RSAConference2020

San Francisco | February 24 – 28 | Moscone Center

HUMAN ELEMENT

SESSION ID: PART1-T12

Machine Learning And Risk Quantification Across A Converged Attack Surface

Kevin Flynn

Sr. Product Manager
Tenable

Sound Familiar?

Security Engineer

VM gives me good info, but I've got 100 other tools to manage and implement – And no one's patching anything anyway.

CISO

All these vulnerabilities every month make it look like my team isn't doing any work!
I need better data!

SysAdmin / DBA

Stop giving me 12,000 page reports on patching things I can't patch. Things will break! Stop telling me how to do my job!

CIO

Manage more tools, give more access, deploy more appliances. It never ends and my team is already overwhelmed!

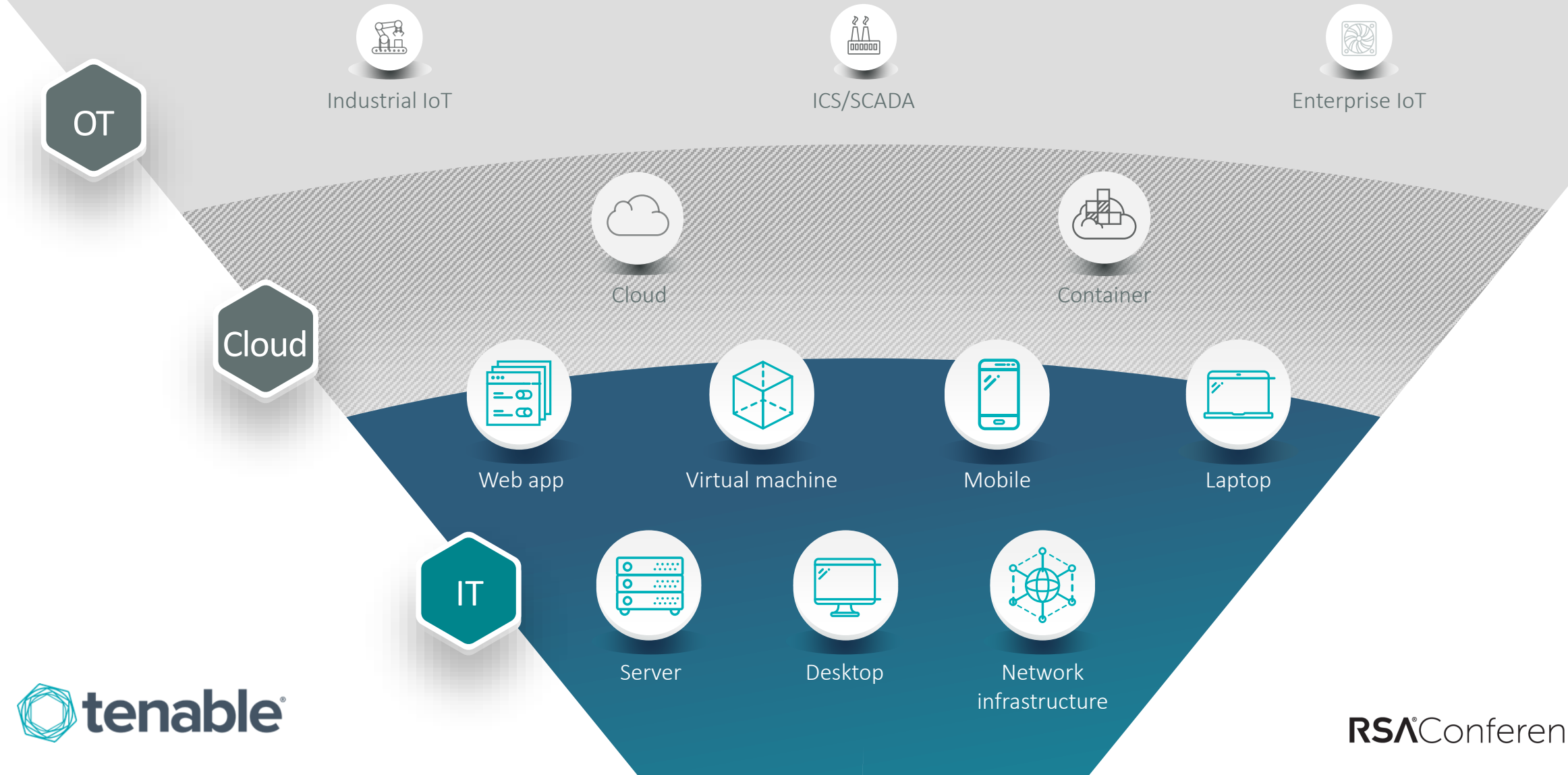
CFO

We can't afford a data breach, but the security team keeps asking for more money, and I have no idea if it's helping or not.

Developers

I always write secure code. We don't need anymore security tools slowing everything down. Just going to ignore all of that.

The Attack Surface Is Expanding & Converging Creating A Cyber Exposure Gap



tenable

RSAConference2020

RISK QUANTIFICATION

When business leaders ask

“HOW SECURE ARE WE?”

They don’t want a 300 page answer


METRICS ARE THE ROSETTA STONE
OF BUSINESS COMMUNICATION

METRICS ARE THE ROSETTA STONE OF BUSINESS COMMUNICATION

"Successful leaders will enjoy better performing tools to assess and understand where an enterprise's cyber security practices are working effectively, ***including more accurate and descriptive company-wide security metrics and ratings.****"*

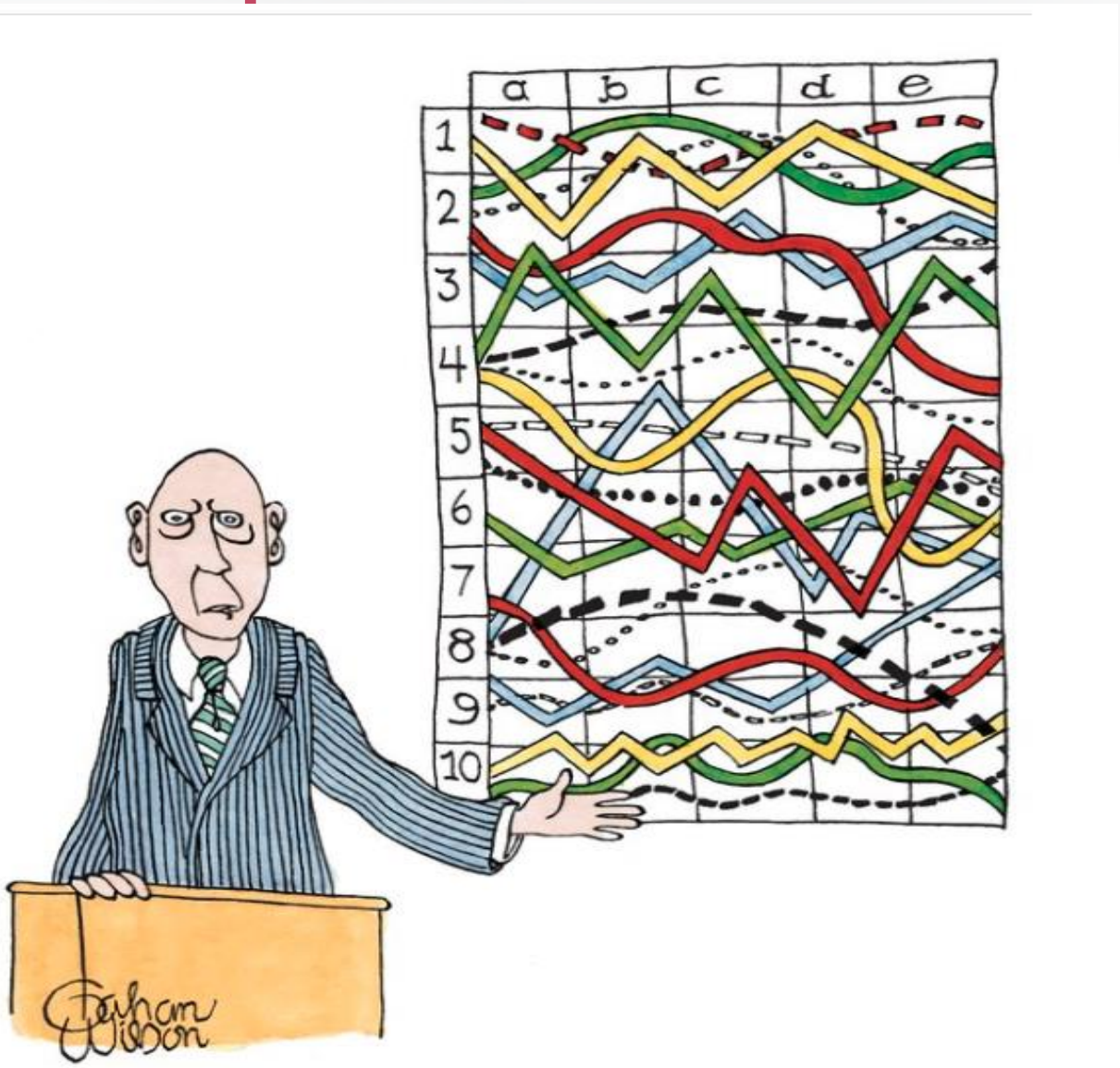
- Why 2020 Is A Turning Point For Cyber Security. January, 2020

WORLD ECONOMIC FORUM

Risk Quantification: Five Key Questions

tenable

Keep The Answers Simple



"I'll pause for a moment so you can let this information sink in."

We've Got A Problem

- 17,300 new vulnerabilities in 2019
- 47 every single day
- 235 while we're at RSA
- 2 in the hour we're sitting here

If Everything Is Important – Nothing Is!

CVSS: High/Critical = 59%

"CVSS is designed to identify the technical severity of a vulnerability. What people seem to want to know, instead, is the risk a vulnerability or flaw poses to them, or ***how quickly they should respond to a vulnerability***."

TOWARDS IMPROVING CVSS
SOFTWARE ENGINEERING INSTITUTE | CARNEGIE MELLON UNIVERSITY
December 2018


WE'RE GONNA NEED
A BIGGER BOAT.

AI? Machine Learning?

ARTIFICIAL INTELLIGENCE

"Artificial intelligence is the science and engineering of making computers behave in ways that, until recently, we thought required human intelligence."

~ Andrew Moore

Dean of the School of Computer Science:
Carnegie Mellon University

MACHINE LEARNING

"Machine learning is the study of computer algorithms that improve automatically through experience."

~ Tom M. Mitchell

Fmr Chair - Machine Learning Department:
Carnegie Mellon University

Chihuahua or Muffin?

Detect Patterns → Create Model → Make Predictions

Machine Learning & Risk Quantification

Traditional

Rules (CVSS Scoring)

+

Data

= Answers

Machine Learning

Answers (Attacked Vulns)

+

Data

= Rules

Risk Management Approaches

Business System Risk

Focus First On
What Matters Most:
Assets + Vulns

+

Process Integrity Risk

Am I Smart Or Lucky?
Assessment Breadth, Depth
& Frequency

Poor Process Risk Management Is All Too Common

Only **5%** of enterprises follow the **Diligent style** and are at a higher level of maturity, displaying a high assessment frequency, comprehensive asset coverage, and targeted, customized assessments.

43% follow the **Investigative style**, indicating a medium to high maturity. These display a good scan cadence, leverage targeted scan templates, and authenticate most of their assets.

19% of enterprises follow the **Surveying style**, placing them at a low to medium maturity. Surveyors conduct broad scope assessments, but with little authentication and little customization of scan templates.

33% of enterprises are at a low maturity, following the **Minimalist style** and conducting only limited assessments of selected assets.

Cyber Defenders Strategy Report: Tenable Research

RSAConference2020

Taking A Predictive Approach

Predictive Prioritization

Leverage threat, vulnerability and asset information to predict likelihood a vulnerability will be exploited in near future.

Predictive Prioritization In Action

"Top 20 Vulnerabilities To Patch"

DARKReading

December 23, 2019

CVSS vs VPR Scores:

- 3 rated as Critical by CVSS
- 8 rated Critical by Predictive Prioritization

Vulnerabilities list based on number of times exploited by sophisticated cyber-attack groups.

CVE	CVSS Score	Predictive (VPR)
CVE-2017-11882	7.8	9.9
CVE-2018-8174	7.5	9.9
CVE-2017-0199	7.8	9.9
CVE-2018-4878	9.8	9.9
CVE-2017-10271	7.5	7.4
CVE-2019-0708	9.8	9.8
CVE-2017-5638	10.0	10.0
CVE-2017-5715	5.6	8.3
CVE-2017-8759	7.8	9.9
CVE-2018-20250	7.8	9.8

Predictive Impact

Predict criticality of asset to the business via indicators of importance – ex. mission critical service or asset location.

Place Context On Risk Probabilities

- If it **doesn't** rain on Thursday, is prediction wrong?
- What if it **does** rain on Saturday?
- What if I'm planning an outdoor wedding for Saturday?

Taking Action

Prediction

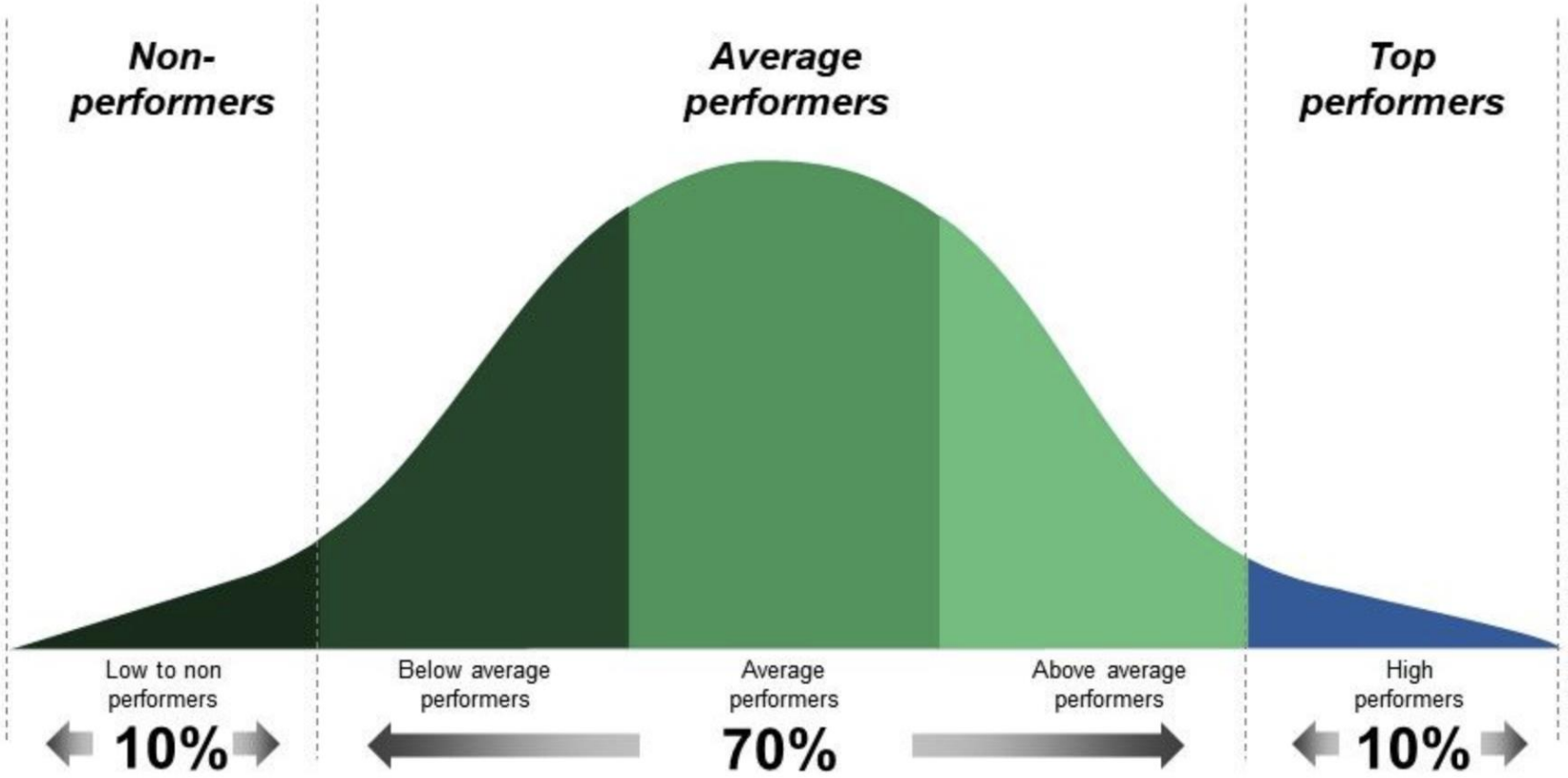
+

Judgement

=

Action

Benchmarking
Context - Peer Comparisons For Strategic Decision Support



Industry, Regions, Asset Types, BU's

“Apply” What We We’ve Discussed

- Immediate Actions:
  - Take a Risk Based Approach:
    Identify Business System and Process Integrity Risks
  - Establish metrics for the ‘five key questions’
- In three months:
  - Implement process changes
  - Benchmark internally and begin benchmarking externally

RSAConference2020

Thank You