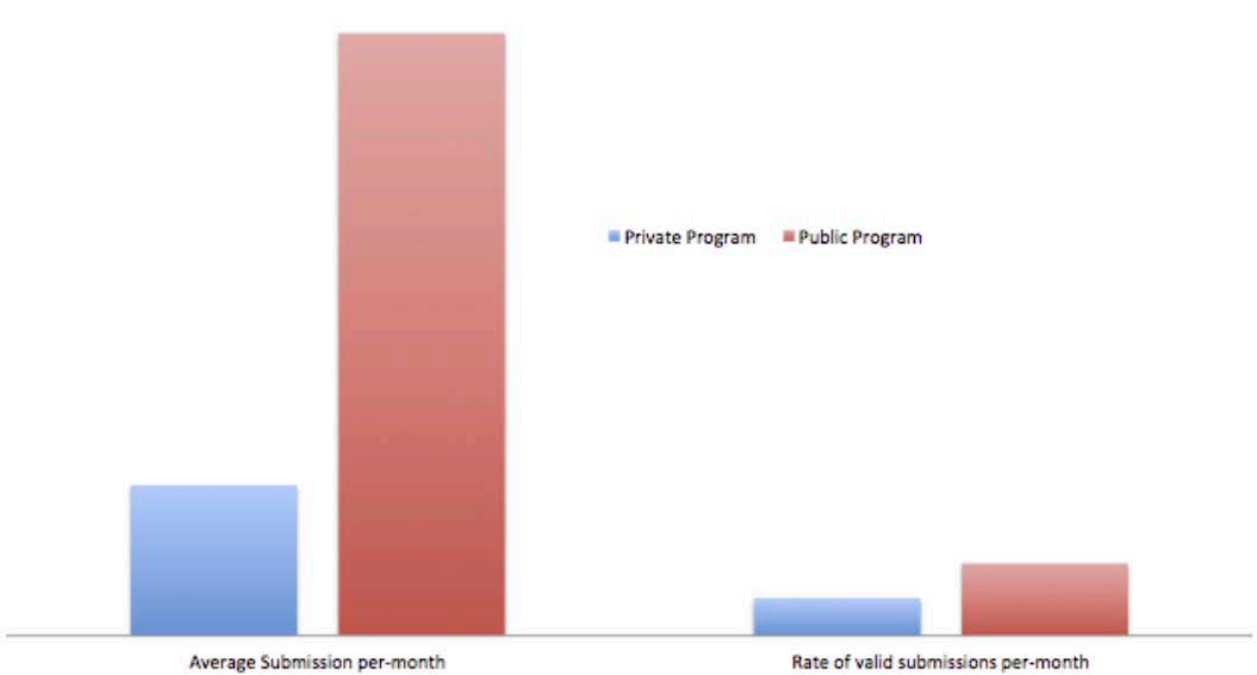
The Why


External Validation
Disclosure Channel
Resource Augmentation
Goals
Improve time2fix
Trust Building
Security Brand
Cost Saving

Strategy

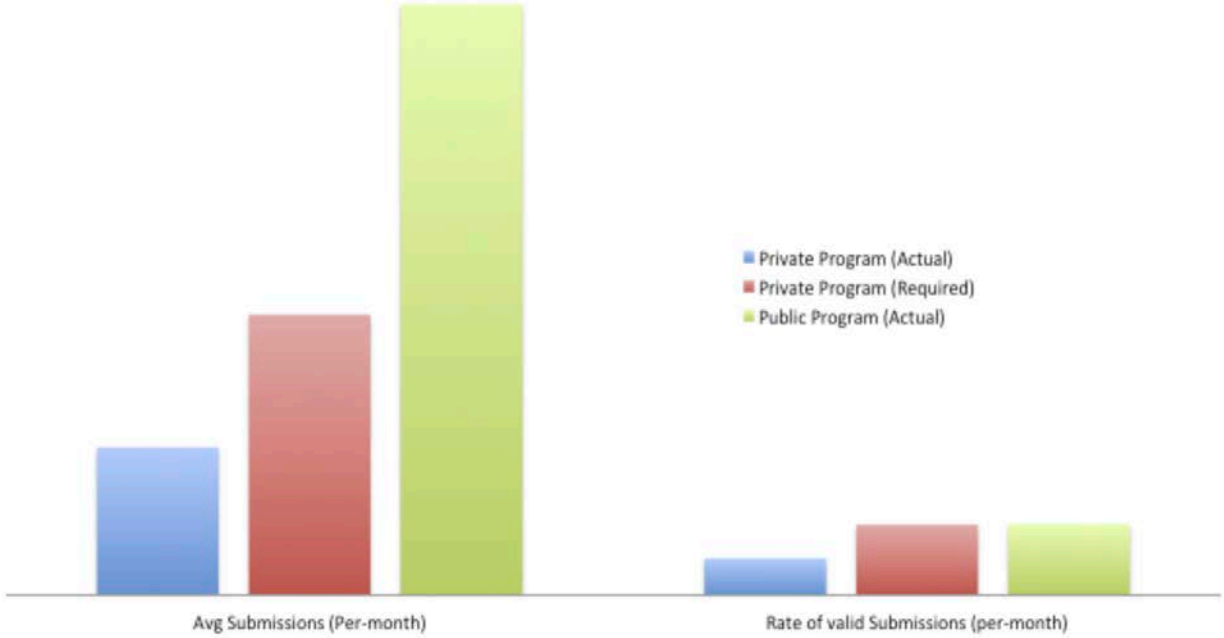
Type of Program

Value	Valid Submissions
Noise	X
Activity	X
Go with	Public Program



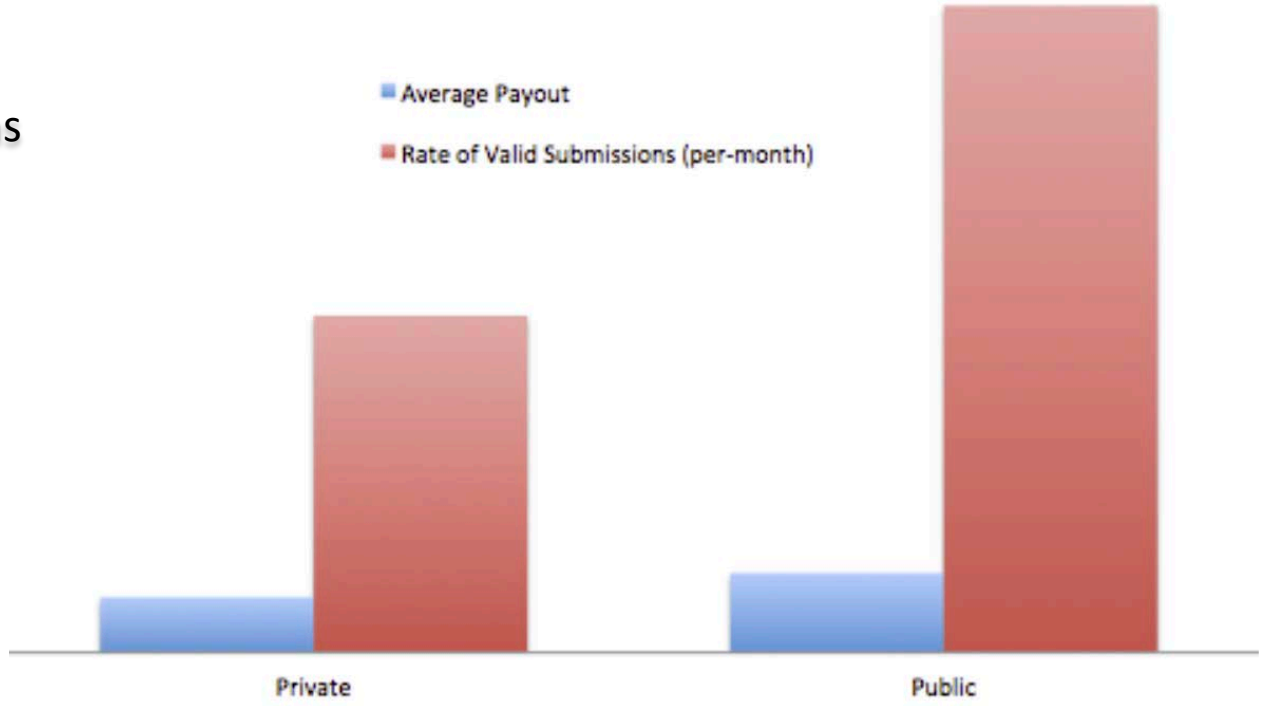
Type of Program

Value	Valid Submissions
Noise	✓
Activity	✓
Go with	Private Program



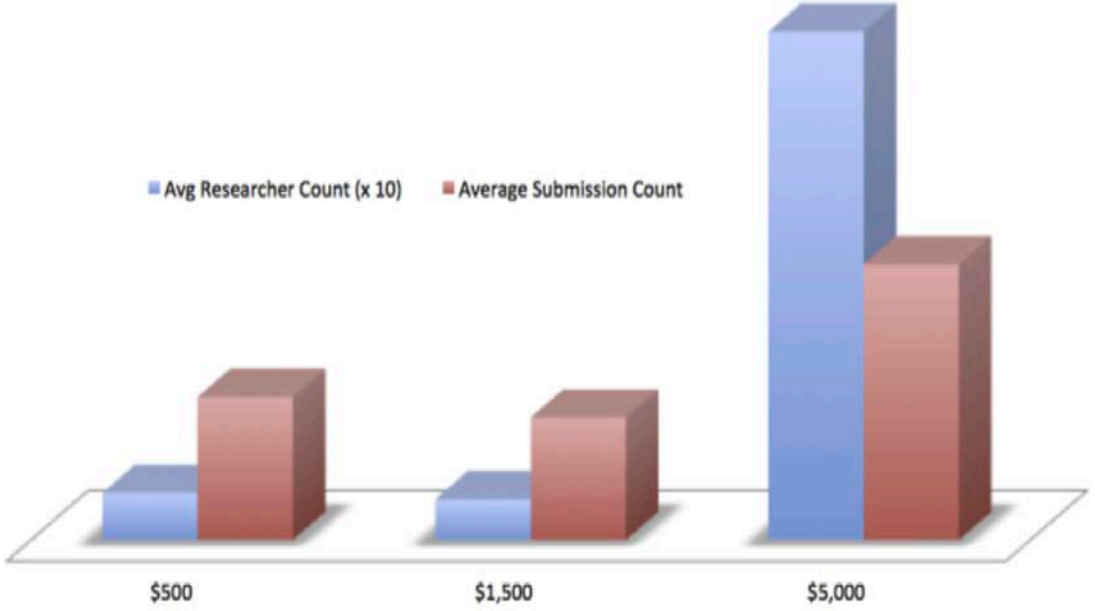
Type of Program

Value	Impactful Submissions
Noise	X
Activity	X
Go with	Public Program



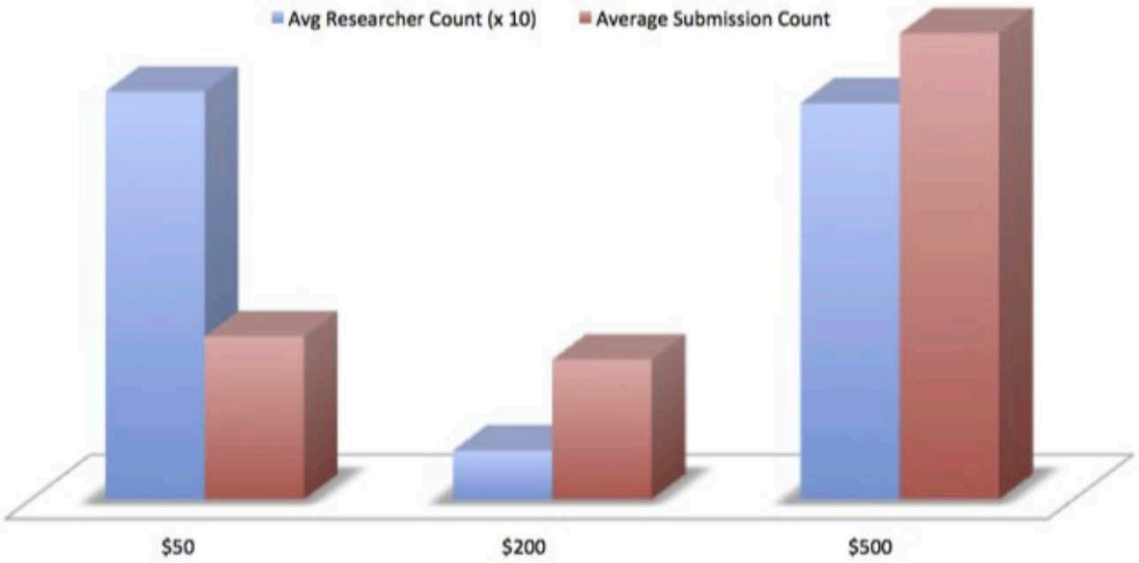
The Payout Range

Upper Bound	↑
Lower Bound	✗
Impact	Negligible



The Payout Range

Upper Bound	✗
Lower Bound	↑
Impact	Significant

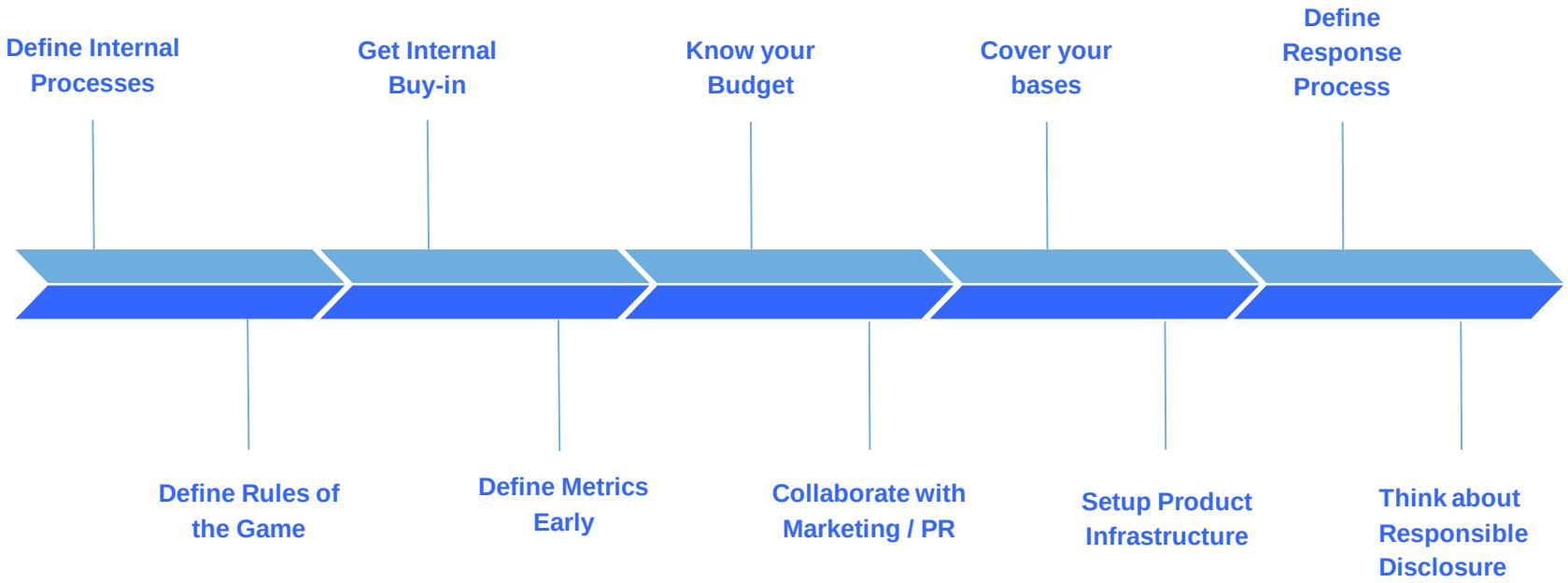


The Plan

"If you fail to plan, you are planning to fail"

- Benjamin Franklin

The 10 commandments

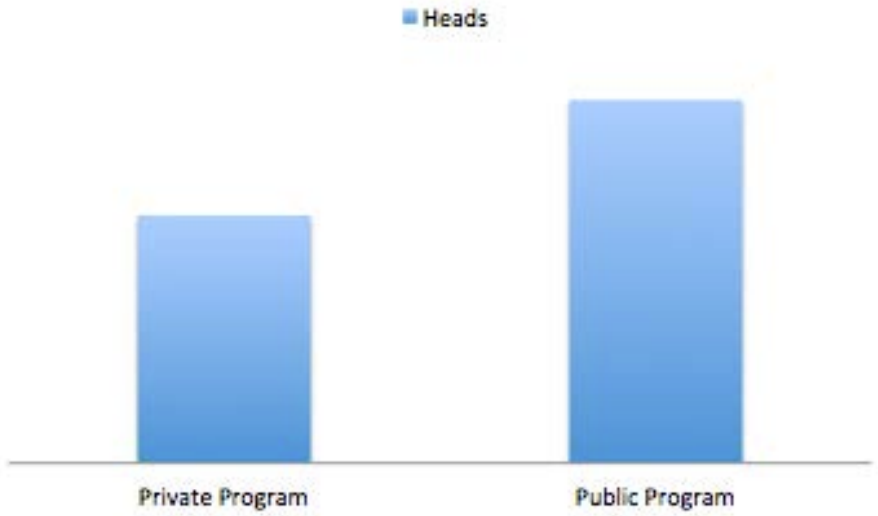


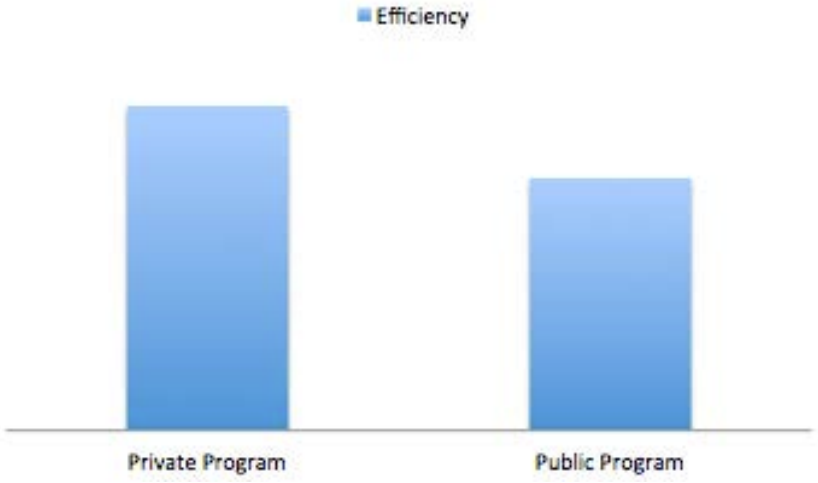
The Return on Investment

ROI = Depends on your Goals

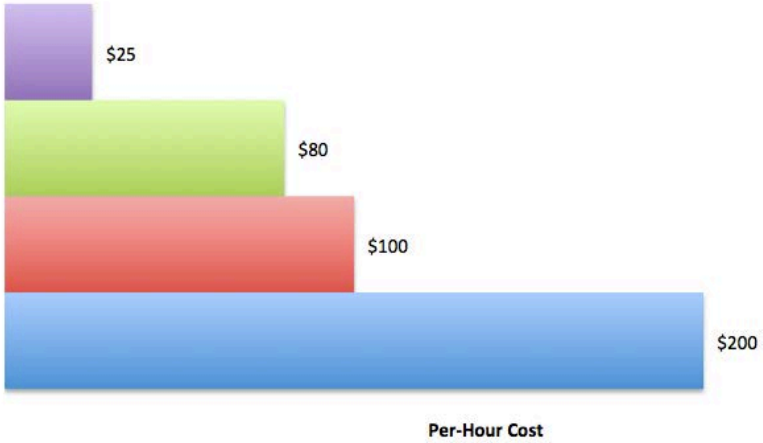
- Resource Augmentation
- Cost Savings

ROI – Resource Augmentation





ROI – Cost Savings



Bug Bounty	#Bugs	#Hunters	
In-House Resource	Quality		
Offshore Firm	Quality	Hours	Location
Local Firm	Quality	Hours	

Applying in your organization

1. First define the Goals of your Bug Bounty Program
2. Identify the Budget available for your Program
3. Identify the Type of Program and Payout Range to meet your Goals within your Budget
4. Follow the 10 Commandments and spend time in internal preparation before Launch
5. Define and Keep a track of your actual ROI from the Program