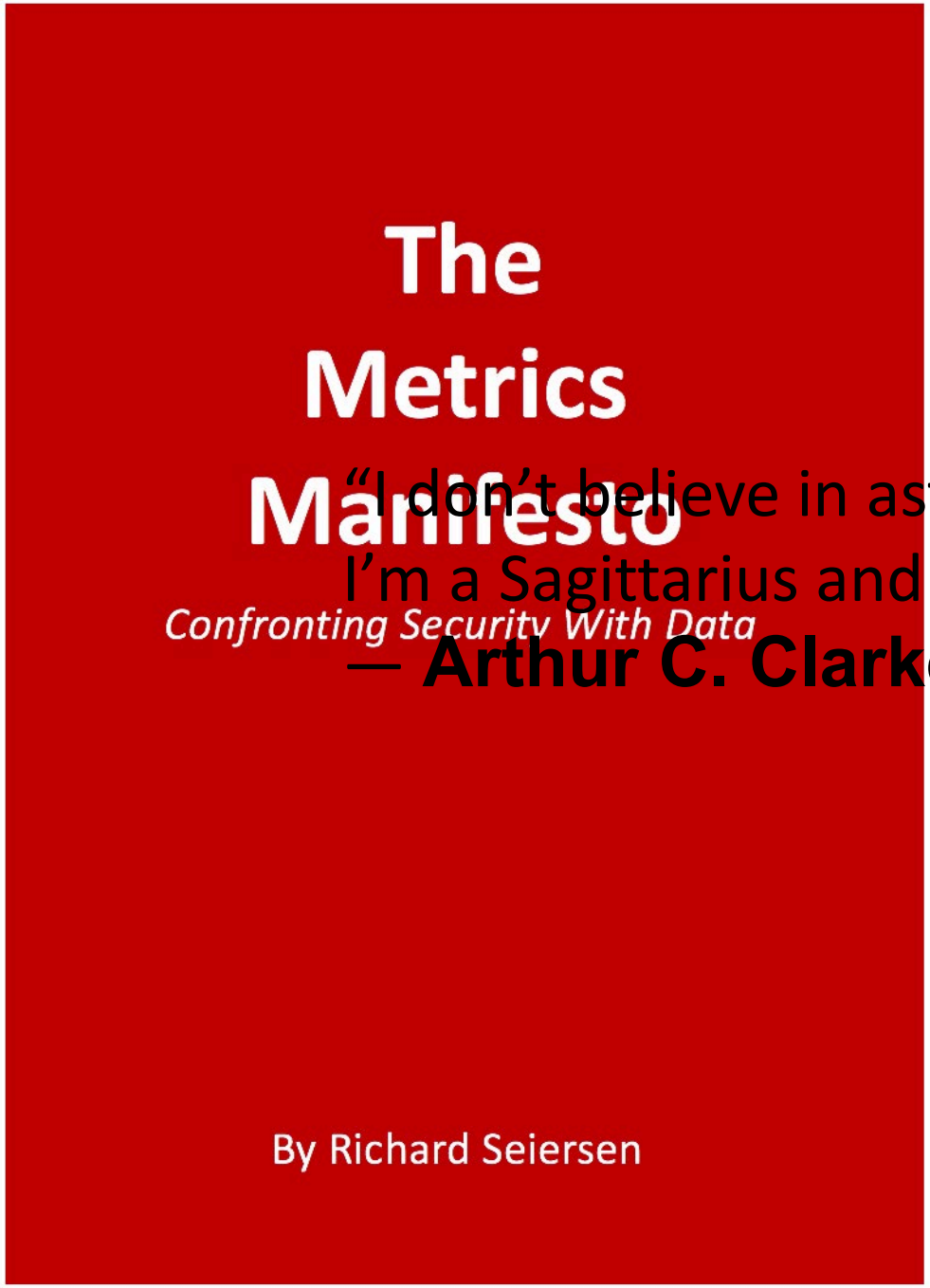
RSAConference2019
San Francisco | March 4–8 | Moscone Center

SESSION ID: GRC-T07

The Metrics Manifesto

Richard Seiersen

President
M-Cubed
@RichardSeiersen



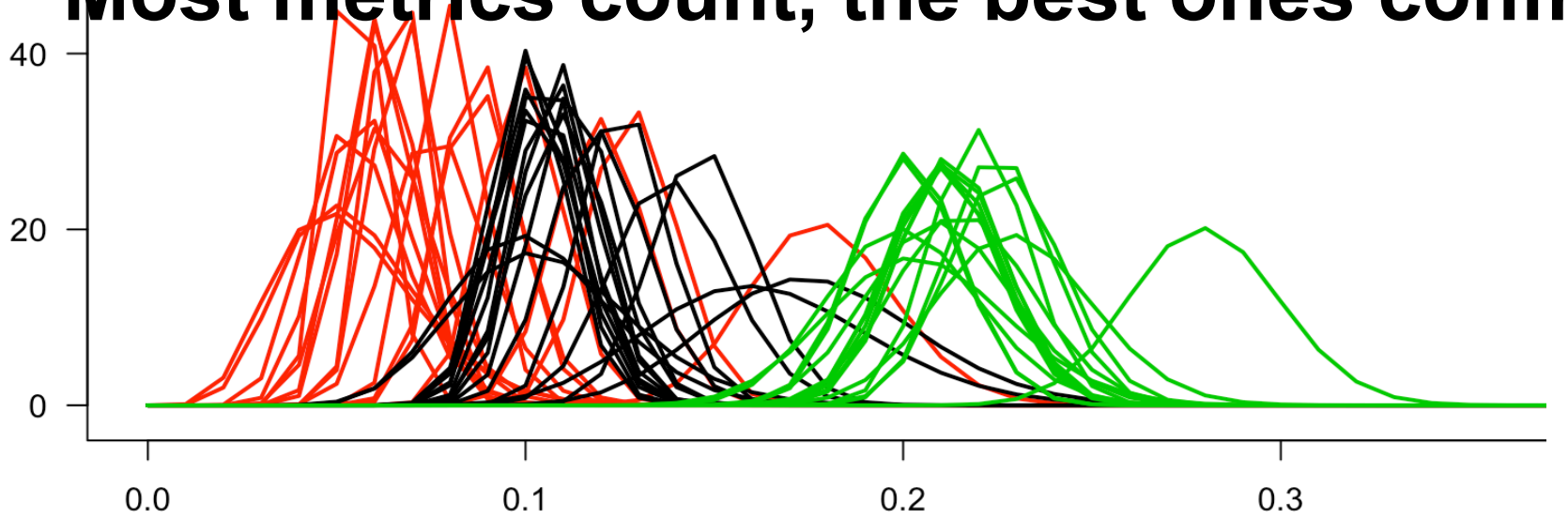
"I don't believe in astrology;
I'm a Sagittarius and we're skeptical."
— **Arthur C. Clarke**

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*

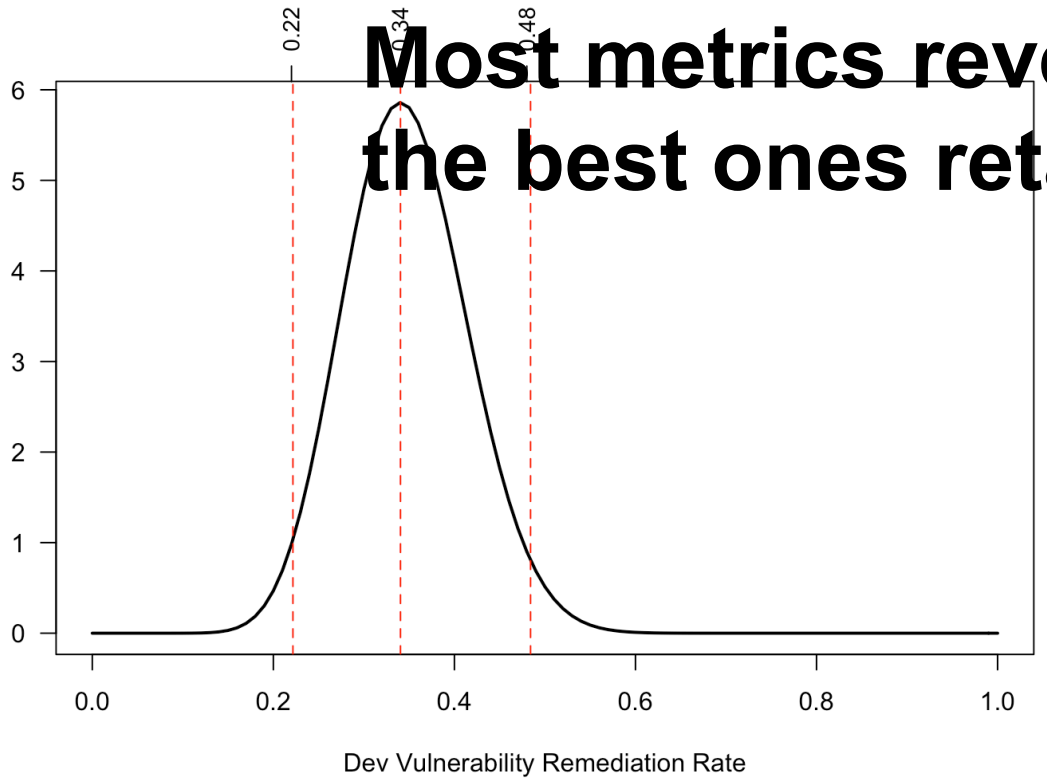
Most metrics count, the best ones confront



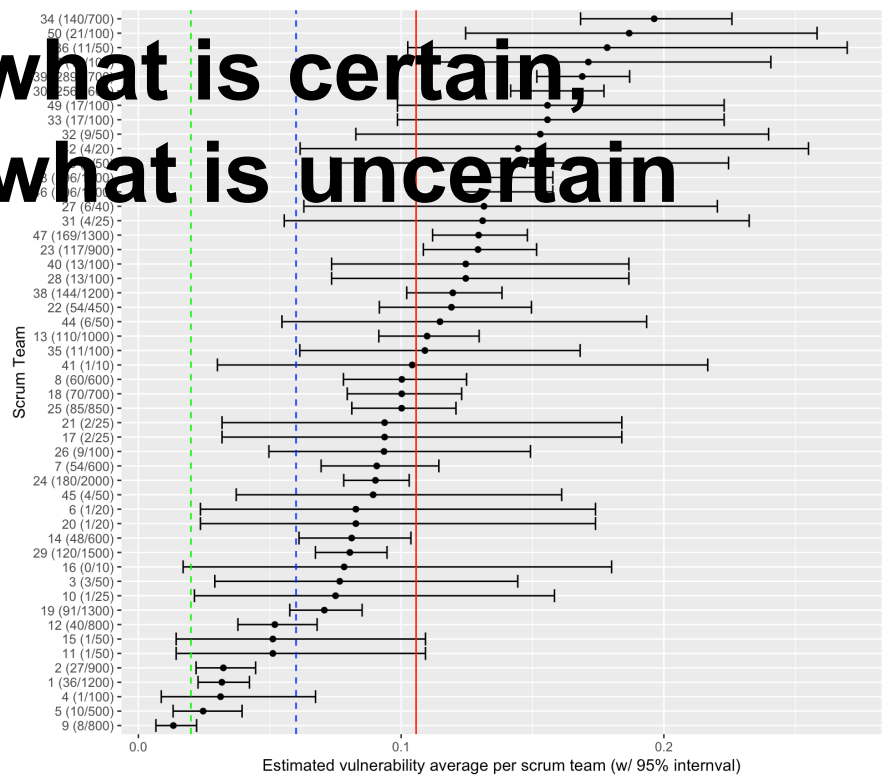
Vulnerability Escape Rates By Severity and By Development Team

The Metrics Manifesto

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



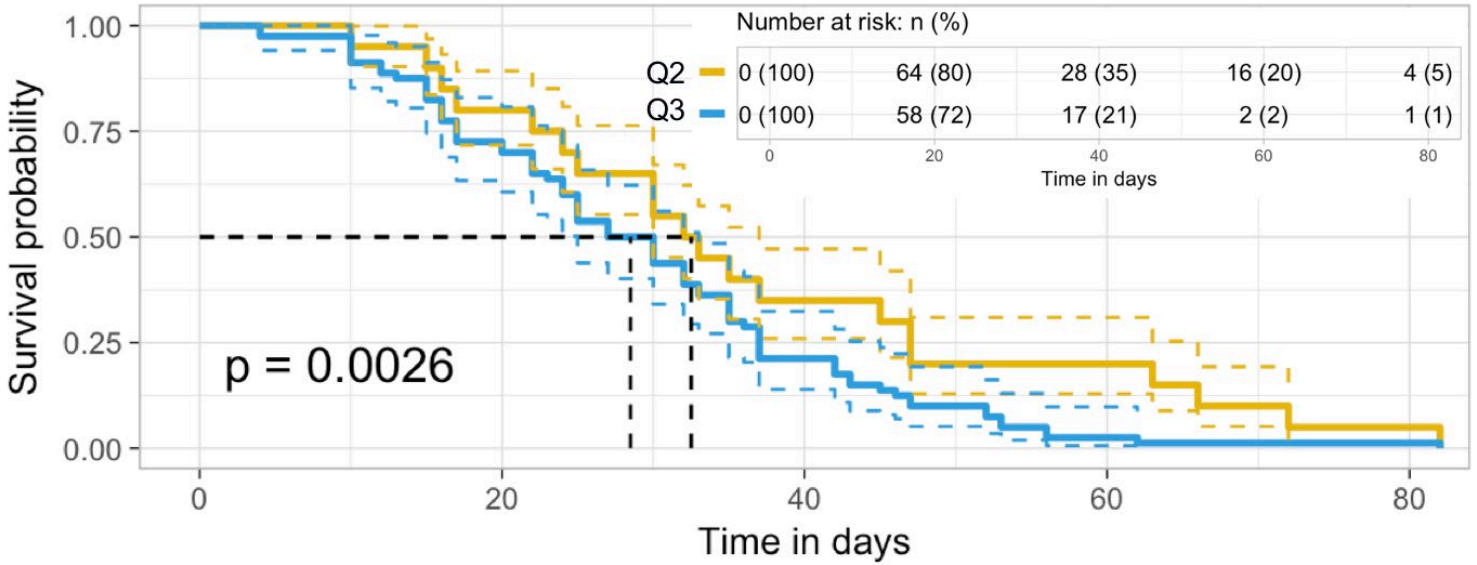
Most metrics reveal what is certain, the best ones retain what is uncertain



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 and our business expose, continuously*

Most metrics focus on beating benchmarks, the best ones focus on beating the competing model



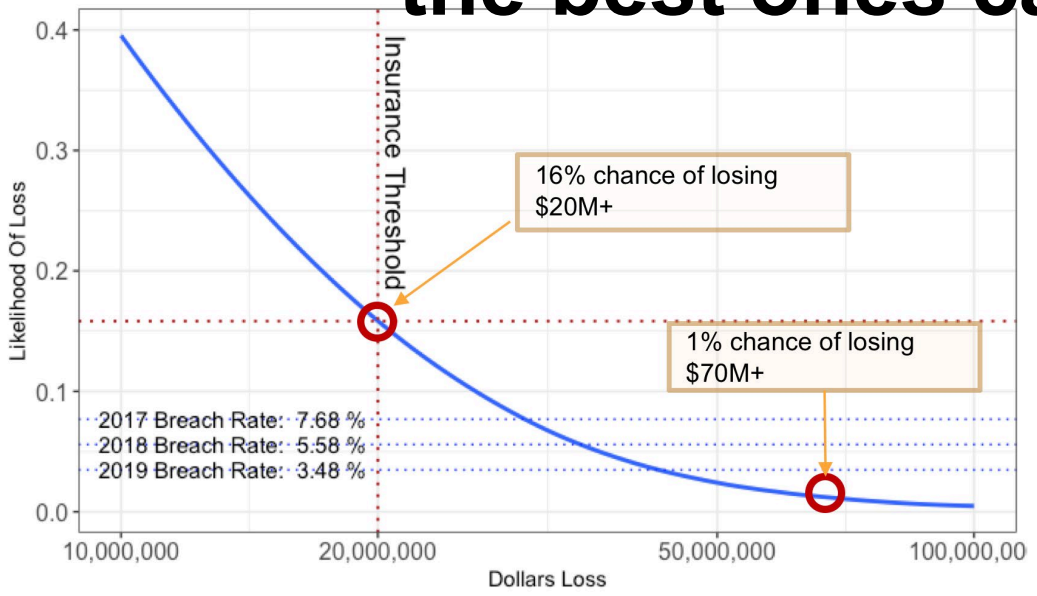
Threat Survival Analysis By Quarter

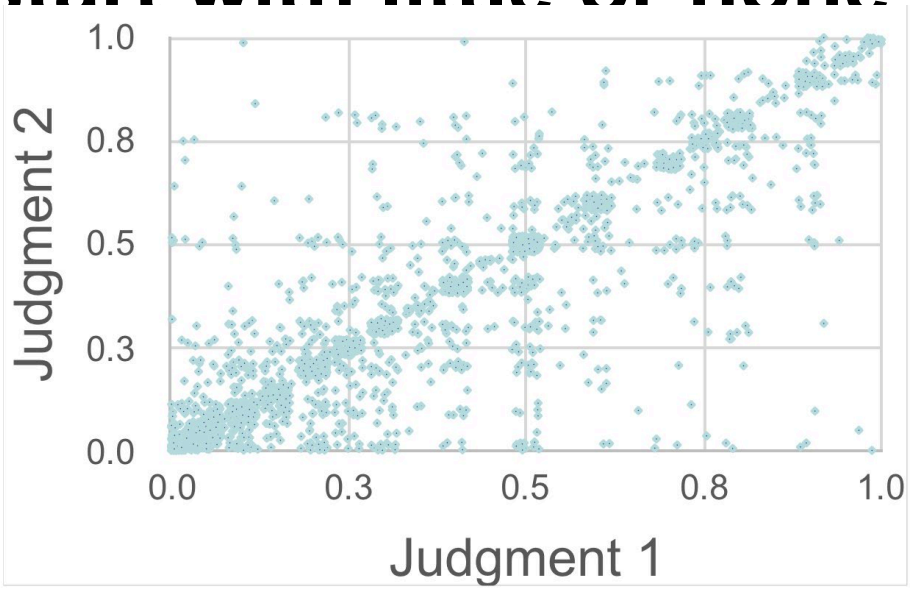
The Metrics Manifesto

5. *We believe resourcefulness with small data is always better than complexity with big data*
6. *We also believe expertise can be turned into data when you have none – data that is*

Most metrics require data,

the best ones can start with little or none





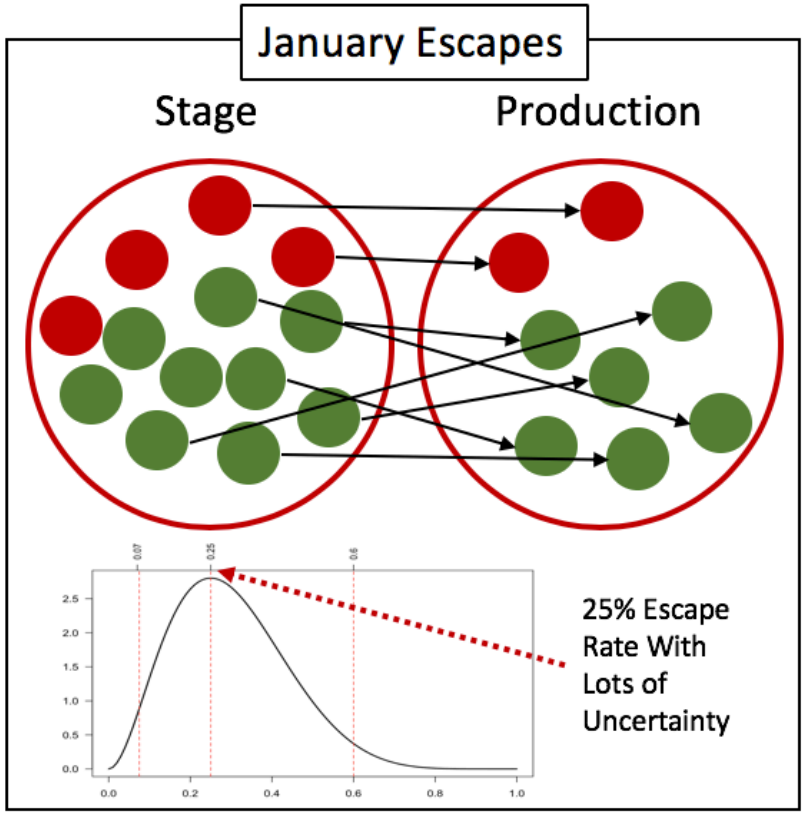
RSAConference2019

The Metrics Manifesto In Action

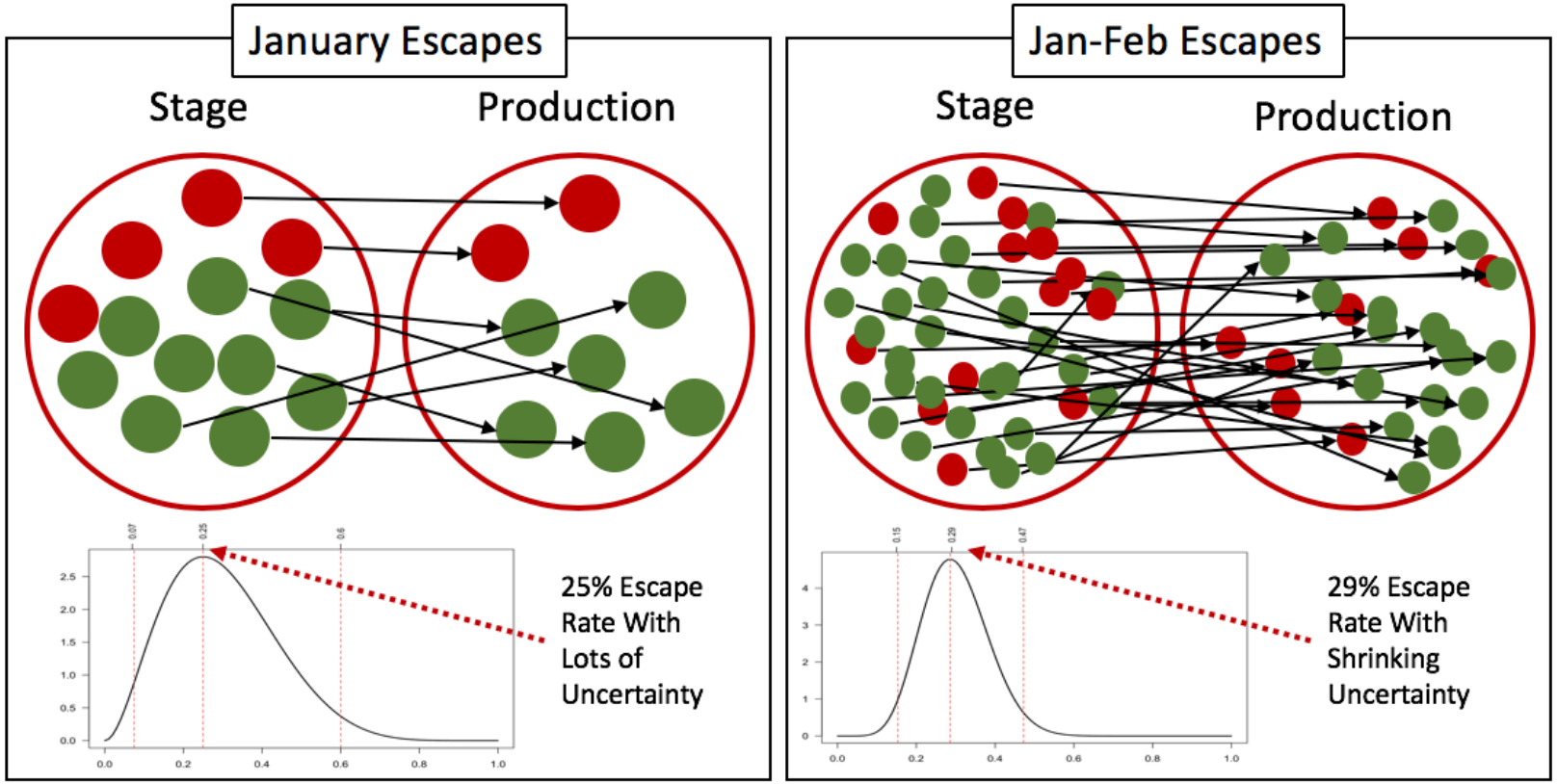
Measuring & Controlling Attack Surface with Escape Rates

The Manifesto In Action: Escape Rates

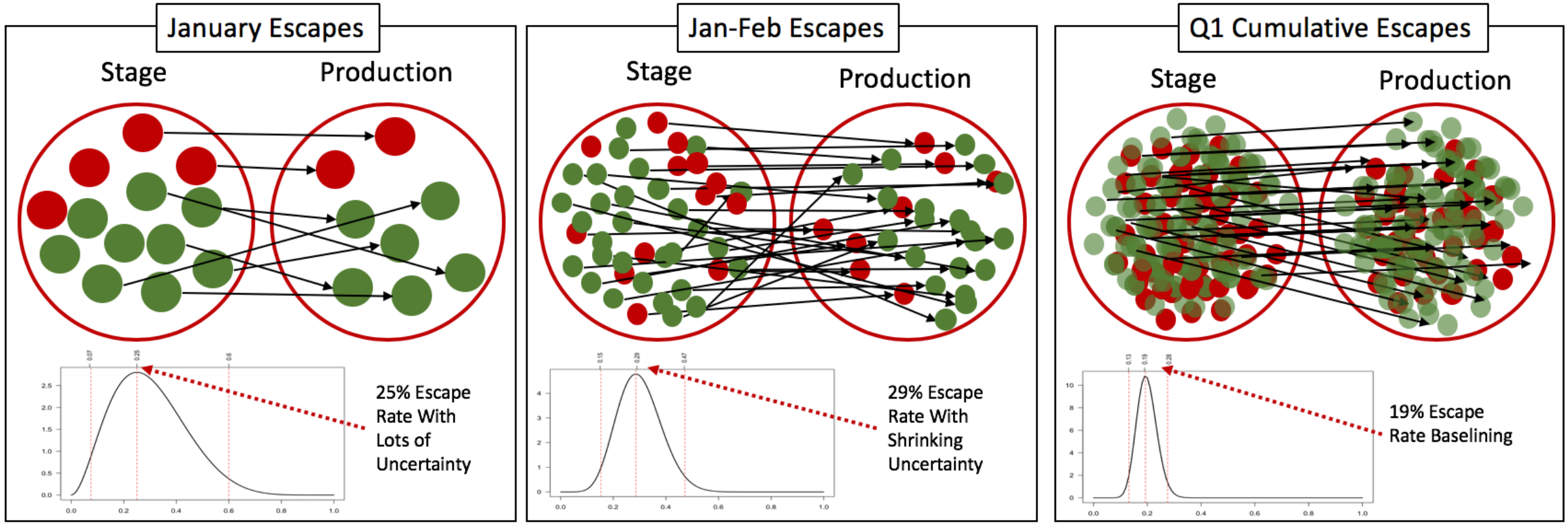
The Manifesto In Action: Escape Rates



The Manifesto In Action: Escape Rates



The Manifesto In Action: Escape Rates

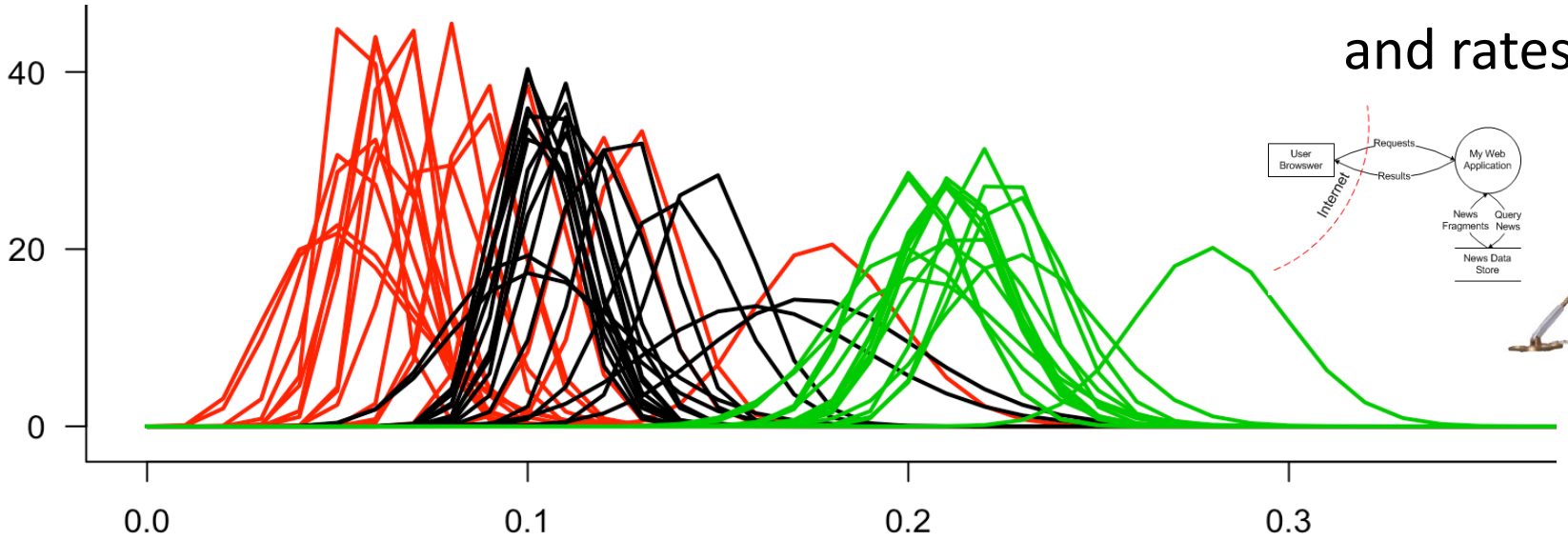


The Manifesto In Action: Escape Rates

```
#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)
```

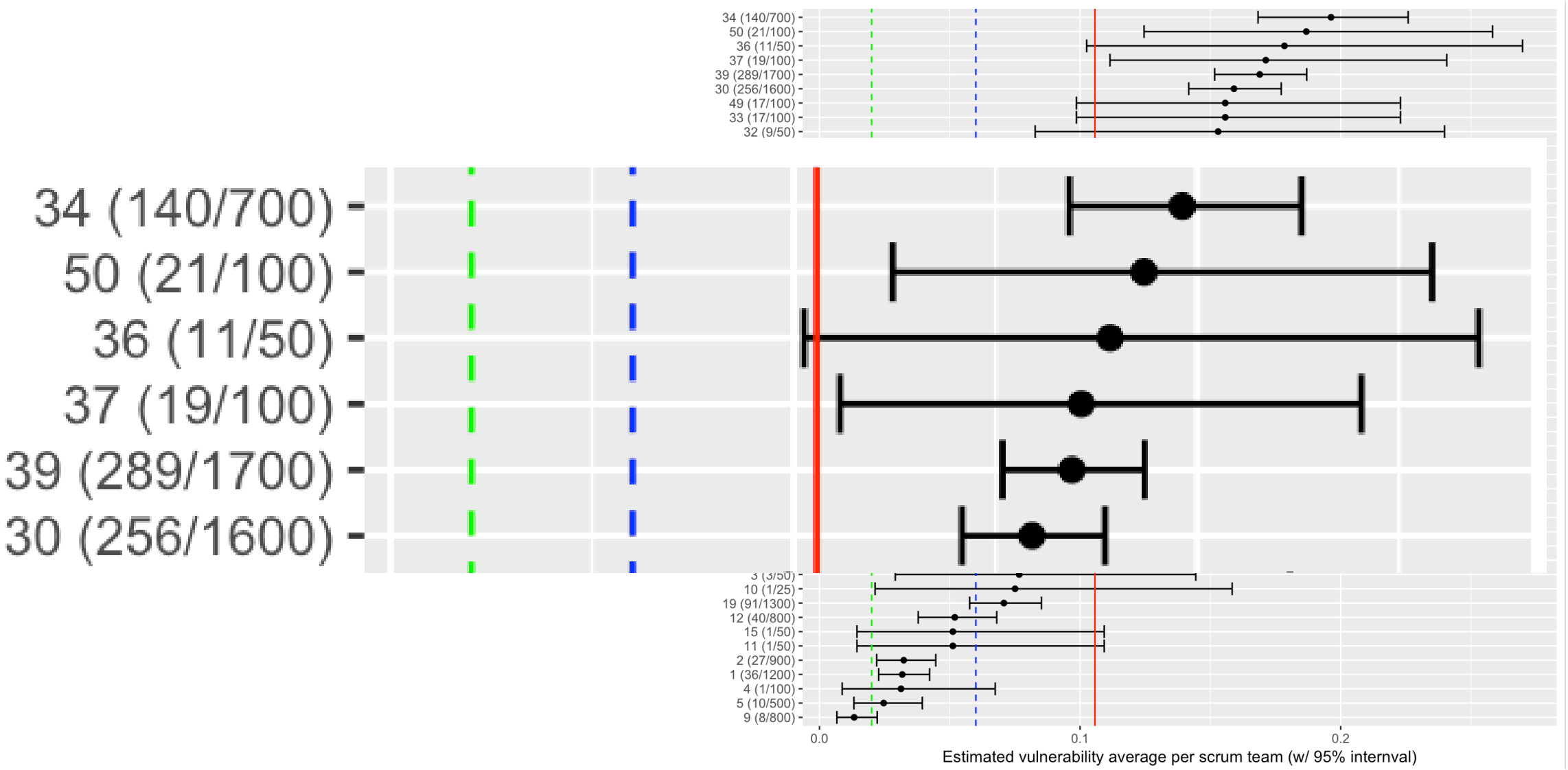
```
#p2 Vulns
extreme.totals <- test.p2 %>% filter(new.expected >= .20)
MakeCurves(extreme.totals, nrow(extreme.totals),3)
```



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

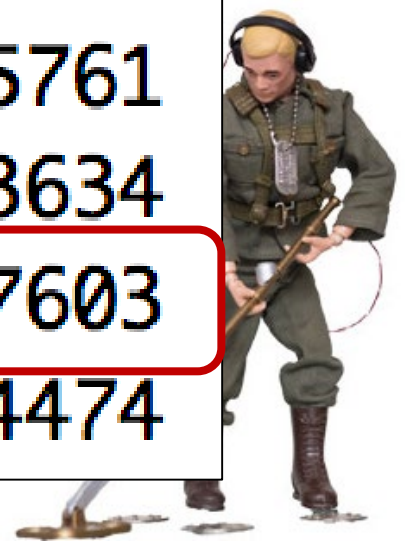


The Manifesto In Action: Advanced Rates

	(Intercept)	Reme
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_SLAContinous	-0.017095
Remediate_SLAScheduled	-0.025761
DynamicBasic	-0.033634
DynamicContinuous	-0.087603
DynamicScheduled	-0.044474

ntinuous	DynamicScheduled
.08734552	-0.04433257
.08797798	-0.04467973
.08929643	-0.04540343
.08755133	-0.04444554
.08582520	-0.04349806
.09021944	-0.04591008
.08500567	-0.04304822



RSAConference2019

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.

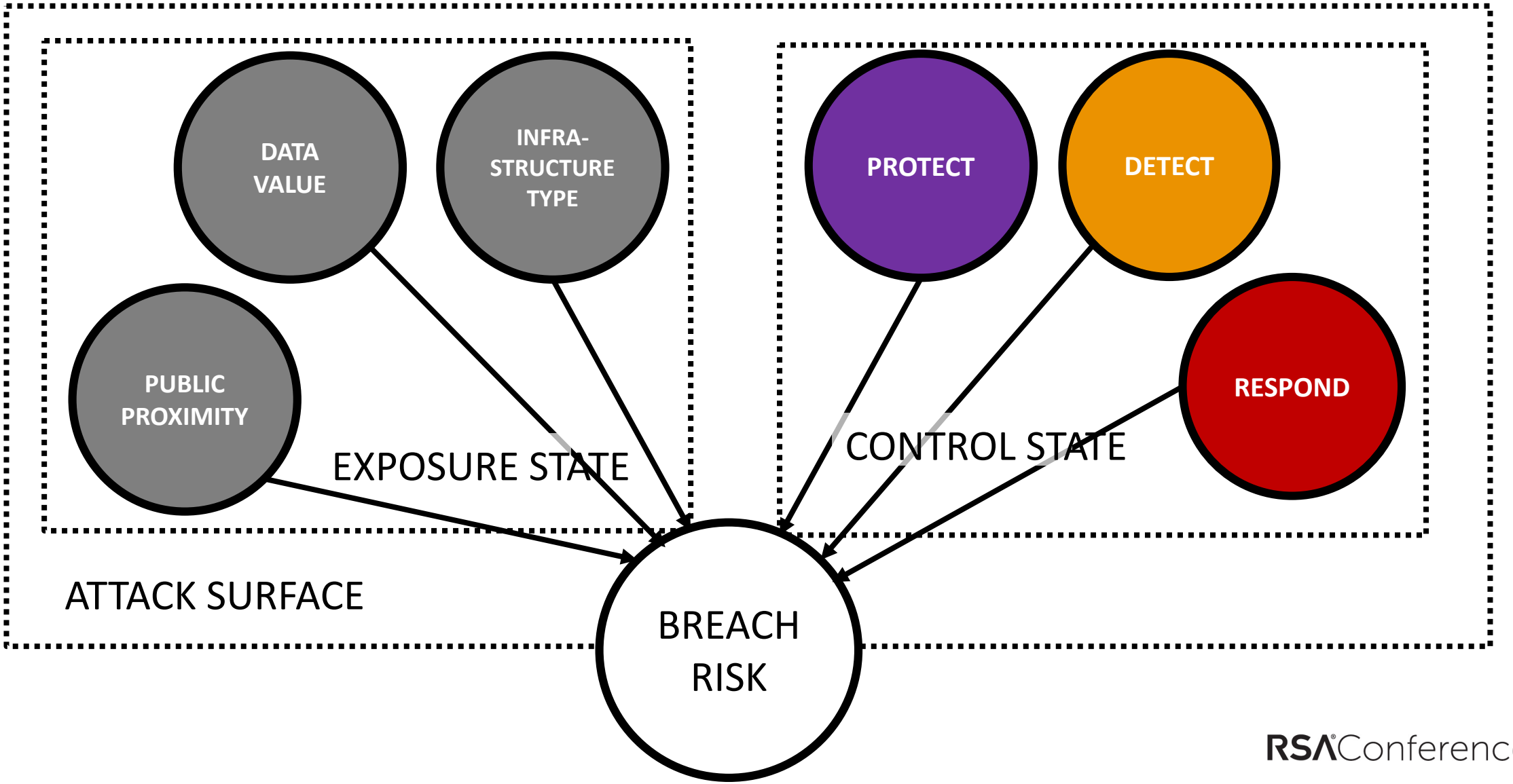
RESPOND

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					nuous
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

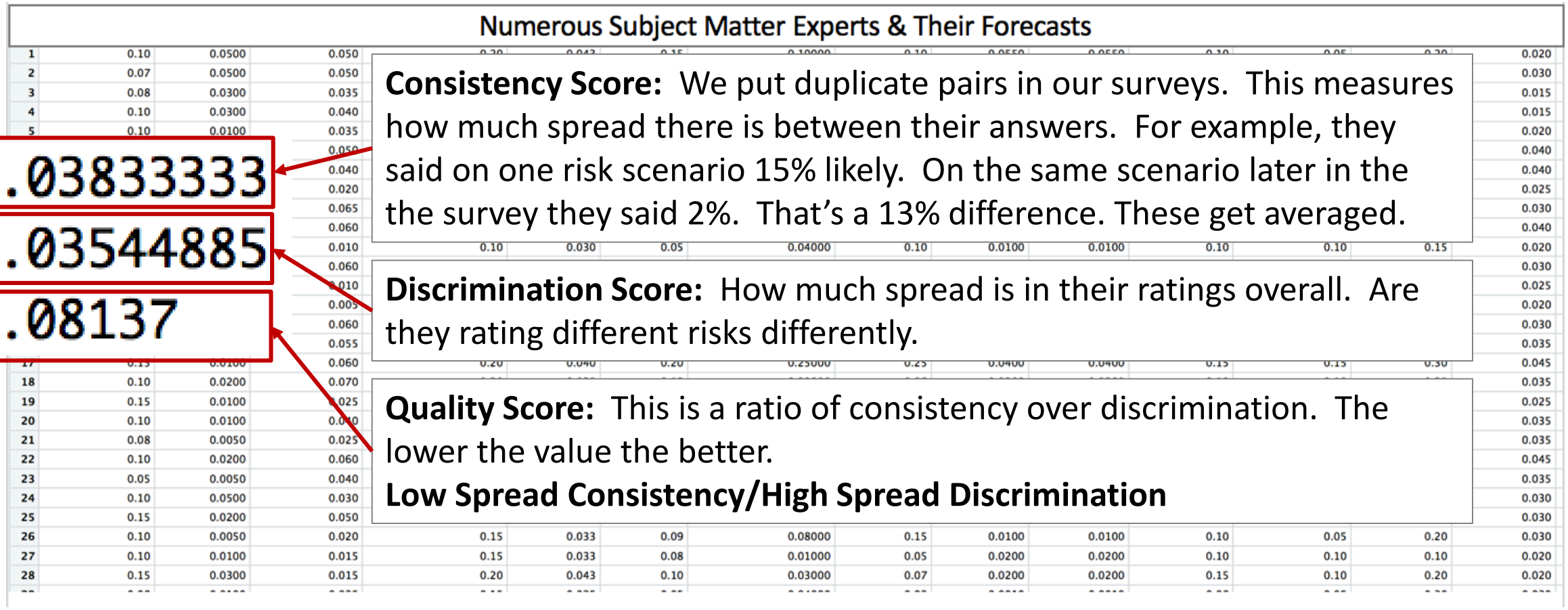
The Metric Manifesto: Incorporating Frameworks

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

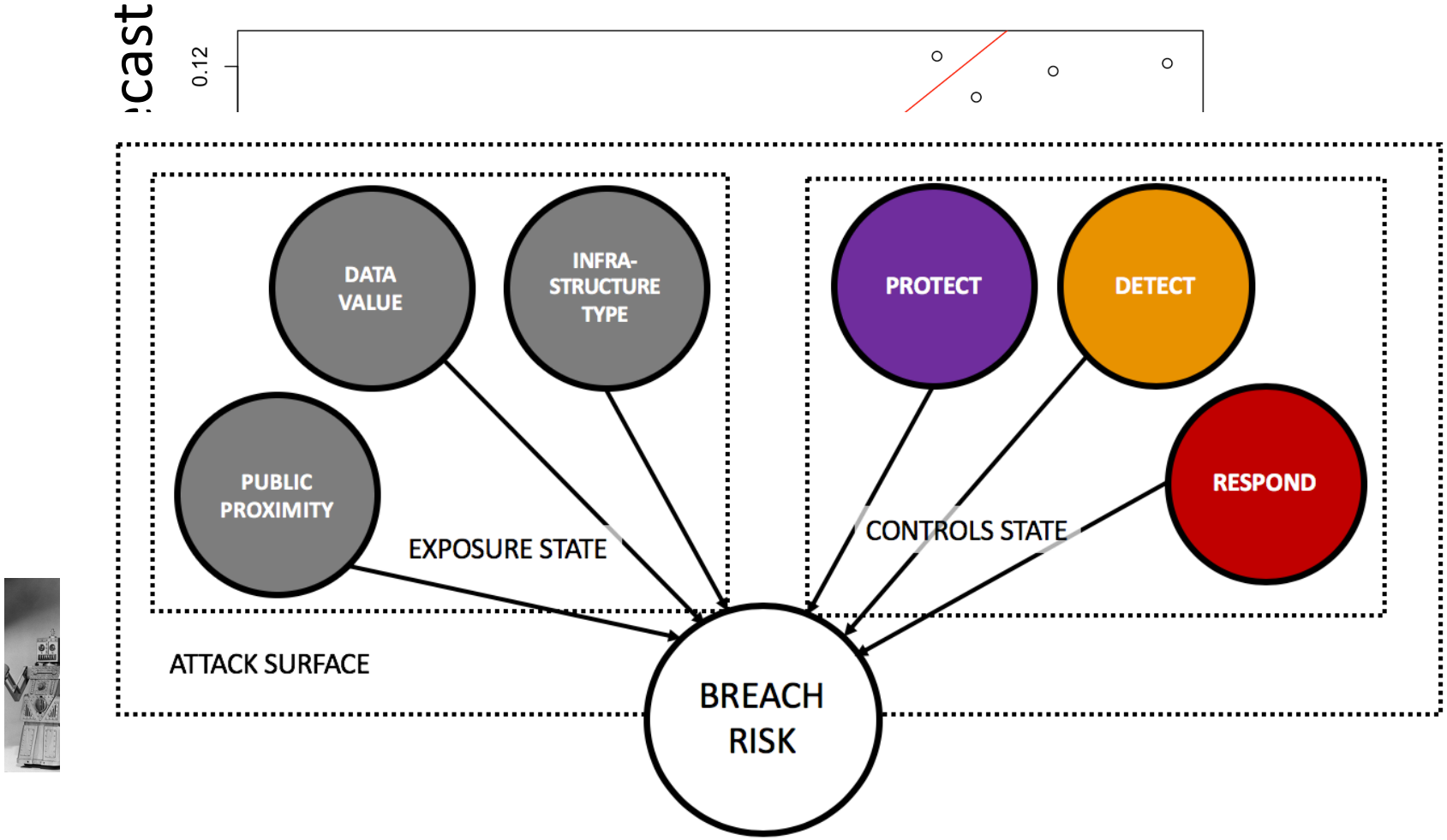
The Metric Manifesto: Incorporating Frameworks

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

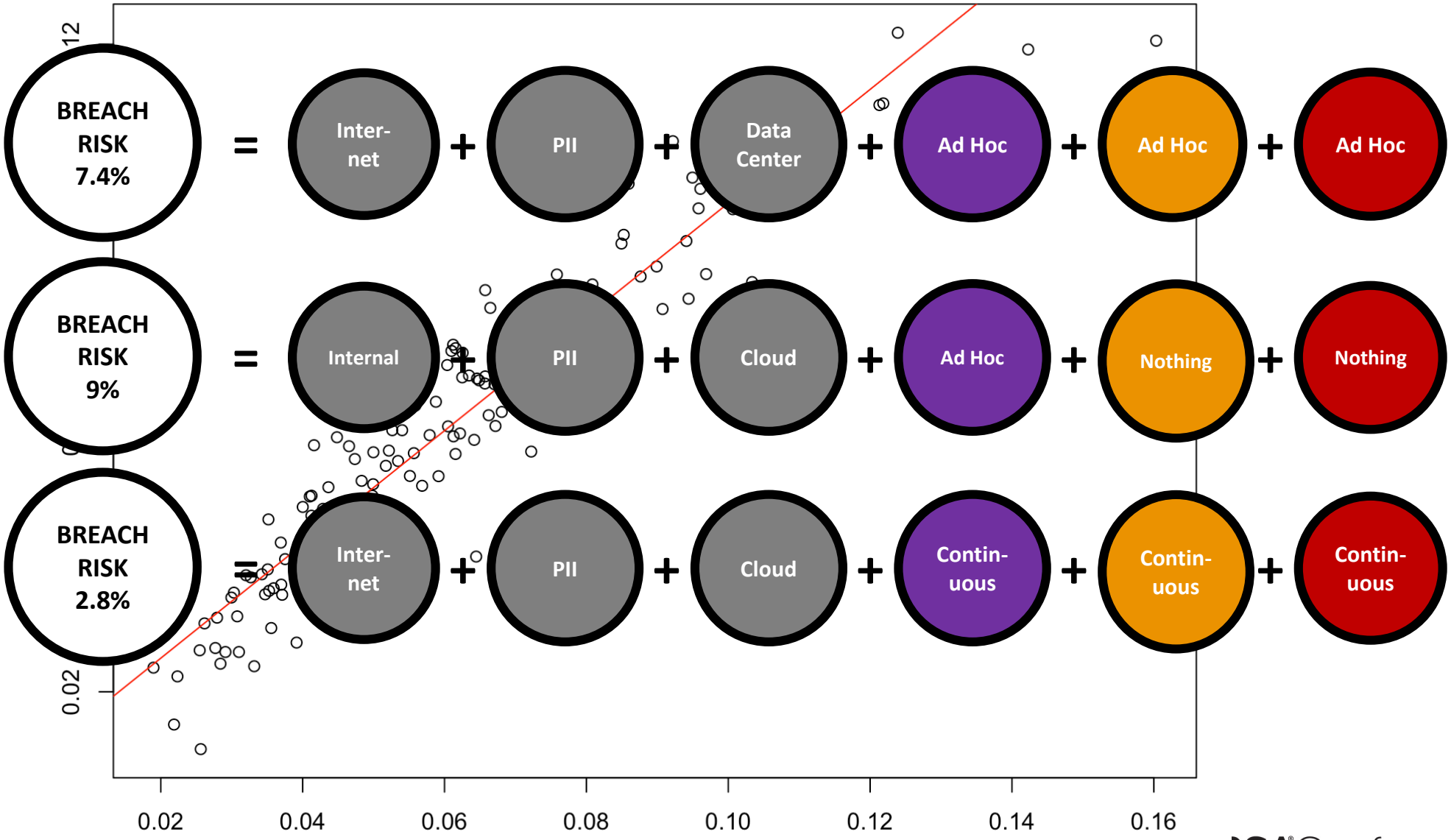


The Metric Manifesto: Incorporating Frameworks



Subject Matter Expert's Forecast

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 Tru
meanin

Comple
5.5% du

Comple
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

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%)

RSAConference2019

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

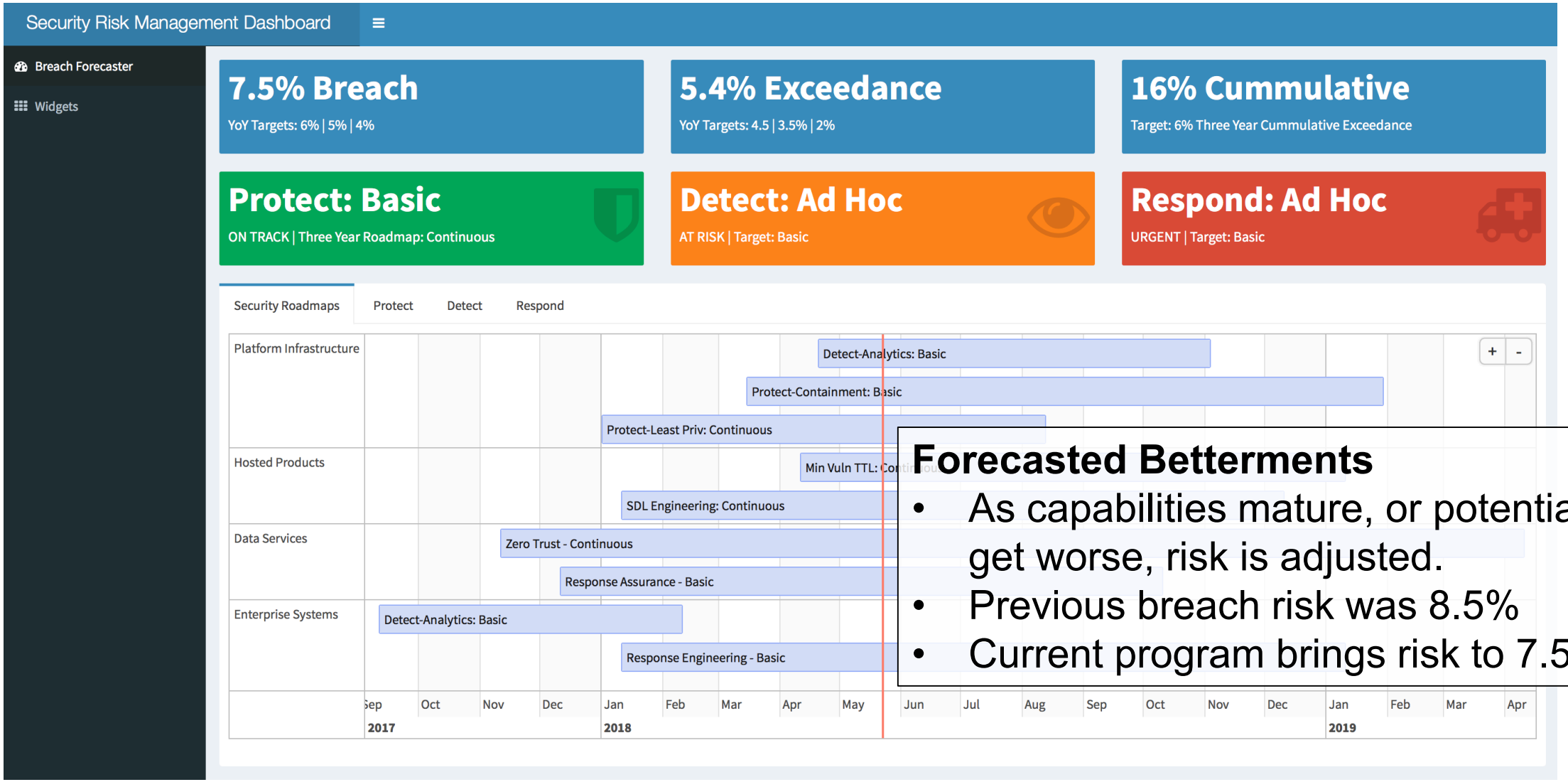
It's Risk As A Curve!: We build a ***model*** that relates impact (money) and likelihood.

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 irriducible 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*

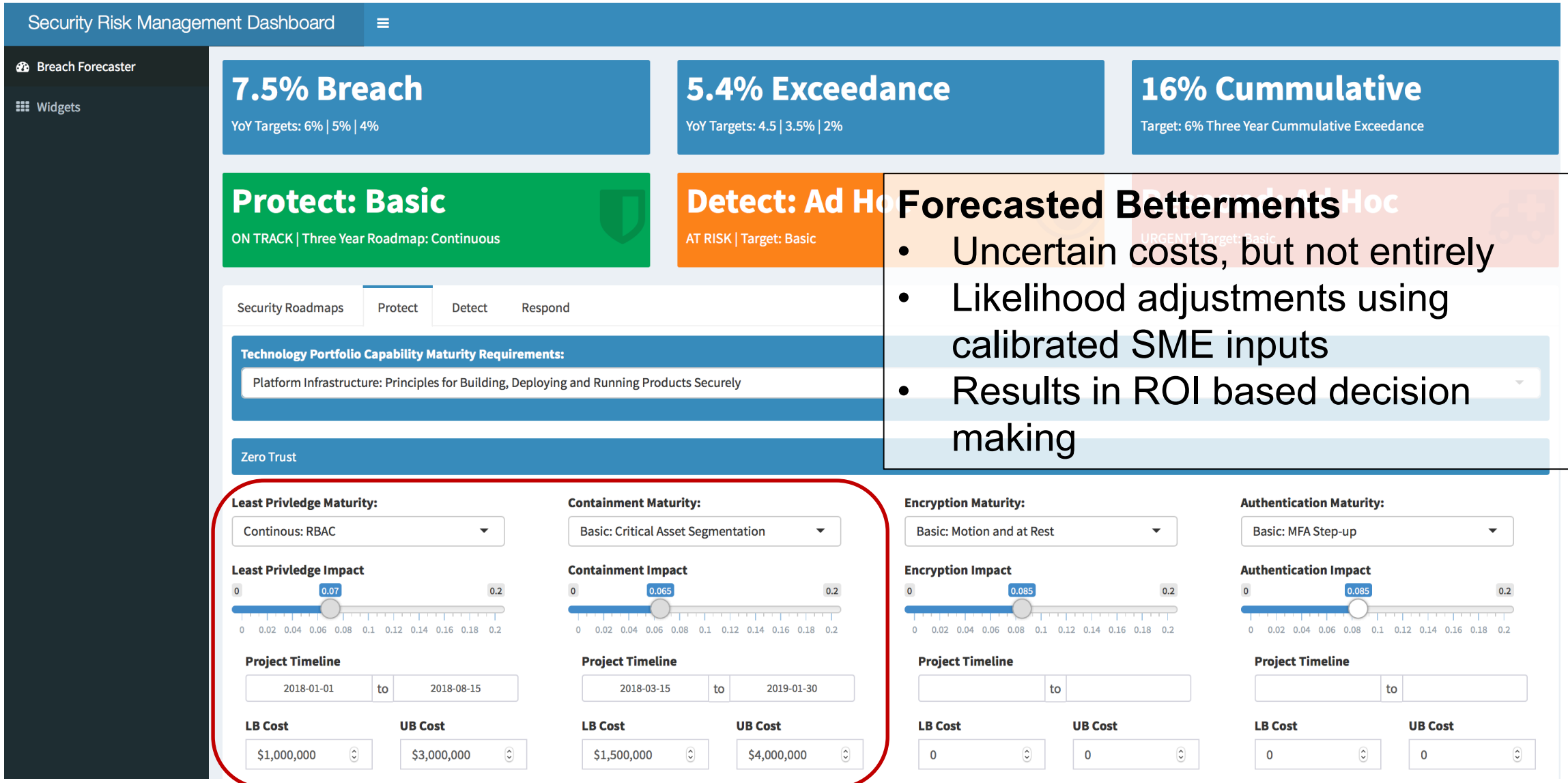
The Metric Manifesto: Digital Risk Management



Forecasted Betterments

- As capabilities mature, or potentially get worse, risk is adjusted.
- Previous breach risk was 8.5%
- Current program brings risk to 7.5%

The Metric Manifesto: Digital Risk Management



Forecasted Betterments

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

RSAConference2019

Thank You!

richard@m3securitysolutions.com