SESSION ID: TV-R11

BUILDING A BUG BOUNTY PROGRAM: FROM THE TRENCHES

Yogesh Badwe
Director of Security
Okta, Inc.
Planning Cycle

- Goals
- Metrics
- Strategies

The diagram shows the interconnection between Goals, Metrics, and Strategies.
The Why

Goals

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

The Why
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

X

Significant
The Plan

“If you fail to plan, you are planning to fail”

○ Benjamin Franklin
The 10 commandments

1. Define Internal Processes
2. Get Internal Buy-in
3. Know your Budget
4. Cover your bases
5. Define Response Process
6. Define Rules of the Game
7. Define Metrics Early
8. Collaborate with Marketing / PR
9. Setup Product Infrastructure
10. Think about Responsible Disclosure
The Return on Investment

ROI = Depends on your Goals

- Resource Augmentation
- Cost Savings
ROI – Resource Augmentation
ROI – Cost Savings

- Bug Bounty: $25
- In-House Resource: $80
- Offshore Firm: $100
- Local Firm: $200

#Bugs #Hunters
Quality
Hours
Location
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