Eliminate Vulnerability Overload with Predictive Prioritisation

tenable


“Thanks for the 300 page security report.”
--Nobody, Ever

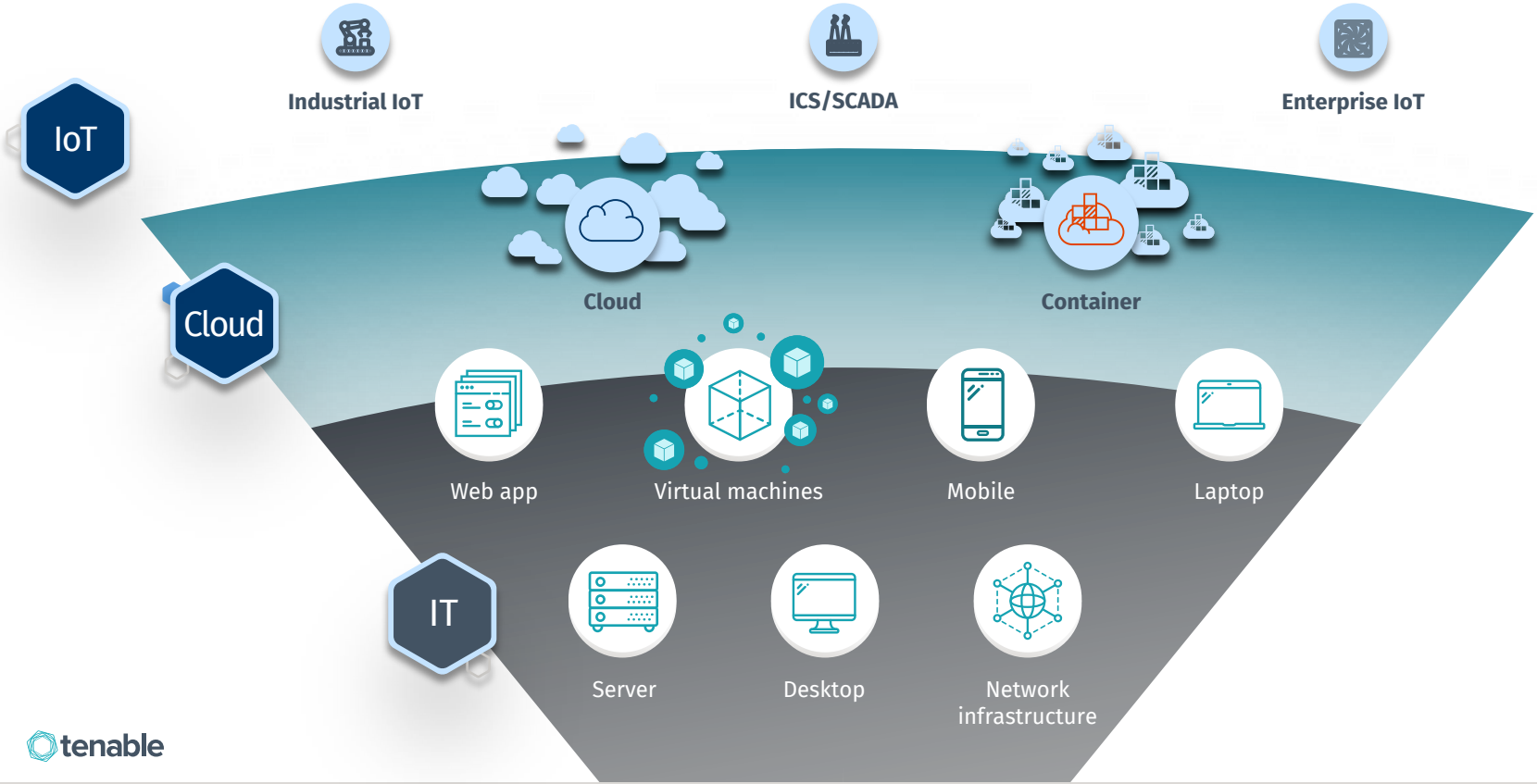
Cyber Exposure

Cyber Exposure
is an emerging discipline for :

Managing and measuring your modern attack surface to accurately understand and reduce your cyber risk

tenable™

The attack surface is **expanding!**



tenable

The new challenges come in all shapes and sizes

New Asset Types

Open Source Adoption

Short-Lived Assets

Off-Network Assets

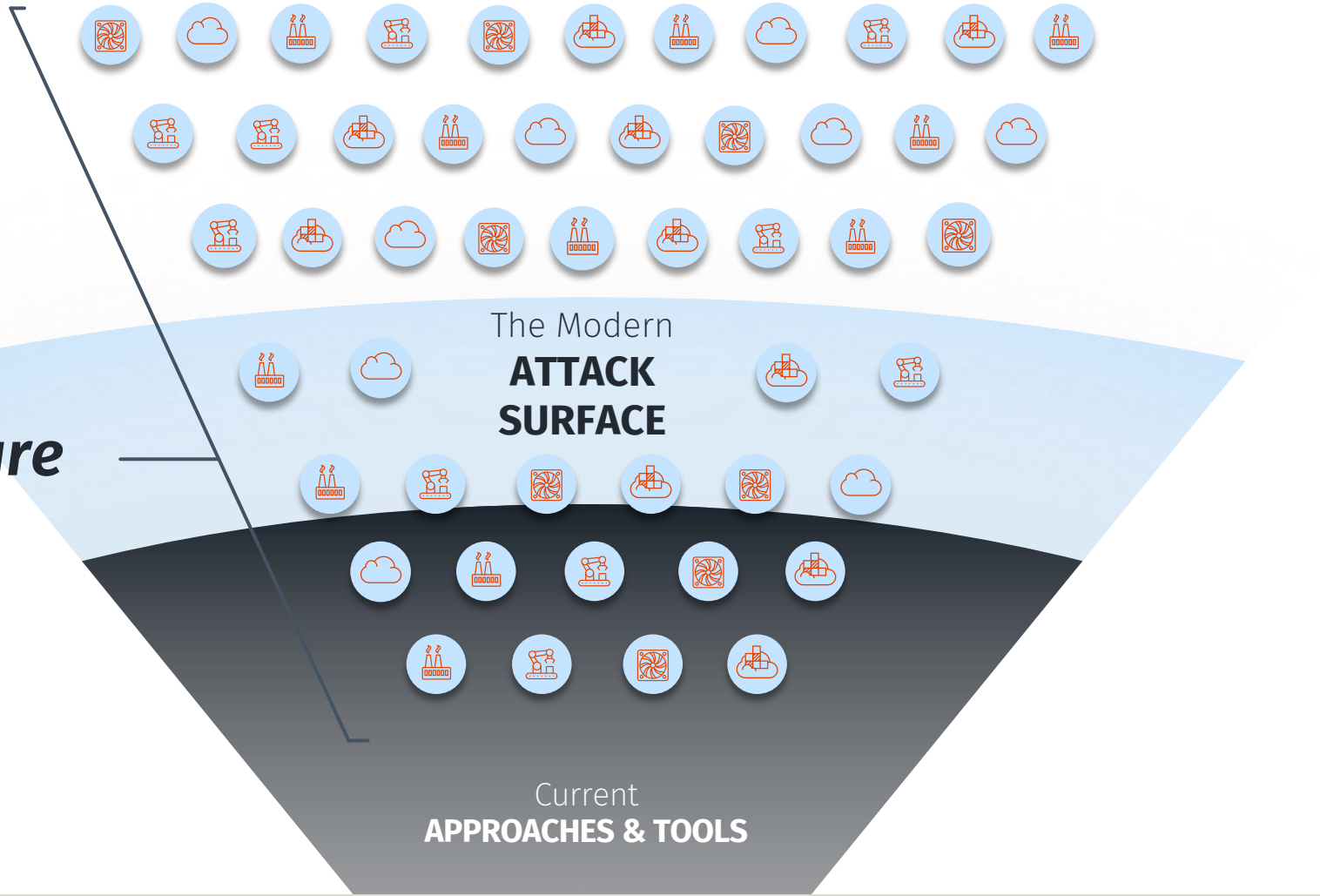
Maturity of Criminal Economy

Practices that Bypass Security

New Colleagues to Work with

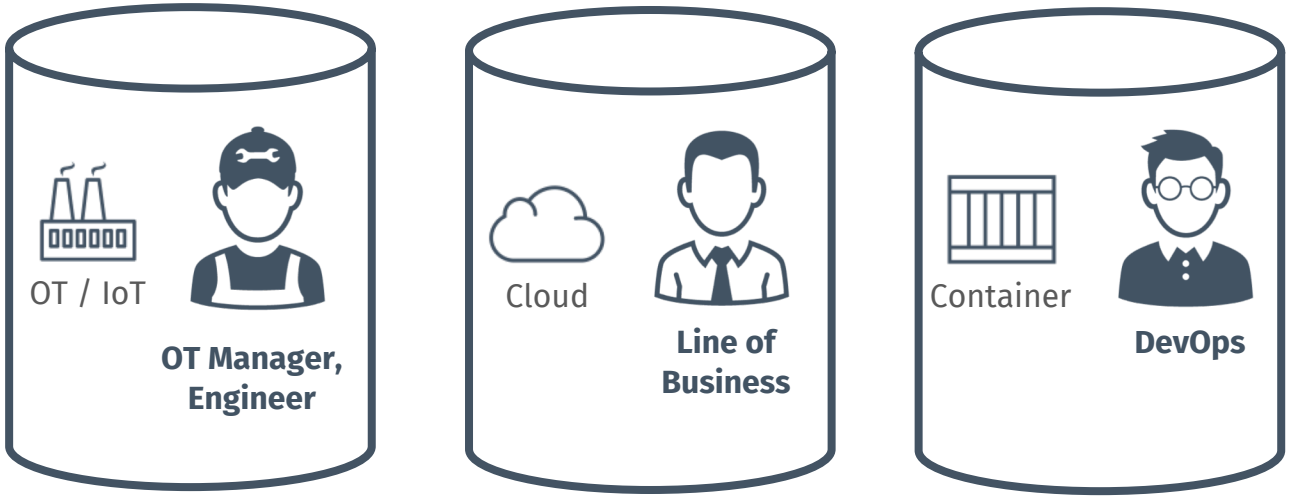
Wild World of IoT and OT

Cyber Exposure Gap



tenable

NEW STAKEHOLDERS AND ASSET OWNERS WILL IMPACT AN ORGANISATION'S CYBER EXPOSURE



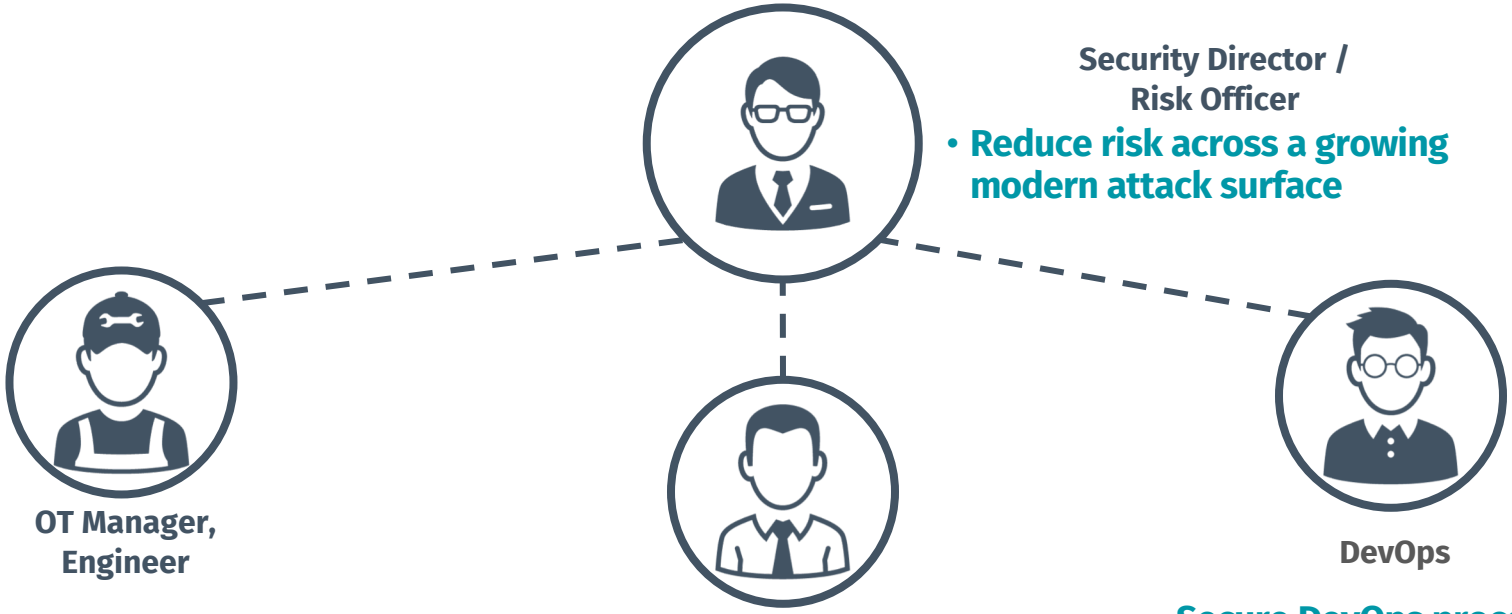
OT assets are becoming an expansive attack surface

Shadow IT and cloud assets are creating blind spots

DevOps velocity requires new security approaches

tenable

SECURITY TEAMS NEED TO PROVIDE STRATEGIC INSIGHT AND MANAGE RISK ACROSS THE ORGANIZATION



Security Director / Risk Officer

- Reduce risk across a growing modern attack surface

OT Manager, Engineer

- Increase SOC efficiency
- Maintain regulatory compliance

Line of Business

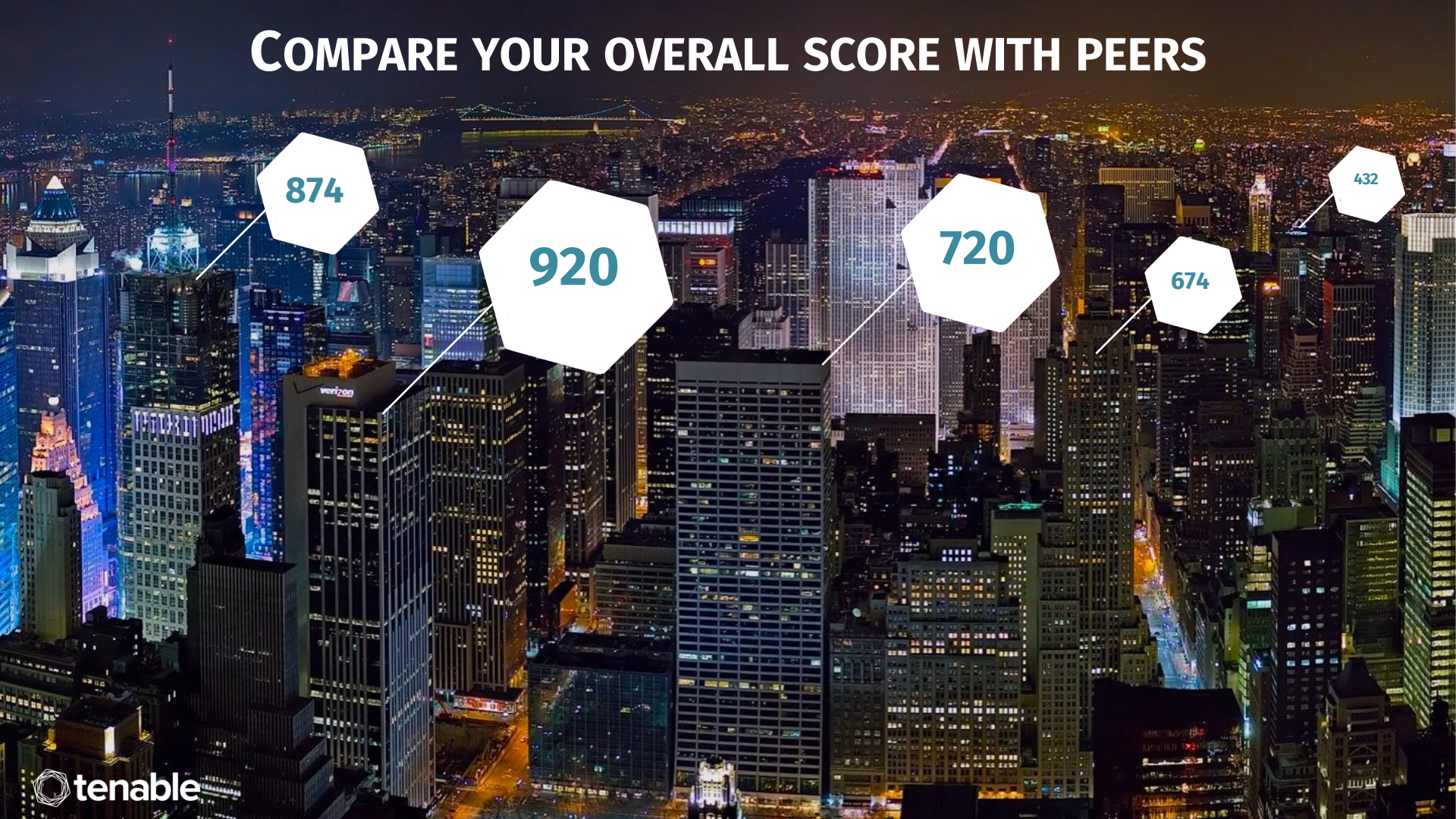
- Protect brand equity
- Gain strategic decision support on risk

DevOps

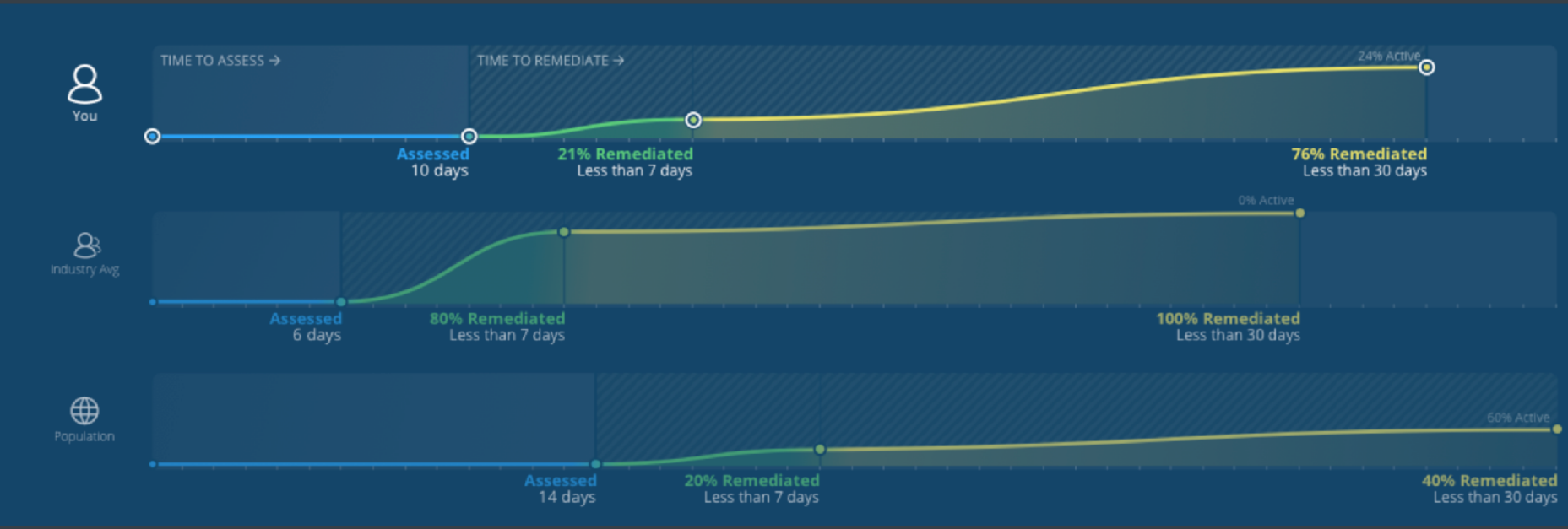
- Secure DevOps processes
- Decrease costs to fix defects

tenable

Compare your overall score with peers



Benchmark Control Effectiveness with their Peers



tenable

Predictive Prioritisation

tenable

The Four Key Questions

Where are we exposed?

Where should we prioritise based on risk?

How are we reducing exposure over time?

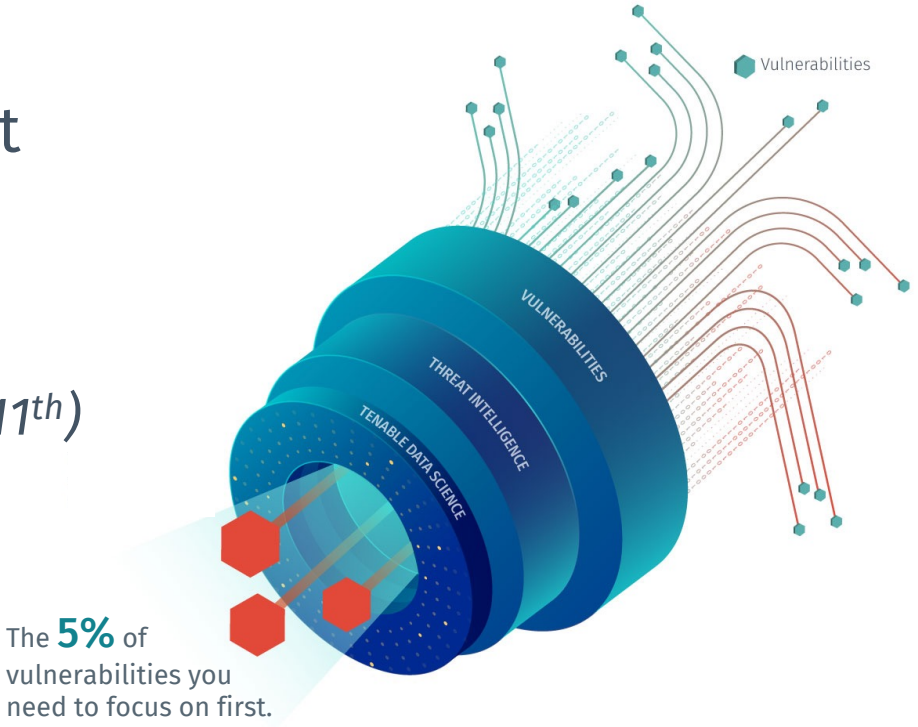
How do we compare?

tenable

Predictive Prioritisation

- Data science approach to Vulnerability Management
- Vast saving in time and resources
- Built into **Tenable.sc** *(Feb 11th)* and **Tenable.io** *(April 16th)*

- **No Added Cost!!**



tenable

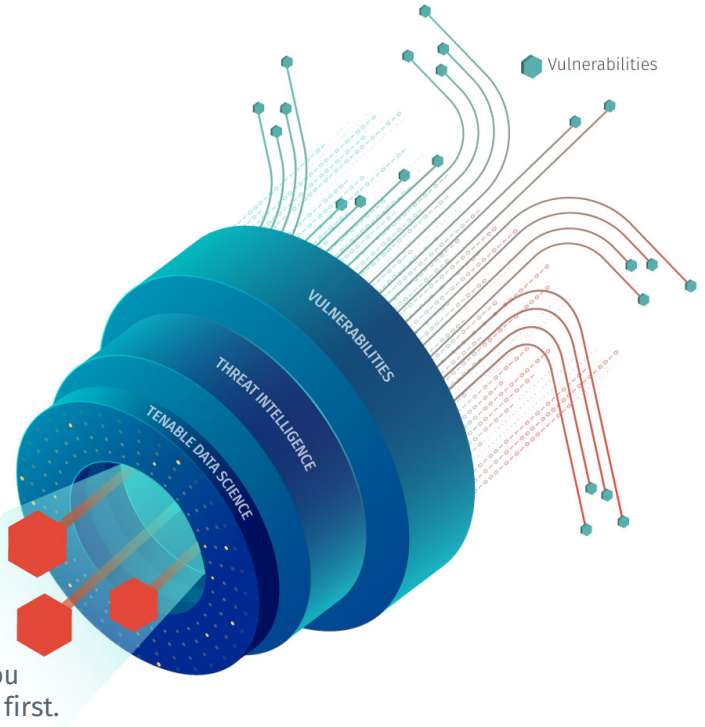
PREDICTING THE NEXT MAJOR VULNERABILITY

+150

Over 150 different aspects to the model, in 7 different categories.

+109K

Priority calculated nightly on over 109,000 different vulnerabilities being tracked.



The **5%** of vulnerabilities you need to focus on first.

tenable

Top Ten Vulnerabilities in 2018

	CVSSv2 Score (Acccording to NVD)	CVSSv3 Score (Acccording to NVD)	Tenable (Vulnerability Priority Rating)
CVE-2018-8174	**7.6**	**7.5**	**9.9**
CVE-2018-4878	**7.5**	**9.8**	**9.5**
CVE-2017-11882	**9.3**	**7.8**	**9.9**
CVE-2017-8750	**7.6**	**7.5**	**9.4**
CVE-2017-0199	**9.3**	**7.8**	**9.9**
CVE-2016-0189	**7.6**	**7.5**	**9.4**
CVE-2017-8570	**9.3**	**7.8**	**9.9**
CVE-2018-8373	**7.6**	**7.5**	**9.5**
CVE-2012-0158	**9.3**		**9.8**
CVE-2015-1805	**7.2**		**8.9**
Average Score	**8.23**	**7.9**	**9.61**

tenable

Extracted from the Recorded Future Report “Top Ten Vulnerabilities of 2018” 03/19/19

Barriers

Figure 5. Perceptions about responding to vulnerabilities and threats

Strongly agree and agree responses combined

Ponemon Institute, Dec 2018

tenable

16,555

VULNERABILITIES DISCLOSED IN 2018, up 13% on 2017

7%

of vulnerabilities had an exploit available

63%

of vulnerabilities discovered in environments are CVSS 7+

9%

of vulnerabilities disclosed in 2018 were CVSS 9+

tenable

If everything is important – Nothing is!

59% High or Critical

Vulnerability Intelligence Report
Tenable Research

tenable

Focus On What Matters

Research Insights

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

Threat Intelligence

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

Vulnerability Rating

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

97%

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

tenable

A Data Science Approach - *Understanding The Model*

- Over 109,000 vulnerabilities tracked
- Forecasts probability of exploit in near-term future
- Updated daily
- 150 different aspects in 7 groups
  - Past threat pattern
  - CVSS
  - NVD
  - Past hostility
  - Vulnerable software
  - Exploit code
  - Past threat source

tenable

Some Of What's In The Model

- CVE Age
- No. Words in NVD Description
- Days Since NVD Last Modified
- Number of References
- CVSS v3 Base Score
- CVSS v3 Exploitability Score
- CVSS v3 Impact Score
- Total Affected Software
- CWE

- Distinct days with cyber exploits
- Days since last cyber exploit
- Total cyber exploit events
- Days since first cyber exploit
- Days since last cyber attack

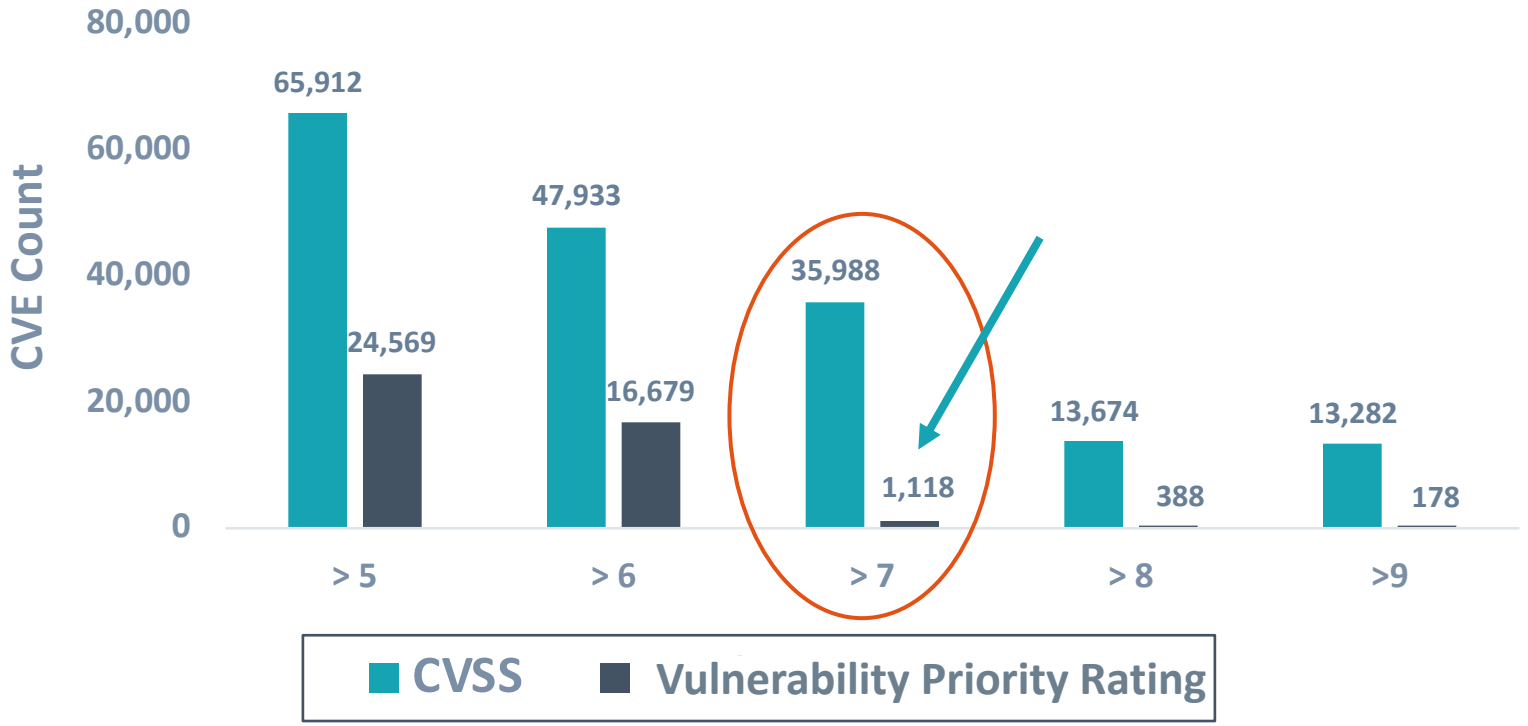
- Days since last ExploitDB entry
- Days since first ExploitDB entry
- Days since last Metasploit entry
- Total ExploitDB entries
- Total Metasploit entries

Terminology

- **Predictive Prioritization:**
  The **process** of re-prioritizing vulnerabilities based on the probability that they ***will*** be leveraged in an attack.

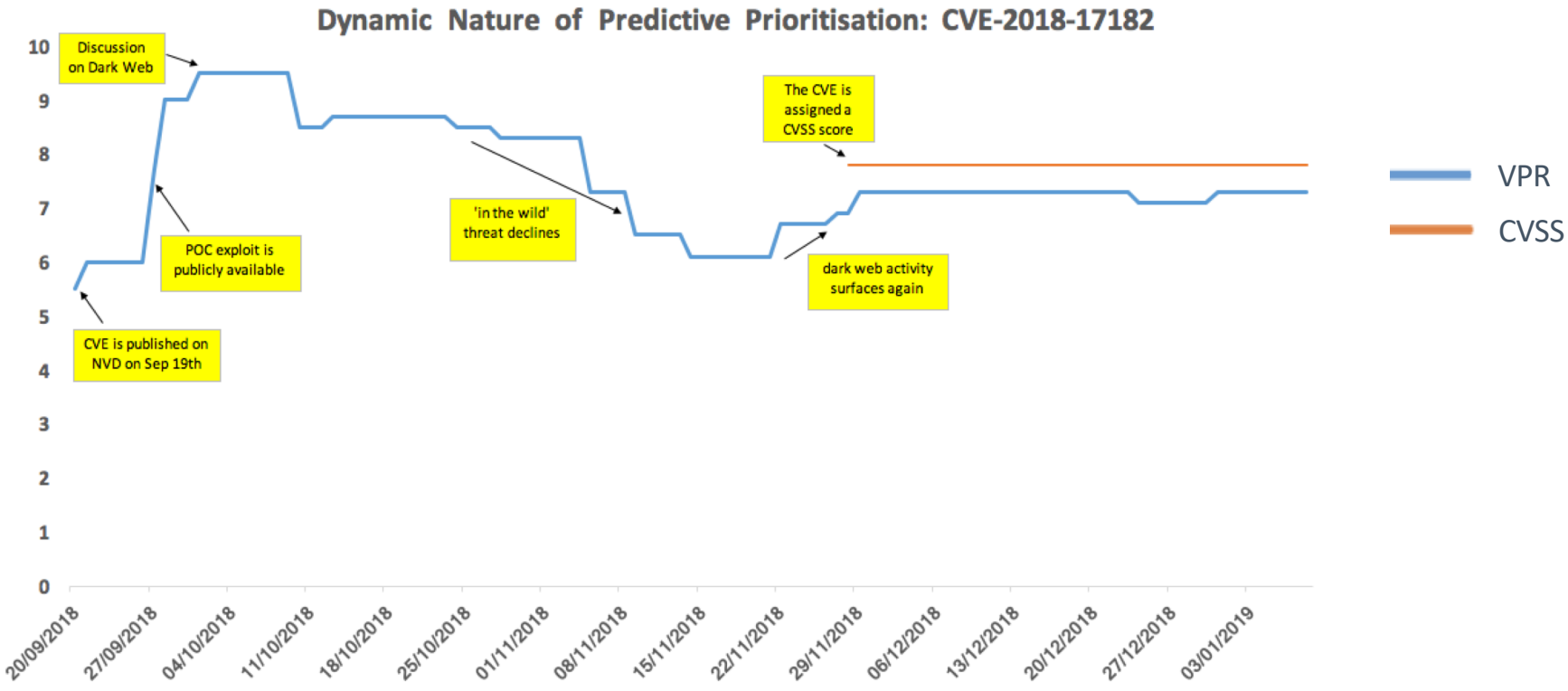
- **Vulnerability Priority Rating (VPR):**
  The **output** of the Predictive Prioritization process. VPR is the number that indicates the ***remediation priority*** (0 through 10, with 10 being the highest severity) of an individual vulnerability.

Focusing on what matters



tenable

VPR Insight - 70 Days Prior to CVSS Score



Linux Kernel Flaw

tenable

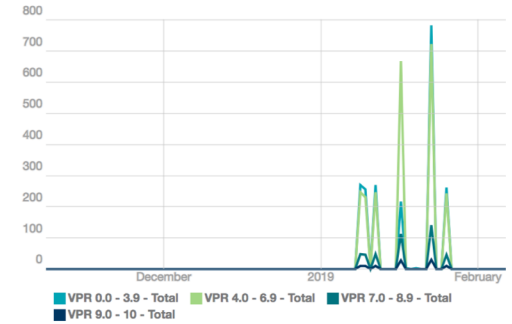
CVSS To VPR: More Low/Medium – *Fewer High/Critical*

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: 2 minutes ago

VPR Summary - Highlighted Patches (VPR 7.0 - 10)

Solution	Risk …	H…	T…	Vulnerability…
Upgrade to Adobe Flash	13.96%	67	468	17.11%
Apply MS17-013: Security Update	13.13%	212	299	10.93%
Apply Microsoft Security Advisory	12.41%	211	275	10.05%
Apply MS16-142: Cumulative	10.26%	165	344	12.57%

VPR Summary - CVSS to VPR Heat Map

	Low (VPR 0.0-3.9)	Medium (VPR 4.0-6.9)	High (VPR 7.0-8.9)	Critical (VPR 9.0-10)
CVSSv3 Low (0-3.9)	67	142	0	0
CVSSv3 Medium (4.0 - 6.9)	615	310	7	1
CVSSv3 High (7.0 - 8.9)	511	5262	338	322
CVSSv3 Critical (9.0 - 10)	14	970	170	94

Last Updated: 2 minutes ago

VPR Summary - First Discovered Vulnerabilities

	Low (VPR 0.0-3.9)	Medium (VPR 4.0-6.9)	High (VPR 7.0-8.9)	Critical (VPR 9.0-10)
Current Month	0	0	0	0
Last Month	7497	14526	1773	574
Current Quarter	7497	14526	1773	574
Last Quarter	603	1103	146	33
> 180 Days	0	0	0	0

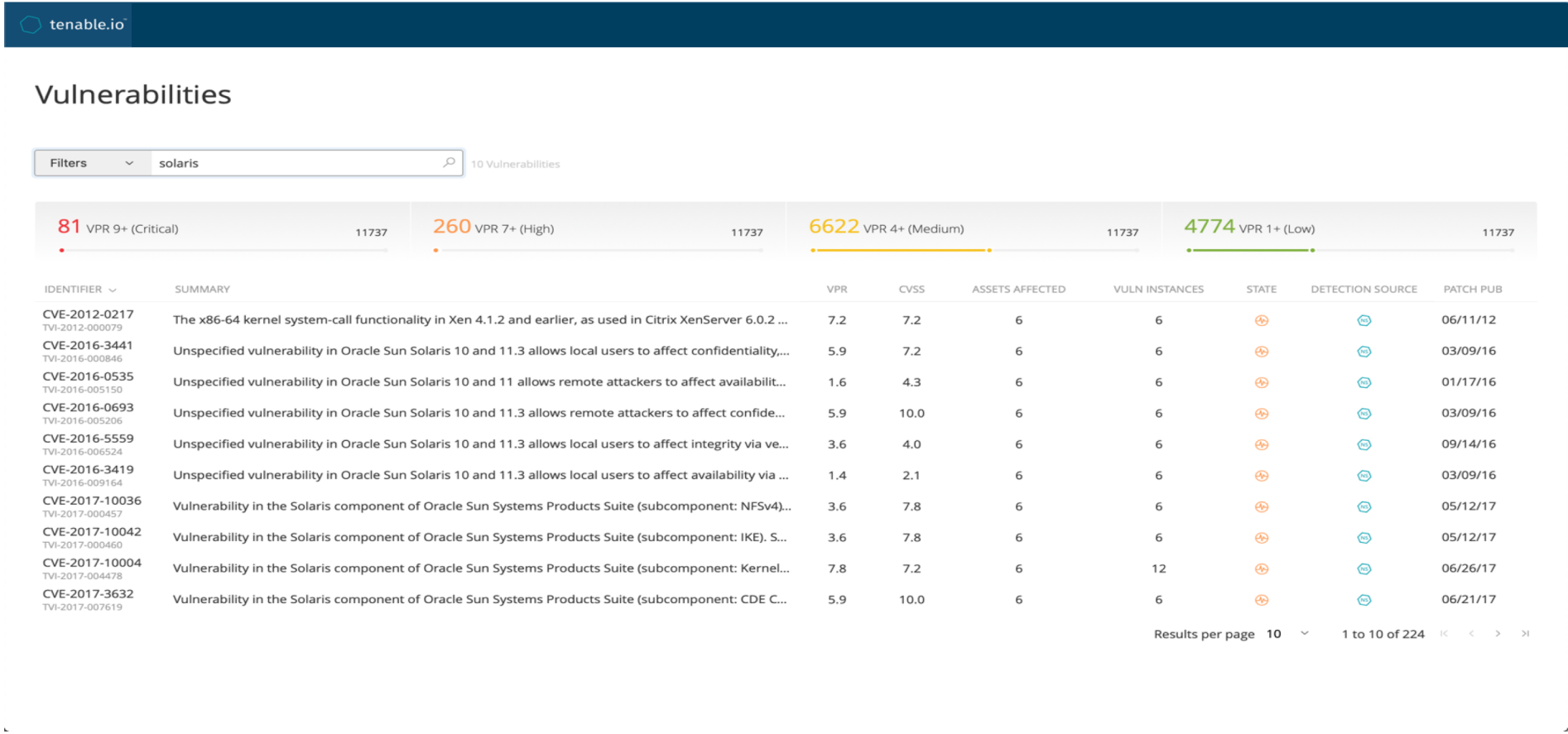
Last Updated: 2 minutes ago

VPR Summary - Mitigated Vulnerabilities

	Low (VPR 0.0-3.9)	Medium (VPR 4.0-6.9)	High (VPR 7.0-8.9)	Critical (VPR 9.0-10)
Current Month	0	0	0	0
Last Month	95	166	9	2
Current Quarter	95	166	9	2
Last Quarter	52	28	11	1
> 180 Days	0	0	0	0

Last Updated: Less than a minute ago

VPR also in Tenable.io



Q & A

tenable


tenable®
Thank You