RSAConference2019

San Francisco | March 4 – 8 | Moscone Center

BETTER.

SESSION ID: MLAI-W12

Build Intelligent Vulnerability Scoring to Optimize Security Residual Risks

Bill Chen

Chief Security Architect

Gyan Prakash

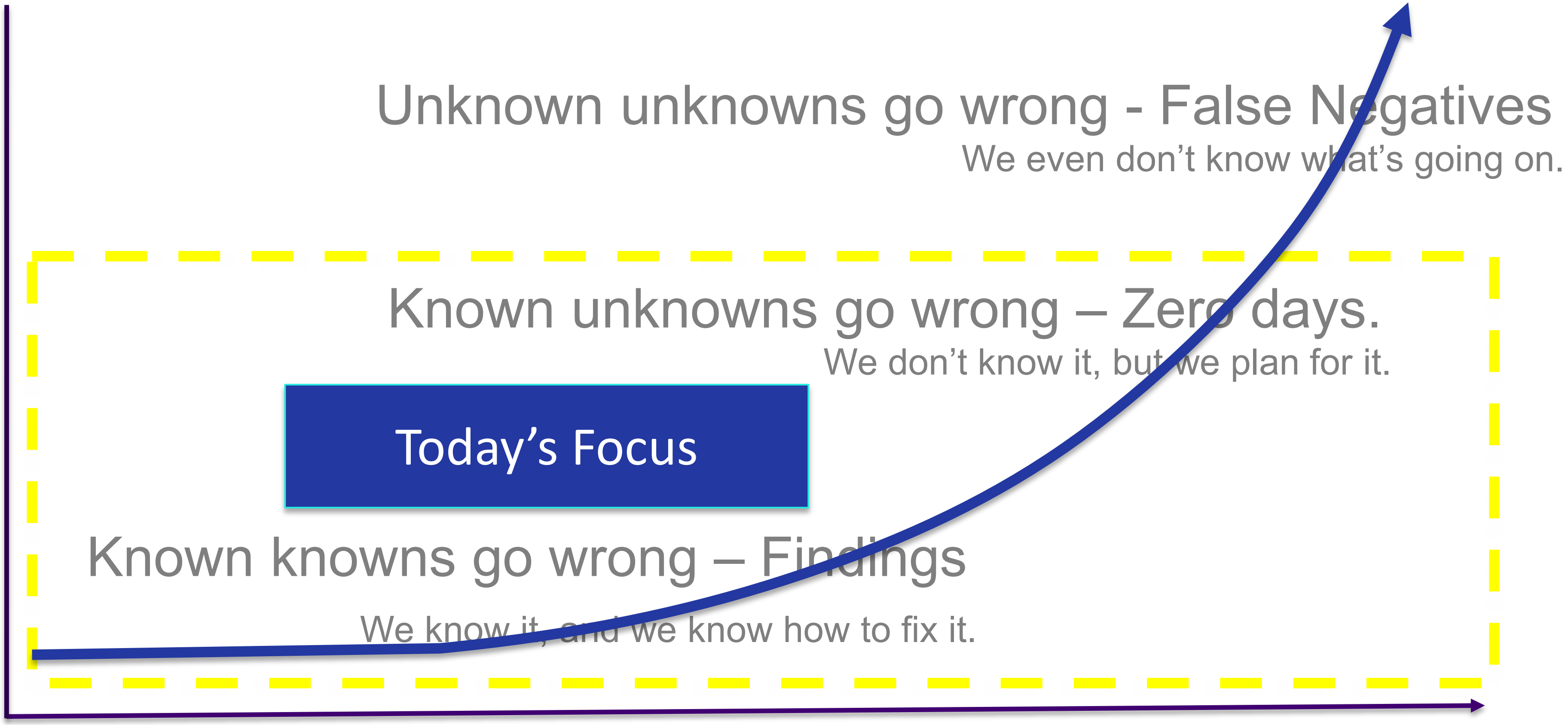
Chief Security Architect

#RSAC

Agenda

1. Ambiguity Effect – Risk Categories and Scope
2. Observations on Attack Pivot Patterns
3. Risk Anatomy - Where It Fails
4. Back to Simplicity
5. Existing Vulnerability Scoring Systems
6. Next Gen Intelligent Risk Management
7. Transforming Risk Management

Ambiguity Effect – Risk Categories & Scope



Unknown unknowns go wrong - False Negatives

We even don't know what's going on.

Known unknowns go wrong – Zero days.

We don't know it, but we plan for it.

Today's Focus

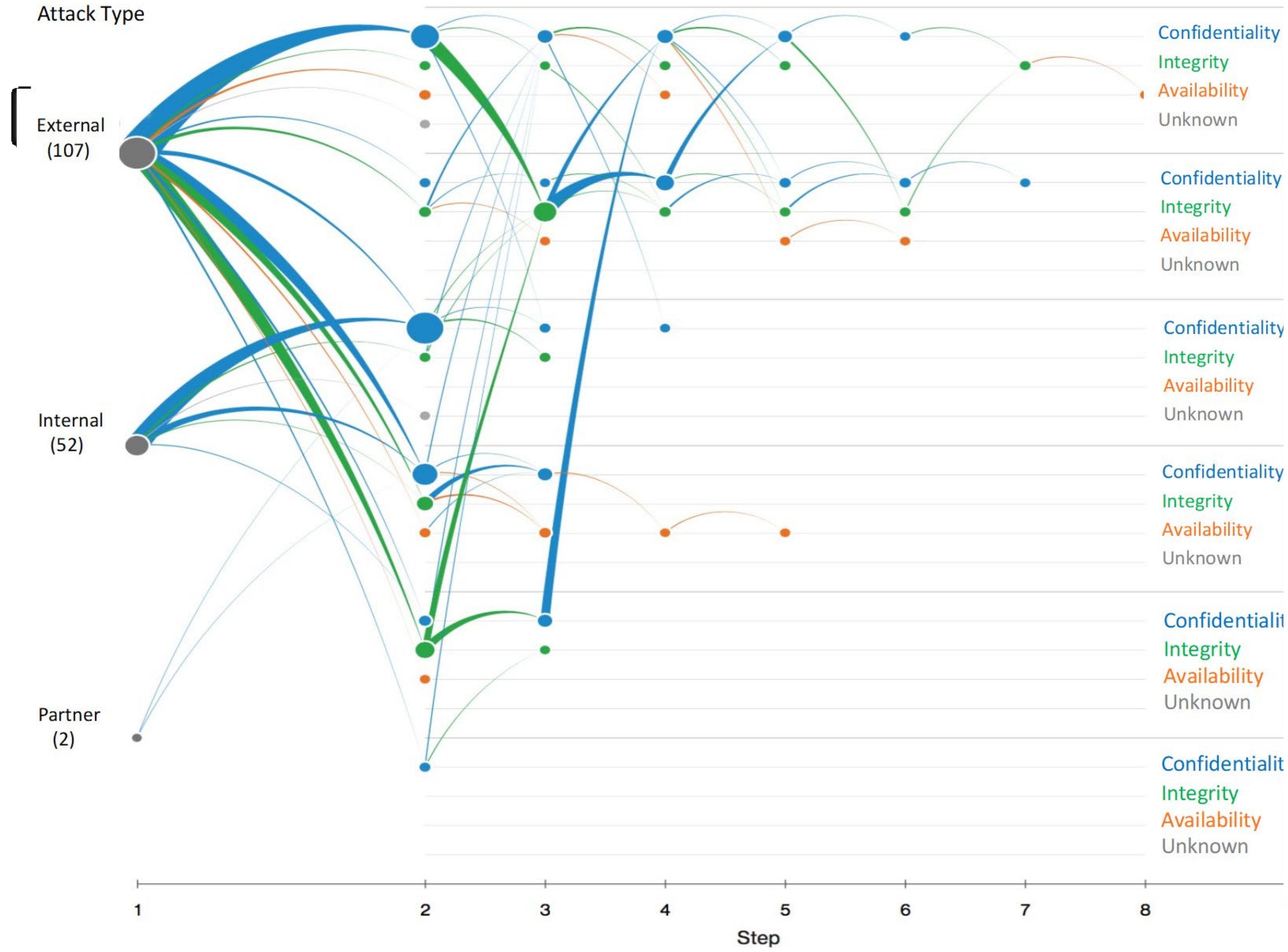
Known knowns go wrong – Findings

We know it, and we know how to fix it.

"Anything that can go wrong will go wrong."   - Murphy's Law

2018 - Successful Attack Pivot Patterns*

Over 53,000 incidents and 2,216 confirmed data breaches in 2018



48% Hacks/OWASP Top 10

30% Malware/Bots

17% Errors

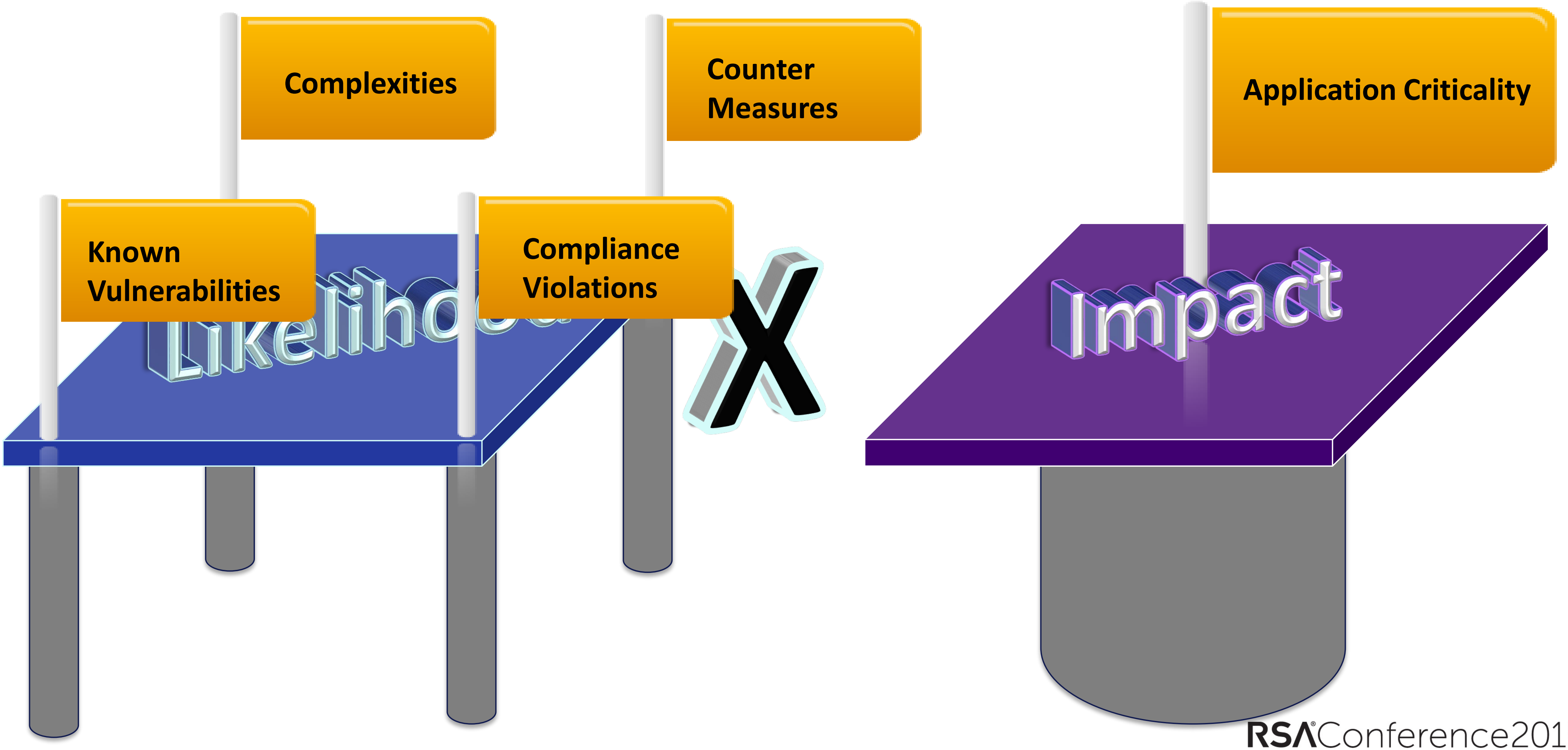
17% Social Attacks

12% Privilege Misuse

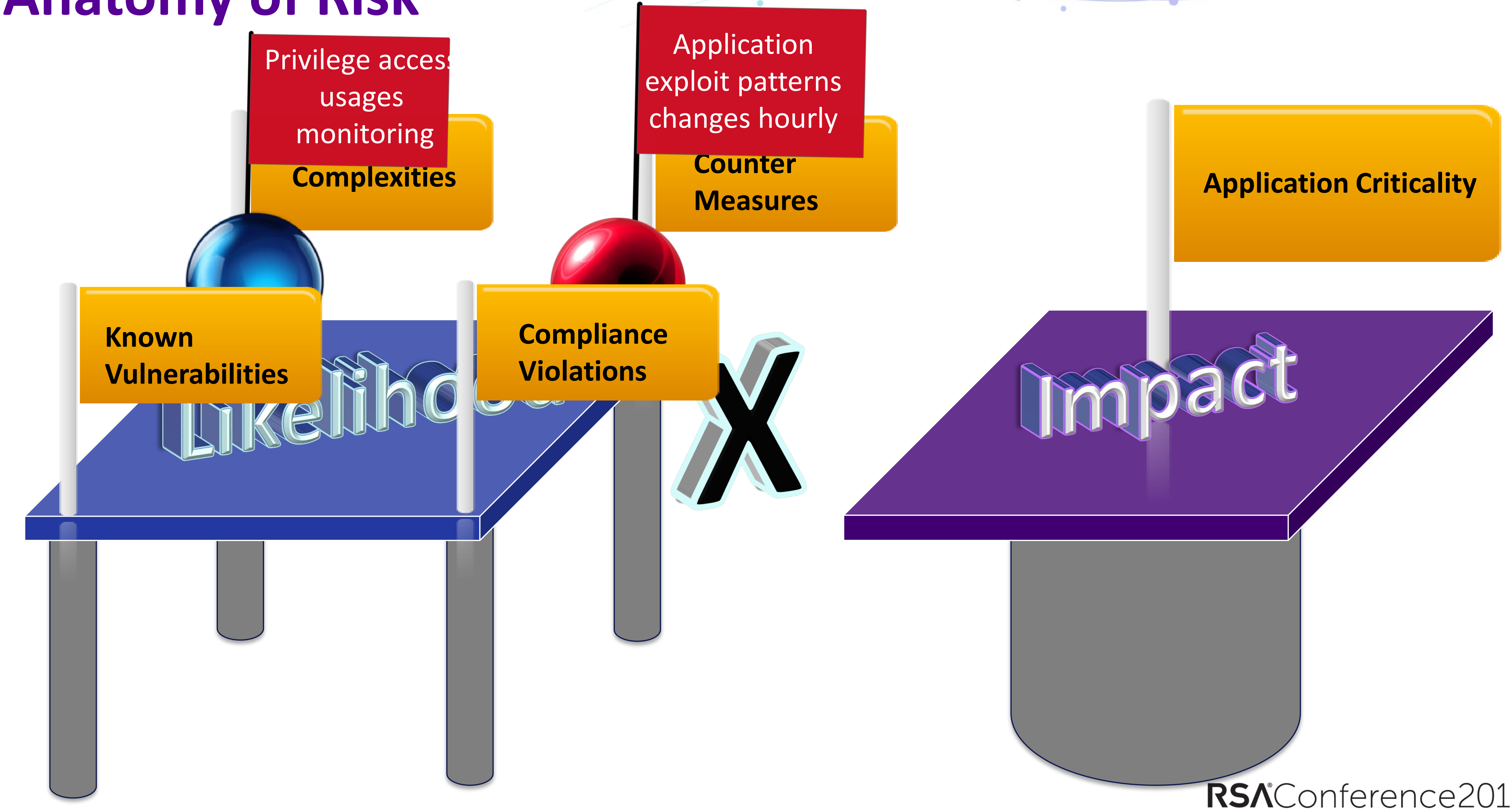
11% Physical Attacks

* *Source: Verizon Data Breach Report, 2018.*

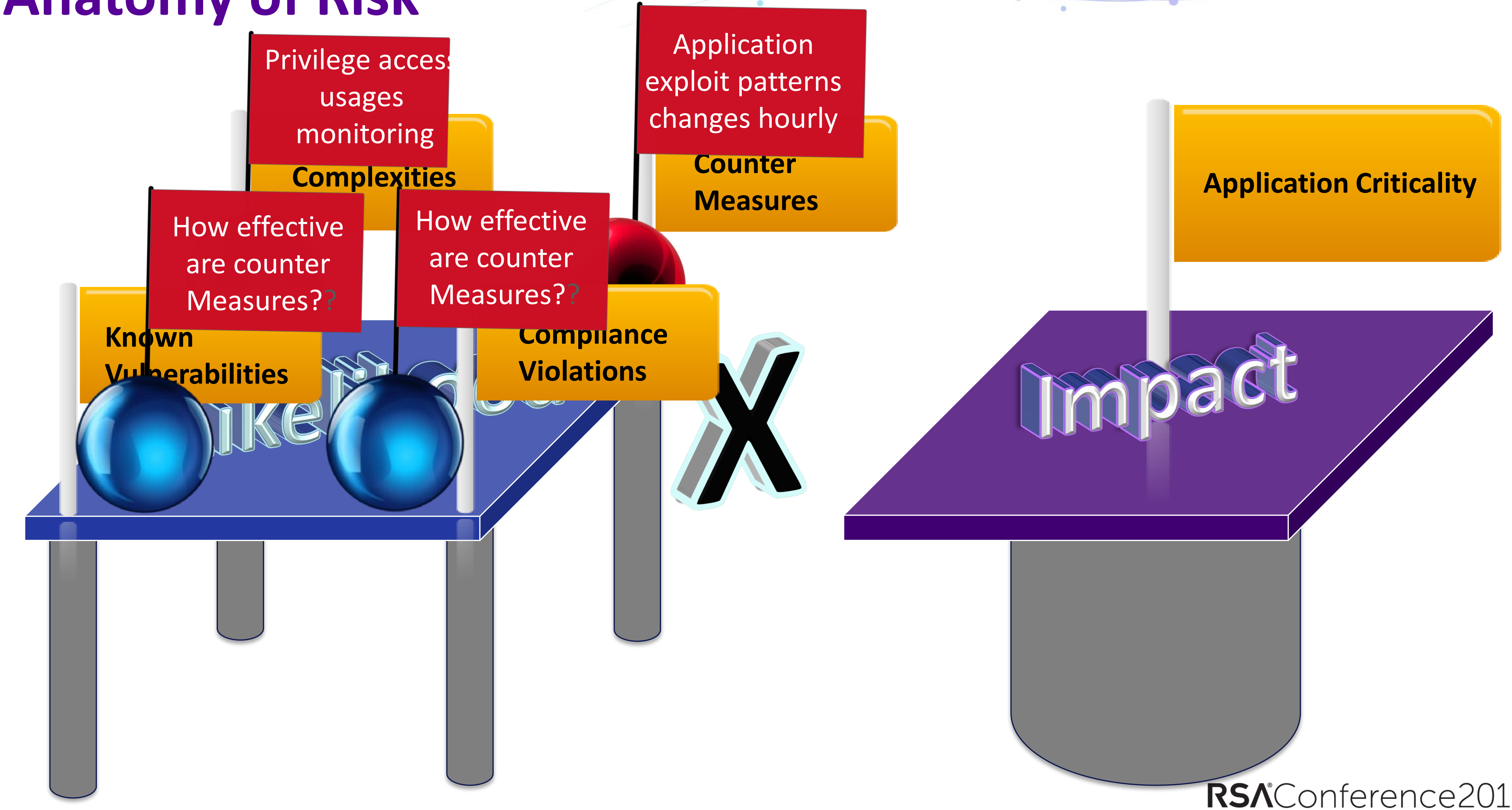
Anatomy of Risk



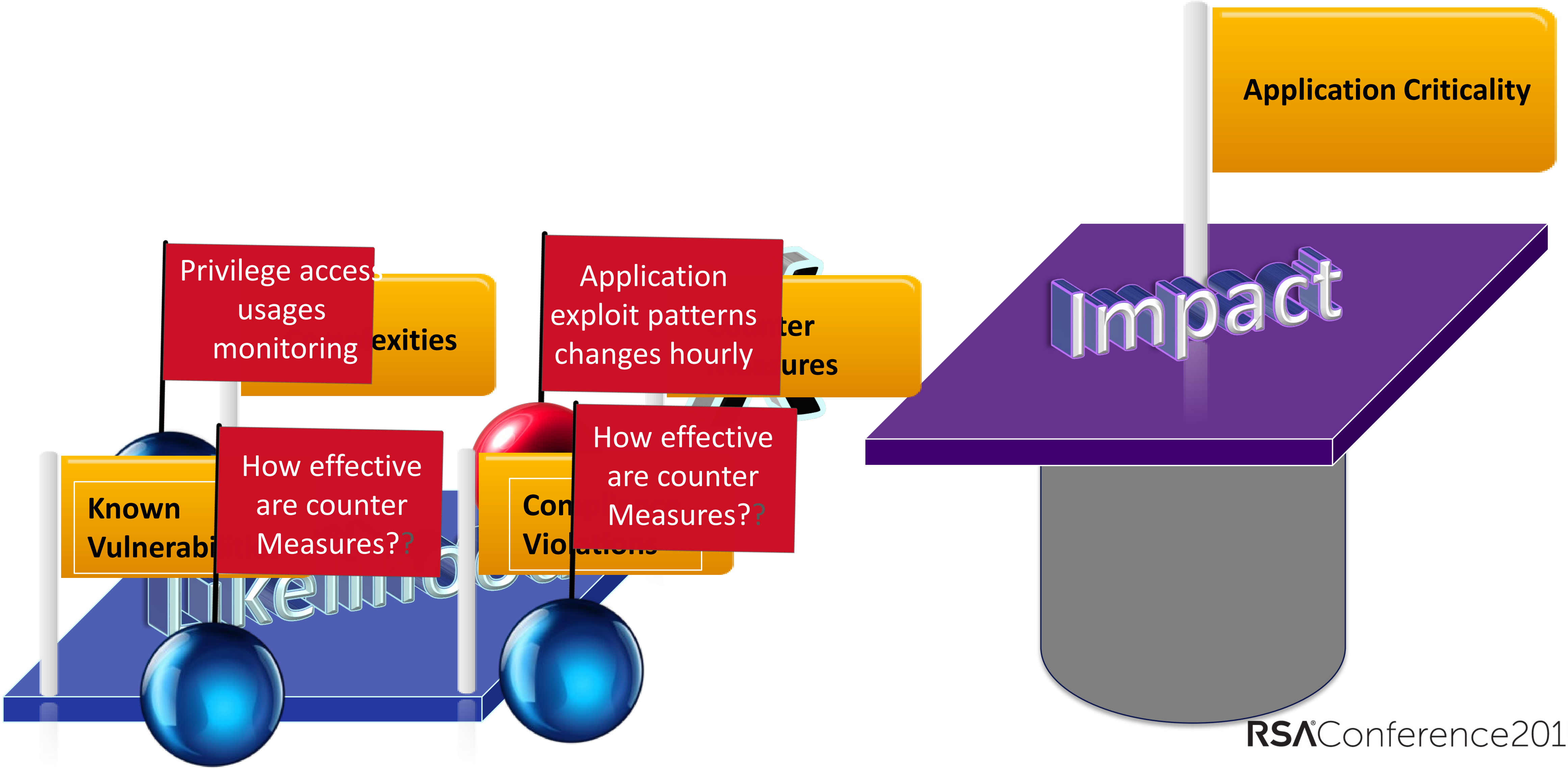
Anatomy of Risk



Anatomy of Risk


Privilege access usages monitoring
Complexities
Application exploit patterns changes hourly
Counter Measures
How effective are counter Measures??
How effective are counter Measures??
Known Vulnerabilities
Compliance Violations
Likelihood
X
Application Criticality
Impact

Subjective Ambiguity


Application Criticality
Impact
Privilege access usages monitoring
exities
Application exploit patterns changes hourly
ter
ures
Known Vulnerabi
How effective are counter Measures??
Con
Violations
How effective are counter Measures??
Likelihood

Subjective to Objective

Known Vulnerabilities

- Static Code Testing
- Dynamic Testing
- Design Vuln.
- Pen Testing

Risk = **Likelihood** x Size of Loss

$$\boldsymbol{Likelihood} = (vd) * (RTv\ ) * (\text{Compliance Violations}) * (\text{Config Violations})$$

$$\boldsymbol{Vd = Vulnerbility\ Density} = \left(\frac{\textbf{Total known Vulnerability}}{\textbf{Size of Software}}\right)$$

$$\textbf{RTv = RunTime Vuln.} = \left(\frac{\textbf{\# Failed Applications Attacks 24 hrs}}{\textbf{Total Traffic Volume in m per 24 hrs.}}\right)$$

$$\textbf{Compliance Violations} = \left(\frac{\textbf{Failed Complaince Requirements}}{\textbf{Total Compliance Requirements}}\right)$$

$$\textbf{Ops Violations} = \left(\frac{\textbf{Configurations Violations}}{\textbf{Total Servers}}\right)$$

Known Unknown

- Open Source Vuln
- NW & Infra Scans
- Configurations Scans
- Daily Attack Pattern

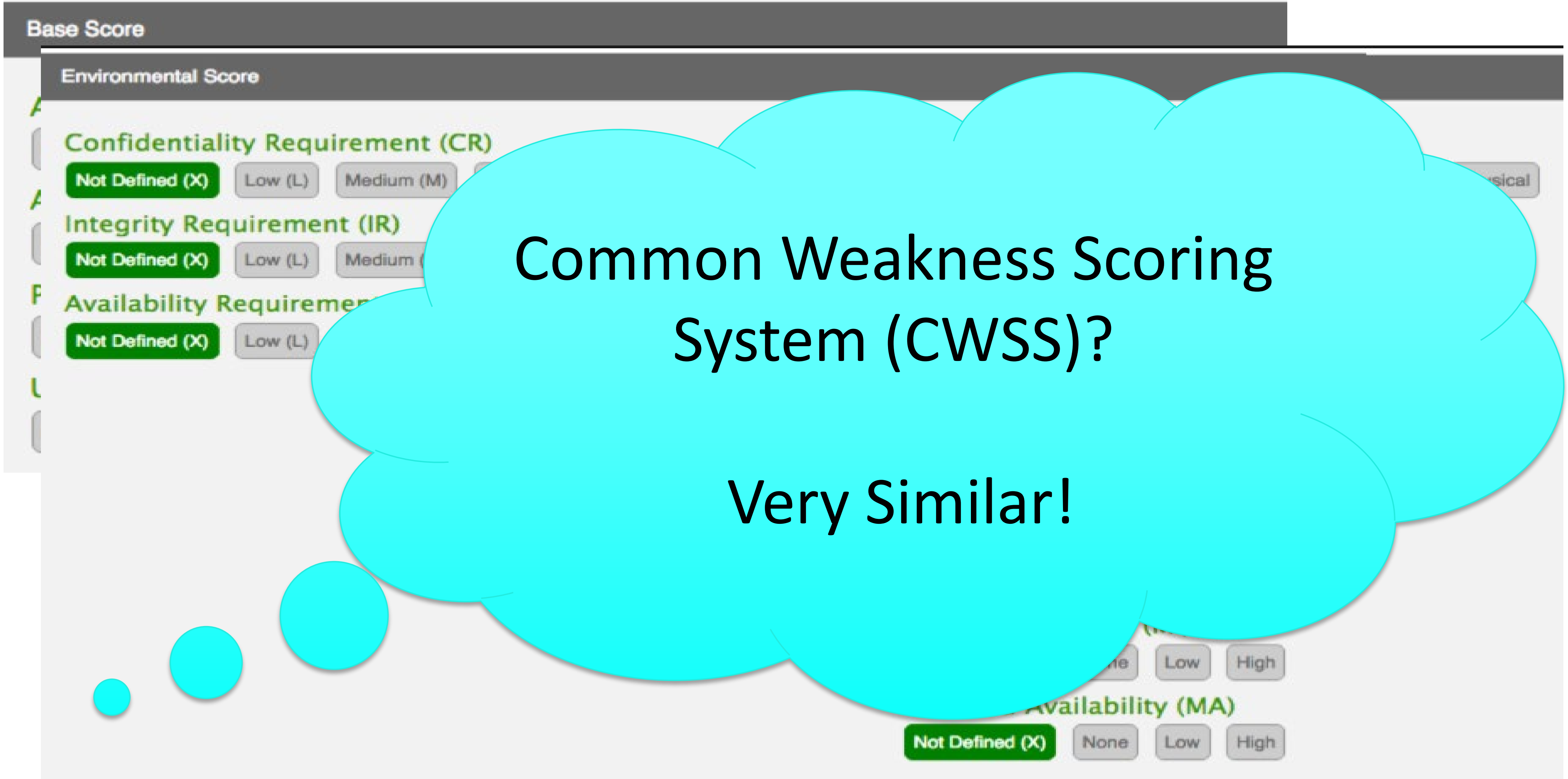
Back to Simplicity

It’s all about prioritization.

It is about sorting a list of findings.

In the end of the day, it is all about the ability to compare the risk of any two vulnerabilities.

Existing Vulnerability Scoring Systems



Base Score

Environmental Score

Confidentiality Requirement (CR)

Not Defined (X) | Low (L) | Medium (M) | ...sical

Integrity Requirement (IR)

Not Defined (X) | Low (L) | Medium (

Availability Requiremen

Not Defined (X) | Low (L)

...ne | Low | High

...vailability (MA)

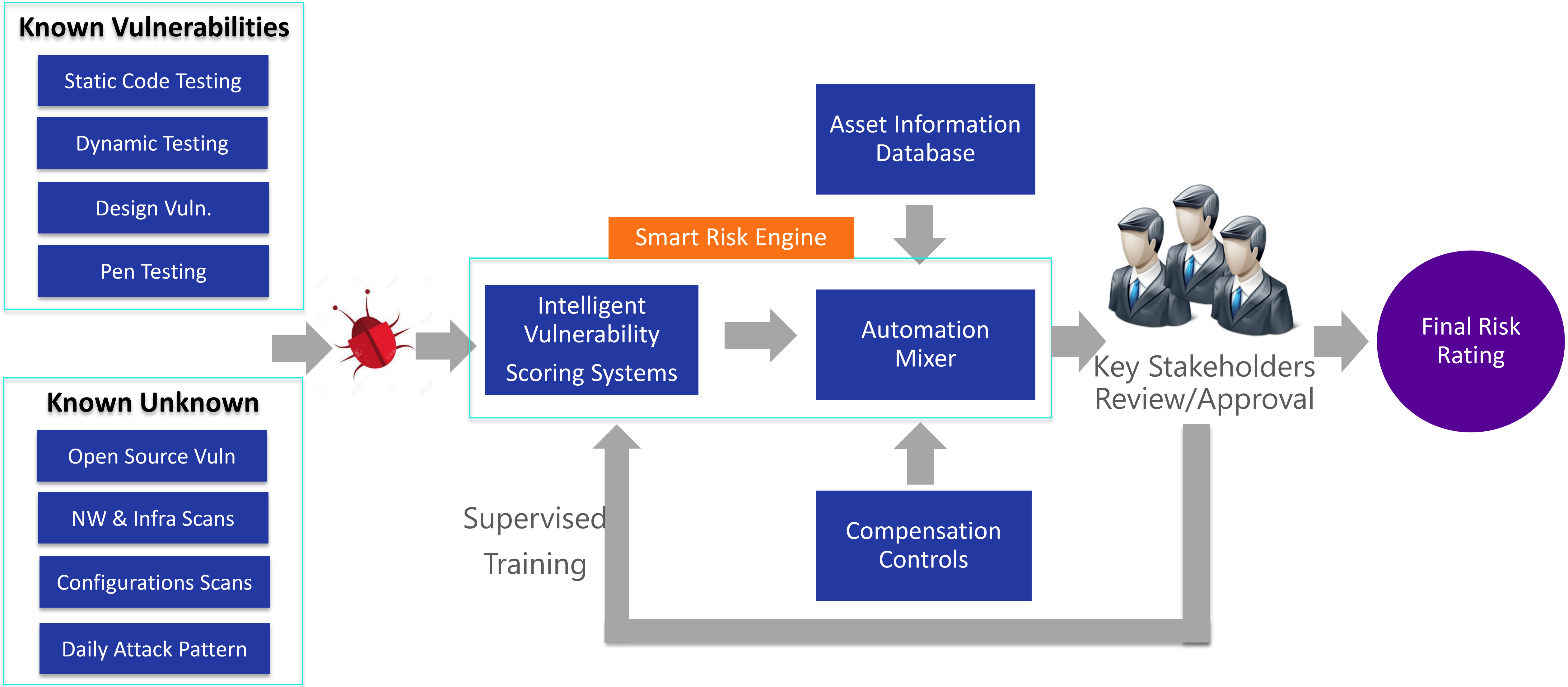
Not Defined (X) | None | Low | High

Common Weakness Scoring System (CWSS)?

Very Similar!

* https://www.first.org/cvss

Next Gen Intelligent Risk Management



Known Vulnerabilities

- Static Code Testing
- Dynamic Testing
- Design Vuln.
- Pen Testing

Known Unknown

- Open Source Vuln
- NW & Infra Scans
- Configurations Scans
- Daily Attack Pattern

Smart Risk Engine

Intelligent Vulnerability Scoring Systems

Asset Information Database

Automation Mixer

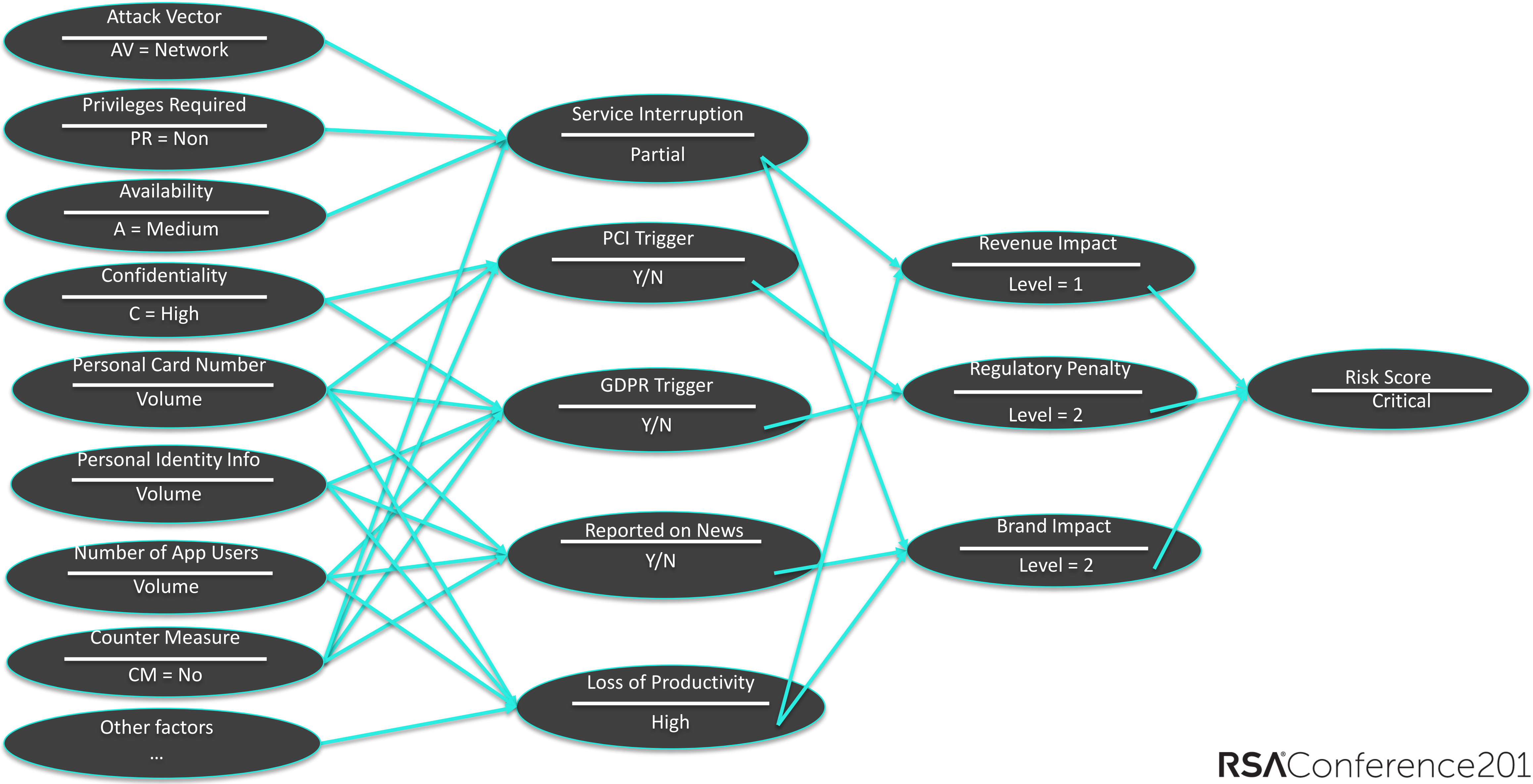
Compensation Controls

Supervised Training

Key Stakeholders Review/Approval

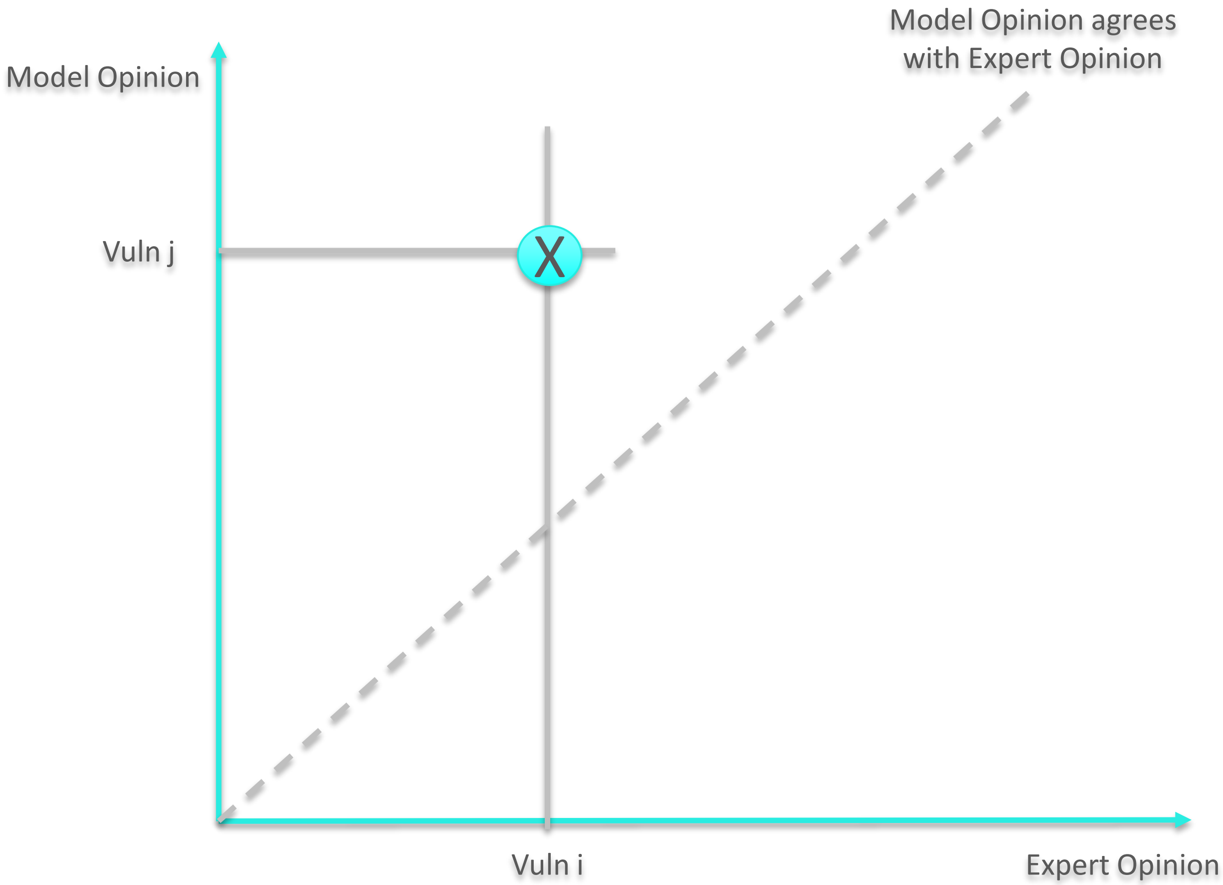
Final Risk Rating

Bayesian/Neural Networks for Vulnerability Scoring



Cost Function

- Prioritizing is a sorting problem
- Pairwise comparison from Expert Opinion to Model Prediction *



If Expert says Vuln i is more sever than Vuln j, but The prediction model says the reverse, then it is counted as a clash

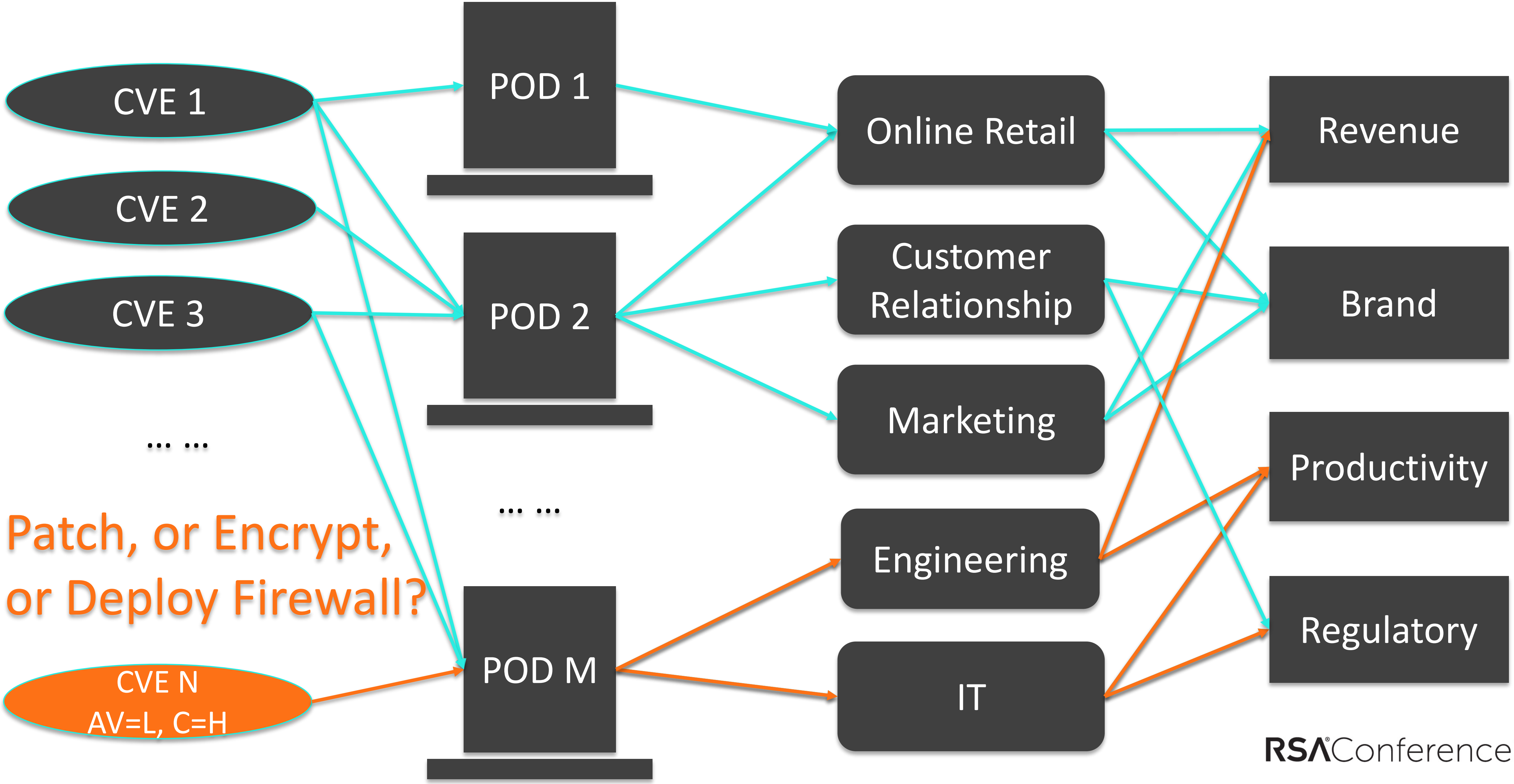
Model Performance

Accuracy of prediction
= Number of agreements/Total Number of comparisons

In the sampled training set.

** Bill Chen, “Software Security Economics and Threat Modeling Based on Attack Path Analysis”, PhD Dissertation, USC, 2007*

Estimate ROI of Security Investment with Result Chain



Patch, or Encrypt, or Deploy Firewall?

Transforming Risk Management

Today		Next Gen Risk Management
Subjective	→	Objective
Non repeatable	→	Repeatable
Lack of technical traceability	→	Exactly traceable to specific vulnerabilities
Focus on rating every finding	→	Focus on scoring model training & calibration
One rating fits a year	→	Real time risk profile based on findings, alerts, and mitigation implementation status

Q&A