RSAConference2019
San Francisco | March 4–8 | Moscone Center

SESSION ID: SPO2-R09

Cyber Risk Management: New Approaches For Reducing Your Cyber Exposure

Kevin Flynn

Sr. Product Marketing Manager
Tenable

Predictions: Intuition & Luck

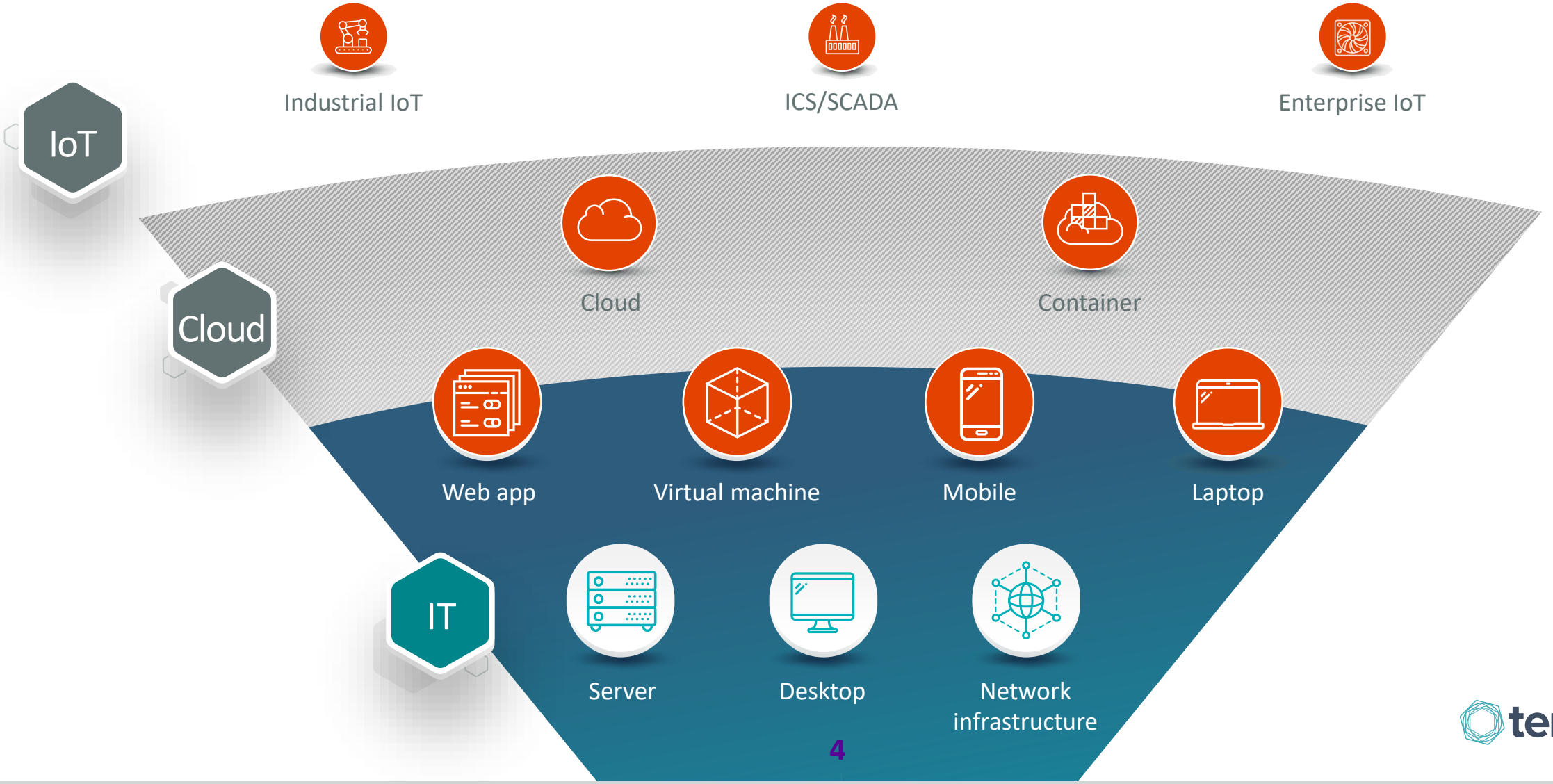
Predictions: Modeling & Data

The Washington Post

The amazing improvements in winter weather forecasting since the 1970s

"like comparing television resolution in 1960 to 4k-flat screen models that are available today"
- February 3, 2017

The Cyber Exposure Gap



tenable

The Four Key Questions

Where are we exposed?

Where should we prioritize based on risk?

How are we reducing exposure over time?

How do we compare?

Manual Processes Are A Barrier

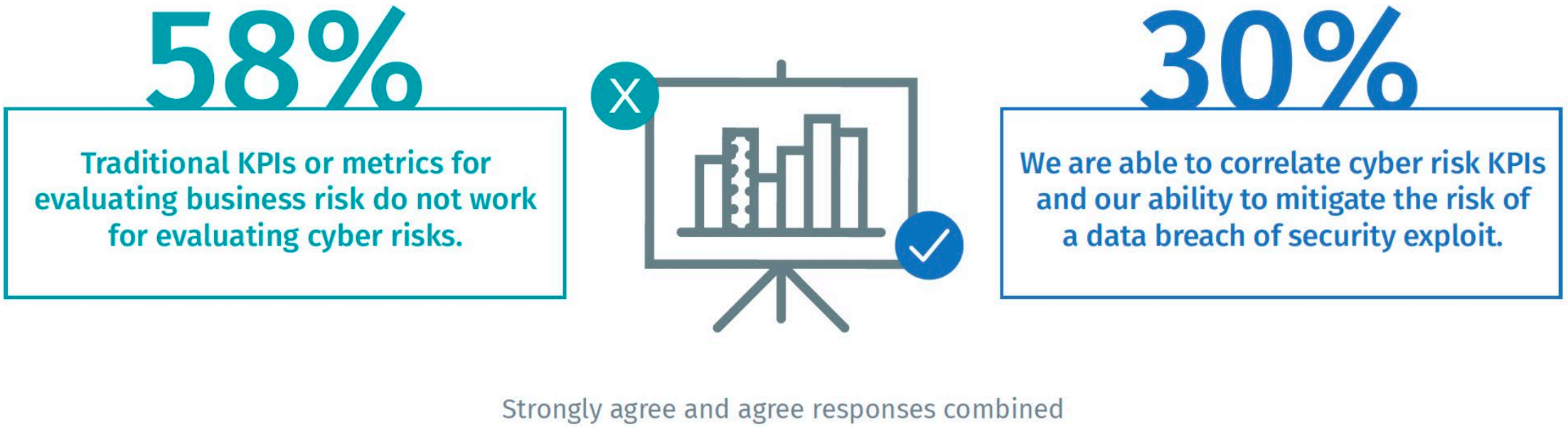
Figure 5. Perceptions about responding to vulnerabilities and threats

Strongly agree and agree responses combined

Ponemon Institute, Dec 2018

New Approaches To Measuring Cyber Risks Are Needed

Figure 7. Perceptions about KPIs

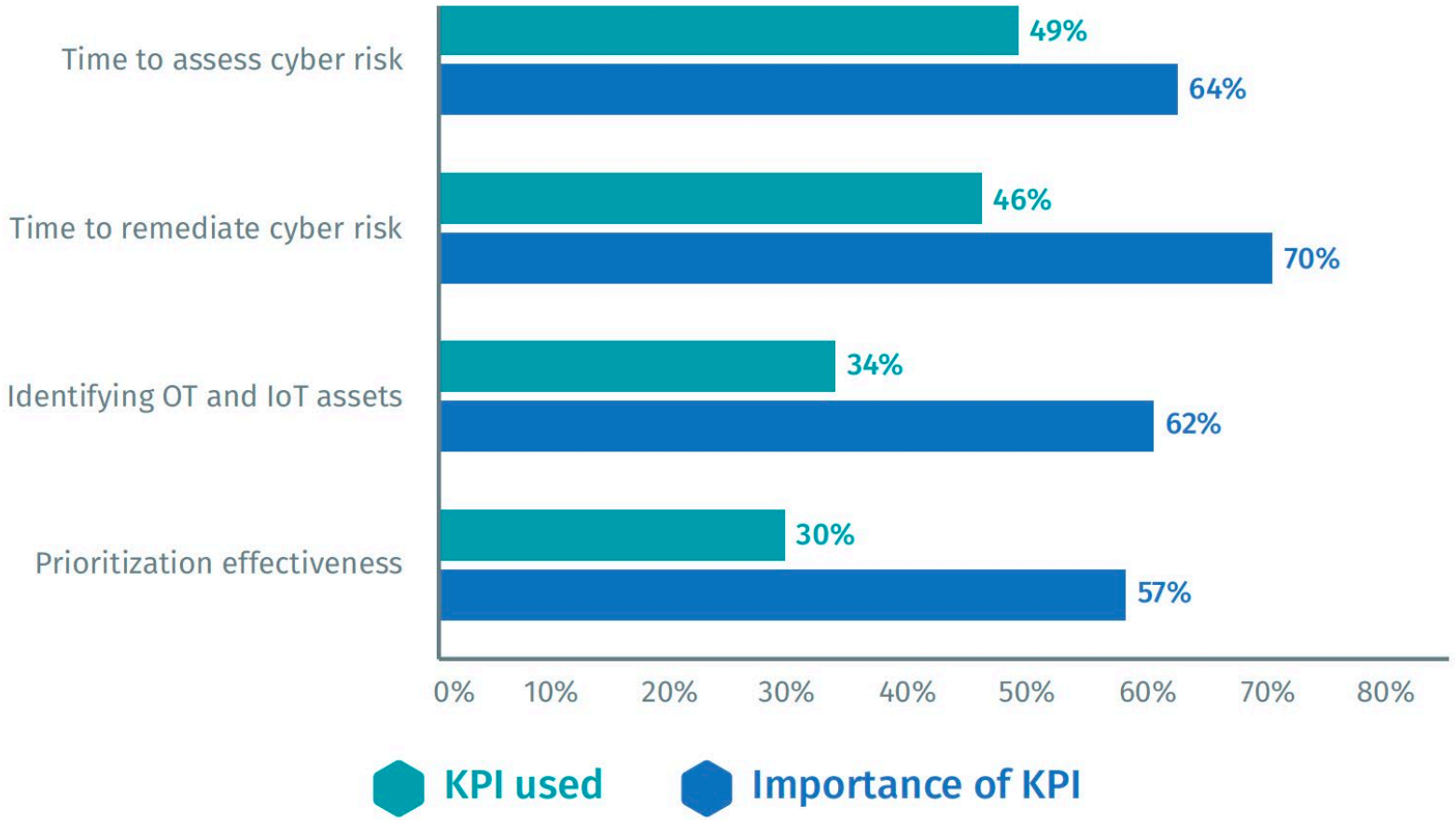


Ponemon Institute, Dec 2018

Important KPIs Are Not Being Used

Figure 10. Gap in the use and importance of KPIs

Yes responses and Very important and essential responses presented

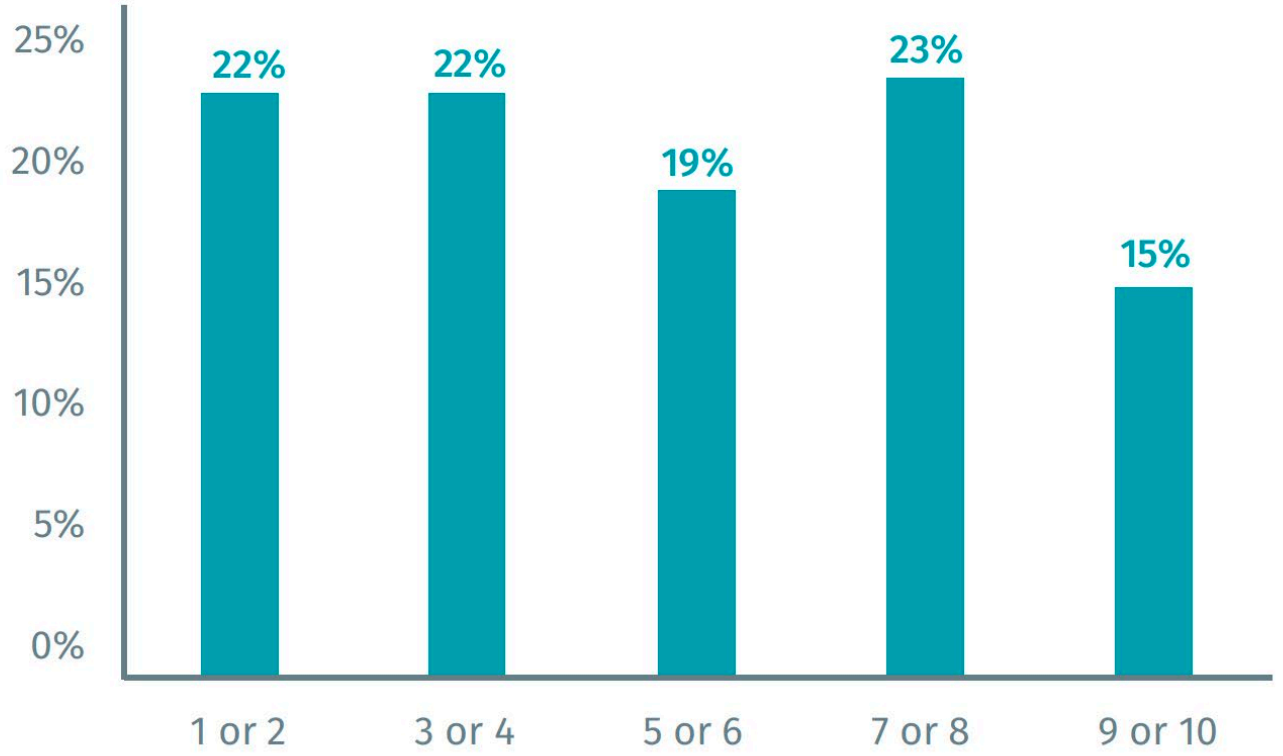


Ponemon Institute, Dec 2018

Most Are Not Accurately Measuring Cyber Risk

Figure 9.
How accurate is your organization in measuring the business costs of cyber risk?

On a scale of 1 = not accurate to 10 = very accurate



As shown in Figure 9, only

38%

of respondents believe their measures are very accurate
(23 percent + 15 percent)

Ponemon Institute, Dec 2018

A Better Way

Deal With Vulnerability Overload

16,500

VULNERABILITIES DISCLOSED IN 2018

7%

of vulnerabilities had an exploit available

63%

of vulnerabilities discovered in environments are CVSS 7+

12%

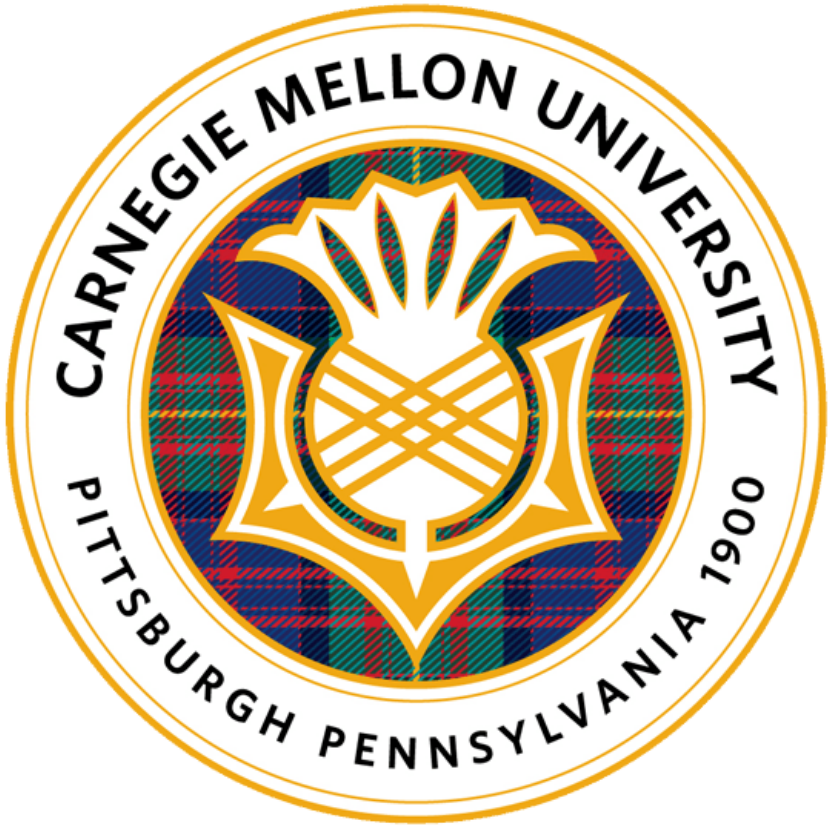
of vulnerabilities disclosed in 2018 were CVSS 9+

If Everything Is Important – Nothing Is

CVSS SCOREs
59% - CRITICAL/HIGH

CVSS – shortcomings

"CVSS is designed to identify the technical severity of a vulnerability. What people seem to want 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

Needles In The Haystack

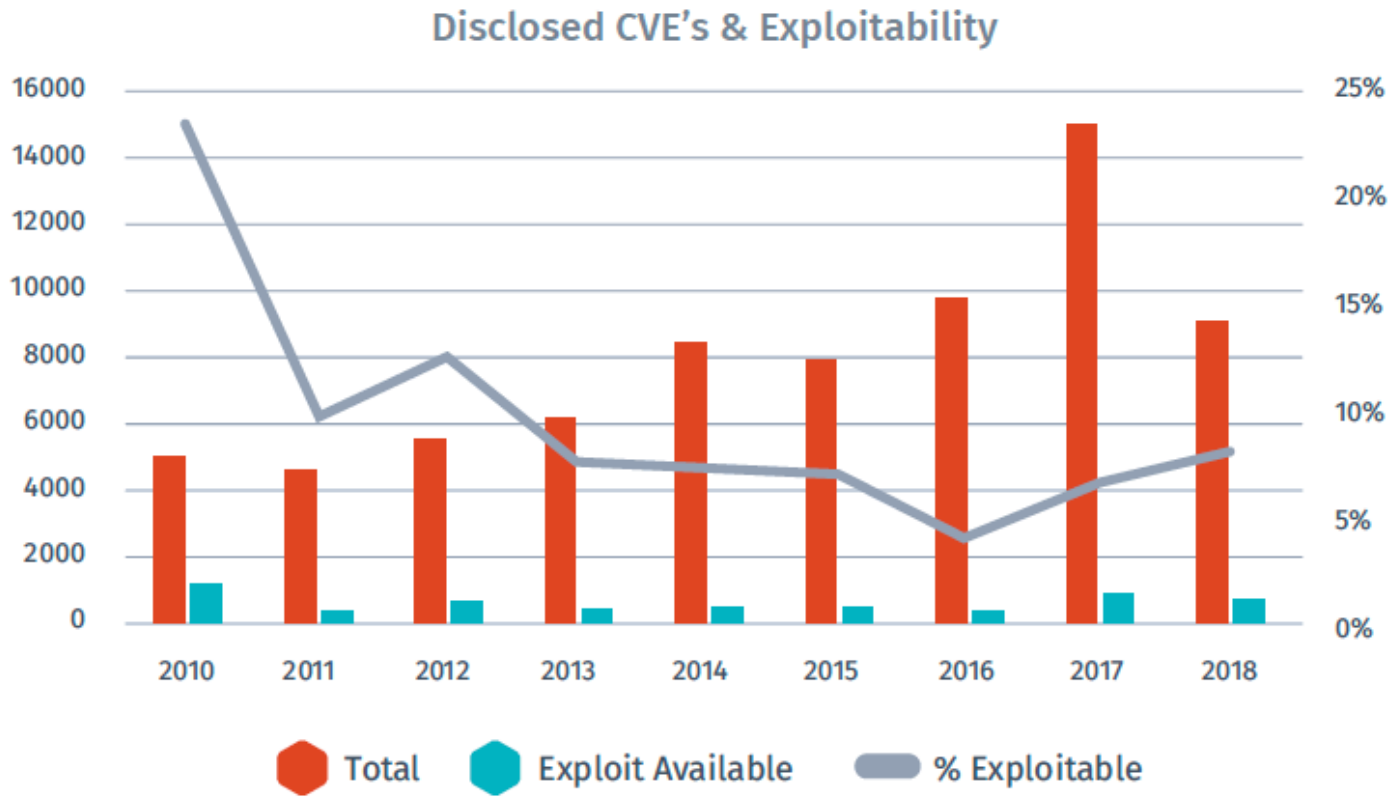
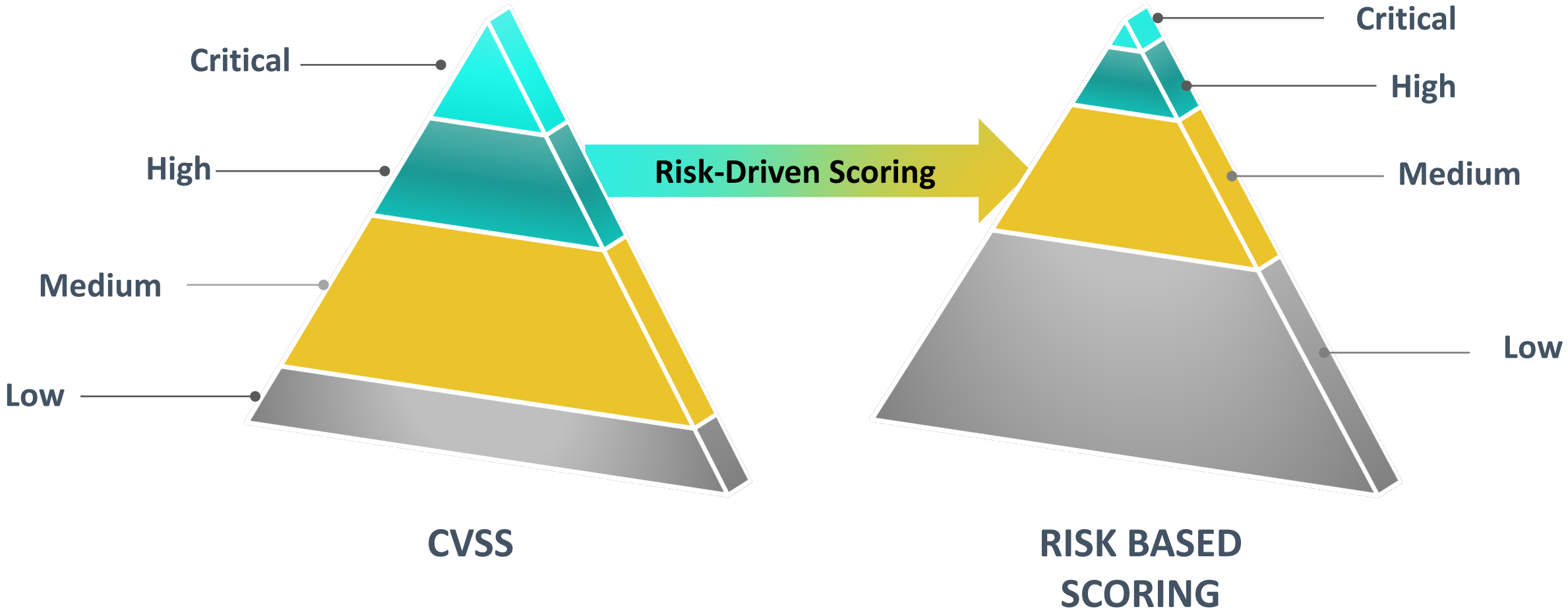


Figure 3. Total CVEs vs. exploitable CVEs

- Approximately 1,500 exploitable vulnerabilities were published in 2018
- Just over 28 exploitable vulnerabilities every week.

Prioritization Is Critical



Reducing The Burden

Research Insights

Data science based analysis of over 100,000 vulnerabilities to differentiate between the real and theoretical risks vulnerabilities pose

Vulnerability Score

The criticality, ease of exploit and attack vectors associate with the flaw.

Threat Intelligence

Insight into which vulnerabilities are actively being exploited by both targeted and opportunistic threat actors.

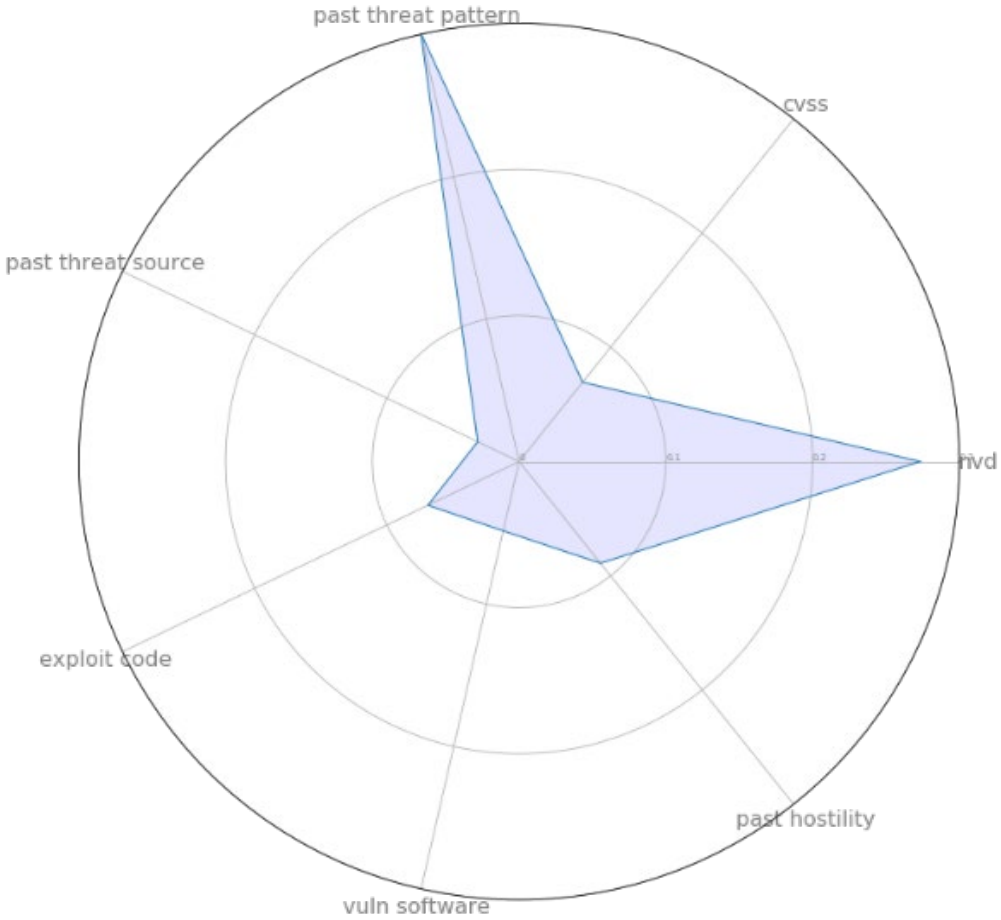
97%

Reduction in vulnerabilities to be remediated with the same impact to the attack surface

Modeling: Predictive Prioritization

150 different aspects in 7 feature groups:

- Past threat pattern
- CVSS
- NVD
- Past hostility
- Vulnerable software
- Exploit code
- Past threat source



Over 109,000 vulnerabilities tracked

Probability of exploit tracked for 28 days

Updated daily

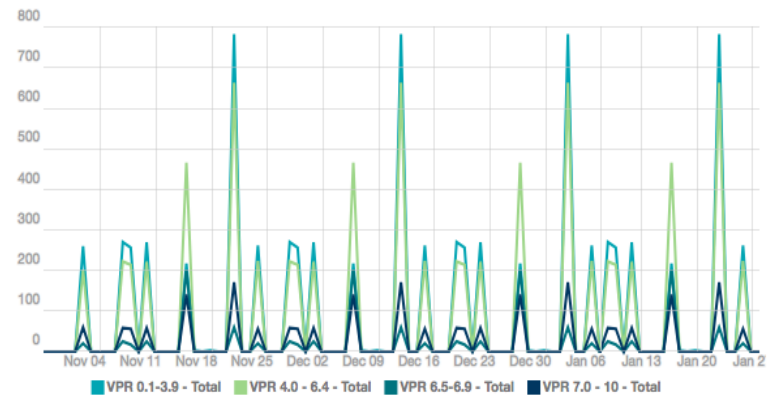
CVSS TO VPR: MORE LOW/MEDIUM – FEWER HIGH/CRITICAL

tenable.sc Dashboard Analysis Scans Reporting Assets Workflow Users

VPR Summary

Switch Dashboard Options

VPR Summary - Vulnerability Trending over the last 90 days



Last Updated: 13 hours ago

VPR Summary - Outstanding Patches by Plugin Family (VPR 7.0 - 10)

Family	Low	Medium	High	Critical
Windows	0	166	796	223
Windows : Microsoft Bulletins	0	34	1203	20
Misc.	0	24	16	24
CentOS Local Security Checks	0	9	30	10
SuSE Local Security Checks	0	4	11	7

Last Updated: 13 hours ago

VPR Summary - CVSS to VPR Heat Map

	Low (VPR 0.0-3.9)	Medium (VPR 4.0-6.4)	High (VPR 6.5-6.9)	Critical (VPR 7.0-10)
CVSSv3 Low (0-3.9)	67	142	0	0
CVSSv3 Medium (4.0 - 6.9)	615	278	32	8
CVSSv3 High (7.0 - 8.9)	511	3800	1462	660
CVSSv3 Critical (9.0 - 10)	14	524	446	264

Last Updated: 13 hours ago

VPR Summary - First Discovered Vulnerabilities

	Low (VPR 0.0-3.9)	Medium (VPR 4.0-6.4)	High (VPR 6.5-6.9)	Critical (VPR 7.0-10)
Current Month	7497	11599	2927	2347
Last Month	380	724	222	156
Current Quarter	7497	11599	2927	2347
Last Quarter	603	879	224	179
> 180 Days	0	0	0	0

Last Updated: Less than a minute ago

VPR Summary - Mitigated Vulnerabilities

	Low (VPR 0.0-3.9)	Medium (VPR 4.0-6.4)	High (VPR 6.5-6.9)	Critical (VPR 7.0-10)
Current Month	95	136	30	11
Last Month	0	0	1	0
Current Quarter	95	136	30	11
Last Quarter	52	27	1	12
> 180 Days	0	0	0	0

Last Updated: Less than a minute ago

Apply What We've Discussed

- Next week you should:
  - Begin developing a plan to reduce your Cyber Exposure
- In the first three months following this presentation you should:
  - Identify all your assets, including IT & OT
  - Prioritize vulnerabilities in a predictive manner
- Within six months you should:
  - Identify your critical assets
  - Measure & benchmark your cyber risks – internally & externally

RSAConference2019

Thank You!

kflynn@tenable.com