

# RSA® Conference 2019

San Francisco | March 4–8 | Moscone Center

The background of the slide features a complex network of thin, curved lines in shades of blue, yellow, and orange, radiating from the top right corner towards the bottom left, creating a sense of connectivity and data flow.

# BETTER.

SESSION ID: GRC-T07

## The Metrics Manifesto

**Richard Seiersen**

President  
M-Cubed  
@RichardSeiersen

#RSAC

# The Metrics

## Manifesto

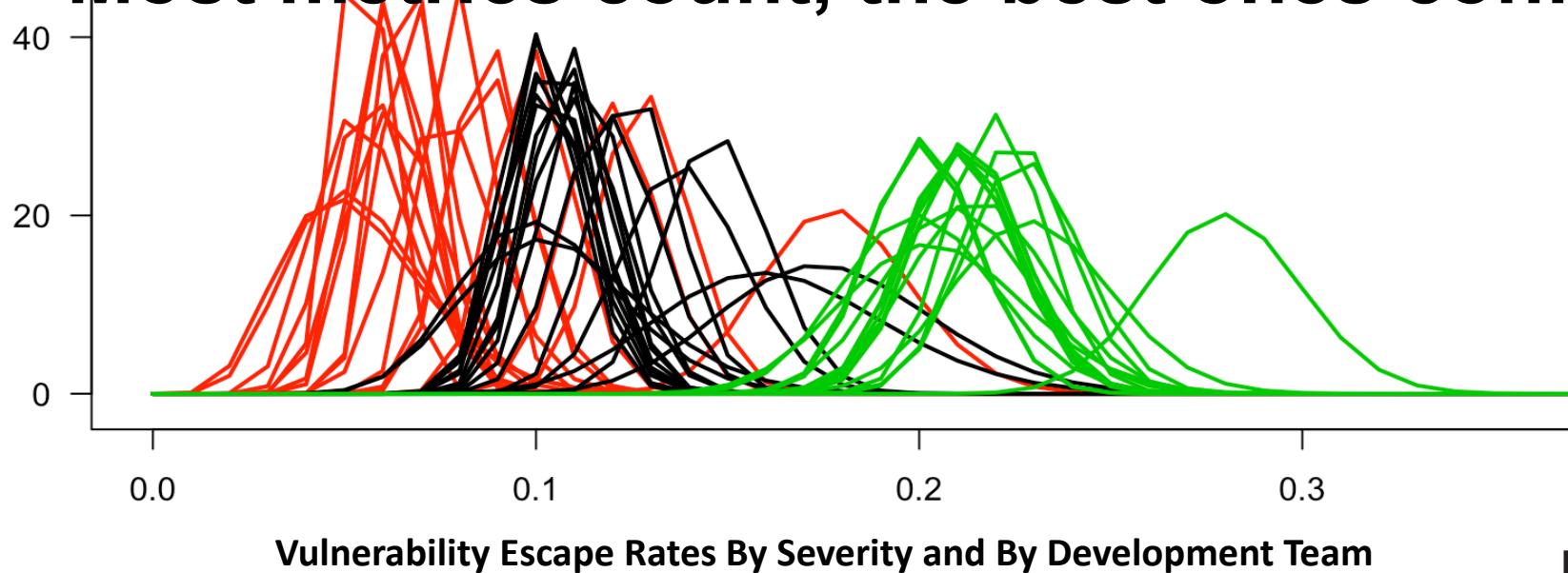
“I don’t believe in astrology;  
I’m a Sagittarius and we’re skeptical.”  
*Confronting Security With Data*  
— Arthur C. Clarke

By Richard Seiersen

# The Metrics Manifesto

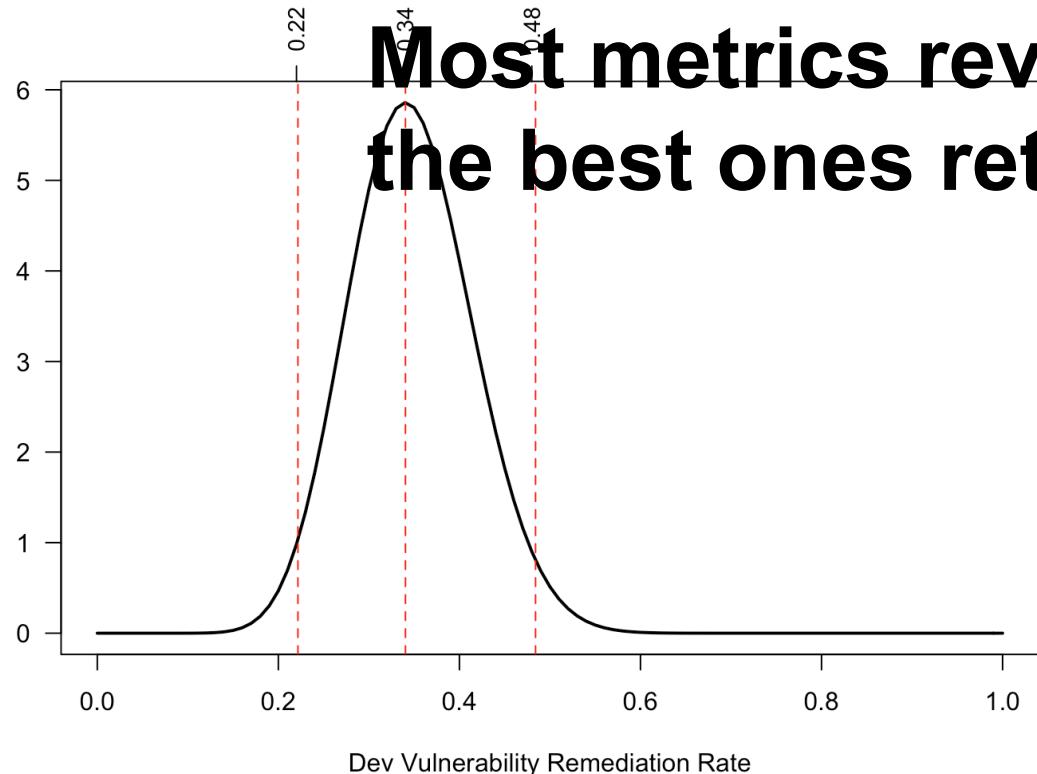
- 1. We believe shrinking attack surface, while not slowing value exposure, is the new job #1 for security*
- 2. We also believe not doing this gives advantage to our adversaries and reduces business opportunity*

**Most metrics count, the best ones confront**

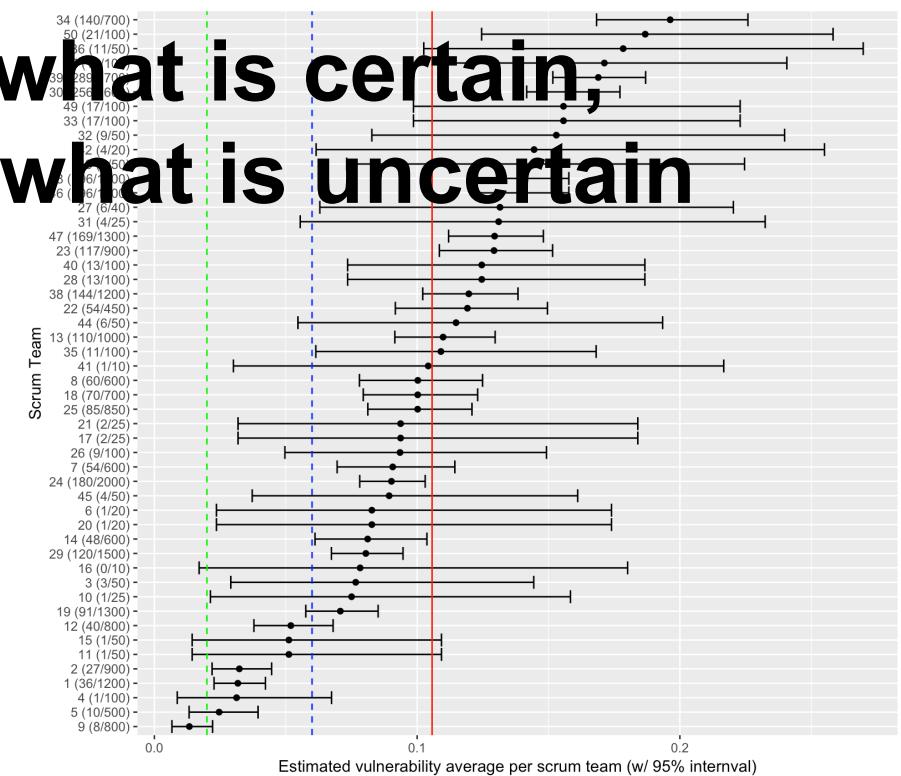


# The Metrics Manifesto

3. *We believe metrics that ignore our uncertainty ignore our adversaries*

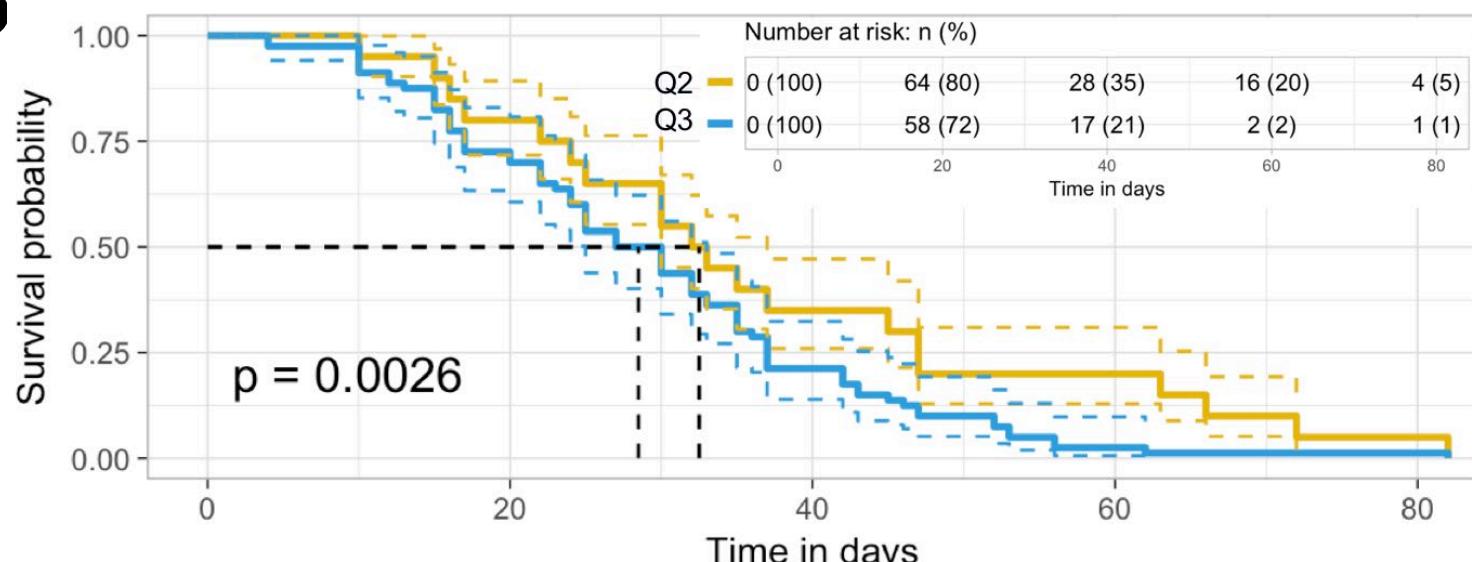


**Most metrics reveal what is certain,  
the best ones retain what is uncertain**



# The Metrics Manifesto

3. *We don't believe in benchmarks (for the most part) and neither do our adversaries*
4. *We believe in continuous improvement because our adversaries do, too. We expose, continuously, best of benchmarks in the competition model*

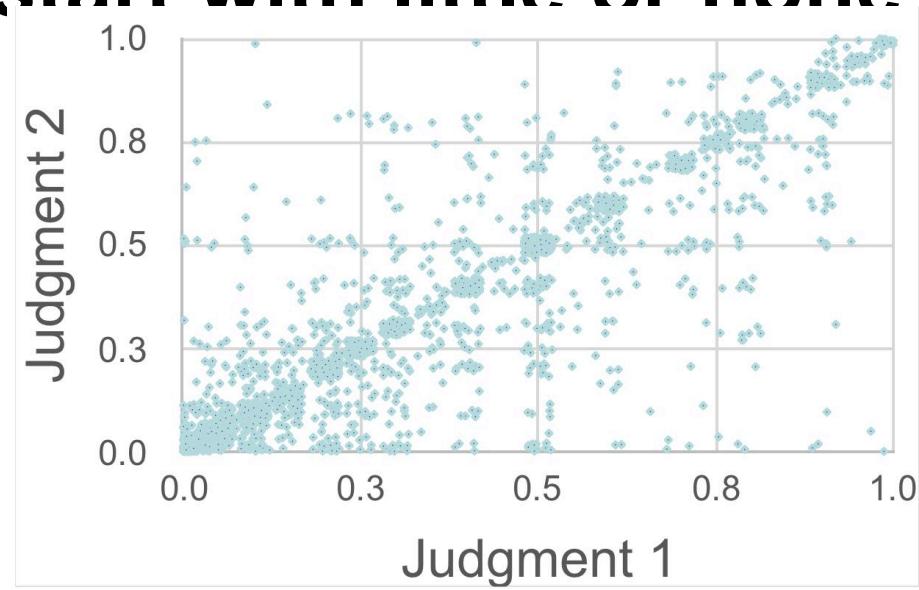
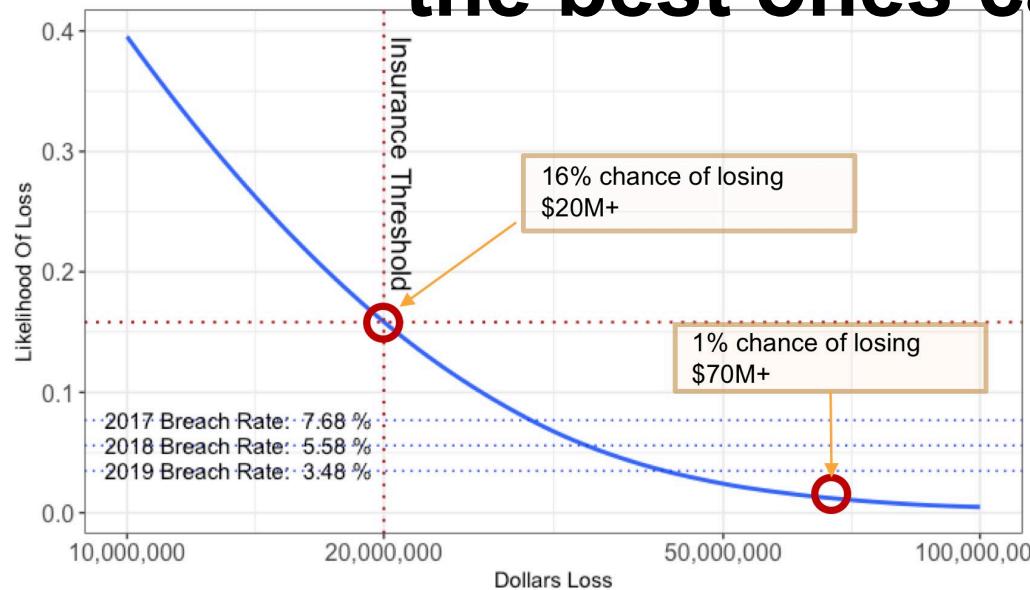


# The Metrics Manifesto

5. *We believe resourcefulness with small data is always better than complexity with big data*

**Most metrics require data.**

6. *We also believe expertise can be turned into data when you have none – data that is the best ones can start with little or none*



RSA® Conference 2019

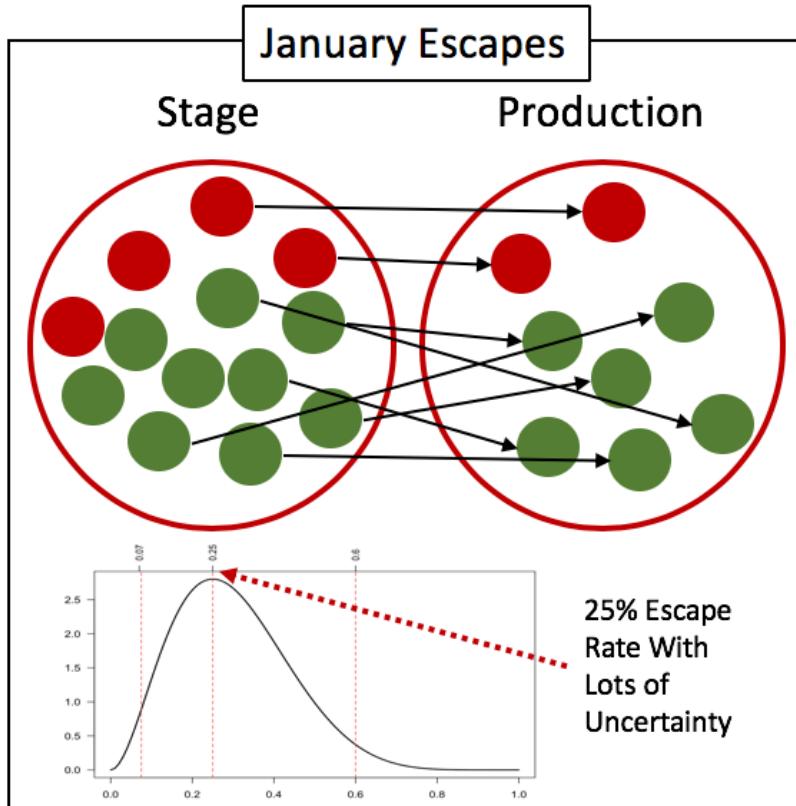
# The Metrics Manifesto In Action

## Measuring & Controlling Attack Surface with Escape Rates

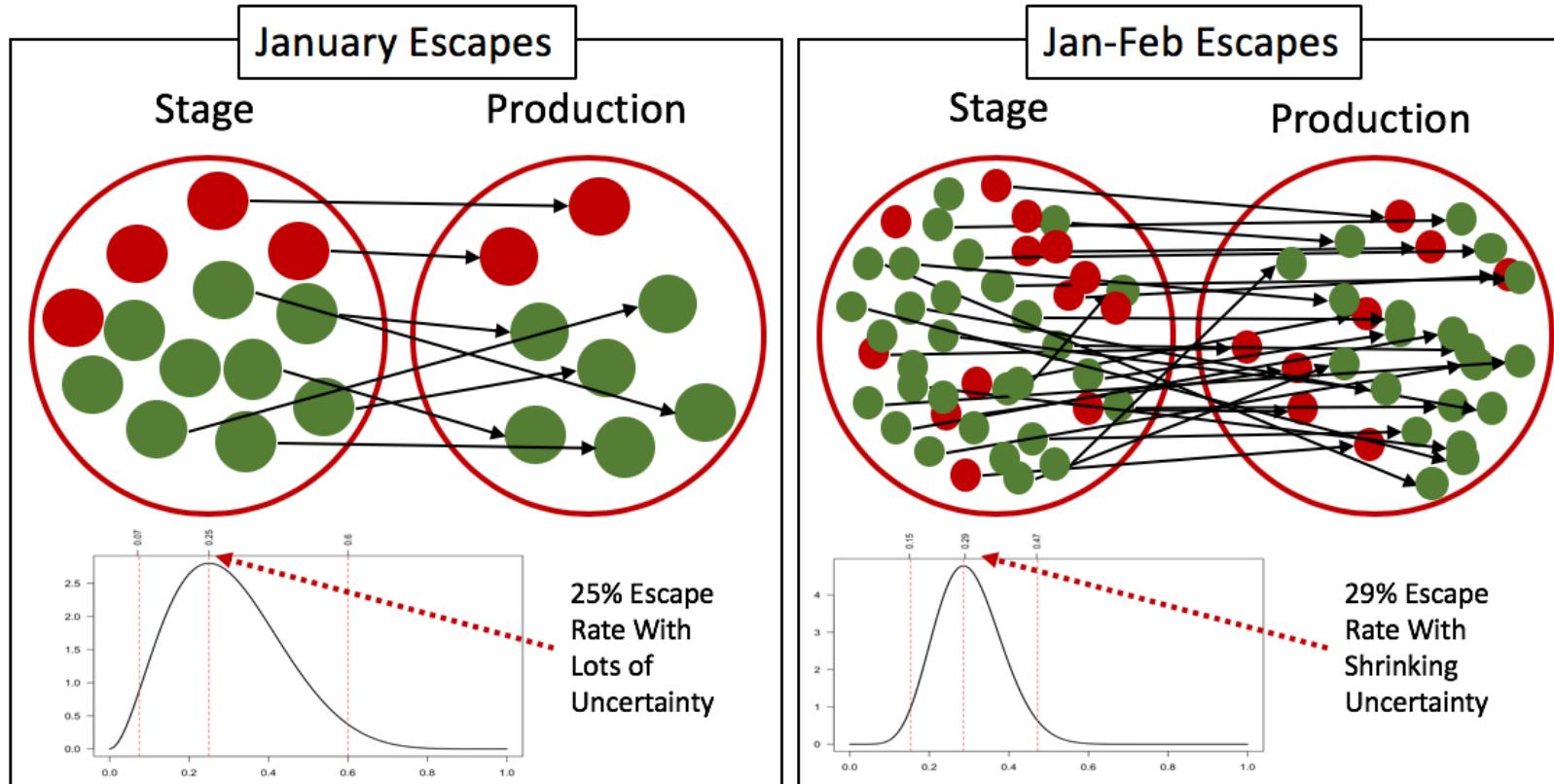
# The Manifesto In Action: Escape Rates



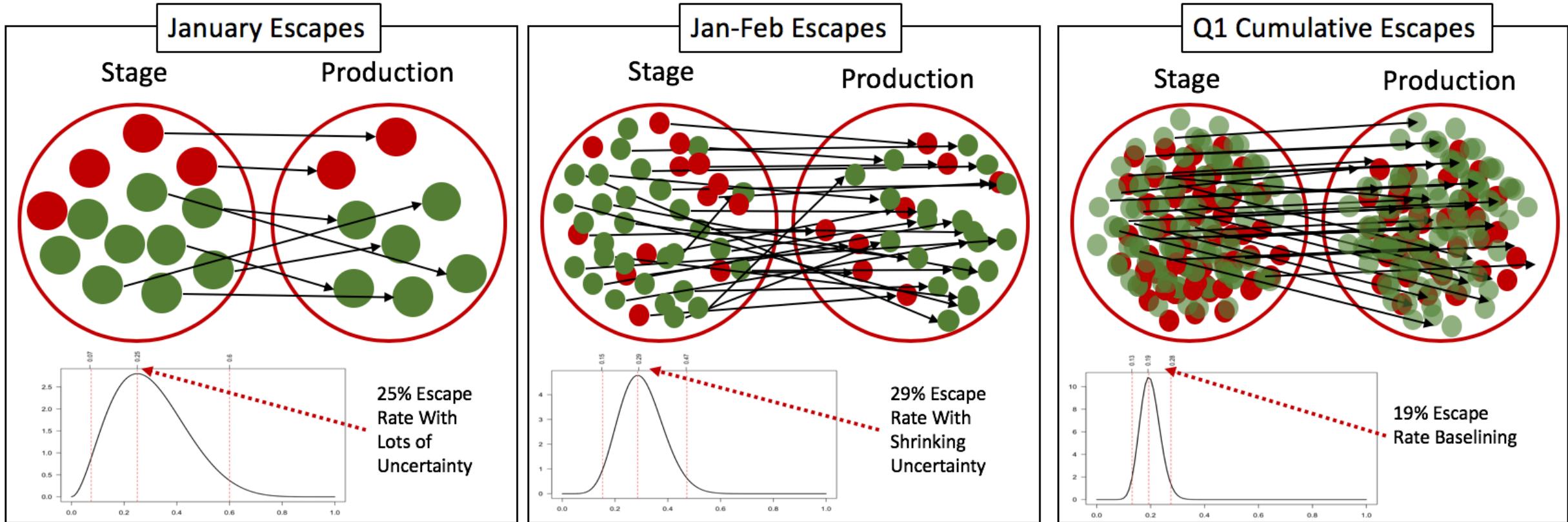
# The Manifesto In Action: Escape Rates



# The Manifesto In Action: Escape Rates



# The Manifesto In Action: Escape Rates



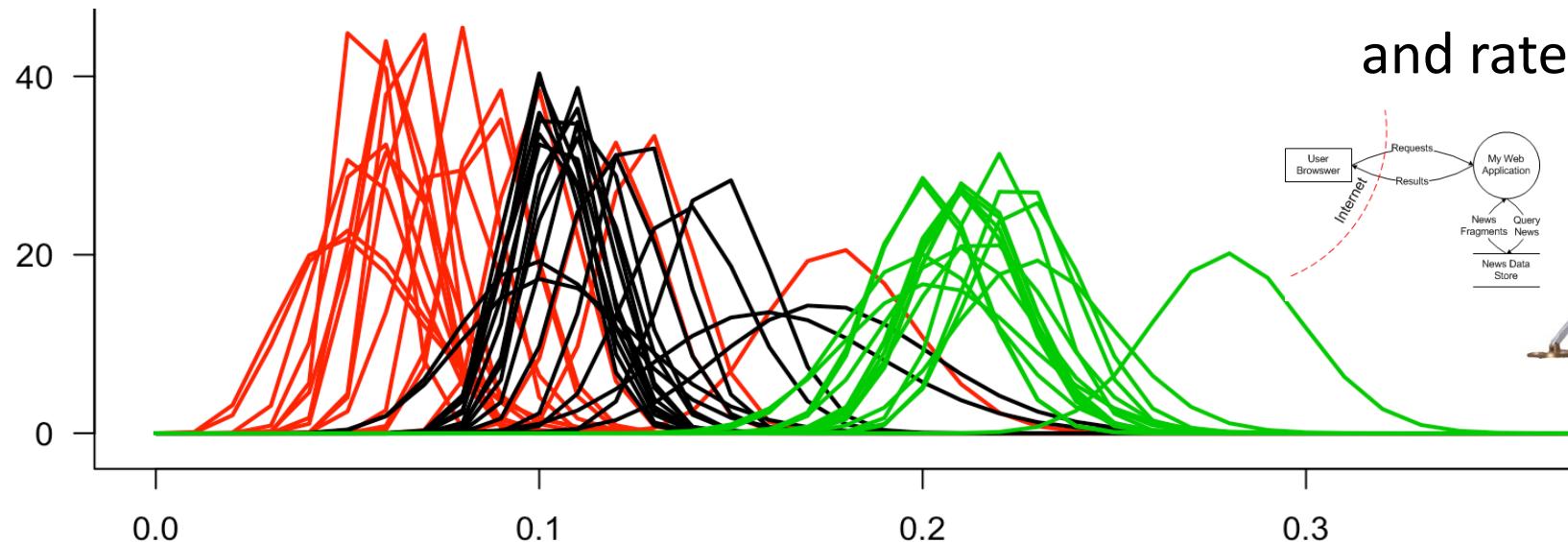
# The Manifesto In Action: Escape Rates



```
#p0 Vulns
extreme.totals <- test.p0 %>% filter(new.expected >= .05)
MakeCurves(extreme.totals, nrow(extreme.totals), 2)
```

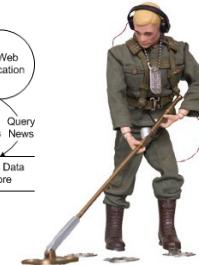
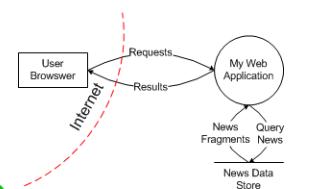
```
#p1 Vulns
extreme.totals <- test.p1 %>% filter(new.expected >= .10)
MakeCurves(extreme.totals, nrow(extreme.totals), 1)
```

```
#p2 Vulns
extreme.totals <- test.p2 %>% filter(new.expected >= .20)
MakeCurves(extreme.totals, nrow(extreme.totals), 3)
```

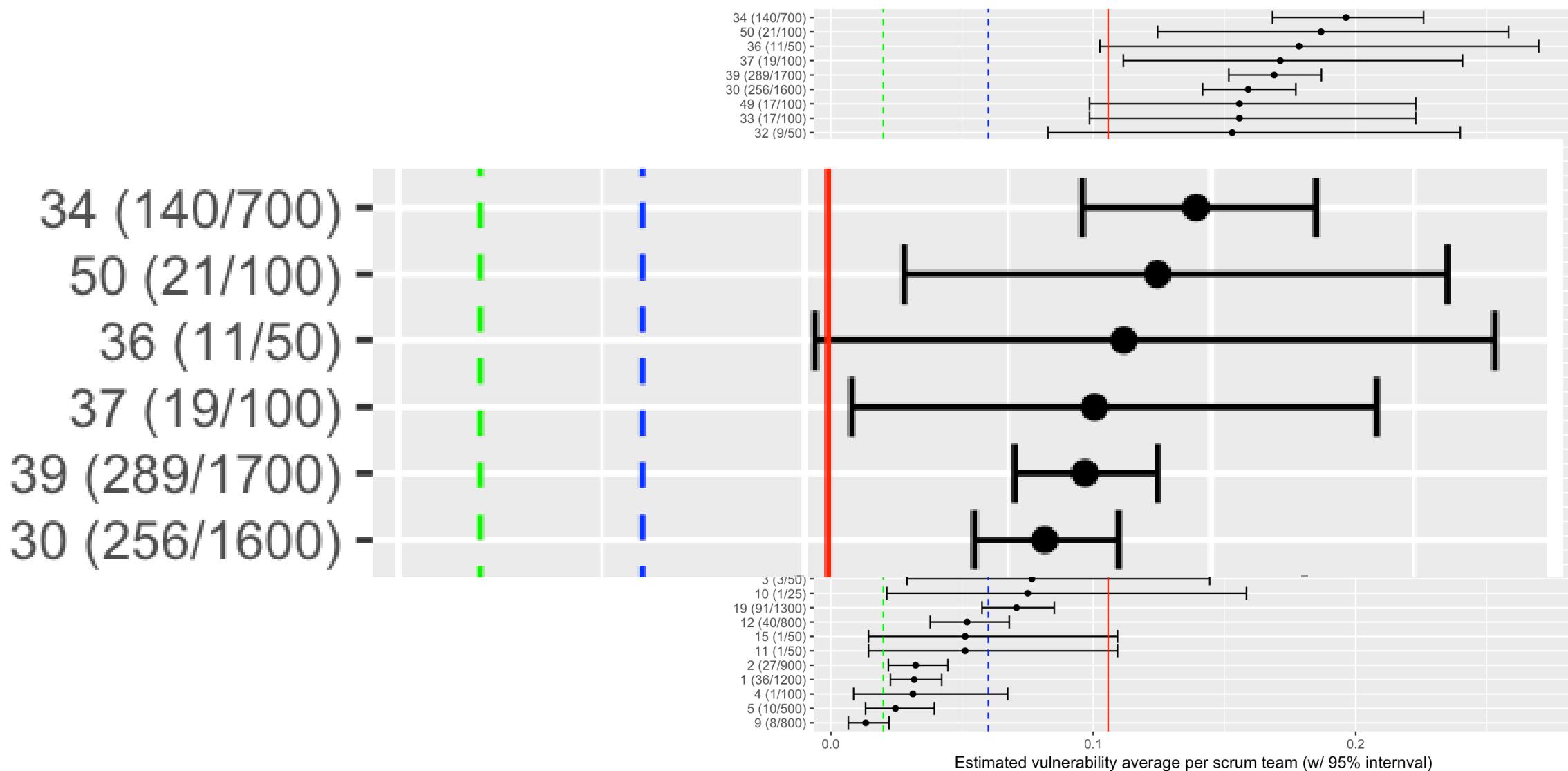


## Observations:

- Escape Rate is a DevOps Metric.
- We use rate as a policy to beat
- We can score the strength of relationships between capabilities and rates.



# The Manifesto In Action: Escape Rates

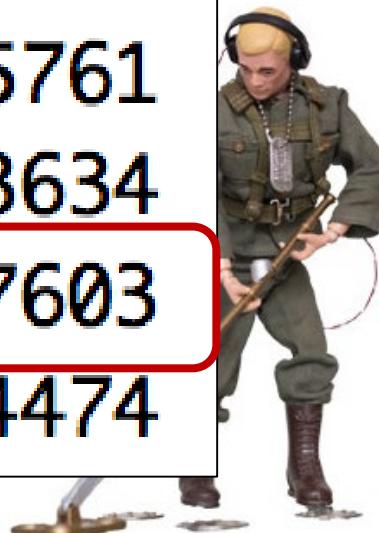


# The Manifesto In Action: Advanced Rates

	(Intercept)	Remediate_SLABasic	Remediate_SLAContinuous	Remediate_SLAScheduled	DynamicBasic	DynamicContinuous	DynamicScheduled
Prod1	0.1153572						
Prod2	0.1113740						
Prod3	0.1304745						
Prod4	0.1446950						
Prod5	0.1276098						
Prod6	0.1264116						
Prod7	0.1168139						



	Estimate
(Intercept)	0.124677
Remediate_SLABasic	-0.023030
Remediate_SLAContinuous	-0.017095
Remediate_SLAScheduled	-0.025761
DynamicBasic	-0.033634
DynamicContinuous	-0.087603
DynamicScheduled	-0.044474



**RSA®**Conference2019

# The Metrics Manifesto In Action

## Using Small Data and SME Input To Measure Risk

# The Metric Manifesto: Incorporating Frameworks

## PROTECT

**Zero Trust:** Progressively fined grained access controls applied to increasingly fine grained assets – from platforms to data.

**Minimal Attack Surface:** Shrinking risk via the Security Development Lifecycle (SDL), vulnerability & configuration management.

**Complete Mitigation:** Capabilities that dynamically block malicious activity.

## DETECT

**Complete Visibility:** Comprehensive telemetry at wire speed with high availability and increasingly longer history.

**Alerting In Depth:** Deterministic, heuristic, behavioral and predictive analytics at depth and in breadth that reduce time to detect.

**Comprehensive Orchestration:** Integrated alerting, workflow and decision analysis that supports response automation.

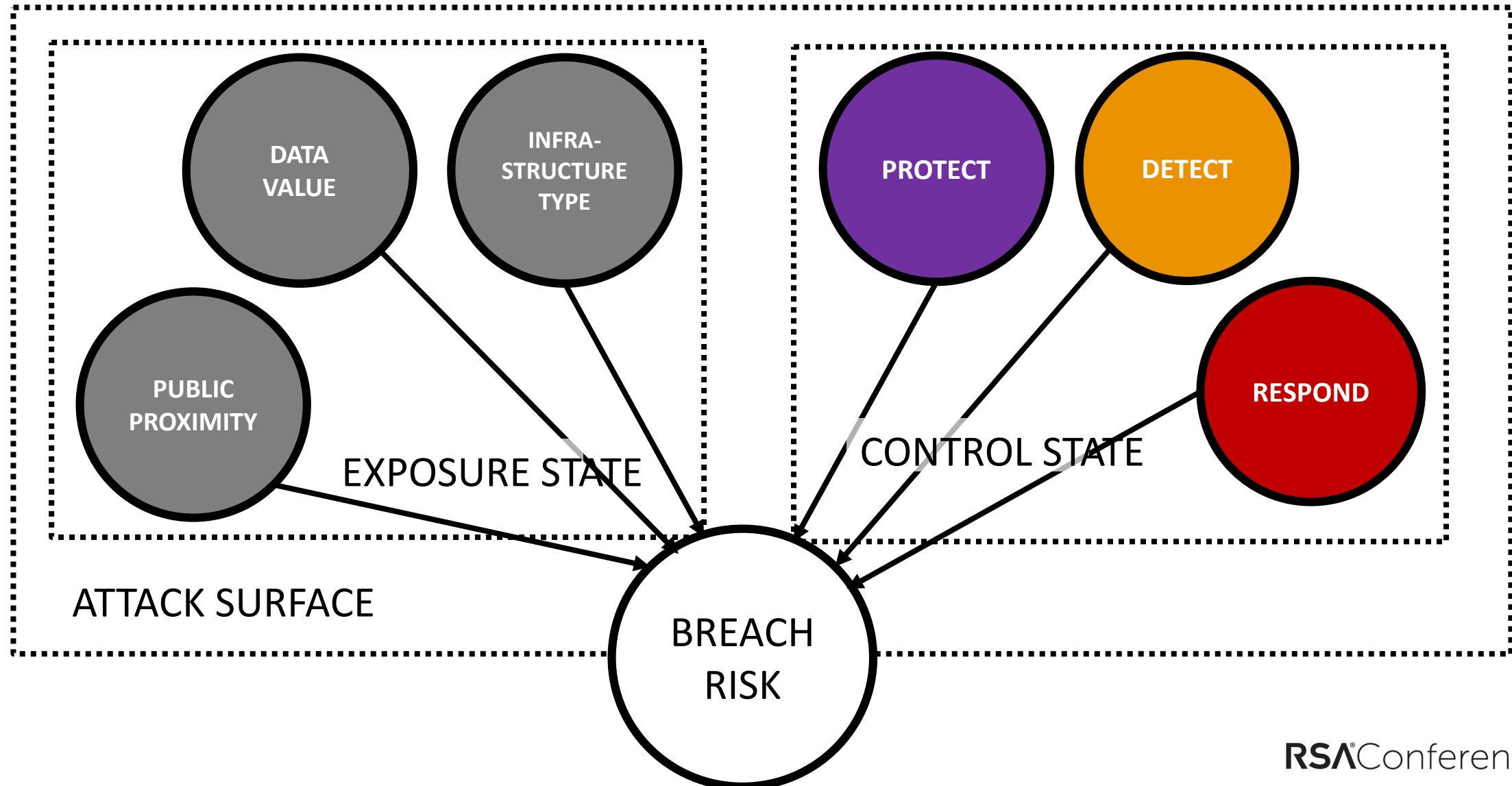
## RESPOND

**Response Assurance:** Logical, physical, structured and unstructured exercises to provide ongoing response/recovery assurance.

**Response Engineering:** Security engineering for pursuing, handling and recovering from incidents.

**Communications :** Communications coordinated across the org, board, third parties, social and general media.

# The Metric Manifesto: Incorporating Frameworks



# The Metric Manifesto: Incorporating Frameworks

Exposure	Data_Value	Infrastructure_Location	Protect	Detect	Respond
Public	Yes	On Prem	Adhoc	Adhoc	Adhoc
Public	No	Cloud Provider	Adhoc	Adhoc	Adhoc
Public	Yes	Data Center Provider	Scheduled	Nothing	Adhoc
Public	Yes	Cloud Provider	Scheduled	Adhoc	Adhoc
Public	No	Data Center Provider	Nothing	Adhoc	Continuous
Private	Yes	Cloud Provider	Nothing	Adhoc	Adhoc
Public	Yes	Cloud Provider	Continuous	Adhoc	Adhoc
Public	Yes	Data Center Provider	Adhoc	Nothing	Scheduled
Public	Yes	Cloud Provider	Nothing	Scheduled	Continuous

**200 Samples Out Of 750+ Possible Variations**

# The Metric Manifesto: Incorporating Frameworks

Exposure	Data_Value	Infrastructure_Location	Protect	Detect	Respond	FNAME Average	FNAME Boundary
Public	Yes	On Prem	Adhoc	Adhoc	Adhoc	0.10	0.20
Public	No	Cloud Provider	Adhoc	Adhoc	Adhoc	0.07	0.10
Public	Yes	Data Center Provider	Scheduled	Nothing	Adhoc	0.08	0.18
Public	Yes	Data Center Provider	Scheduled	Adhoc	Continuous	0.10	0.20
Public	Yes	Cloud Provider	Scheduled	Adhoc	Adhoc	0.10	0.15
Public	No	Data Center Provider	Nothing	Adhoc	Continuous	0.05	0.25
Private	Yes	Cloud Provider	Nothing	Adhoc	Adhoc	0.10	0.15
Public	Yes	Cloud Provider	Continuous	Adhoc	Adhoc	0.08	0.10
Public	Yes	Data Center Provider	Adhoc	Nothing	Scheduled	0.10	0.15

# The Metric Manifesto: Incorporating Frameworks

Exposure	Data Value	Infrastructure Location	Protect	Detect	Respond	Average	Boundary
Public	Yes	On Prem	Adhoc	Adhoc	Adhoc	0.100	0.30
Public	No	Cloud Provider	Adhoc	Adhoc	Adhoc	0.050	0.15
Public	Yes	Data Center Provider	Scheduled	Nothing	Adhoc	0.070	0.20
Public	Yes	Data Center Provider	Scheduled	Adhoc	Continuous	0.070	0.20
Public	Yes	Cloud Provider	Scheduled	Adhoc	Adhoc	0.050	0.17
Public	No	Data Center Provider	Nothing	Adhoc	Continuous	0.100	0.20
Private	Yes	Cloud Provider	Nothing	Adhoc	Adhoc	0.200	0.50
Public	Yes	Cloud Provider	Continuous	Adhoc	Adhoc	0.030	0.17
Public	Yes	Data Center Provider	Adhoc	Nothing	Scheduled	0.100	0.30
Public	Yes	Cloud Provider	Nothing	Scheduled	Continuous	0.200	0.35
Private	Yes	Data Center Provider	Scheduled	Adhoc	Scheduled	0.200	0.50

# The Metric Manifesto: Incorporating Frameworks

Numerous Subject Matter Experts & Their Forecasts									
1	0.10	0.0500	0.050	0.050	0.042	0.042	0.042	0.042	0.042
2	0.07	0.0500	0.050	0.050	0.042	0.042	0.042	0.042	0.042
3	0.08	0.0300	0.035	0.035	0.042	0.042	0.042	0.042	0.042
4	0.10	0.0300	0.040	0.040	0.042	0.042	0.042	0.042	0.042
5	0.10	0.0100	0.035	0.035	0.042	0.042	0.042	0.042	0.042
<b>0.03833333</b>									
<b>0.03544885</b>									
<b>1.08137</b>									
17	0.15	0.0100	0.060	0.060	0.0400	0.0400	0.0400	0.0400	0.0400
18	0.10	0.0200	0.070	0.070	0.0400	0.0400	0.0400	0.0400	0.0400
19	0.15	0.0100	0.025	0.025	0.0400	0.0400	0.0400	0.0400	0.0400
20	0.10	0.0100	0.010	0.010	0.0400	0.0400	0.0400	0.0400	0.0400
21	0.08	0.0050	0.025	0.025	0.0400	0.0400	0.0400	0.0400	0.0400
22	0.10	0.0200	0.060	0.060	0.0400	0.0400	0.0400	0.0400	0.0400
23	0.05	0.0050	0.040	0.040	0.0400	0.0400	0.0400	0.0400	0.0400
24	0.10	0.0500	0.030	0.030	0.0400	0.0400	0.0400	0.0400	0.0400
25	0.15	0.0200	0.050	0.050	0.0400	0.0400	0.0400	0.0400	0.0400
26	0.10	0.0050	0.020	0.020	0.0400	0.0400	0.0400	0.0400	0.0400
27	0.10	0.0100	0.015	0.015	0.0400	0.0400	0.0400	0.0400	0.0400
28	0.15	0.0300	0.015	0.020	0.0400	0.0400	0.0400	0.0400	0.0400

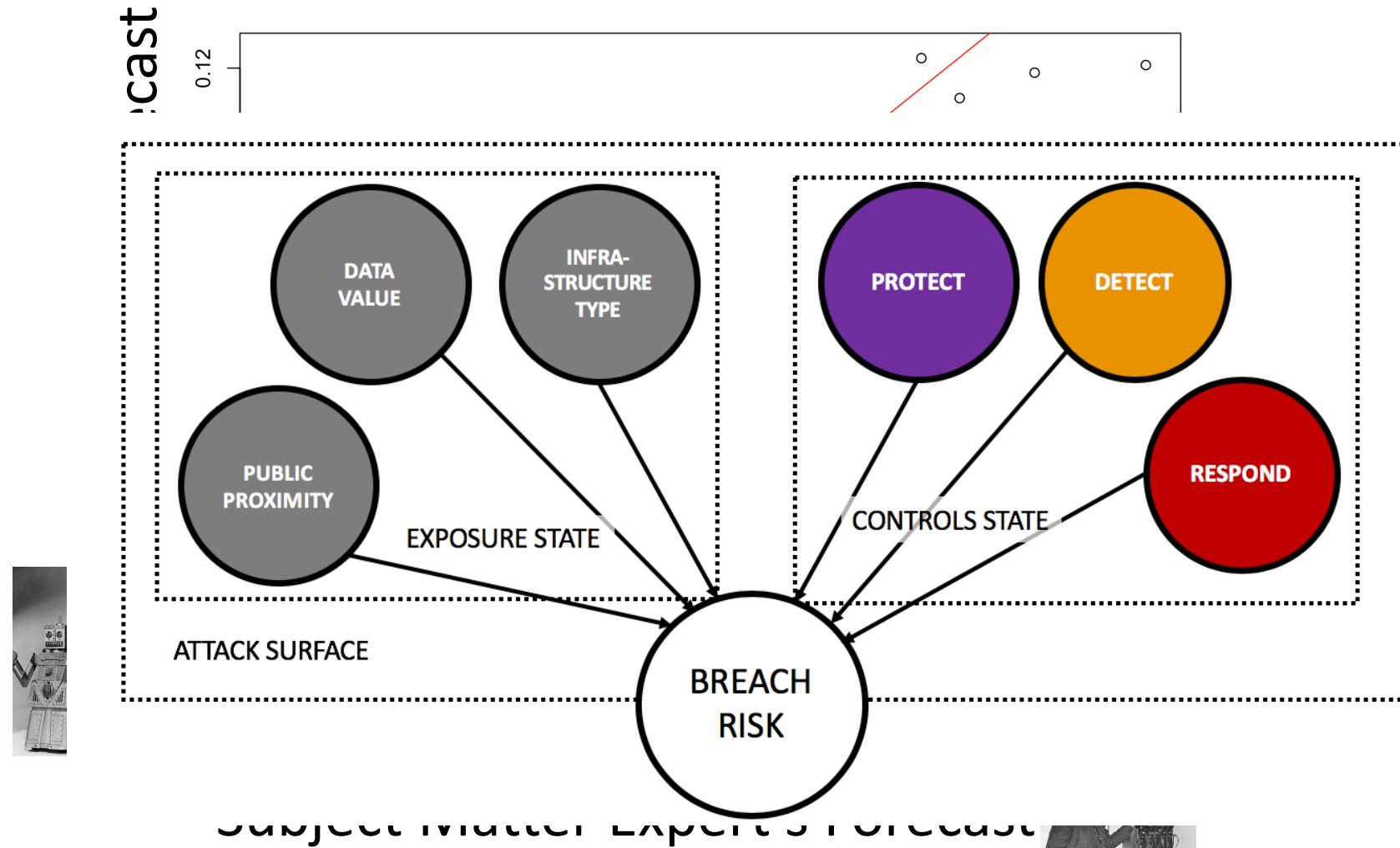
**Consistency Score:** We put duplicate pairs in our surveys. This measures how much spread there is between their answers. For example, they said on one risk scenario 15% likely. On the same scenario later in the survey they said 2%. That's a 13% difference. These get averaged.

**Discrimination Score:** How much spread is in their ratings overall. Are they rating different risks differently.

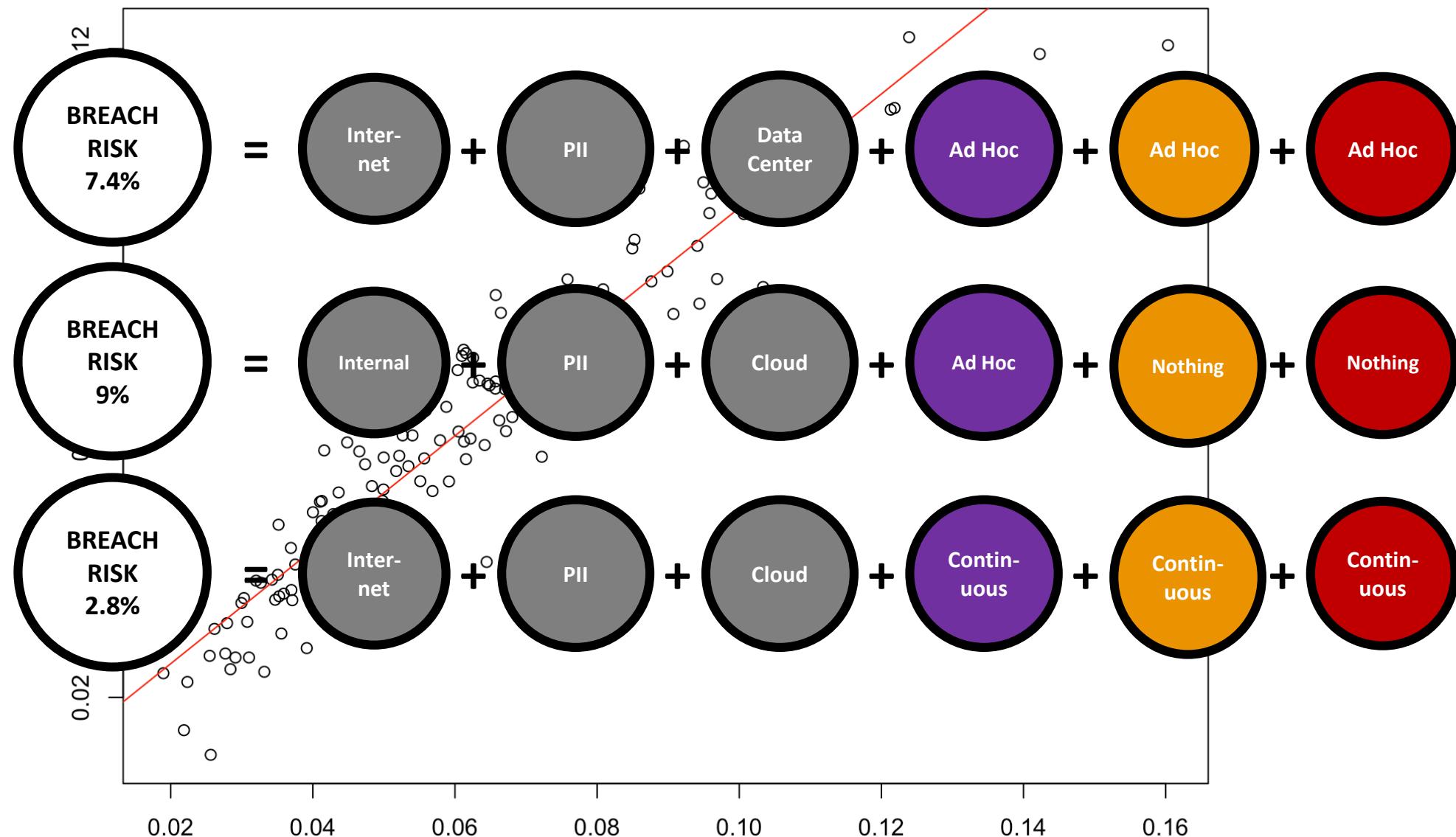
**Quality Score:** This is a ratio of consistency over discrimination. The lower the value the better.

**Low Spread Consistency/High Spread Discrimination**

# The Metric Manifesto: Incorporating Frameworks



# The Metric Manifesto: Incorporating Frameworks



# The Metric Manifesto: Incorporating Frameworks

Original Breach Risk: 6.1%. (Really: 6.050235% but whose counting)  
New Adjusted Risk: 7.0%

Zero Trust  
meaning

Complete  
5.5% due

Complex

to be 6.5% by itself in terms of making breach more likely.

Zero Trust

Mitigation  
Continuous

Complete  
Orchestrate  
Nothing

Response  
7%, once  
Ad Hoc

When we run a simple monte carlo on the model it shows there are the following chances of having N or more events in 3 years:

- 1 or more: 20% (17%)
- 2 or more: 2.1% (2%)
- 3 or more: 0.11% (0.1%)

to be 6.5% by itself in terms of making breach more likely.

Response Assurance – Ad Hoc:

While a critical capability, the team rated its impact as 6.2 in terms of increasing breach risk

BREACH  
RISK

**RSA®**Conference2019

# The Metrics Manifesto

## Making It Real With Digital Risk Management



# The Metric Manifesto: Digital Risk Management

**It's Time Based:** We make multi-year forecasts to help drive strategy.

**It's Tolerance Based:** This one has an imagined insurance threshold

**It's Capability Based:** We model security capability improvement over time

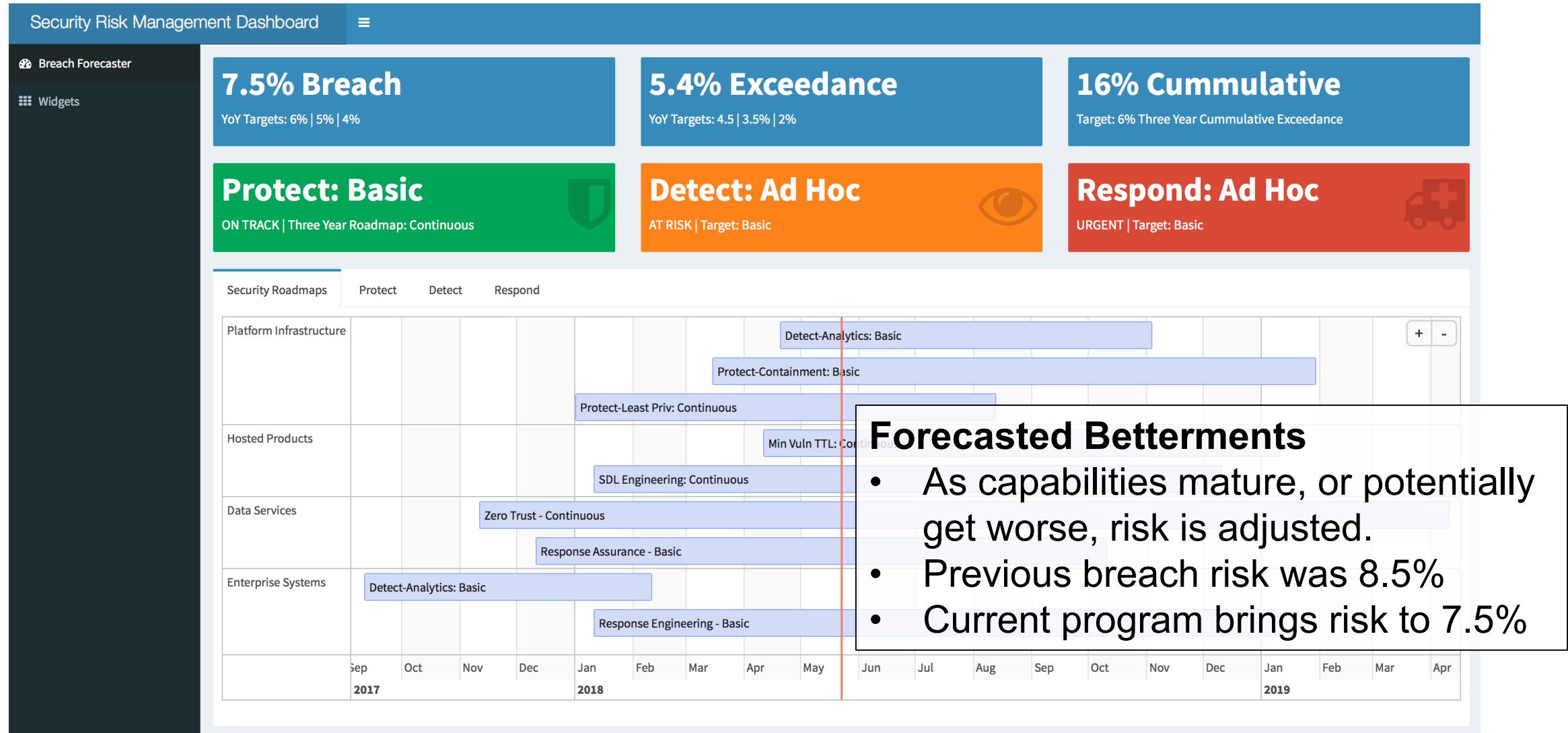
**It's Risk As A Curve!:** We build a model that relates impact (money) and likelihood.

**It Uses Probabilities:** We only use probabilities and dollars – no Red, Yellow, Green or High, Medium, Low.

**Who else uses these methods?**  
Actuaries, big-pharma, military logisticians, nuclear engineers, epidemiologists, meteorologist, project managers, movie producers etc...anyone making forecasts with seemingly irreducible uncertainty.

A map *is not* the territory .... but if correct, it has a *similar structure* to the territory, which accounts for its usefulness. — Alfred Korzybski in *Science & Sanity*

# The Metric Manifesto: Digital Risk Management



# The Metric Manifesto: Digital Risk Management

Security Risk Management Dashboard ≡

Breach Forecaster Widgets

**7.5% Breach**  
 YoY Targets: 6% | 5% | 4%

**5.4% Exceedance**  
 YoY Targets: 4.5 | 3.5% | 2%

**16% Cummulative**  
 Target: 6% Three Year Cummulative Exceedance

**Protect: Basic**  
 ON TRACK | Three Year Roadmap: Continuous



[Security Roadmaps](#) [Protect](#) [Detect](#) [Respond](#)

**Technology Portfolio Capability Maturity Requirements:**  
 Platform Infrastructure: Principles for Building, Deploying and Running Products Securely

**Zero Trust**

**Detect: Ad Hoc**  
 AT RISK | Target: Basic



[Security Roadmaps](#) [Protect](#) [Detect](#) [Respond](#)

**Forecasted Betterments**  
URGENT Target: basic

- Uncertain costs, but not entirely
- Likelihood adjustments using calibrated SME inputs
- Results in ROI based decision making

**Least Privilege Maturity:**

Continous: RBAC

**Least Privilege Impact**



**Project Timeline**

2018-01-01 to 2018-08-15

**LB Cost**

\$1,000,000

**UB Cost**

\$3,000,000

**Containment Maturity:**

Basic: Critical Asset Segmentation

**Containment Impact**



**Project Timeline**

2018-03-15 to 2019-01-30

**LB Cost**

\$1,500,000

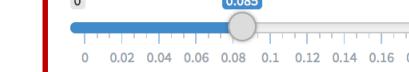
**UB Cost**

\$4,000,000

**Encryption Maturity:**

Basic: Motion and at Rest

**Encryption Impact**



**Project Timeline**

[ ] to [ ]

**LB Cost**

0

**UB Cost**

0

**Authentication Maturity:**

Basic: MFA Step-up

**Authentication Impact**



**Project Timeline**

[ ] to [ ]

**LB Cost**

0

**UB Cost**

0

# RSA® Conference 2019

Thank You!

[richard@m3securitysolutions.com](mailto:richard@m3securitysolutions.com)