RSAConference2020

San Francisco | February 24 – 28 | Moscone Center

HUMAN ELEMENT

SESSION ID: **RMG-F02**

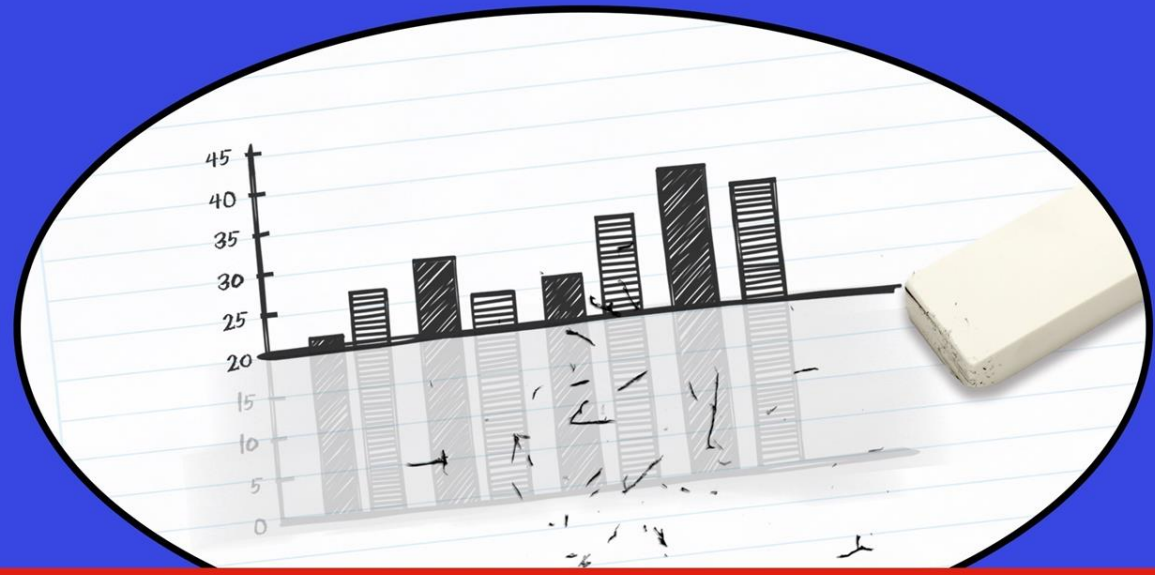
# Beating Security Inertia with Actionable KPIs

**Harshil Parikh**

Security at Medallia, Inc

# HOW TO LIE WITH STATISTICS

Darrell Huff



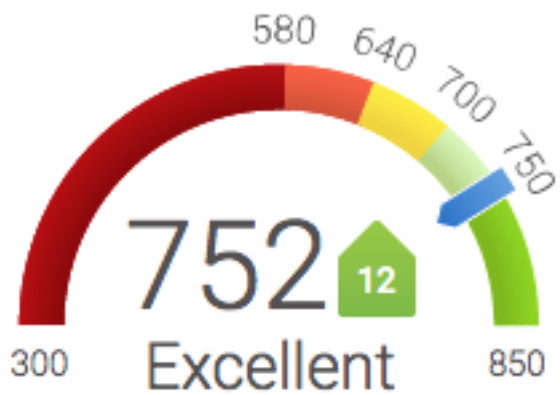

audiobooks.com PUBLISHING

Unabridged - Read by Bryan DePuy


Apple Watch Image from www.verizonwireless.com

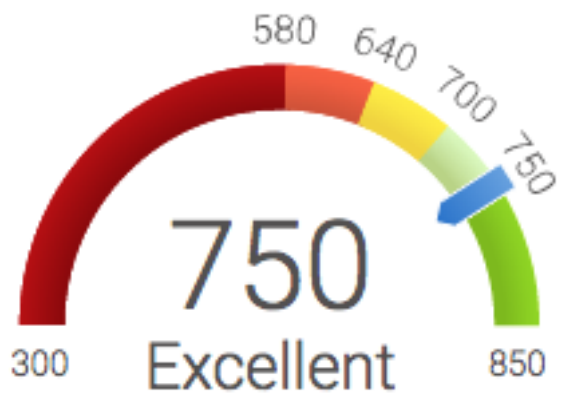
## Your Credit Scores

Provided by TransUnion




Updated Oct 19, 2016
Next Update in 7 days

Provided by EQUIFAX




Updated Oct 19, 2016
Next Update in 7 days

https://medium.com/@adennis4/how-to-improve-your-credit-score-ed441fec89c6

RSAConference2020

***Most great revolutions in science are preceded by revolutions in measurement***

- Prof. Erik Brynjolfsson, MIT

# Agenda

- What are KPIs
- Identifying relevant KPIs
- 3 Categories of KPIs
- Plumbing
- Wrap Up

# Metrics & KPIs

**Metric:** A measurement of performance of any activity

**KPI:** A metric that measures a *key business goal* against a target

If the activity being measured *does not* align with business goals, then it is not a KPI, it is simply a metric.

# Relation to Goals

**Goal**

*Strengthen the human element of security*

**Objective**

*100% completion of employee security awareness training*

# Relation to Goals

**Goal**

*Strengthen the human element of security*

**Objective**

*100% completion of employee security awareness training*

KPI

RSAConference2020

# Identifying KPIs

RSAConference2020

***A problem well stated, is a problem half solved***

- Charles Kettering

# KPI Framework

- My goal is to _____ *<business goal>*
- I will measure _____ *<KPI>*
- My audience is _____ *<target audience>*
- I will communicate every _____ *<frequency>*
- I expect the audience to _____ *<expected action>*

# KPI Example #1 - Laptop Hardening

- My goal is to *minimize risk from user endpoint compromise*
- I will measure *patch latency*
- My audience is *CIO*
- I will communicate every *month*
- I expect the audience to *drive patch latency to under 2 weeks*

# KPI Example #1 - Laptop Hardening KPI

Laptop Patch Latency

94

Days

2020 Target: 30 Days

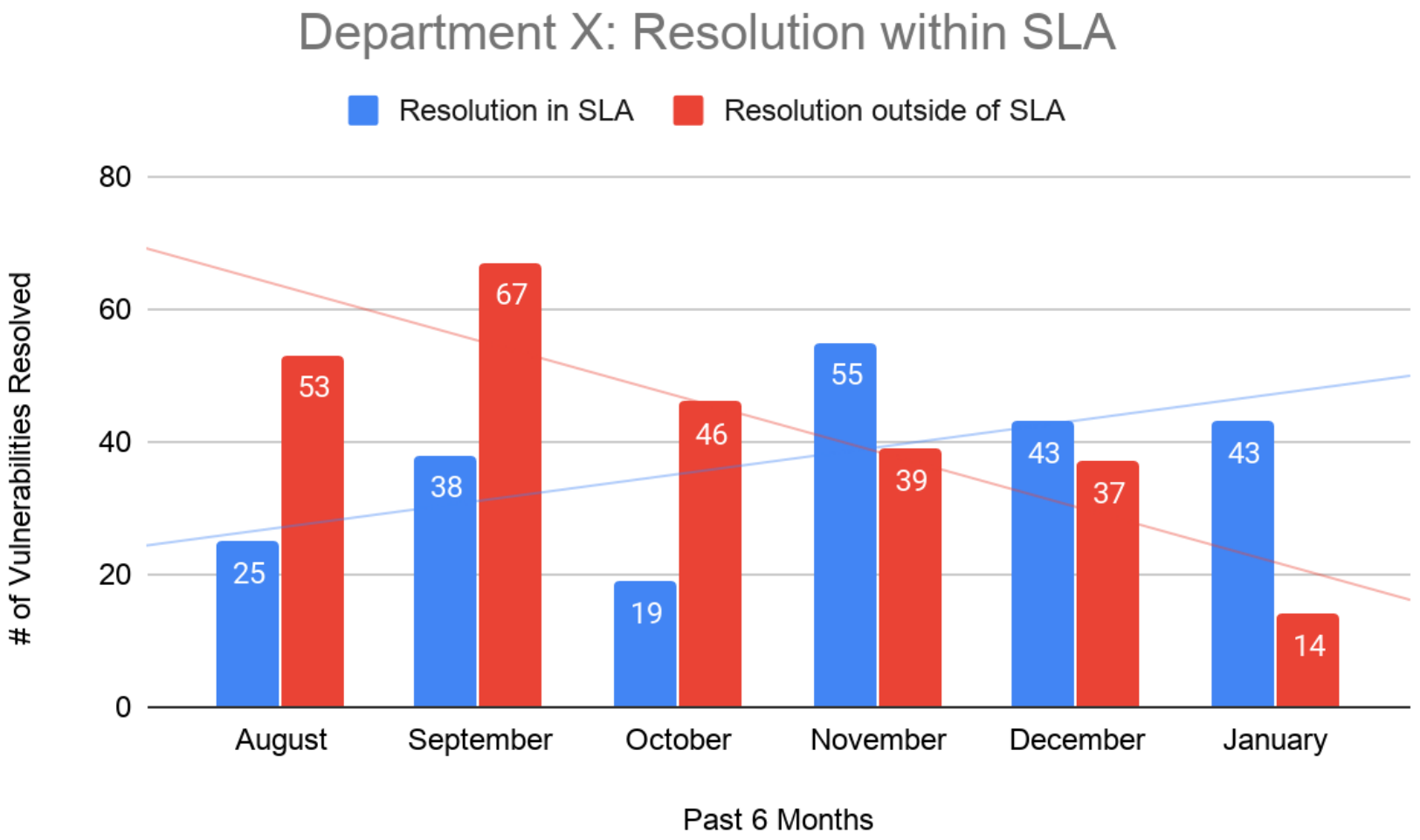
| Laptop Patch Latency by OS | |
|---|---|
| Windows | 44 Days |
| MacOS | 144 Days |

| Department | Patch Latency |
|---|---|
| Corporate IT | 5 Days |
| Engineering | 25 Days |
| Sales | 180 Days |
| Human Resources | 50 Days |
| Finance | 190 Days |

# KPI Example #2 - Vulnerability Management

- My goal is to *ensure vulnerabilities are resolved on time*
- I will measure *Vulnerability SLA Compliance*
- My audience is *Department Leader*
- I will communicate every *month*
- I expect the audience to *resolve vulnerabilities regularly*

# KPI Example #2 - Vulnerability Management

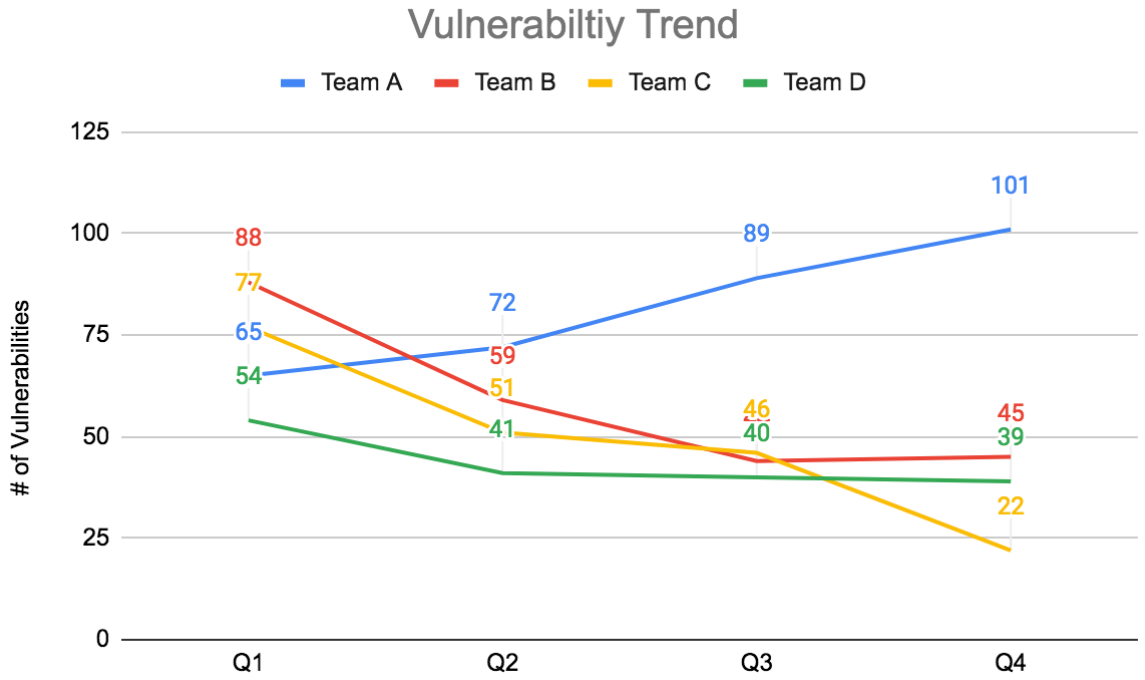


# KPI Example #3 - Shift Left

- My goal is to *detect vulnerabilities prior to production*
- I will measure *security testing coverage in CI pipelines*
- My audience is *CTO*
- I will communicate every *month*
- I expect the audience to *integrate scanners in all CI pipelines*

# KPI Example #3 - Shift Left

| Scanning Coverage in Jenkins Pipelines | | | |
|---|---|---|---|
| | Static Analysis | Open Source Components | Container Security |
| Team A | 0% | 50% | 25% |
| Team B | 25% | 100% | 100% |
| Team C | 80% | 100% | 100% |
| Team D | 50% | 50% | 100% |



RSAConference2020

# 3 Categories of KPIs

# Categories of KPIs

## Organization

Company wide / security program level KPIs

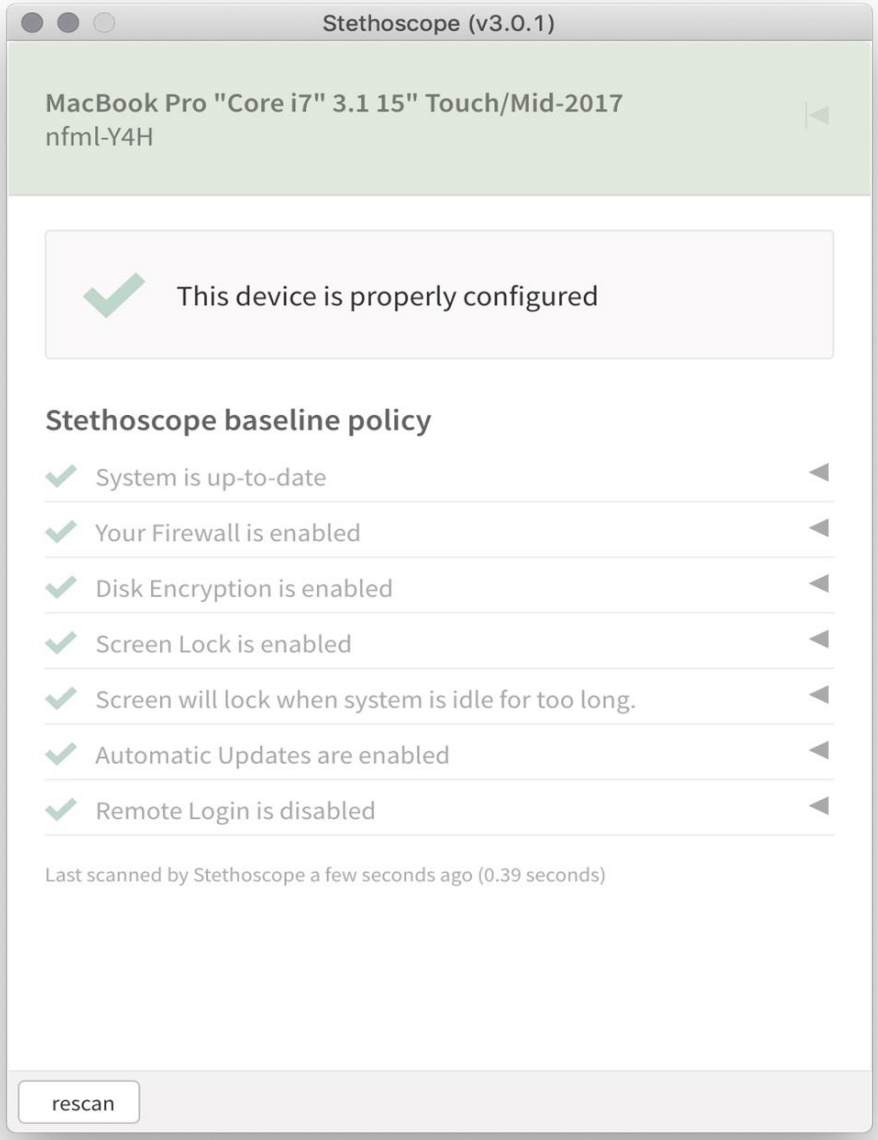
## Team

KPIs for each team / department

## Individual

Specific to an individual

# Individual KPIs - Drive Behavior Change




- Must be actionable
- Easy to complete
- Set against a goal
- Should evoke an emotion - Achievement, Altruism, Social Standing, Competition etc

# Individual KPIs - Examples

- Phishing & Training
  - Phishing test failure rate
  - Training completion status
- Secure Behavior
  - # of malicious sites visited
  - # of DLP alerts triggered
  - # of passwords shared in clear text
- Endpoint Security
  - # of Vulnerable applications installed
  - Configuration compliance status
  - OS Patch Status
- Secure Coding
  - # of vulnerabilities in pull requests

# Individual KPIs - Examples

- Phishing & Training
  - Phishing test failure rate
  - Training completion status
- Secure Behavior
  - # of malicious sites visited
  - # of DLP alerts triggered
  - # of passwords shared in clear text
- Endpoint Security
  - # of Vulnerable applications installed
  - Configuration compliance status
  - OS Patch Status
- Secure Coding
  - # of vulnerabilities in pull requests

# Team KPIs - Prioritize Security

KPIs for security responsibilities of a team / department

- Align with strategic objectives
- Set goals (e.g. quarterly)
  - Top down driven targets
  - Gamification for bottoms up growth
- Communicate frequently & positively
- Leading & lagging indicators

# Team KPIs - Example KPI

**Strategic Objective**: Resolve at least 80% of vulnerabilities within SLA

**KPI:** % of vulnerabilities resolved within SLA

# of vulnerabilities due in next 2 weeks

Supporting Metric

% of vulnerabilities 'Not Started'

Supporting Metric

Additional Supporting Metrics

- # of unresolved overdue vulnerabilities
- vulnerability backlog trend
- % of time budgeted for security work
- % of team members with security training

# Organizational KPIs - Measure Performance

Measure company wide risk management goals

- Aid in decision making and planning
- Customize for your leadership team
- Simple to understand, not dumbed down

# Organizational KPIs - Examples

### Security Baseline Coverage

- % of endpoints meeting config baseline (e.g CIS)
- % of endpoints under active defense (e.g. EDR)

Bonus: Group by Endpoint Type / OS / Team / Geo

### Patch Latency

- % of laptops with critical patches missing
- % of endpoints with patch latency > 90d

Bonus: Group by OS / Missing Patch / Team / Geo

### Vulnerability Management

- Created vs Resolved
- % of Vulnerabilities Resolved In SLA

Bonus: Analyze by Team / Product / Asset Category

### Detection & Response

- Mean Time To Detect
- Mean Time To Respond

Bonus: Analyze by Severity / Asset Class / Environment

# Organizational KPIs - Examples

Security Baseline Coverage

- % of endpoints meeting config baseline (e.g CIS)
- % of endpoints under active defense (e.g. EDR)

Bonus: Group by Endpoint Type / OS / Team / Geo

Patch Latency

- % of laptops with critical patches missing
- % of endpoints with patch latency > 90d

Bonus: Group by OS / Missing Patch / Team / Geo

Vulnerability Management

- Created vs Resolved
- % of Vulnerabilities Resolved In SLA

Bonus: Analyze by Team / Product / Asset Category

Detection & Response

- Mean Time To Detect
- Mean Time To Respond

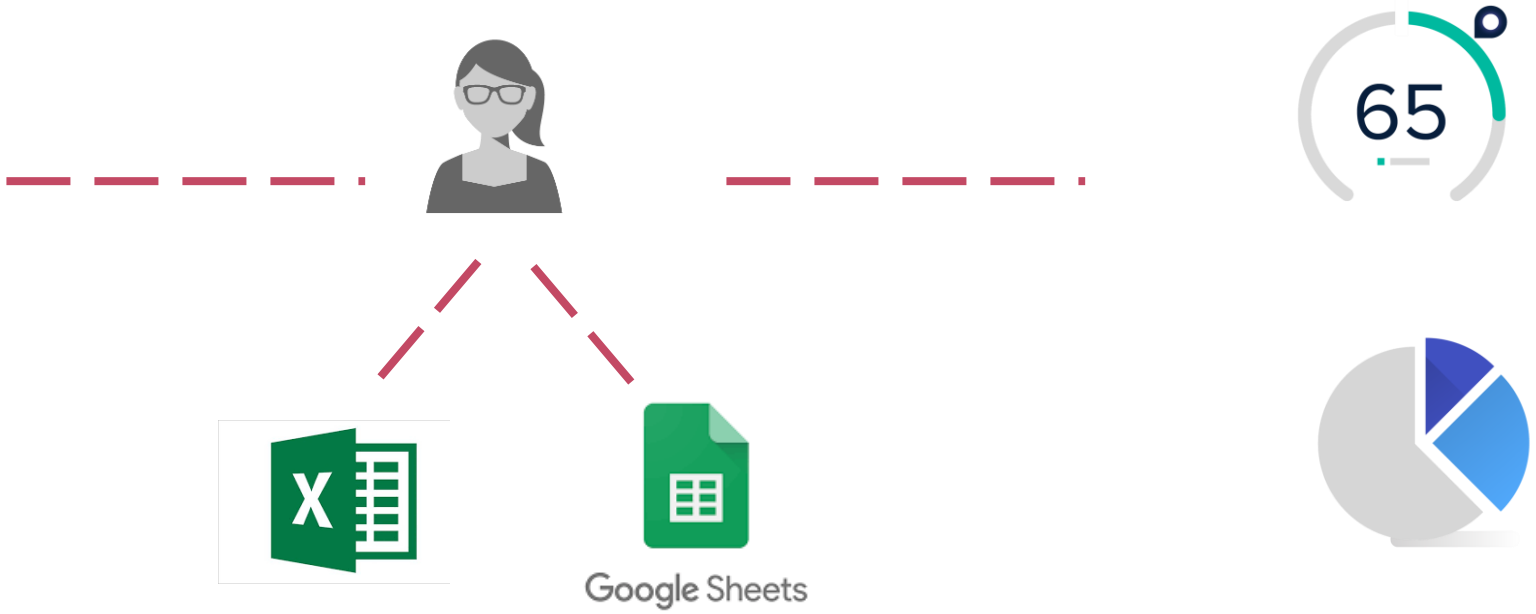
Bonus: Analyze by Severity / Asset Class / Environment

RSAConference2020

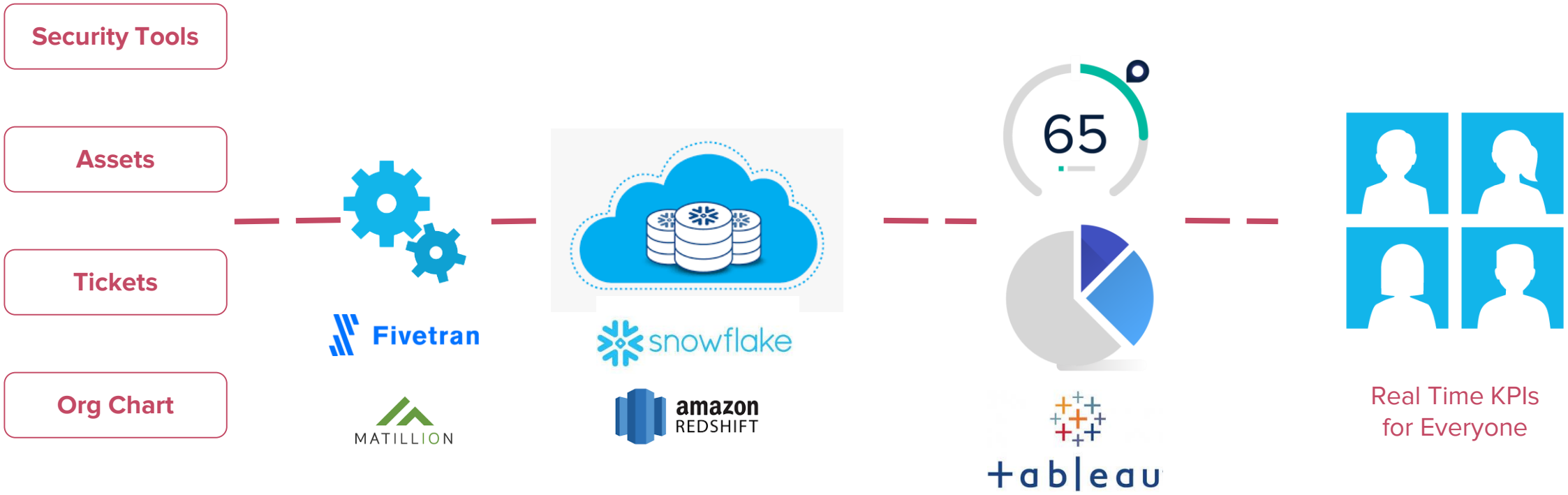
# Generating KPIs

# The Plumbing

- Vulnerabilities
- Assets
- Tickets
- Org Chart



# The Plumbing - Future



RSAConference2020

***Build a little, test a little, learn a lot***

- Rear Adm. Wayne E. Meyer

# “Apply” Slide

- Start with your goals
- Identify KPIs that align with goals
- Security KPIs should be ‘owned’ by everyone (not just security team)
- Start manually, get feedback, automate later

RSAConference2020

# Questions

https://www.linkedin.com/in/harshil/