
# Security Metrics That Count

Harini & Yash

# Introductions

**Harini**

- 6 years in infosec
- Manages Prodsec @ Twilio
- Based out of Denver

**Yash**

- ~8 years in infosec
- Interim Director of Security at Twilio
- Bay area resident

# Agenda

- Why metrics?
- What metrics?
- Manual way of metrics
- What was missing?
- Designing the new solution
- Implementation
- Did this work?
- Future State
- Q&A

# Why Metrics?

SECURITY POSTURE OF YOUR COMPANY

PROGRESS OVER TIME

CAPABILITIES

MATURITY OF YOUR SECURITY PROGRAM

ARGUE FOR RESOURCES

AND MORE….

# What Metrics

- Appsec:
  - Dependency Security
  - SAST / DAST
  - Container Scans
- Patch Management
  - Systems without the latest patches
  - Hosts not on the latest golden image

# What Metrics

- Cloud Security:
  - Users with old / unused CLI creds
  - Ips exposed to the internet
  - ALBs without WAF
- Enterprise Sec
  - Laptops without EDR agents
  - Laptops on older OS

# Some context…

- DevSecOps Tools
  - SAST, DAST , Container Scanning , Secrets scanning
  - Findings ticketed in Eng Team’s jira queue

- Manual Reviews
  - Threat Models are ticketed in our queue, with findings ticketed in Eng Team’s queue
  - Pentest “master ticket” in our queue, findings in team’s queues
  - Bug bounty reports in team’s queues

# Some context…

- TL;DR
  - Vulnerability tickets -> Eng team's JIRA queue
  - "Task ticket" -> Prodsec queue
- Twilio has BUs

# How We Were Doing Metrics

# What was missing

- Some level of automation
- Better visualization of trends
- Near real time data
- Customizability for different audiences
- RBAC
- Cool factor

# Unanswered Questions

- From the CSO
  - Do you have some scary data for me to use?
- From the E Team
  - What's the Security posture of the different BU’s ?
- From Eng. Managers
  - Where can I get vuln data from all the tools you have got?
- From Product Managers
  - Which vulns should I prioritize ?

# How do we change this?

# Requirements of a New Solution

- Metrics for Leadership
  - 10,000 view of how Twilio was doing from a security perspective
  - Ability to focus on which parts of Twilio are lagging behind

# Requirements of a New Solution

- Simple & Easy to consume
  - Open vulnerabilities that are out of SLA
  - Trends of vulnerabilities over time
  - Open Blocker & Critical (P0 & P1) vulnerabilities
  - Open vulnerabilities related to specific sources

# Requirements of a New Solution

- Integrates with the Engineering Workflow
    - Ability to embed the metrics dashboard as a component in wiki, gdocs etc
    - RBAC using existing systems

# Requirements of a New Solution

- Extensibility
  - Ability to combine data from multiple security teams
- Flexibility
  - Ability to create different metrics for different audience

# Requirements of a New Solution

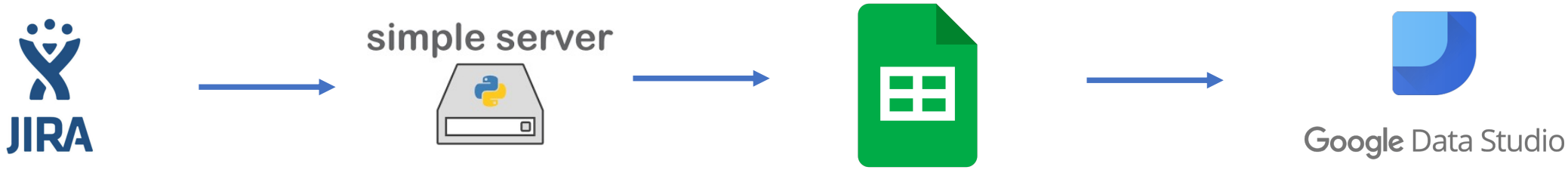
- No Overcomplications
- Easy maintainability

# Pre - Implementation

- Identify product ownership
- Ownership hierarchy to the E-Team
- Setting a baseline for vulnerability ticketing process
- Hydrating old data (to an extent…)
  - JQL-fu

# Implementation

- Issue tracking system has all the data
- Python based automation to collect data from issue tracking system
- Google Sheet as the Data Source
- Google Data Studio for the Dashboard



# Why we picked this stack?

Because python

Light weight and easy integration of Google sheet with GDS

GDS part of the gsuite package, feature rich

# Live Demo

# Live-ish Demo

1

# Security Vulnerability

Attach Create subtask Link issue

**Description**

Security Vulnerability

**Environment**

None

**Activity**

Show: All Comments History Work log Newest first

HR Add a comment...

**Pro tip:** press M to comment

To Do

**Pinned fields**

Click on the ☆ next to a field label to start pinning.

**Details**

| | |
|---|---|
| Assignee | Unassigned |
| Reporter | HR Harini Rangarajan |
| Labels | None |
| Priority | = Medium |

**More fields** Original estimate, Time tracking, Epic Link, Components, Fix versions, Aff...

Created 54 minutes ago
Updated 54 minutes ago

Configure

# Did This Work?

- Wins:
  - Execs liked it
  - We customize dashboards for different audiences
  - Few Engineering Teams asked access to the raw data and built better dashboards for their retro's (which we totally did not steal)
  - Product Managers loved it
  - We saw the needle move

# Did This Work?

- Minor setbacks:
  - Google Data Studio sometimes broke
  - Needs a manual refresh every time data syncs within a 15min window
  - Google being google

# Future State

Integrate other data into the metrics

Generate a Risk score card

Individually customized dashboards for teams

# Resources

## Slides

- https://yashvier.box.com/v/security-metrics-ppt

## Sample Google Data Studio Link

- https://yashvier.box.com/v/security-metrics-gds

## Sample Data Source

- https://yashvier.box.com/v/infosec-metrics-sampledata

# Questions?