tenable®

The Cyber Exposure Company

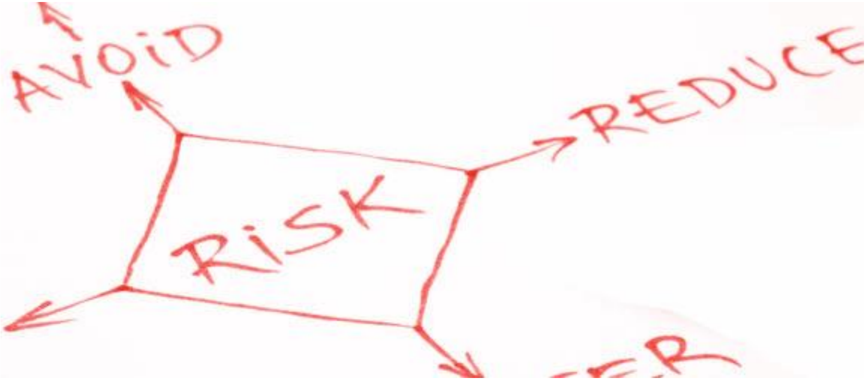
Risk-based Vulnerability Management

PRYOR
12-9-93

Most VM programs are stale and generally viewed as either ineffective or broken!

tenable

“There is no such thing as "being secure" there's just operating at an acceptable level of risk.”



The Four Key Questions

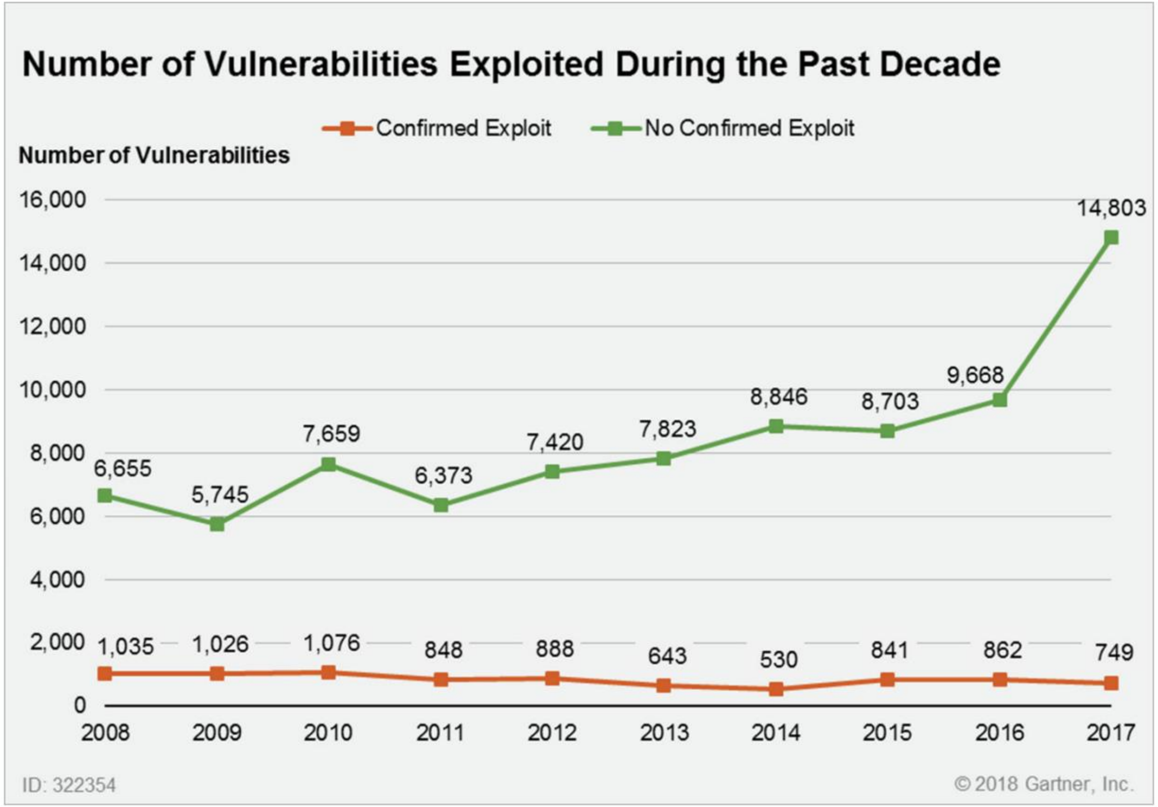
Where are we exposed?

What should we focus on first?

How are we reducing exposure over time?

How do we compare to our peers?

Figure 2. Number of Vulnerabilities During The Past Decade



Source: IBM X-Force/Analysis Gartner (June 2018)

Gartner Market Guide for Vulnerability Assessment, Craig Lawson, Prateek Bhajanka, June 19, 2018

TOP 10 VULNERABILITIES USED BY CYBERCRIMINALS IN 2018

Of the top 10 Only **4** have **“Critical”** CVSS Score

CVE	CVSSv2 Score
CVE-2018-8174	7.6
CVE-2018-4878	7.5
CVE-2017-11882	**9.3**
CVE-2017-8750	7.6
CVE-2017-0199	**9.3**
CVE-2016-0189	7.6
CVE-2017-8570	**9.3**
CVE-2018-8373	7.6
CVE-2012-0158	**9.3**
CVE-2015-1805	7.2

Recorded Future

March 19,2019

tenable

17,313*

VULNERABILITIES DISCLOSED IN 2019

59%

of vulnerabilities discovered
in environments
are CVSS 7+

15%

of vulnerabilities disclosed in
2017
were CVSS 9+

7%

of vulnerabilities had
an exploit available

*National Vulnerability Database

tenable

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

WHAT'S THE MISSING INGREDIENT?

TERMINOLOGY

- **Predictive Prioritization:**
  The **process** of re-prioritizing vulnerabilities based on the probability 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.

A DATA SCIENCE APPROACH
UNDERSTANDING THE MODEL

150 different aspects in 7 groups

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

Over 140,000 vulnerabilities tracked

Forecasts probability of exploit in near term future

Updated daily

SOME OF WHAT'S IN THE MODEL

NVD

- 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

Recorded Future

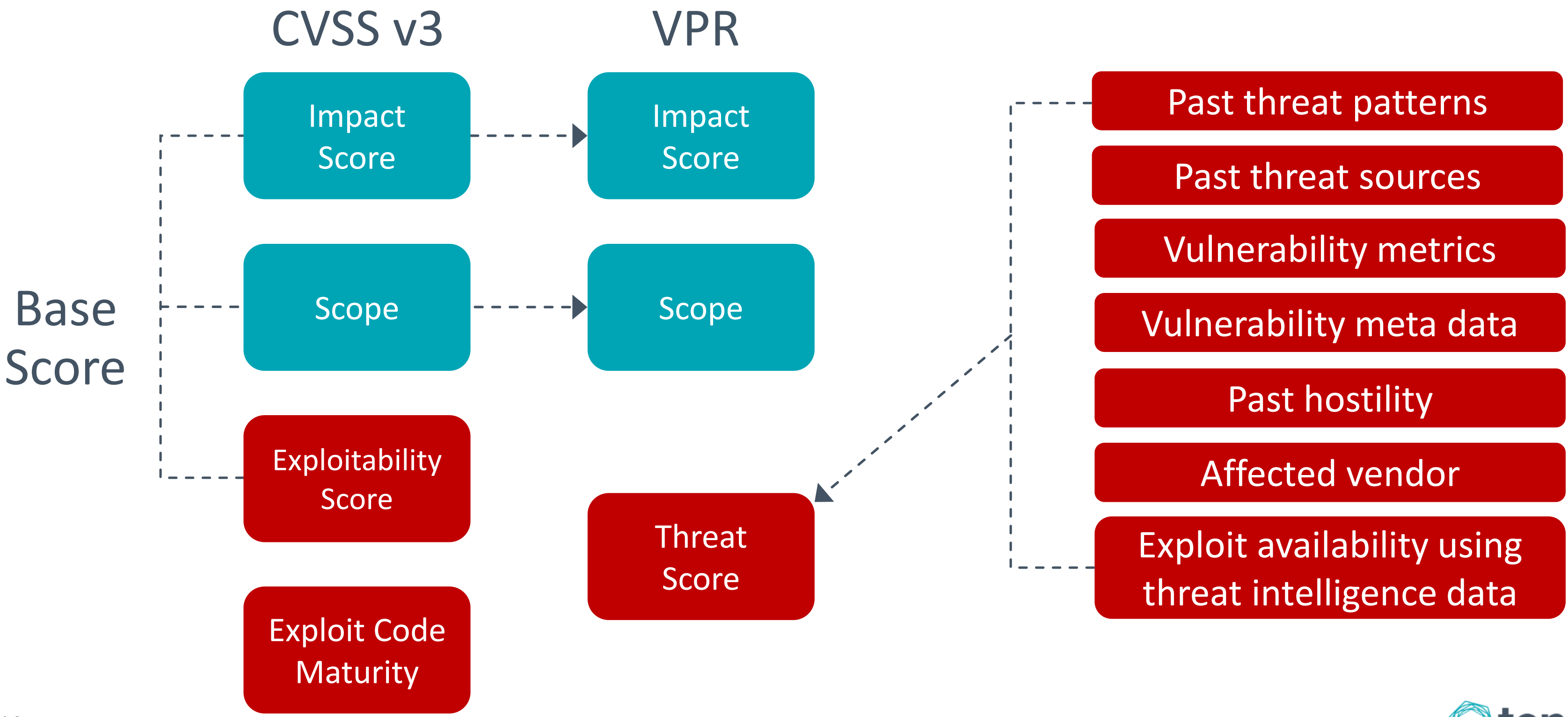
- Distinct days with cyber exploits
- Days since last cyber exploit
- Total cyber exploit events
- Days since first cyber exploit
- Days since last cyber attack

EXPLOIT DATABASE

- Days since last ExploitDB entry
- Days since first ExploitDB entry
- Days since last Exploit tool entry
- Total ExploitDB entries
- Total Exploit tool entries

VPR Framework

VPR Framework: How does it Work?



CVSS v3

VPR

Base Score

Impact Score

Scope

Exploitability Score

Exploit Code Maturity

Impact Score

Scope

Threat Score

Past threat patterns

Past threat sources

Vulnerability metrics

Vulnerability meta data

Past hostility

Affected vendor

Exploit availability using threat intelligence data

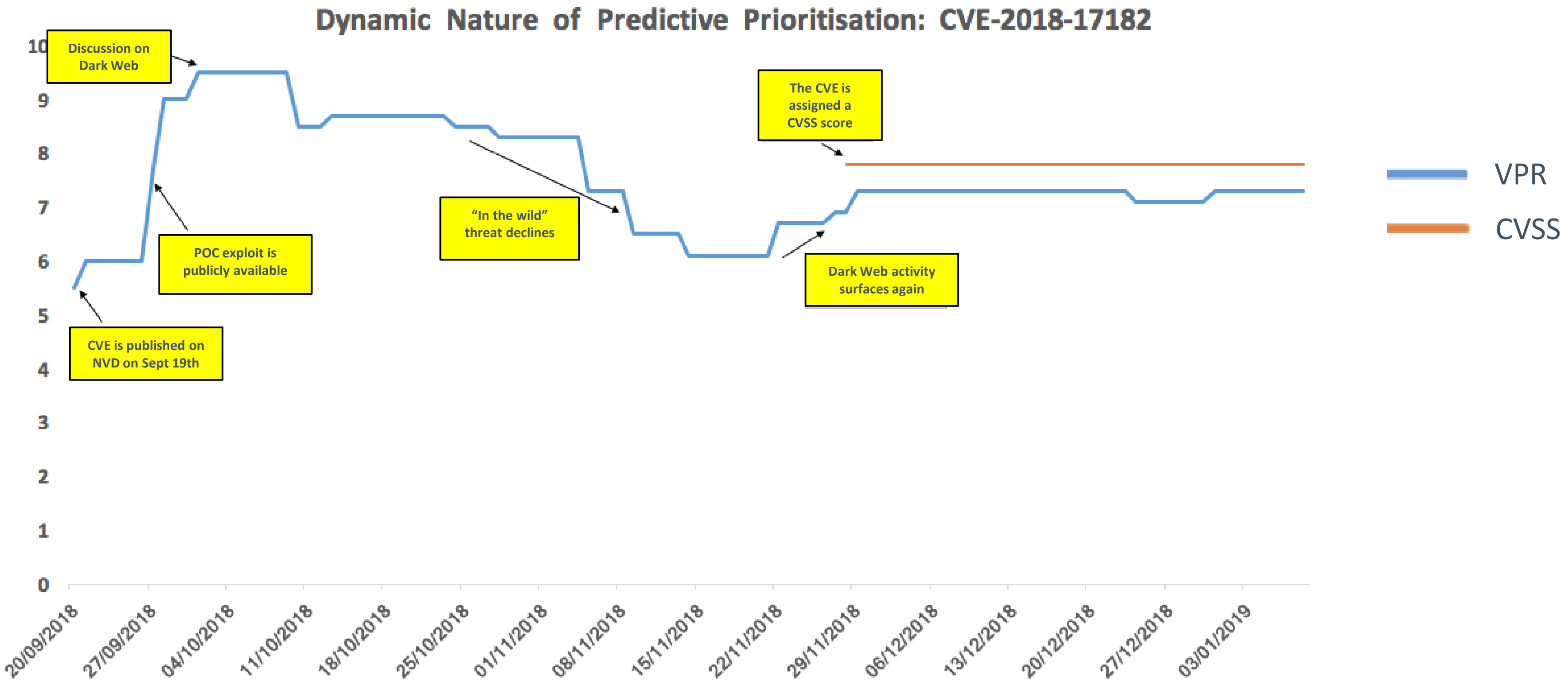
VPR vs CVSS scores

- VPR score is dynamic and reflects threat intelligence collected on a daily basis

- VPR score is provided weeks before a CVSS score is made public

- Often time-lag between when a CVE is published and when a CVSS score is derived

VPR INSIGHT - 70 DAYS PRIOR TO CVSS SCORE



Discussion on Dark Web

POC exploit is publicly available

CVE is published on NVD on Sept 19th

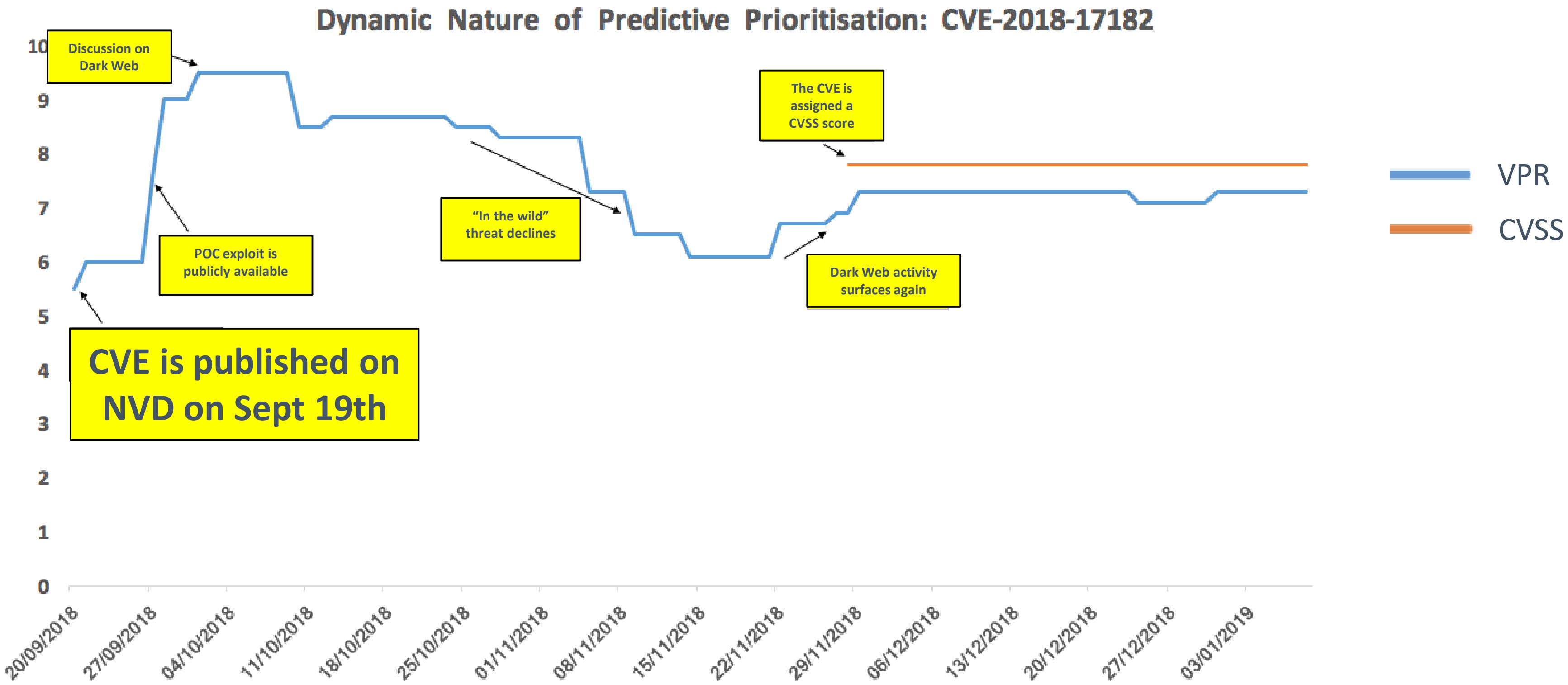
"In the wild" threat declines

The CVE is assigned a CVSS score

Dark Web activity surfaces again

Linux Kernel Flaw

VPR INSIGHT - 70 DAYS PRIOR TO CVSS SCORE



Discussion on Dark Web

POC exploit is publicly available

"In the wild" threat declines

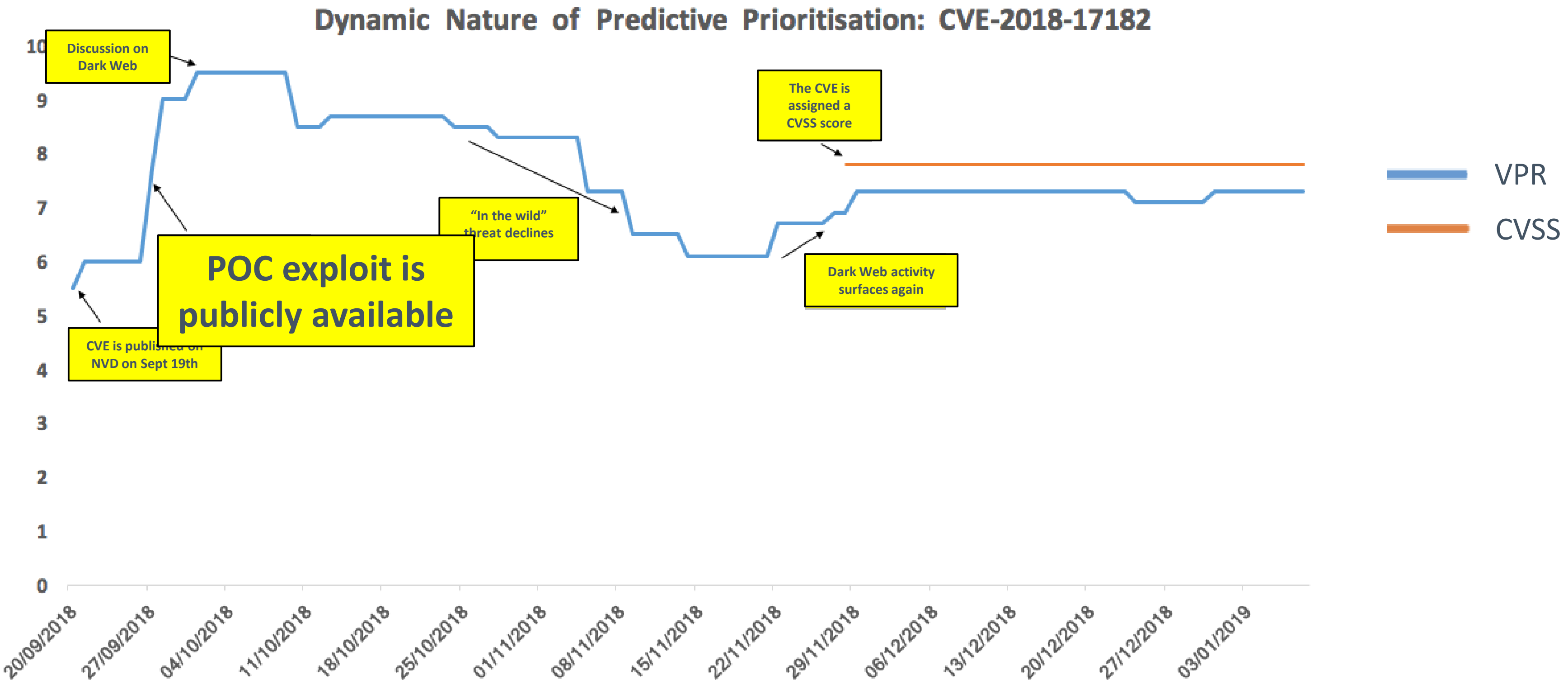
The CVE is assigned a CVSS score

Dark Web activity surfaces again

CVE is published on NVD on Sept 19th

Linux Kernel Flaw

VPR INSIGHT - 70 DAYS PRIOR TO CVSS SCORE


Dynamic Nature of Predictive Prioritisation: CVE-2018-17182

Discussion on Dark Web

CVE is published on NVD on Sept 19th

POC exploit is publicly available

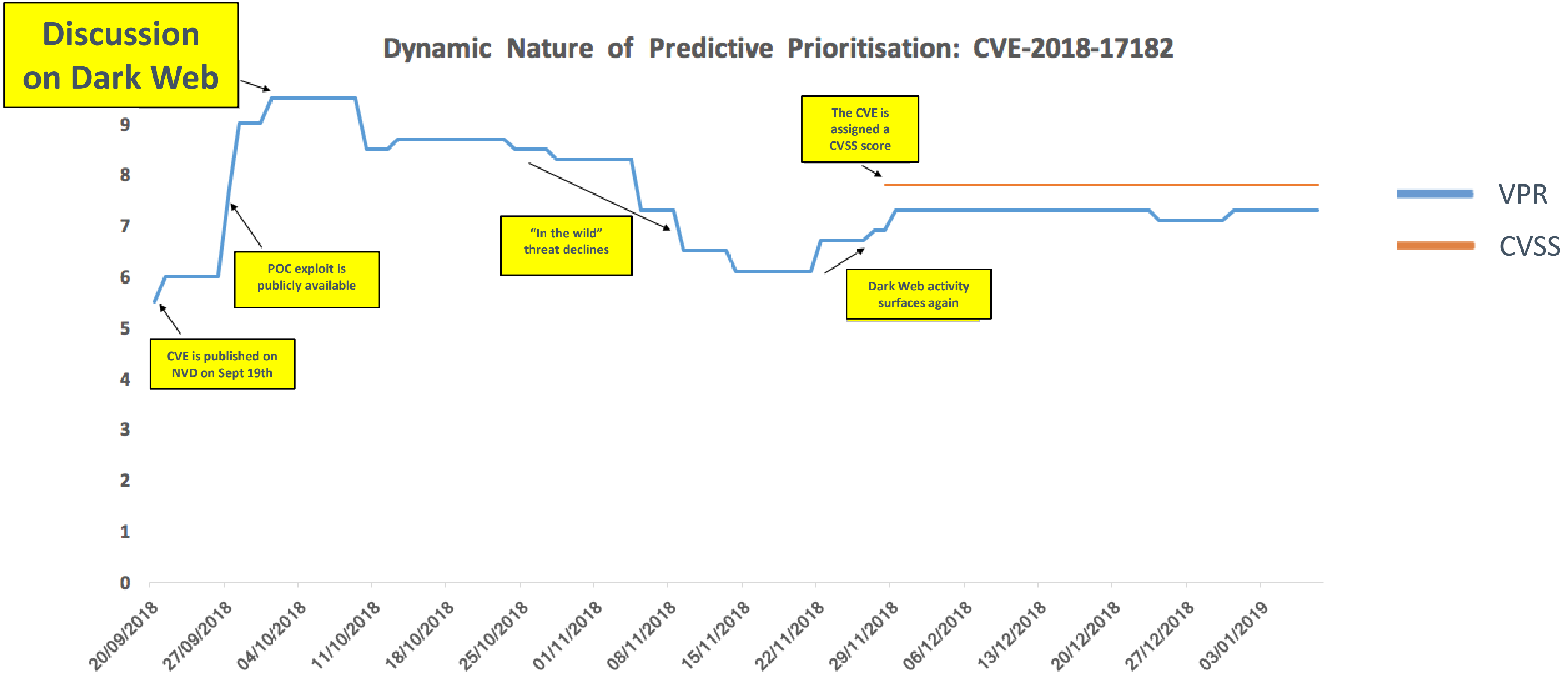
"In the wild" threat declines

The CVE is assigned a CVSS score

Dark Web activity surfaces again

Linux Kernel Flaw

VPR INSIGHT - 70 DAYS PRIOR TO CVSS SCORE



Discussion on Dark Web

POC exploit is publicly available

CVE is published on NVD on Sept 19th

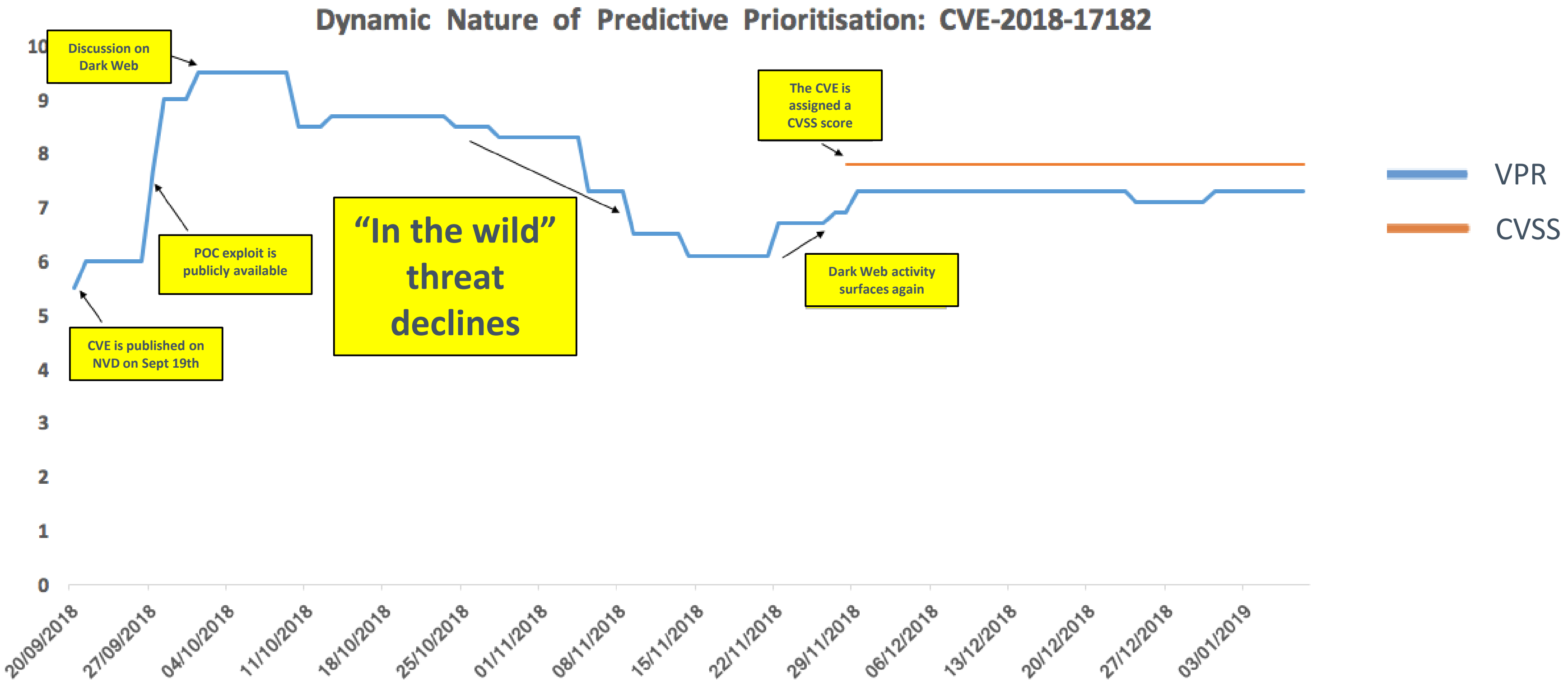
"In the wild" threat declines

The CVE is assigned a CVSS score

Dark Web activity surfaces again

Linux Kernel Flaw

VPR INSIGHT - 70 DAYS PRIOR TO CVSS SCORE



Discussion on Dark Web

CVE is published on NVD on Sept 19th

POC exploit is publicly available

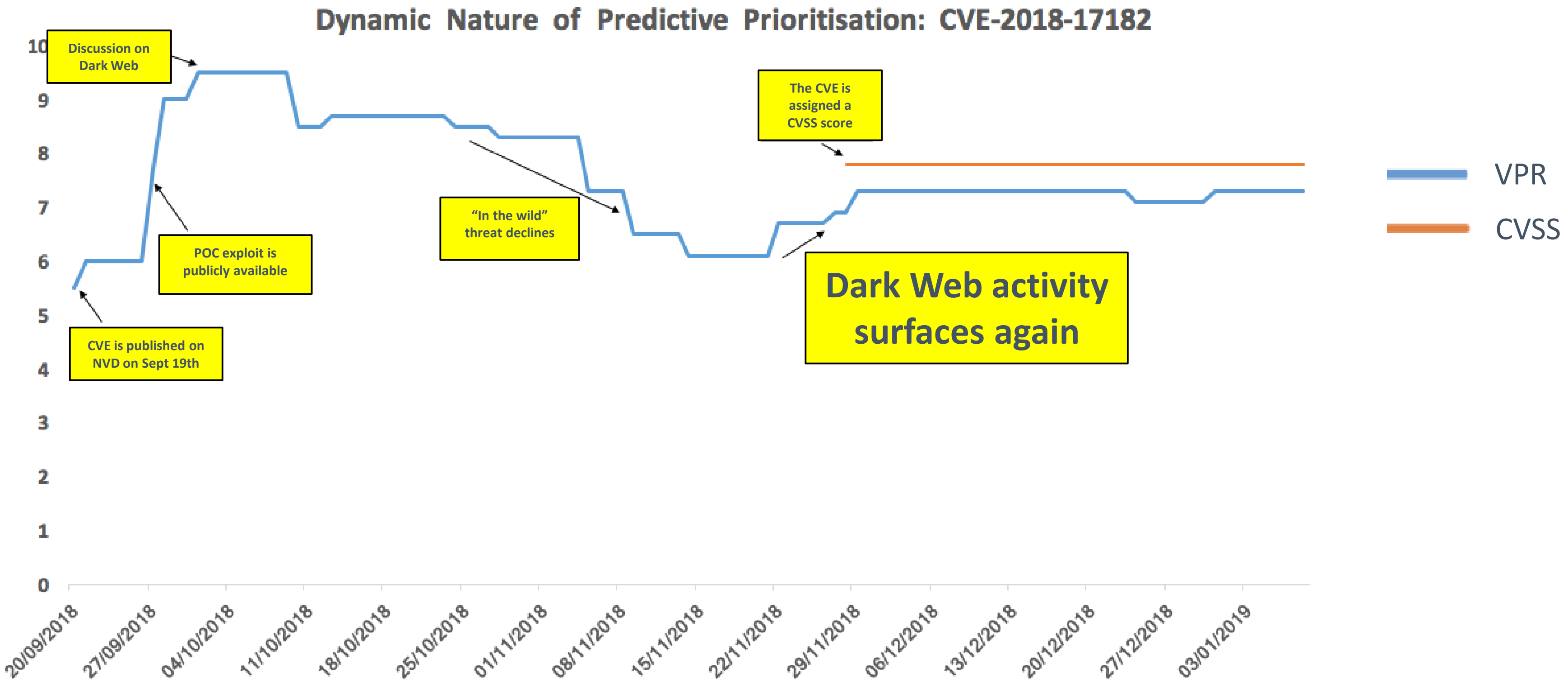
"In the wild" threat declines

The CVE is assigned a CVSS score

Dark Web activity surfaces again

Linux Kernel Flaw

VPR INSIGHT - 70 DAYS PRIOR TO CVSS SCORE



Discussion on Dark Web

POC exploit is publicly available

CVE is published on NVD on Sept 19th

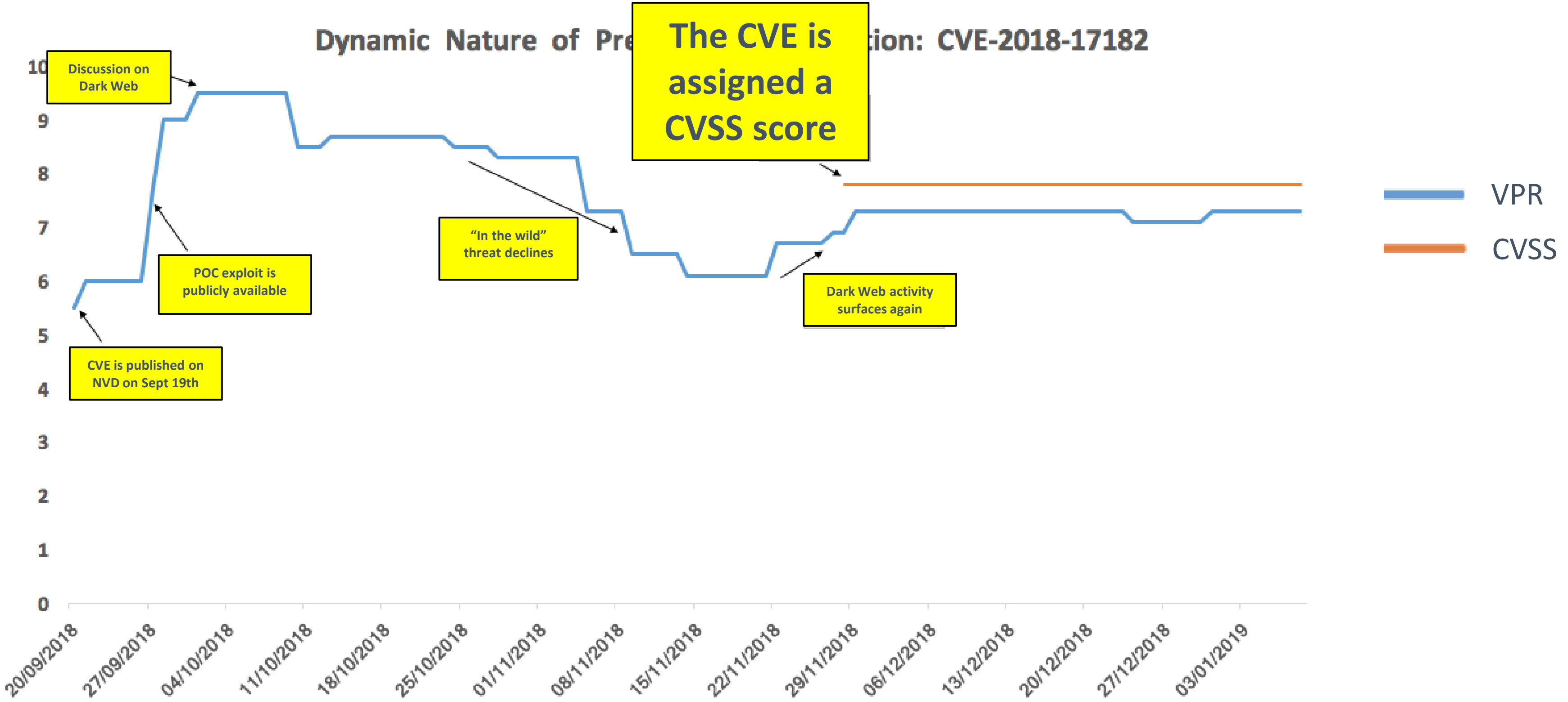
"In the wild" threat declines

The CVE is assigned a CVSS score

Dark Web activity surfaces again

Linux Kernel Flaw

VPR INSIGHT - 70 DAYS PRIOR TO CVSS SCORE



Dynamic Nature of Pre tion: CVE-2018-17182

The CVE is assigned a CVSS score

Discussion on Dark Web

POC exploit is publicly available

CVE is published on NVD on Sept 19th

"In the wild" threat declines

Dark Web activity surfaces again

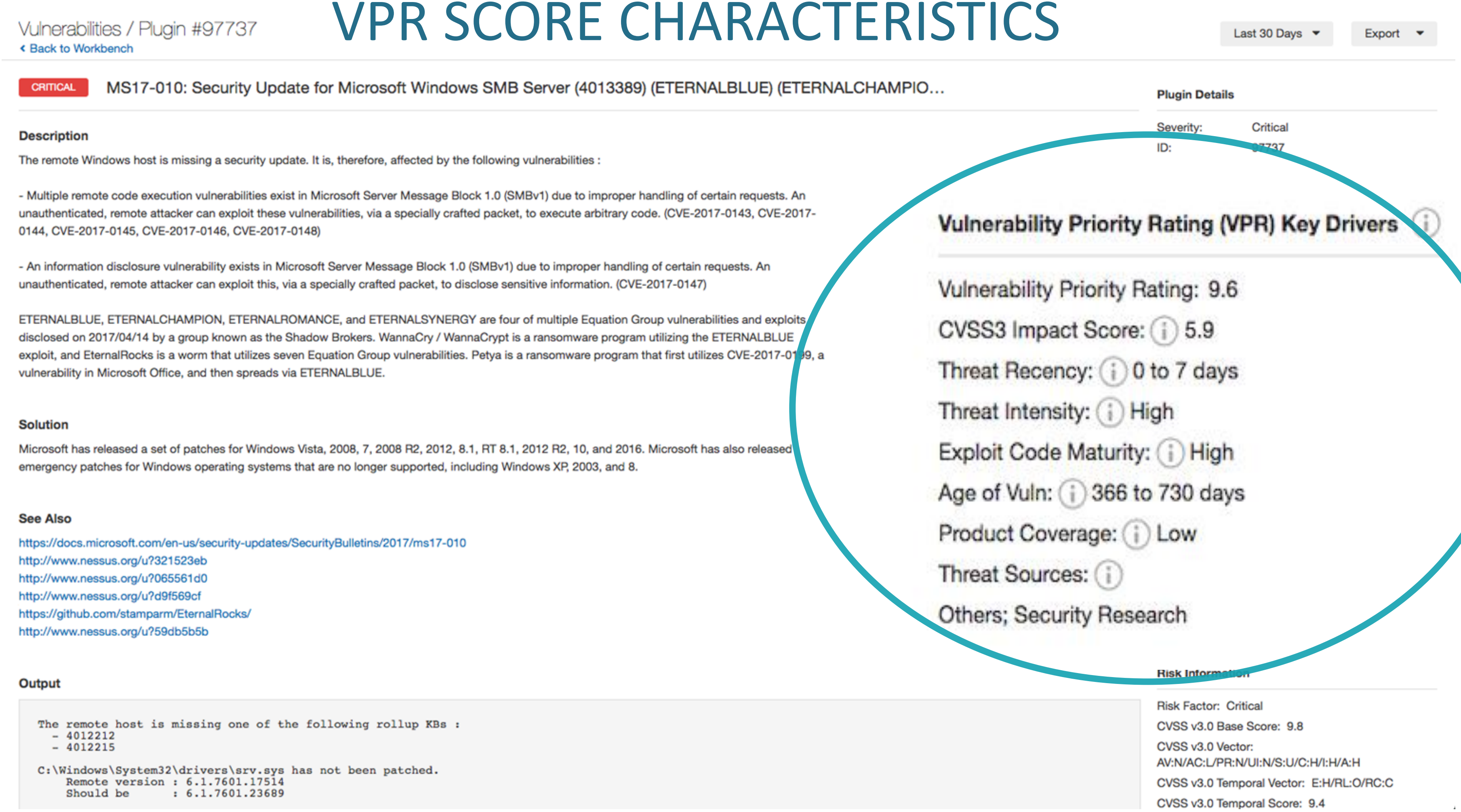
Linux Kernel Flaw

Top Five Vulnerabilities in 2018

CVE	CVSSv2 Score (Acccording to NVD)	CVSSv3 Score (Acccording to NVD)	VPR (Vulnerability Priority Rating)
CVE-2018-8174 Windows VB Script	7.6	7.5	9.9
CVE-2018-4878 Adobe Flash	7.5	9.8	9.5
CVE-2017-11882 MS Office Memory Corruption	9.3	7.8	9.9
CVE-2017-8750 Internet Explorer Memory Corruption	7.6	7.5	9.4
CVE-2017-0199 MS Office/Wordpad Remote Code Execution	9.3	7.8	9.9

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

VPR SCORE CHARACTERISTICS



MS17-010: Security Update for Microsoft Windows SMB Server (4013389) (ETERNALBLUE) (ETERNALCHAMPIO…

Description

The remote Windows host is missing a security update. It is, therefore, affected by the following vulnerabilities :

- Multiple remote code execution vulnerabilities exist in Microsoft Server Message Block 1.0 (SMBv1) due to improper handling of certain requests. An unauthenticated, remote attacker can exploit these vulnerabilities, via a specially crafted packet, to execute arbitrary code. (CVE-2017-0143, CVE-2017-0144, CVE-2017-0145, CVE-2017-0146, CVE-2017-0148)

- An information disclosure vulnerability exists in Microsoft Server Message Block 1.0 (SMBv1) due to improper handling of certain requests. An unauthenticated, remote attacker can exploit this, via a specially crafted packet, to disclose sensitive information. (CVE-2017-0147)

ETERNALBLUE, ETERNALCHAMPION, ETERNALROMANCE, and ETERNALSYNERGY are four of multiple Equation Group vulnerabilities and exploits disclosed on 2017/04/14 by a group known as the Shadow Brokers. WannaCry / WannaCrypt is a ransomware program utilizing the ETERNALBLUE exploit, and EternalRocks is a worm that utilizes seven Equation Group vulnerabilities. Petya is a ransomware program that first utilizes CVE-2017-0199, a vulnerability in Microsoft Office, and then spreads via ETERNALBLUE.

Solution

Microsoft has released a set of patches for Windows Vista, 2008, 7, 2008 R2, 2012, 8.1, RT 8.1, 2012 R2, 10, and 2016. Microsoft has also released emergency patches for Windows operating systems that are no longer supported, including Windows XP, 2003, and 8.

See Also

https://docs.microsoft.com/en-us/security-updates/SecurityBulletins/2017/ms17-010
http://www.nessus.org/u?321523eb
http://www.nessus.org/u?065561d0
http://www.nessus.org/u?d9f569cf
https://github.com/stamparm/EternalRocks/
http://www.nessus.org/u?59db5b5b

Output

```
The remote host is missing one of the following rollup KBs :
  - 4012212
  - 4012215

C:\Windows\System32\drivers\srv.sys has not been patched.
    Remote version : 6.1.7601.17514
    Should be      : 6.1.7601.23689
```

Plugin Details

Severity: Critical
ID: 97737

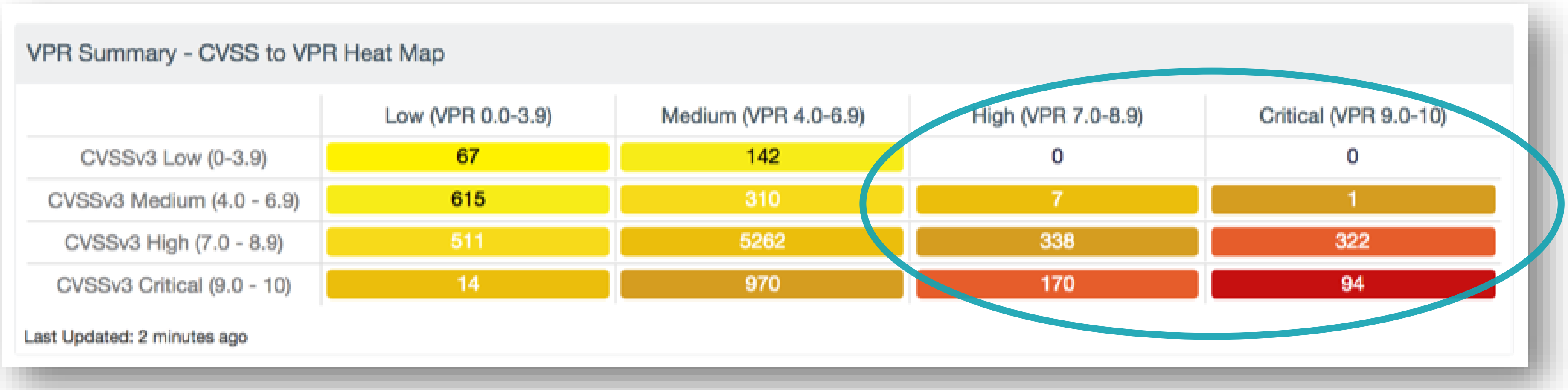
Vulnerability Priority Rating (VPR) Key Drivers

Vulnerability Priority Rating: 9.6
CVSS3 Impact Score: 5.9
Threat Recency: 0 to 7 days
Threat Intensity: High
Exploit Code Maturity: High
Age of Vuln: 366 to 730 days
Product Coverage: Low
Threat Sources:
Others; Security Research

Risk Information

Risk Factor: Critical
CVSS v3.0 Base Score: 9.8
CVSS v3.0 Vector: AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
CVSS v3.0 Temporal Vector: E:H/RL:O/RC:C
CVSS v3.0 Temporal Score: 9.4

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



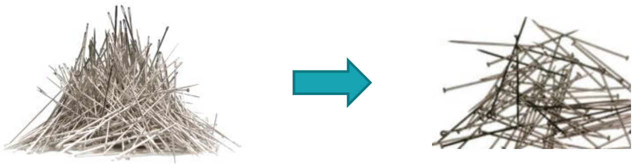
VPR Summary - CVSS to VPR Heat Map

	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

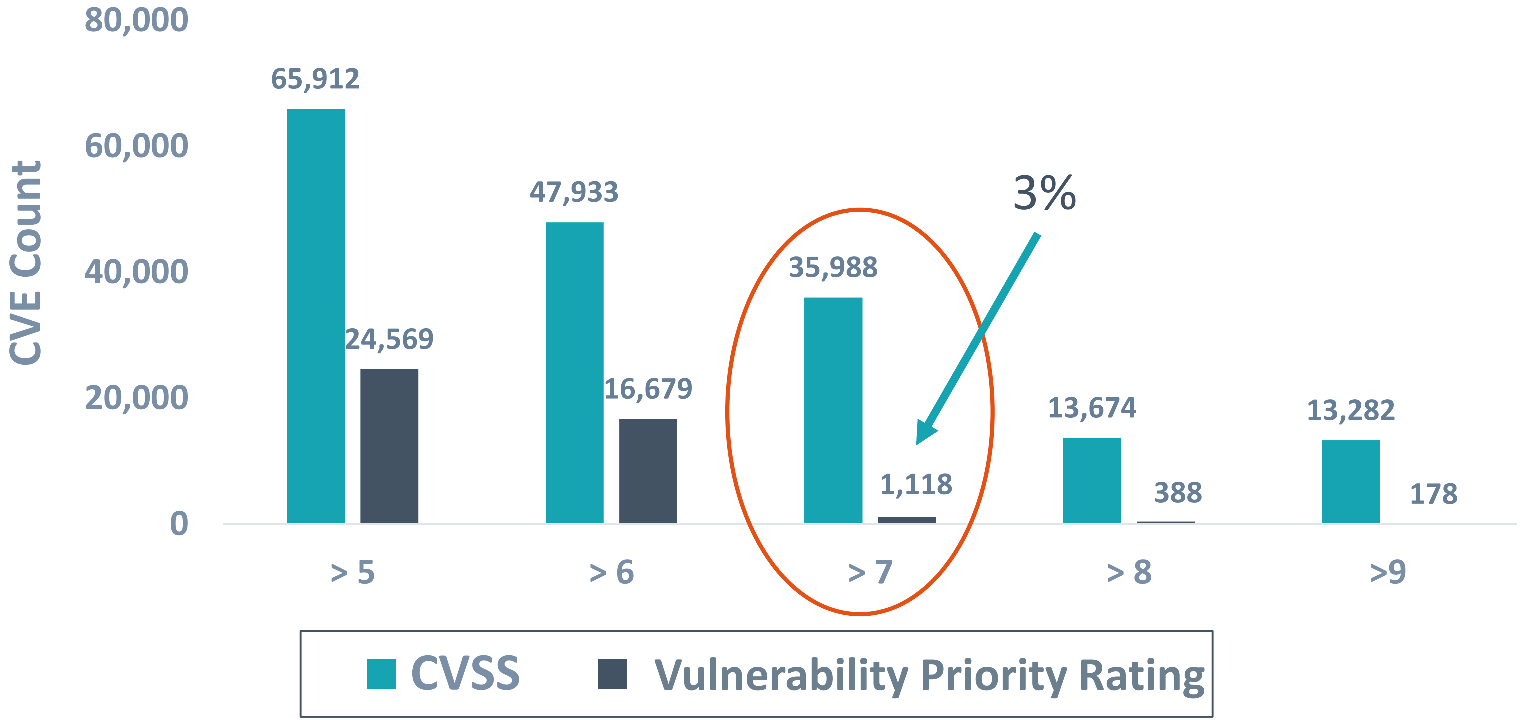
10,214 CVSSv3/v2 High and Critical vulnerabilities become:

- 417 vulnerabilities with a Critical VPR
- 515 vulnerabilities with a High VPR



tenable

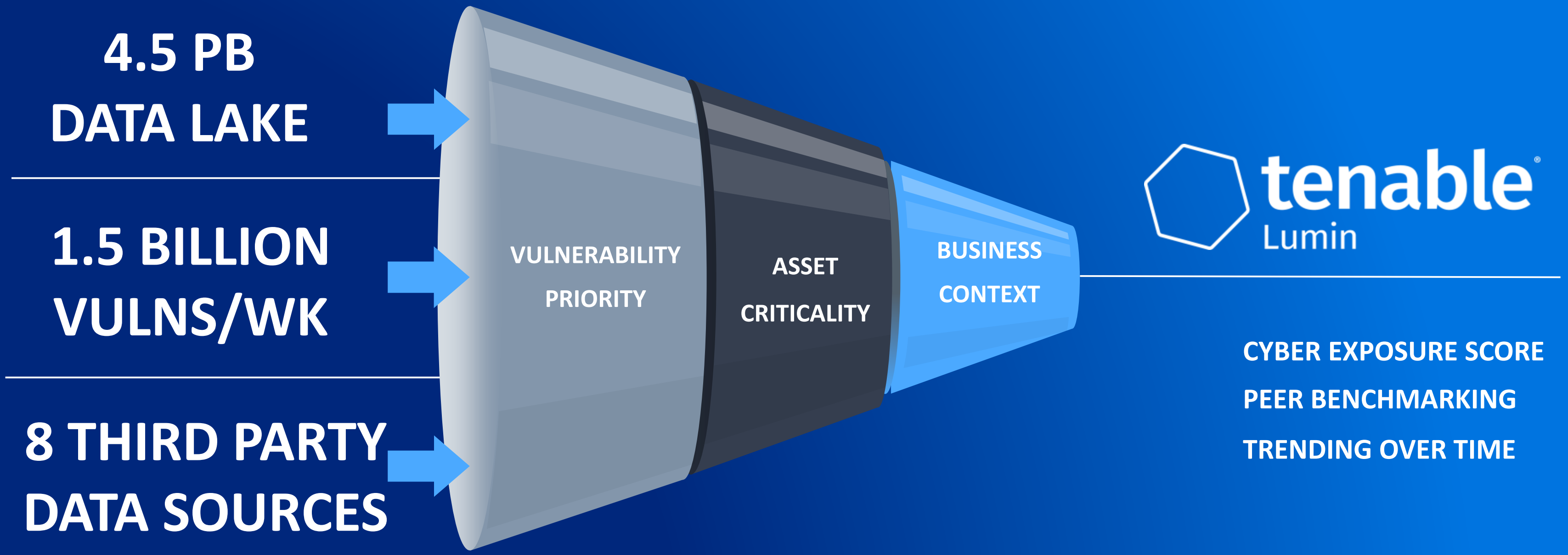
PRIORITIZING NEAR TERM THREAT



tenable

Introducing…Lumin

Cyber Exposure and Lumin



4.5 PB DATA LAKE

1.5 BILLION VULNS/WK

8 THIRD PARTY DATA SOURCES

CYBER EXPOSURE SCORE

PEER BENCHMARKING

TRENDING OVER TIME

Prioritize based on importance of asset AND risks posed by vulnerabilities on the asset

VPR + ACR

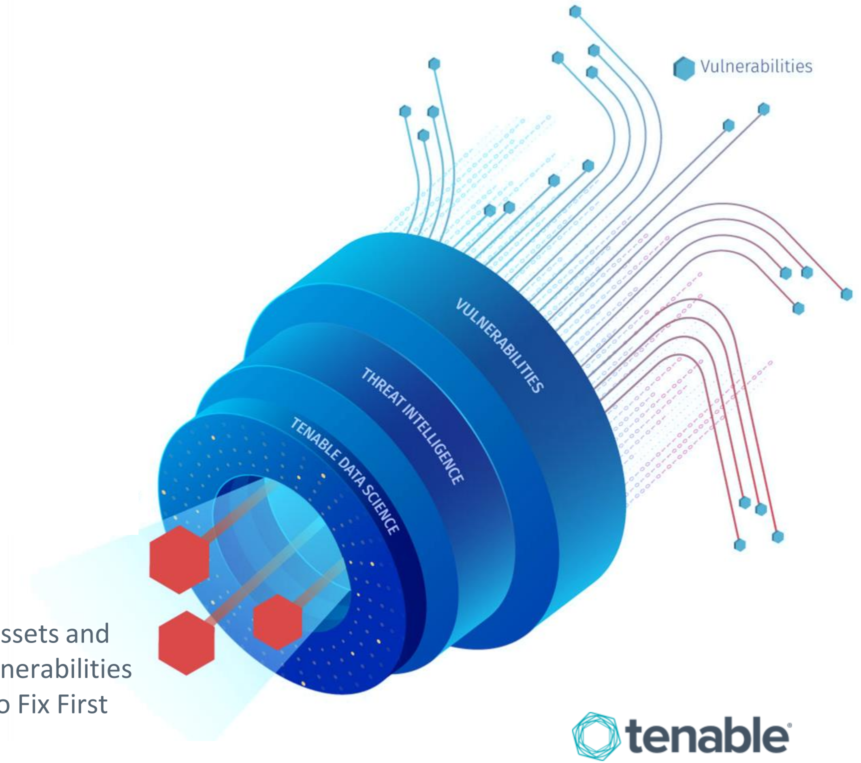
VULNERABILITY PRIORITY RATING

ASSET CRITICALITY RATING

Leverage machine learning and threat intelligence to prioritize vulnerabilities based on real world risk

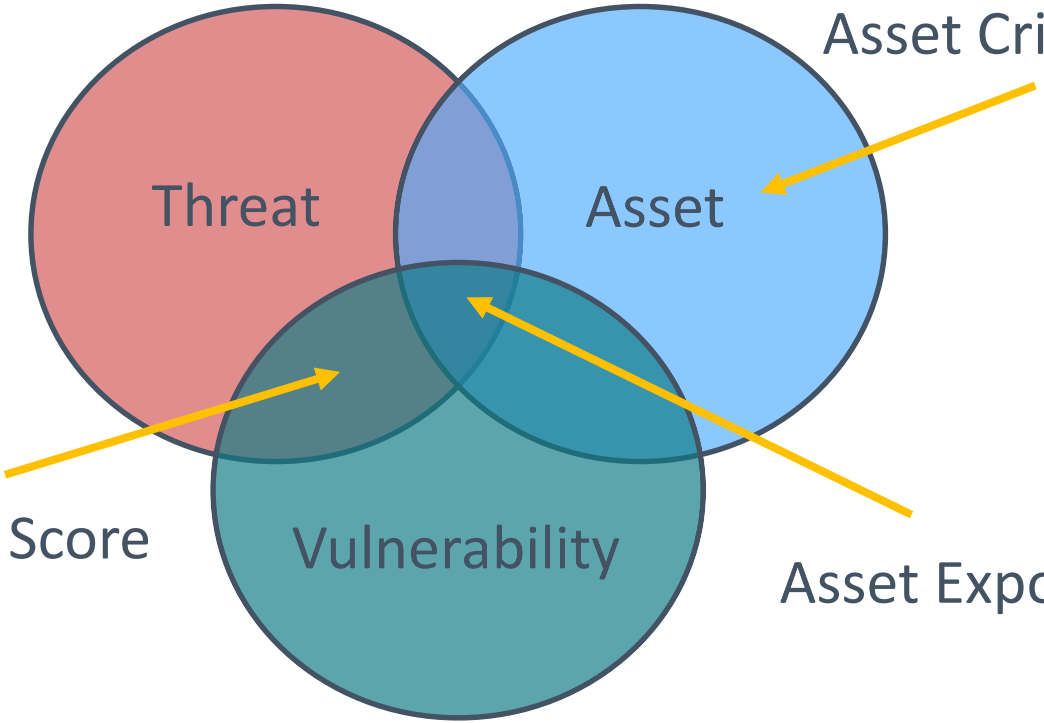
Prioritize assets based on indicators of business value and criticality

Focus First On What Matters Most



tenable

Risk Exposure Score



Threat

Asset

Vulnerability

Asset Criticality Score

Vulnerability Score

Asset Exposure Score

382

490

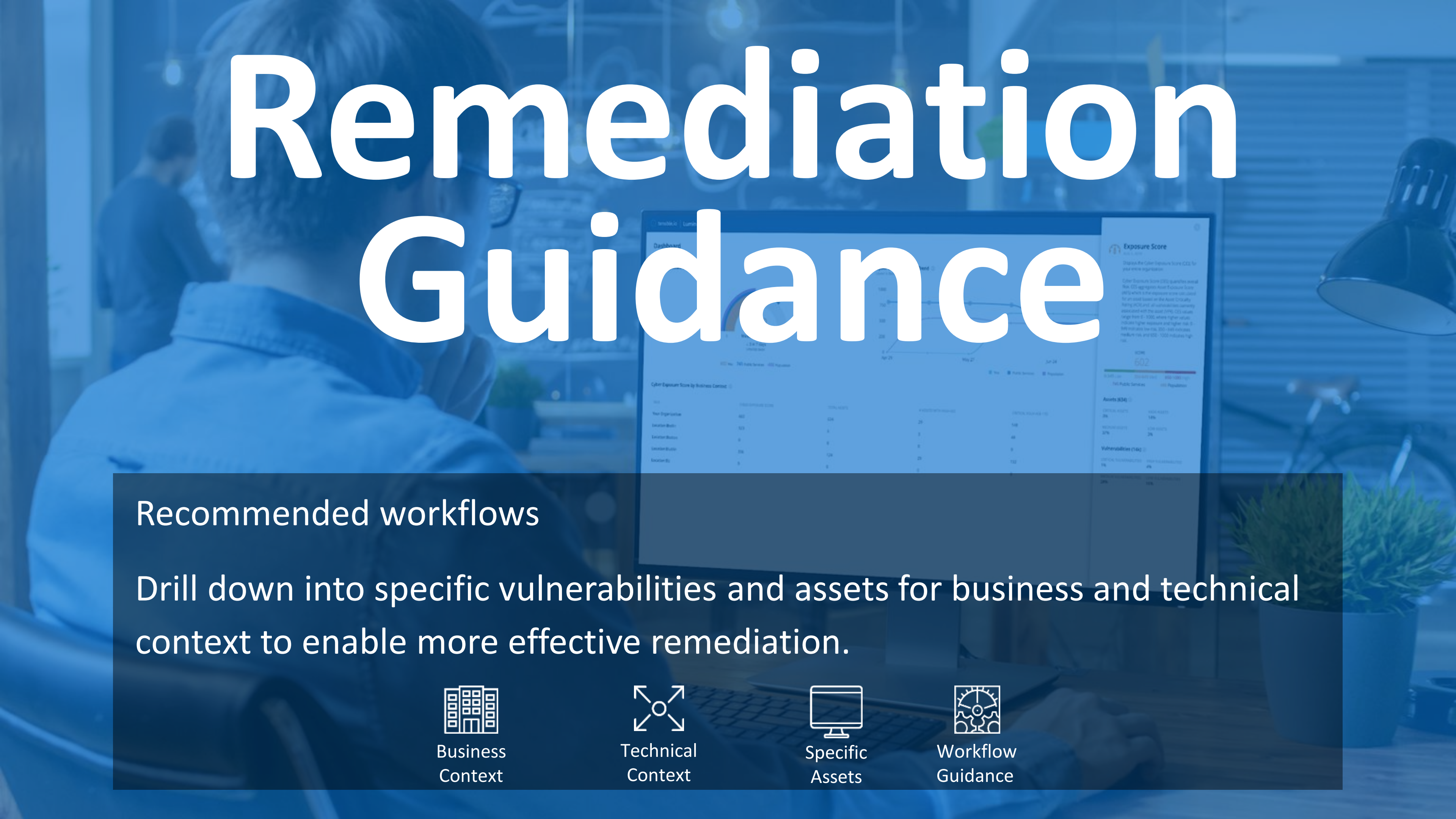
873

254

COMPARE

WITH PEERS AND POPULATION
FOR STRATEGIC DECISION SUPPORT

tenable



Remediation Guidance

Recommended workflows

Drill down into specific vulnerabilities and assets for business and technical context to enable more effective remediation.

Business Context

Technical Context

Specific Assets

Workflow Guidance

Gartner®

“BY 2022, ORGANIZATIONS THAT USE THE RISK-BASED VULNERABILITY MANAGEMENT METHOD WILL SUFFER 80% FEWER BREACHES.*”

* Gartner, A Guide to Choosing a Vulnerability Assessment Solution, Prateek Bhajanka, Mitchell Schneider, Craig Lawson, April 3, 2019.

tenable

tenable

tenable®

Thank You

RESOURCES

White Papers

Predictive Prioritization: How to Focus on the Vulnerabilities That Matter Most
https://www.tenable.com/whitepapers/predictive-prioritization-how-to-focus-on-the-vulnerabilities-that-matter-most

Predictive Prioritization: Data Science Lets You Focus on the 3% of Vulnerabilities Likely to Be Exploited
https://www.tenable.com/whitepapers/predictive-prioritization-data-science-lets-you-focus-on-3-percent-of-vulnerabilities

Carnegie Mellon University – "Towards Improving CVSS"
https://resources.sei.cmu.edu/asset_files/WhitePaper/2018_019_001_538372.pdf

Recorded Future Report "Top Ten Vulnerabilities of 2018" 03/19/19
https://www.recordedfuture.com/top-vulnerabilities-2018/