

RSA® Conference 2019 **Asia Pacific & Japan**

Singapore | 16–18 July | Marina Bay Sands



BETTER.

SESSION ID: HPS-W08

Is Your SOC Any Good? Proving and Improving Your Value with Metrics

Amy Parde

Director, Security Operation Center
Sony Corporation

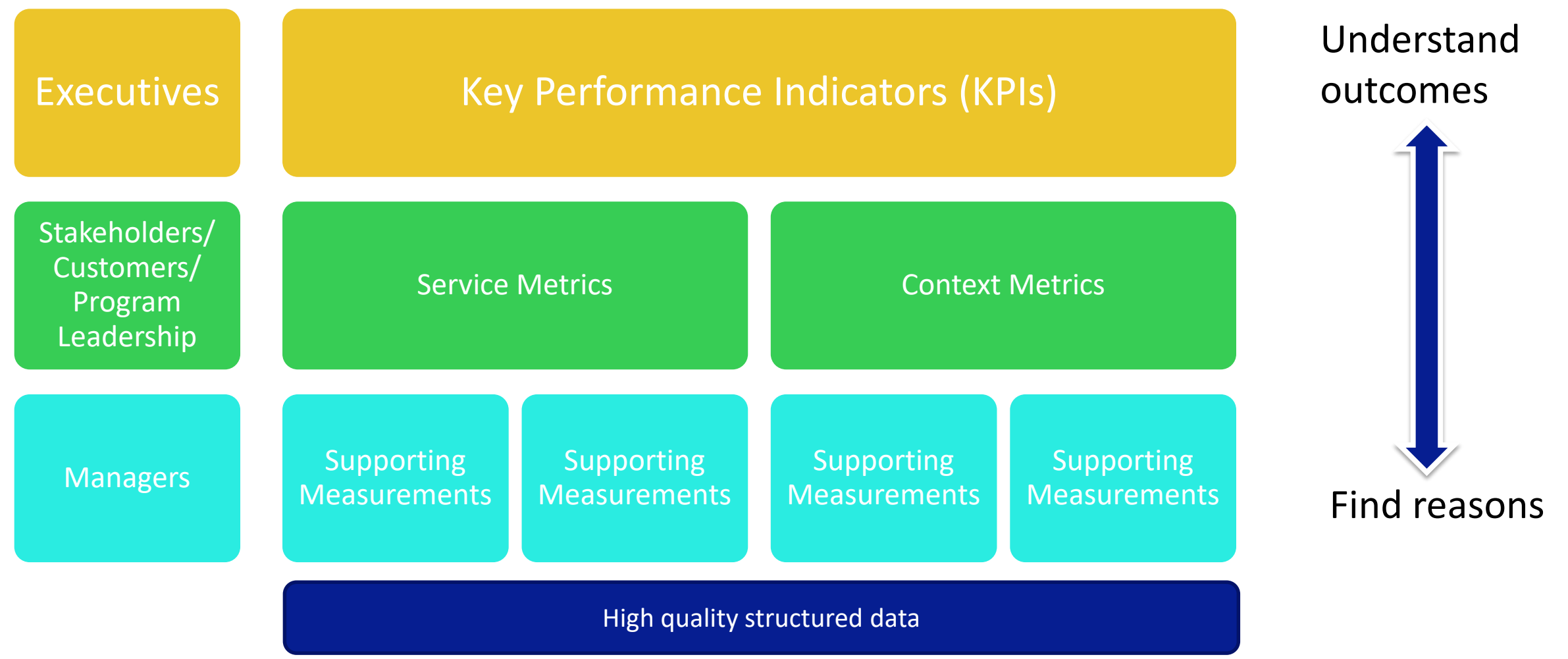


#RSAC

Have you ever...?

- Struggled to advocate successfully for security funding
- Wondered what your gaps are
- Struggled to find out where to focus to close gaps

The Metrics Ecosystem



RSA[®]Conference2019
Asia Pacific & Japan

The Basic Building Blocks of Metrics

Disclaimer: All Numbers Used in This Deck are Fictitious

Example 1: Measuring efficiency



Measurements: Time in each workflow state



Metric: Detect Time

Metric: Notify Time


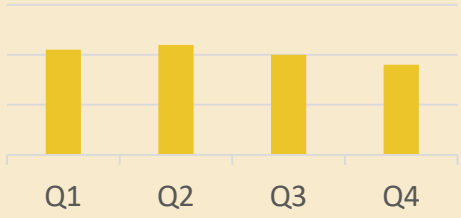
Metric: Response Time



KPI: Dwell time

Executive View: Dwell Time



Metric	Last Quarter	This Quarter	Change	Trend
Average Dwell Time	100 hours	90 hours	-10% 	 <p>Example Data</p>

- Dwell Time = Time the adversary had access to a system
- Measurement of actual risk exposure window, which is often an aggregate of multiple teams' performance
- One bad incident can significantly impact the measure

Customer View: Time to Notify



Severity	Target Notification Time	Median Notification Time	% of Tickets within Target this Month	% of Tickets within Target Last Month	Change
High	< 1 hour	40 minutes	99%	98%	+1%
Medium	< 4 hours	3.4 hours	95%	98%	-3%
Low	< 8 hours	6.2 hours	99%	99%	0%

Example Data

- Notification Time = Time between discovery and notification for action, including analysis and scoping
- Measures how quickly the analyst team performed their function
- Really critical to understand the start and stop times for service providers for this type of metric

Manager View: Time in State Breakdown



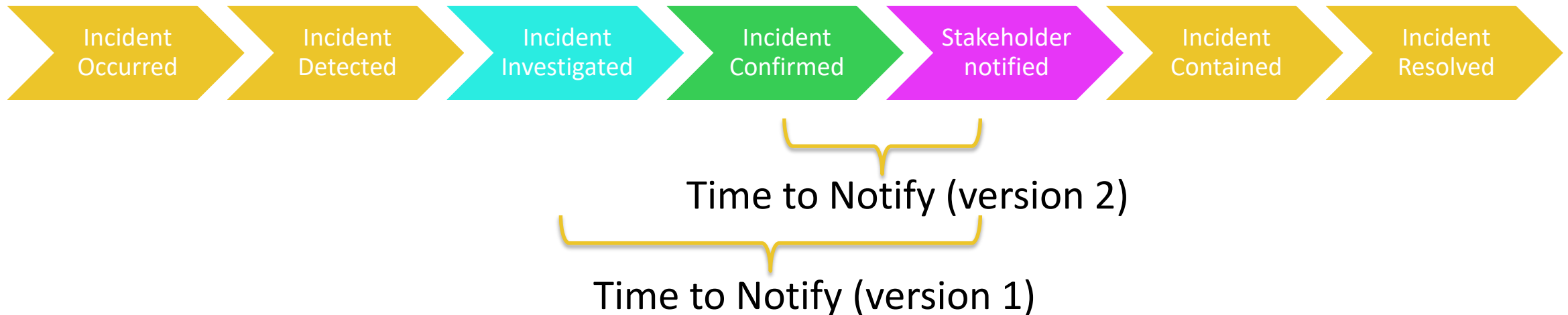
Shift	Total tickets	Time in Investigation		Time in Confirmed	
		Average Time in State	Total Time in State	Average Time in State	Total Time in State
1st	50	6 hours	300 hours	0.75 hours	37.5 hours
2nd	40	5 hours	200 hours	1 hour	40 hours
3rd	20	6.5 hours	130 hours	3 hours	60 hours

Example Data

Not a lot of variance here might indicate appropriate resourcing

This might indicate a resource constraint on the shift or a training gap

Pay Attention to Metric Definitions



- Measuring from confirmation time is commonly used when you want higher likelihood that the metric will be good or consistent
- Determining when the clock starts is critical to understanding what the measure is telling you
 - Service providers often define an SLA for the time to notify from time of confirmation rather than time of detection or investigation
 - These time stamps often matter for legally required notifications

Considerations for Efficiency Metrics

The Good

- Useful for various levels (managers, executives, customers)
- Can help identify bottlenecks and opportunities
- Relatively easy to define and measure
- You can tie improvements in efficiency back to initiatives to articulate return on investment

The Challenges

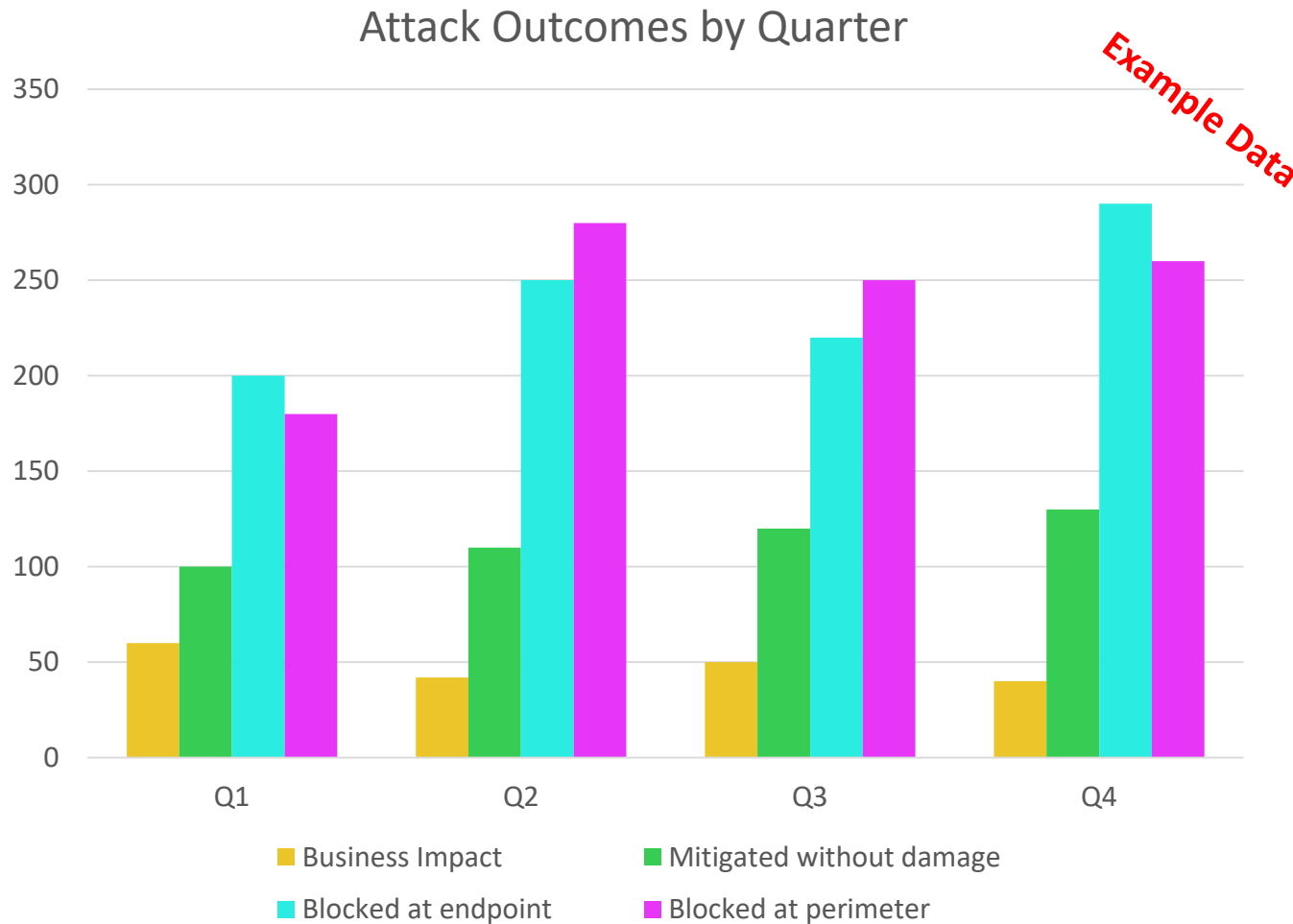
- One bad incident can significantly impact your numbers
- Typically high variance in the numbers, makes trending difficult
- Many factors outside your control can influence efficiency
- Pressure to define measures and targets you can reliably hit

Example 2: Measuring Effectiveness



- Part of the closure process should include capture of final assessments of the investigation
- Numerous options exist to capture the outcome:
 - What did we do to resolve it?
 - Remediation outcomes
 - How far did it get?
 - Kill chain
 - Defense in depth measure
 - What was impacted?
 - Data types
 - System types
 - How significant was the impact?
 - Business impact or criticality rating
 - Cost of incident

Executive/Customer View: Attack Outcomes Example

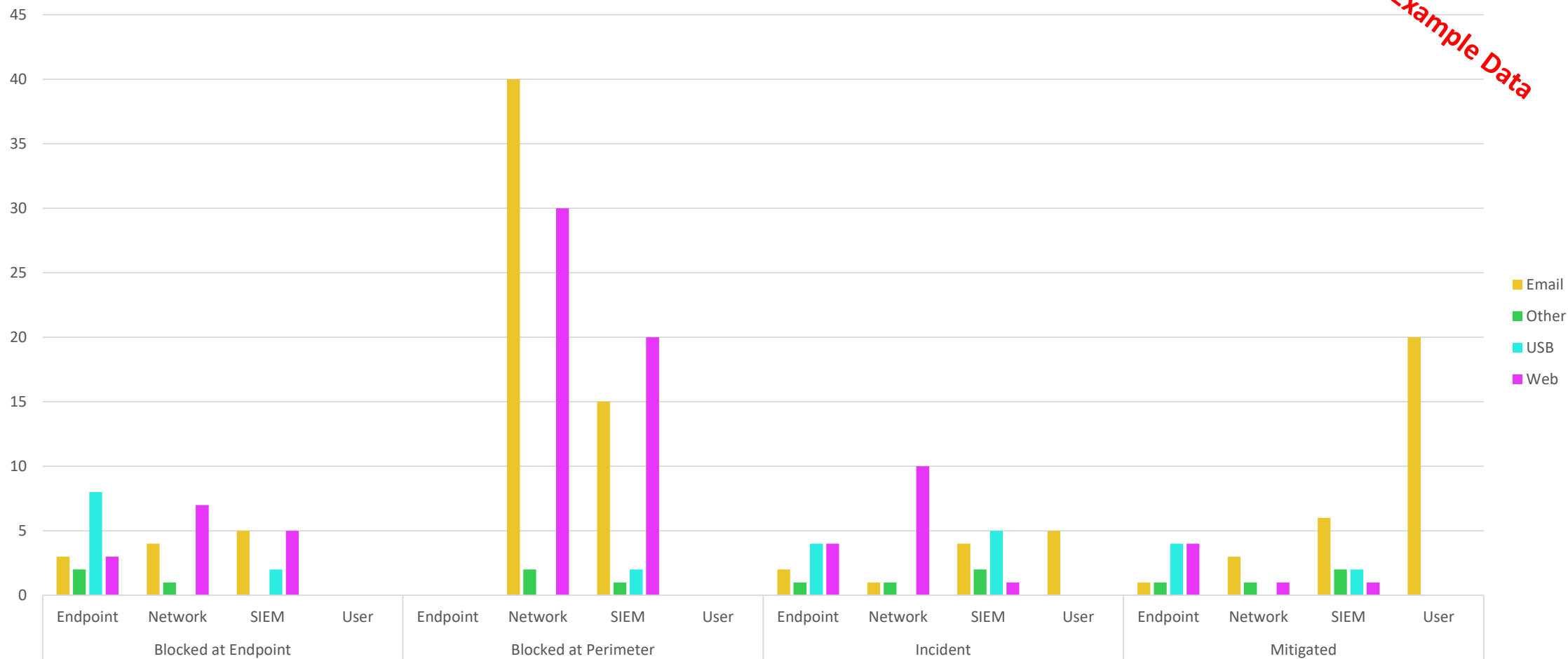


Highlights

- 33% increase in attacks detected in Q4 over Q1
- 50% fewer incidents in Q4 than Q1
- 18% of attacks mitigated before damage due to SOC action

Manager View: Detection efficacy by type of attacks

Success of Different Detection Methods for Attack Vectors



Example Data

Considerations for Effectiveness Metrics

The Good

- Can tell a good story demonstrating value for various teams or tools
- Helps drive focus to gaps and challenges that lead to incidents

The Challenges

- Counting 'attacks' that did not result in incidents can be very problematic
- Easy to get too technical for executives
- Good cost or business impact metrics require collaboration with the business

Example 3: Context metrics – Volume measurements



- Uses
 - Show growth over time
 - Articulate need to funding
- The Good
 - Help people understand your scale
 - Opportunity to show value of technology, processes, and people
- The Challenges
 - Be prepared to explain each tier in non-technical terms
 - Many layers are outside your control

RSA®Conference2019 **Asia Pacific & Japan**

Advanced Uses

Putting Metrics Together for Compelling Stories

Finding Opportunities to Automate - Before

Ticket type	Total tickets	Time in Investigation	
		Average Time in State	Total Time in State
Malware infection	5	6 hours	30 hours
Phishing email	50	3 hours	150 hours
Unauthorized software	15	2 hours	30 hours

Example Data

Look here for process improvements or automation opportunities

Automation prioritization factors to consider:

- Total time saved
- Level of effort to build
- Analyst satisfaction
- Error/inconsistency improvement

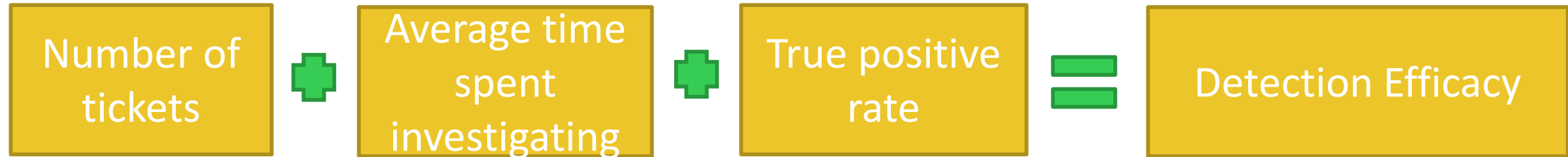
Finding Opportunities to Automate - After

Example Data

Ticket type	Total tickets	Time in Investigation - Before		Time in Investigation - After	
		Average Time in State	Total Time in State	Average Time in State	Total Time in State
Phishing email	50	3 hours	150 hours	1 hour	50 hours

- Measure the impact:
 - 66% reduction in time to investigate each ticket
 - 100 hours per month saved = 0.5 employees
- Other benefits:
 - X% reduction in ticket errors
 - Positive analyst feedback and increased job satisfaction
 - Y% increase in other investigations due to more time available
 - Z% decrease in dwell time, incident impact, etc.
- Bottom line: Articulate why having an automation tool or team pays for itself!

Measuring tool efficacy



- By detection source or signature, score the overall efficacy of the detection
- Uses:
 - Systematically identify technologies or signatures for tuning
 - Report on increases/decreases in overall efficacy to leadership
- This same methodology can be applied to evaluating a service provider

Final Thoughts

General Advice

- Start simple and build over time
- Start with a question first, then figure out how to measure it
- Be careful about corrosive metrics
- High quality data is required
- Combine metrics with anecdotes and examples to make briefings effective

For reference: Data Elements Required for these Metrics

- Investigation outcome
- Detection Source
 - Tool
 - Signature
- Attack Vector
- Workflow timestamps
- Ticket severity
- Investigation/incident type

Apply What You Have Learned Today

- Next week you should:
 - Identify your metrics consumers and what their concerns are
- In the first three months following this presentation you should:
 - Identify your proposed metrics
 - Define and refine processes and underlying data sets for metrics
- Within six months you should:
 - Pilot metrics calculation and initial trending

RSA[®]Conference2019
Asia Pacific & Japan

Thank You!

