tenable

「知己知彼，百戰百勝」之漏洞處理

1 DEC 2022

TENABLE: FROM VULNERABILITY TO EXPOSURE MANAGEMENT LEADERSHIP

MARKET LEADERSHIP

#1

VM Market Share

3 years in a row

IDC

RESEARCH DEPTH

“Tenable has its own research team and is usually able to build new detections within 24 hours of finding new vulnerabilities.”

IDC

EXPANDING SCOPE

Leader in Forrester Wave for ICS Security Solutions

FORRESTER®

Named CNAPP & Active Directory Defense vendor

Gartner

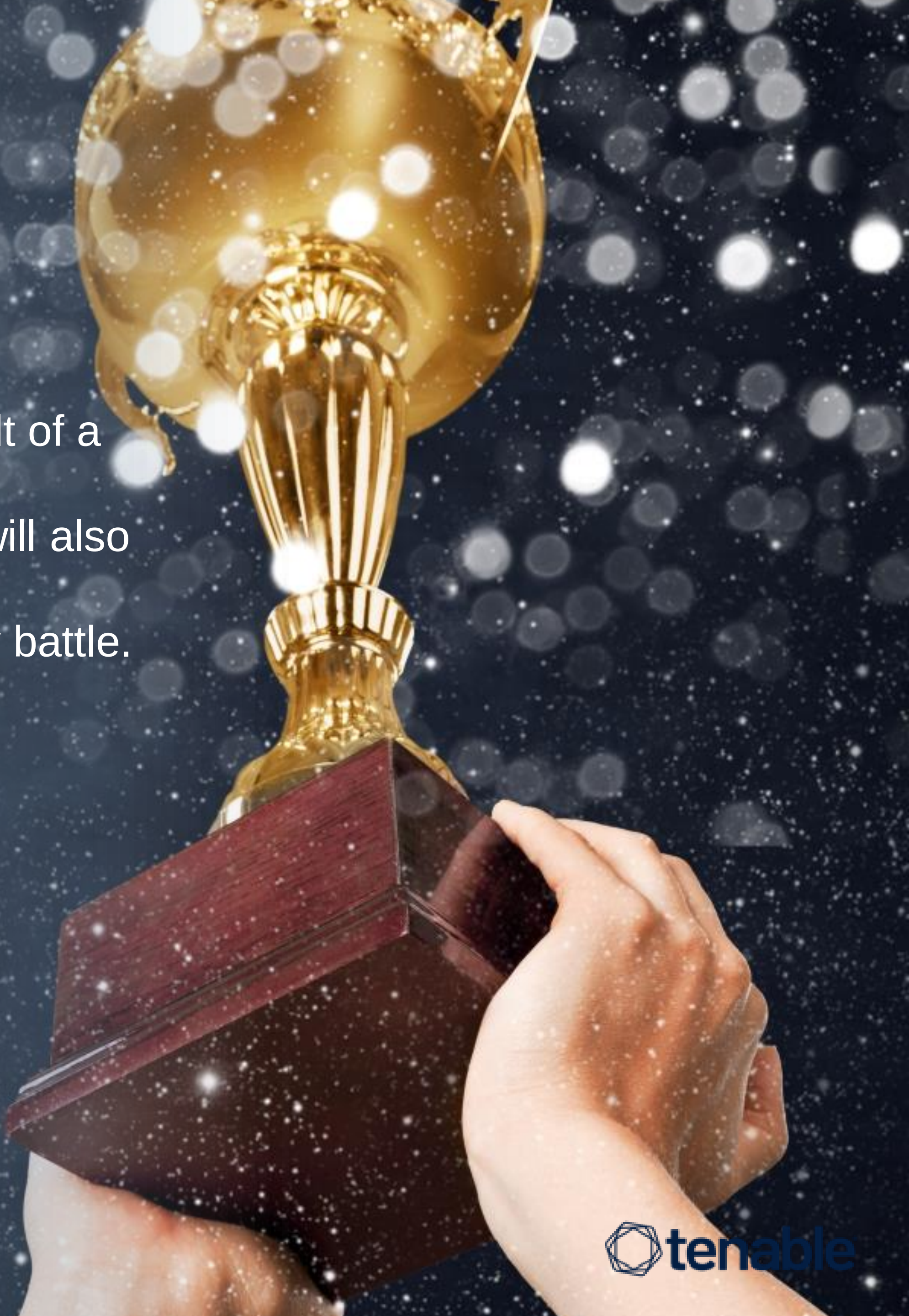
tenable

THE ART OF WAR

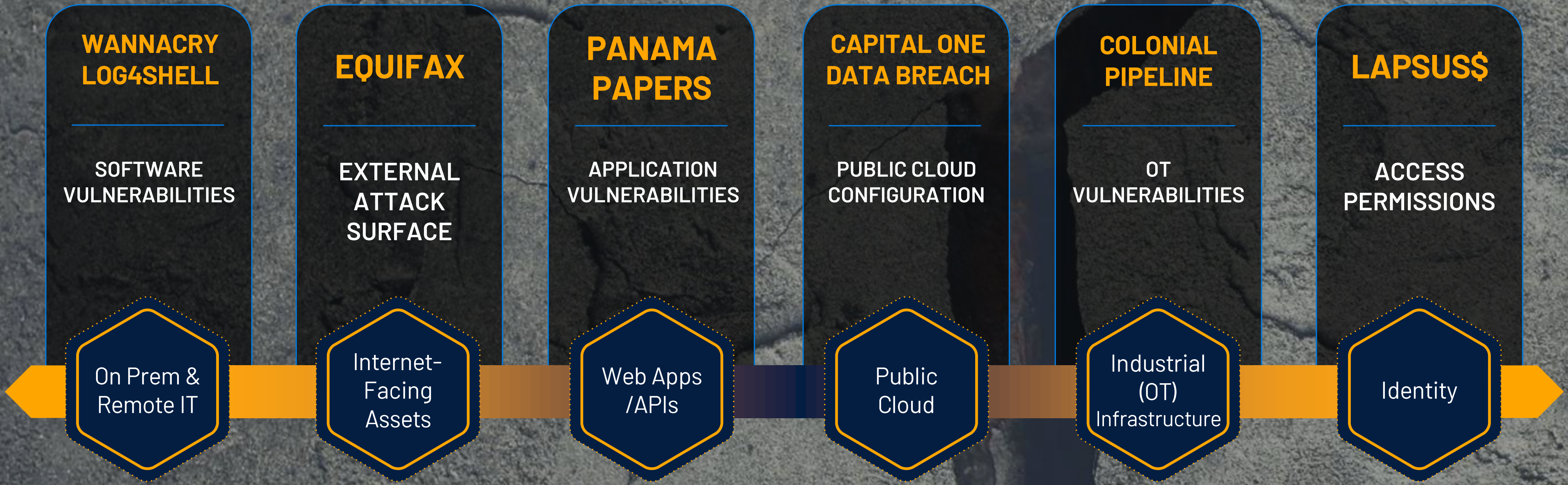
If you know the enemy and know yourself, you need not fear the result of a hundred battles.
If you know yourself but not the enemy, for every victory gained you will also suffer a defeat.
If you know neither the enemy nor yourself, you will succumb in every battle.

知己知彼，百戰不殆；
不知彼而知己，一勝一負；
不知彼，不知己，每戰必殆

孫子兵法 《謀攻篇》

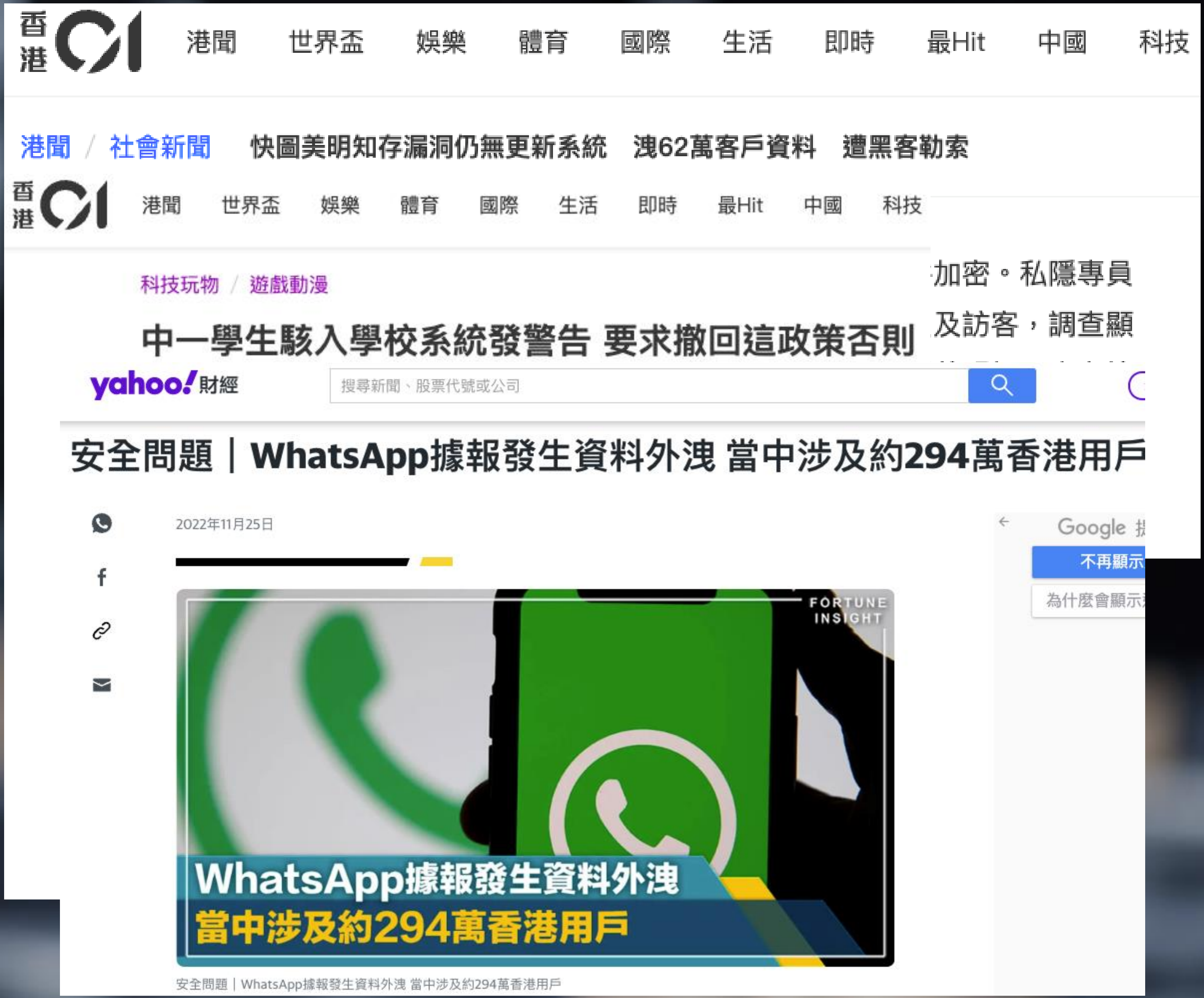


SIGNIFICANT BREACHES TARGET THE WEAKEST LINK ACROSS THE ENTIRE ATTACK SURFACE



WANNACRY LOG4SHELL	EQUIFAX	PANAMA PAPERS	CAPITAL ONE DATA BREACH	COLONIAL PIPELINE	LAPSUS$
SOFTWARE VULNERABILITIES	EXTERNAL ATTACK SURFACE	APPLICATION VULNERABILITIES	PUBLIC CLOUD CONFIGURATION	OT VULNERABILITIES	ACCESS PERMISSIONS
On Prem & Remote IT	Internet-Facing Assets	Web Apps /APIs	Public Cloud	Industrial (OT) Infrastructure	Identity

tenable



港聞 / 社會新聞

快圖美明知存漏洞仍無更新系統 洩62萬客戶資料 遭黑客勒索

科技玩物 / 遊戲動漫

中一學生駭入學校系統發警告 要求撤回這政策否則

加密。私隱專員

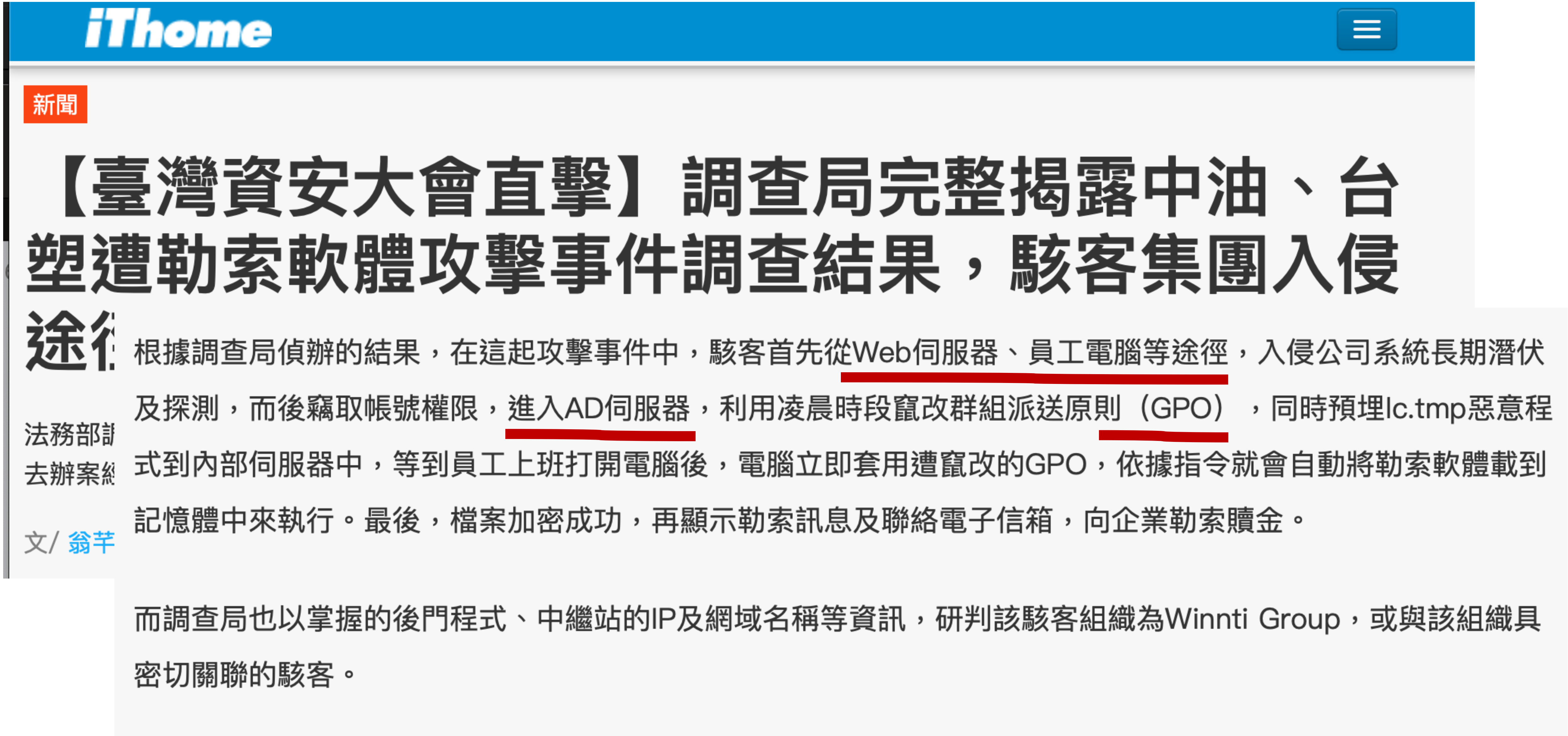
及訪客，調查顯

安全問題｜WhatsApp據報發生資料外洩 當中涉及約294萬香港用戶

2022年11月25日

安全問題｜WhatsApp據報發生資料外洩 當中涉及約294萬香港用戶

BEHIND ALMOST EVERY **BREACH** HEADLINE IS A **KNOWN VULNERABILITY** AND **MISCONFIGURATION**



新聞

【臺灣資安大會直擊】調查局完整揭露中油、台塑遭勒索軟體攻擊事件調查結果，駭客集團入侵途徑

法務部
去辦案

文/ 翁芊

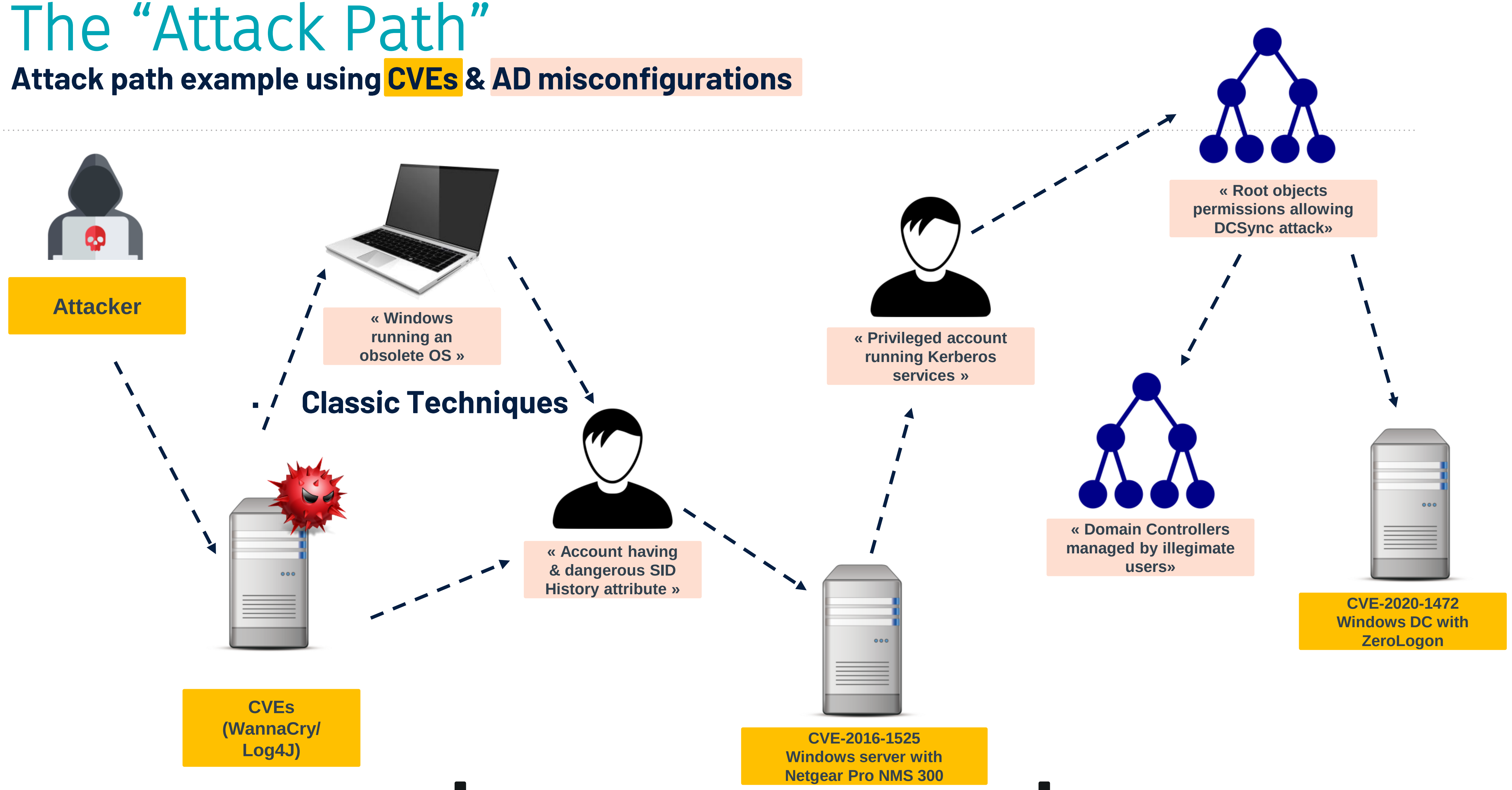
根據調查局偵辦的結果，在這起攻擊事件中，駭客首先從Web伺服器、員工電腦等途徑，入侵公司系統長期潛伏及探測，而後竊取帳號權限，進入AD伺服器，利用凌晨時段竄改群組派送原則（GPO），同時預埋Ic.tmp惡意程式到內部伺服器中，等到員工上班打開電腦後，電腦立即套用遭竄改的GPO，依據指令就會自動將勒索軟體載到記憶體中來執行。最後，檔案加密成功，再顯示勒索訊息及聯絡電子信箱，向企業勒索贖金。

而調查局也以掌握的後門程式、中繼站的IP及網域名稱等資訊，研判該駭客組織為Winnti Group，或與該組織具密切關聯的駭客。

Source: ithome.com.tw

The “Attack Path”

Attack path example using CVEs & AD misconfigurations



Attacker

« Windows running an obsolete OS »

Classic Techniques

CVEs (WannaCry/ Log4J)

« Account having & dangerous SID History attribute »

CVE-2016-1525 Windows server with Netgear Pro NMS 300

« Privileged account running Kerberos services »

« Root objects permissions allowing DCSync attack»

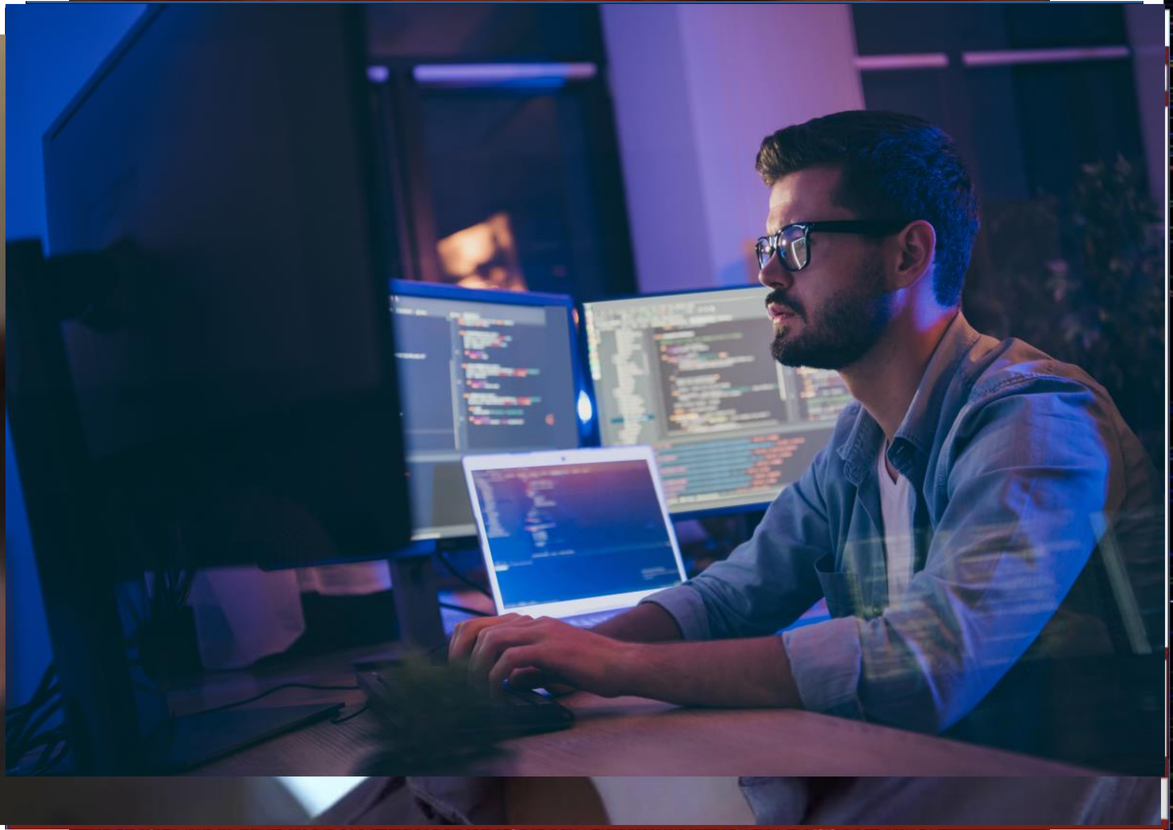
« Domain Controllers managed by illegimate users»

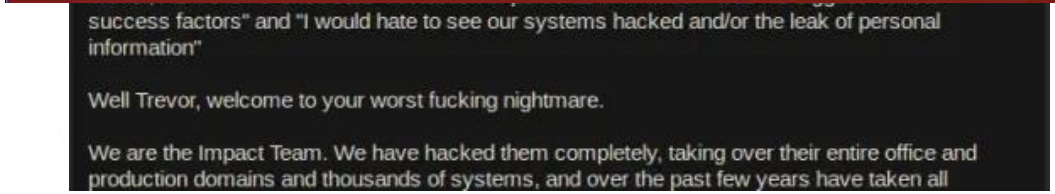
CVE-2020-1472 Windows DC with ZeroLogon

Primo-infection & Pivoting | **Lateral movement & privileges escalation** | **Domain dominance**

REASONS OF **HACKING**

AM AND EM MUST SHUT DOWN





success factors" and "I would hate to see our systems hacked and/or the leak of personal information"

Well Trevor, welcome to your worst fucking nightmare.

We are the Impact Team. We have hacked them completely, taking over their entire office and production domains and thousands of systems, and over the past few years have taken all

FUN AND SHOW OFF

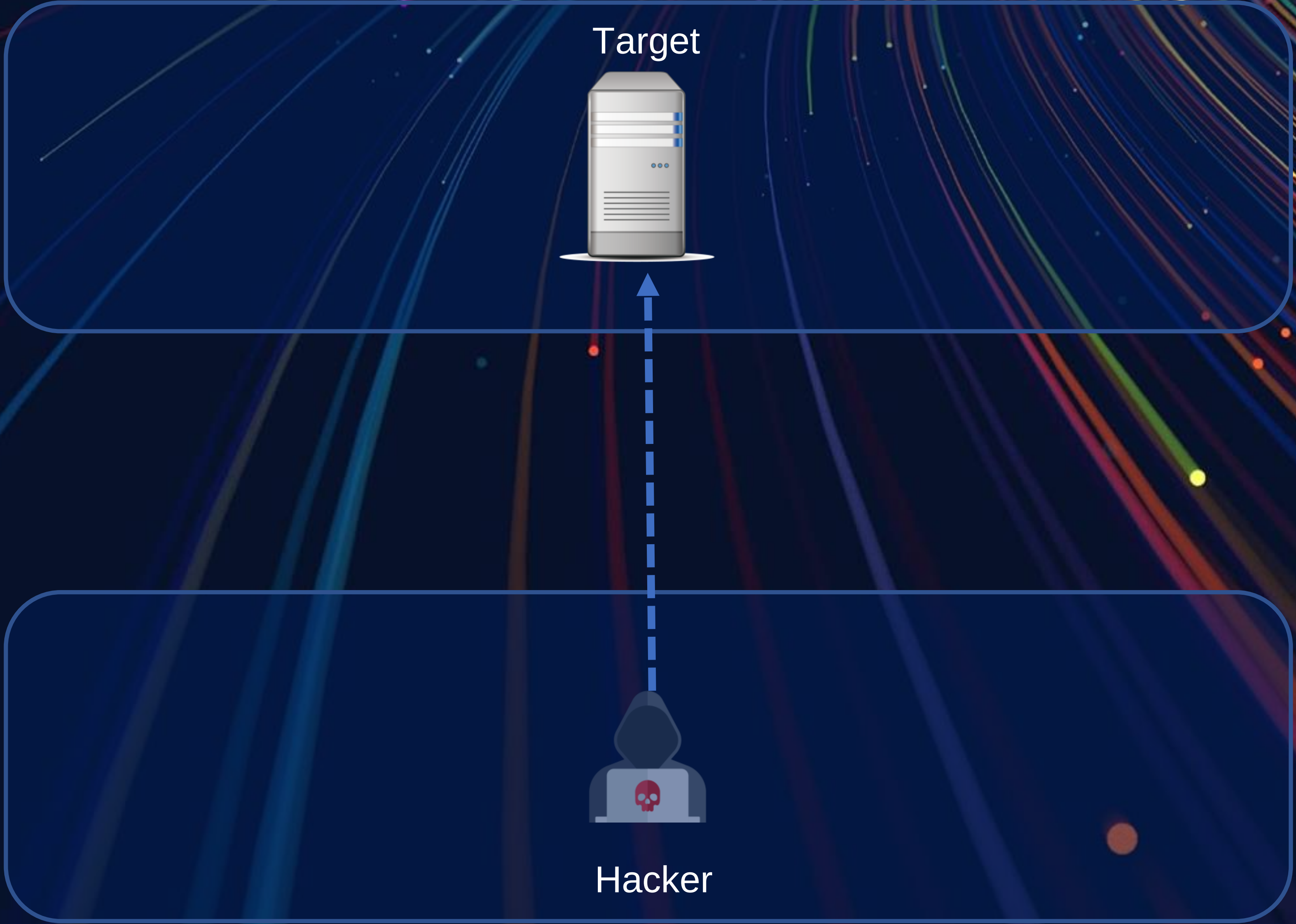
MONEY

HACKTIVISM

POLITICAL HACKING

PENETRATION TEST

How do Attackers Attack?



Target

Hacker

What is Vulnerability ?

Software bug or weak point in

- Operating System,
- Hypervisor,
- Application,
- Database,
- Javascript,
- etc etc

What is **Exploit**?

Exploits are the means through which a vulnerability can be leveraged for malicious activity by hackers

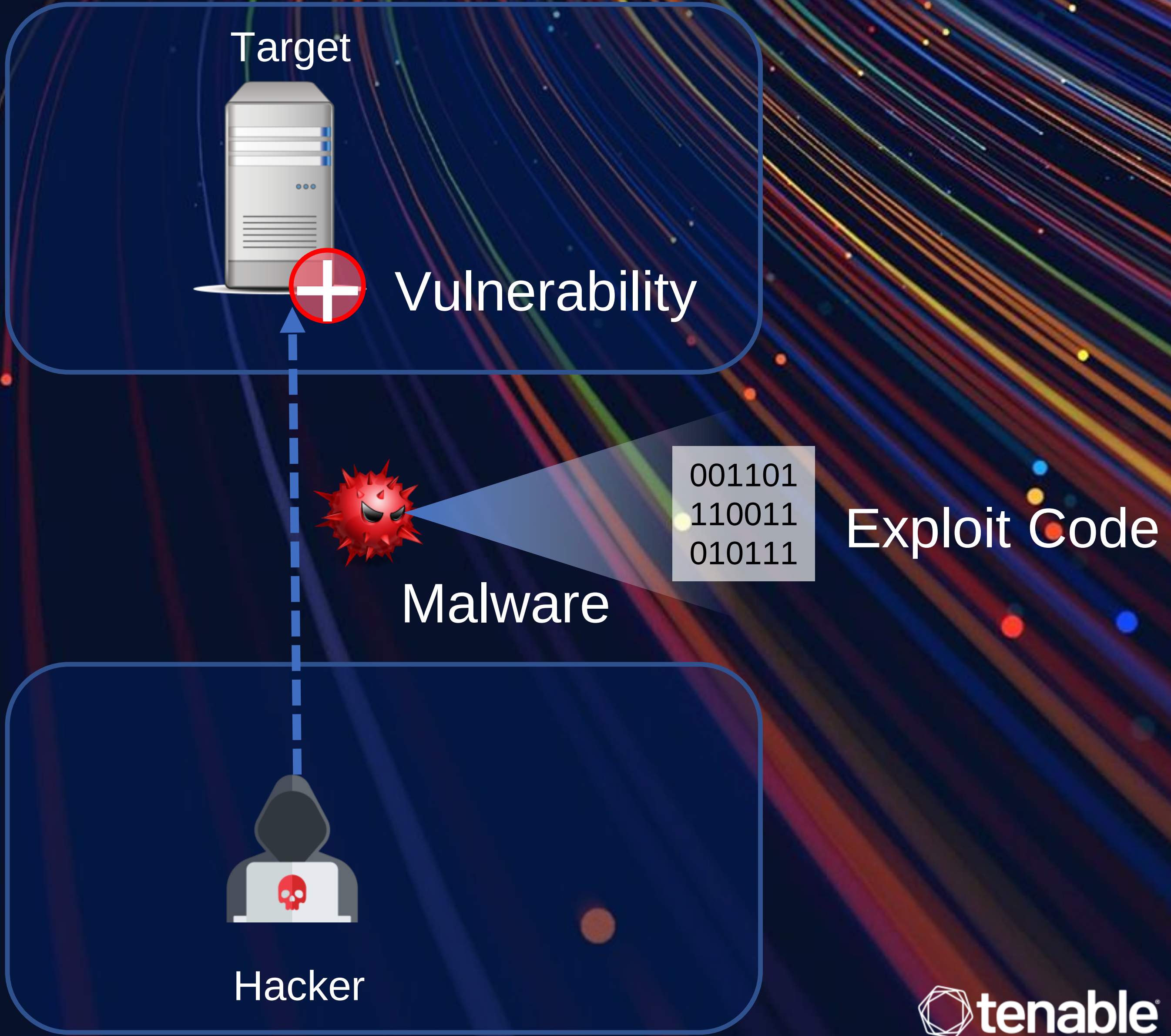
- pieces of software,
- sequences of commands
- open-source exploit kits

What is Malware & Ransomware?

- **Computer program** written to use (exploit) a **Vulnerability**

How do Attackers Attack?

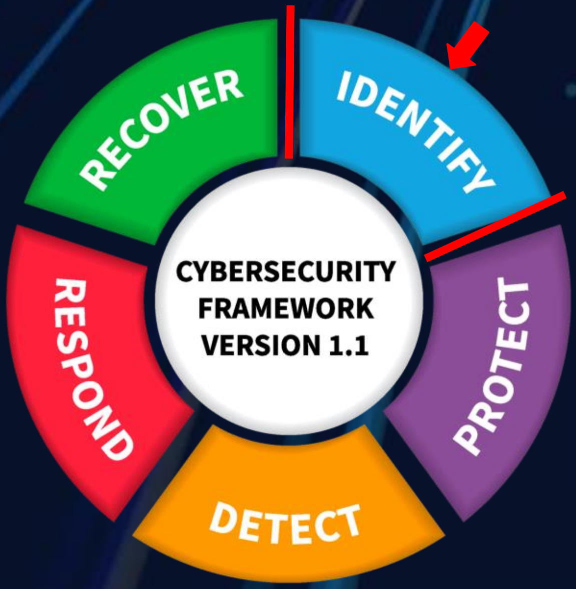
1. Locate target(eg Shodan.io)
2. Discover its weak point (vulnerability)
3. Use relative weapon to attack target (eg WannaCry)
4. Take control, steal or encrypt data, cause chaos, etc



KNOW YOURSELF , KNOW YOUR ENEMY, HOW?

Understanding the visibility

Visibility is foundational to cybersecurity



NIST Cybersecurity Framework

Basic

1 Inventory and Control of Hardware Assets

3 Data protection

2 Inventory and Control of Software Assets

5 Account management

CIS Controls, Version 8

VISIBILITY | Know yourself

ATTACKERS **DON'T DIFFERENTIATE** BETWEEN ASSET TYPES

Known Asset:

- Vulnerabilities/misconfiguration
- Running Service and installed application is authorized or not
- Critical/important asset

UnKnown Asset:

- Authorized or Unauthorized
- Vulnerabilities/misconfiguration
- Running Service and installed application is authorized or not

INFRA STRUCTURE

INTERNET ATTACK SURFACE

WEB APPLICATION

CLOUD INFRA

OT INFRA

PRIORITIZE RESOURCE TO REACT | Know the enemy

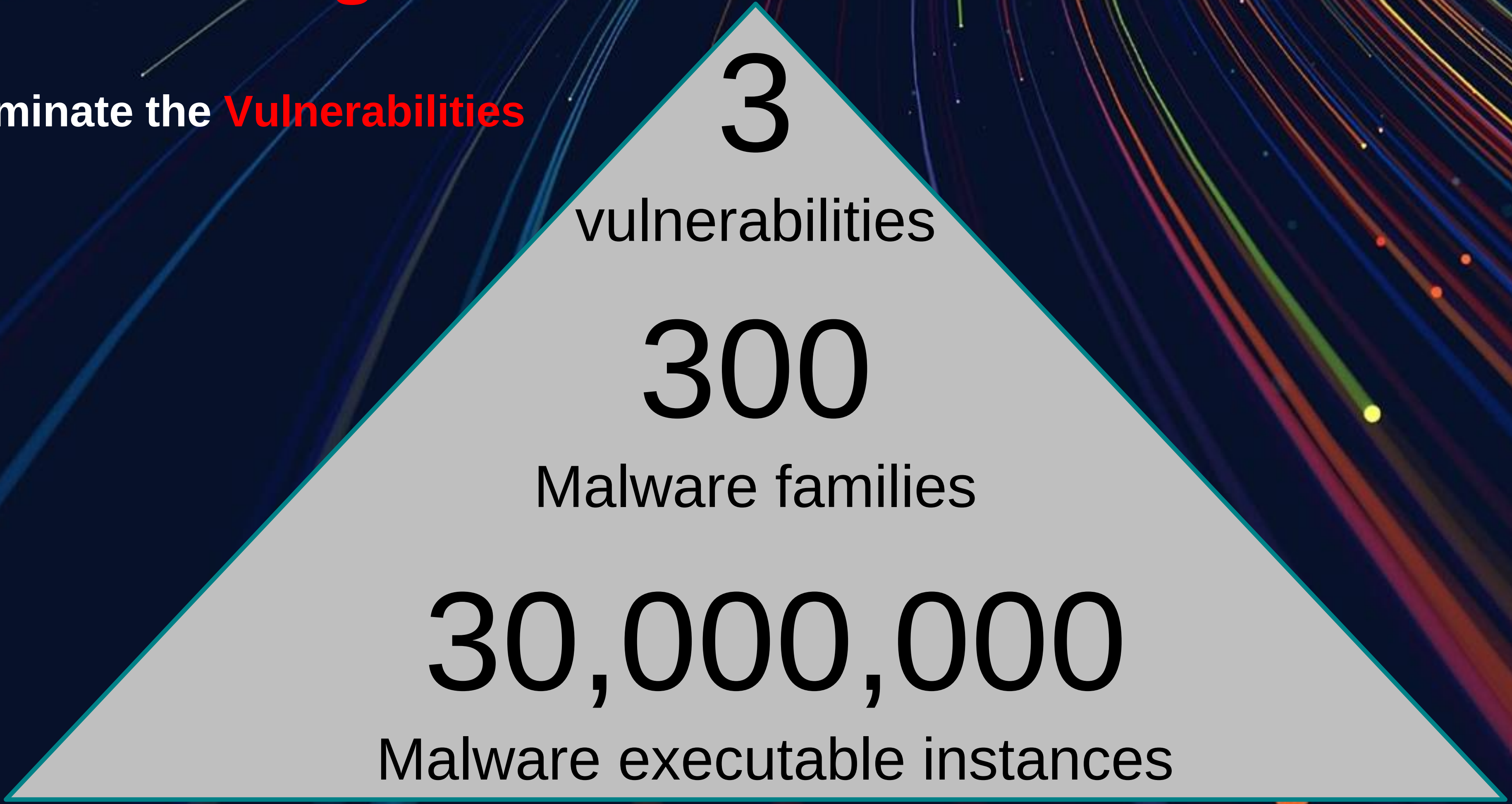
What do the hacker want?	-Business/customer information -System control/ Denial of service
Where is the attack entry point?	-Every attack surface
What is the threat actor's weapon?	- Exploit for vulnerability - Exploit for misconfiguration
Is the vulnerability exploitable?	-Allocate resource for higher priority to handle

WHEN WE GOT THE ASSET INVENTORY,
VULNERABILITY LIST,
THEN WHAT’S NEXT ?

Which Problem do You Want to Solve?

Solve the Right Problem

Eliminate the Vulnerabilities



3

vulnerabilities

300

Malware families

30,000,000

Malware executable instances

What is CVE and CVSS?

CVE
Common Vulnerabilities and Exposures.
(CVE-2018-2879)

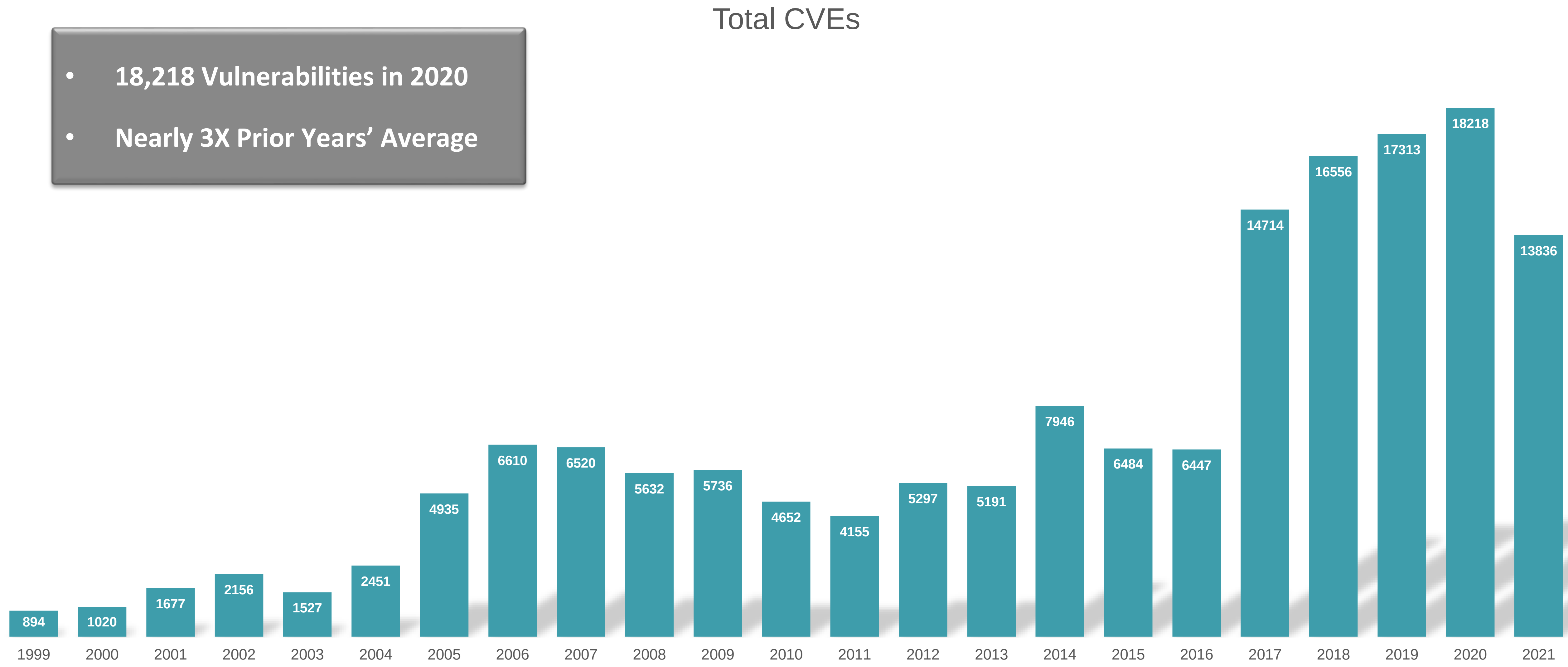
CVSS
Common Vulnerability Scoring System
Prioritizing the security of vulnerabilities.

Severity	Base Score
None	0
Low	0.1-3.9
Medium	4.0-6.9
High	7.0-8.9
Critical	9.0-10.0

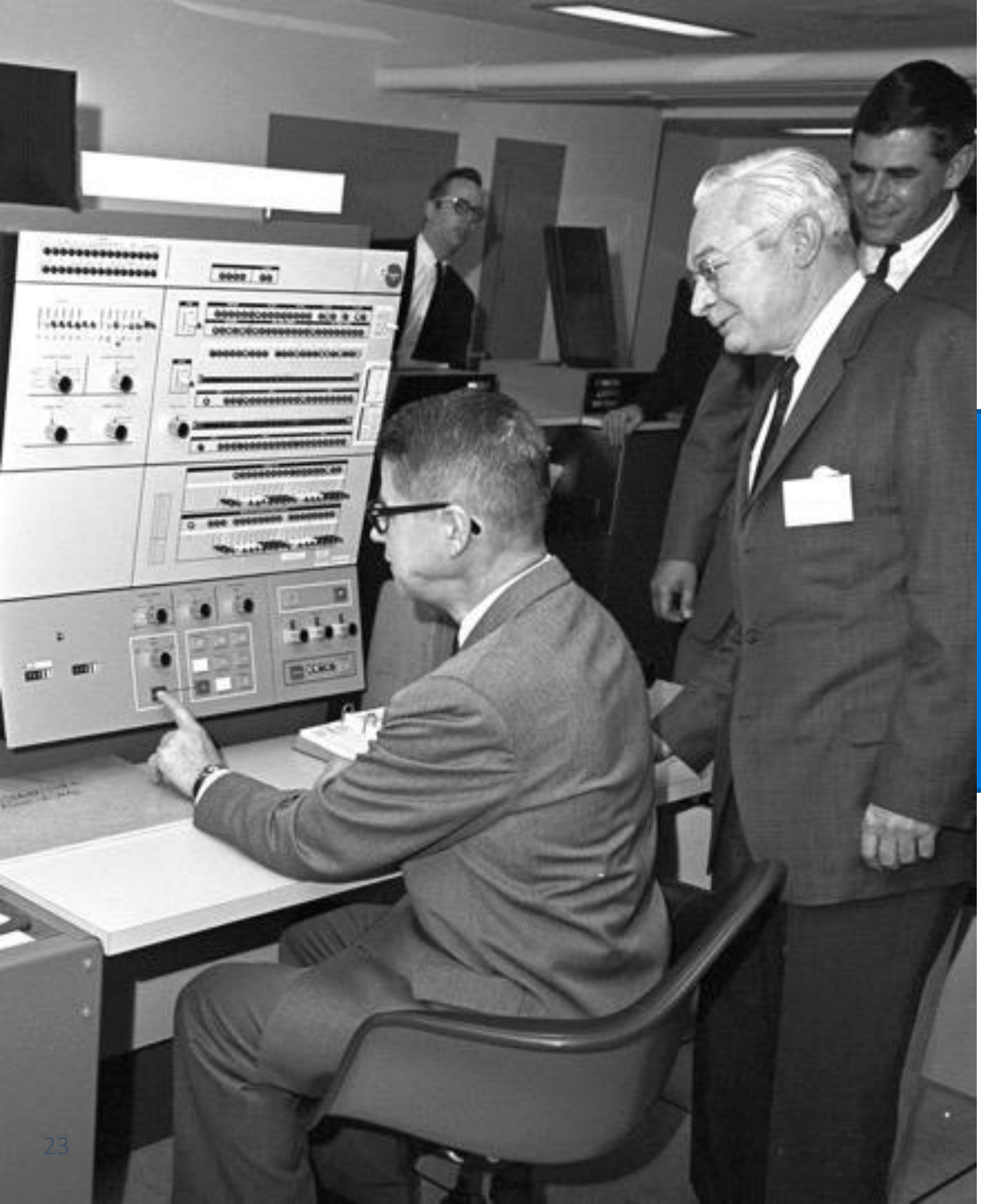
tenable

The Number of New Vulnerabilities Continues to Grow

- 18,218 Vulnerabilities in 2020
- Nearly 3X Prior Years' Average



Source: Vulnerability Intelligence Report, Tenable Research



Legacy Vulnerability Management Can't Keep Up

Limited Visibility	Ineffective Prioritization	Poor Communication

Legacy Tools Can't Handle The Modern Attack Surface

CVSS is Heavily Flawed

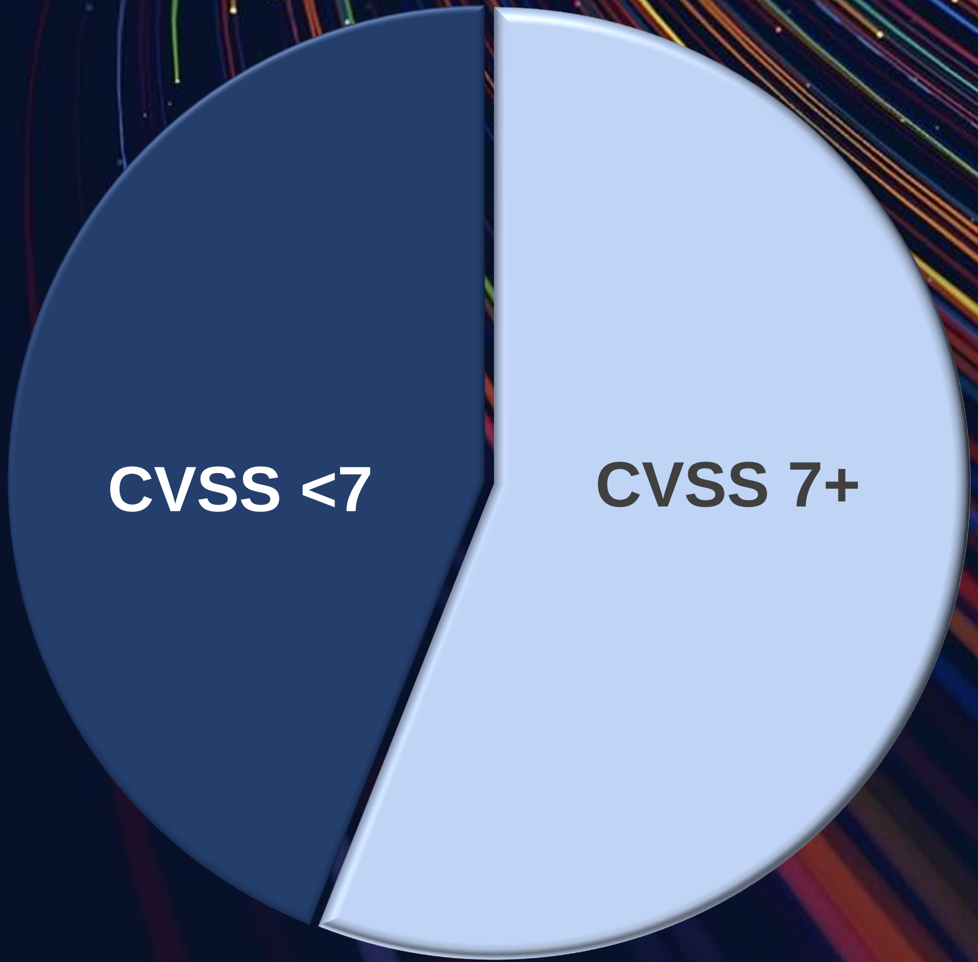
"CVSS is designed to identify the technical severity of a vulnerability. What people seem to want to know, instead, is the risk a vulnerability or flaw poses to them, or ***how quickly they should respond to a vulnerability***."

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

If Everything is CRITICAL, Nothing is …

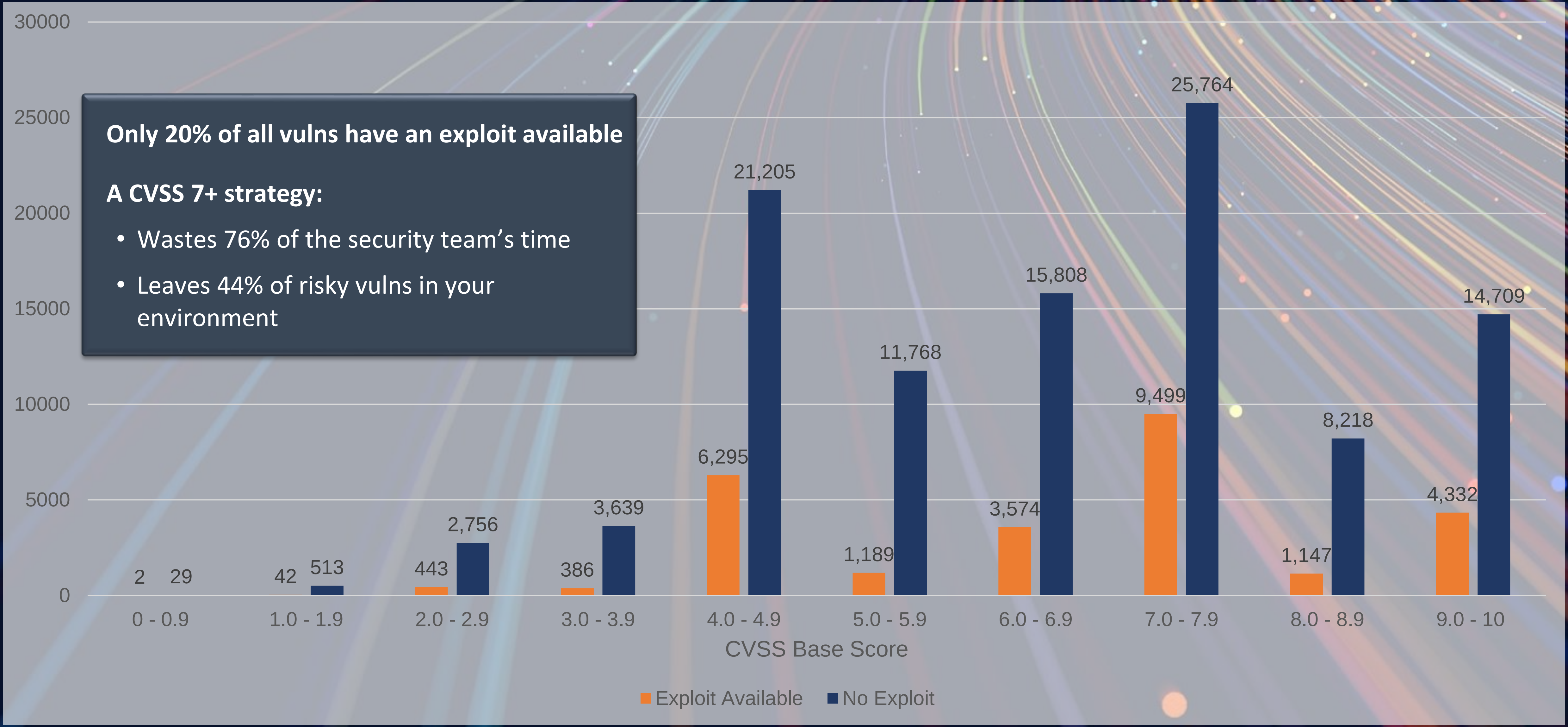
56% of all vulns
are rated **High or Critical**.

Teams waste the majority of their time chasing after the **wrong issues**.



Source: Vulnerability Intelligence Report, Tenable Research

CVSS is a Poor Indicator of Risk



Only 20% of all vulns have an exploit available

A CVSS 7+ strategy:

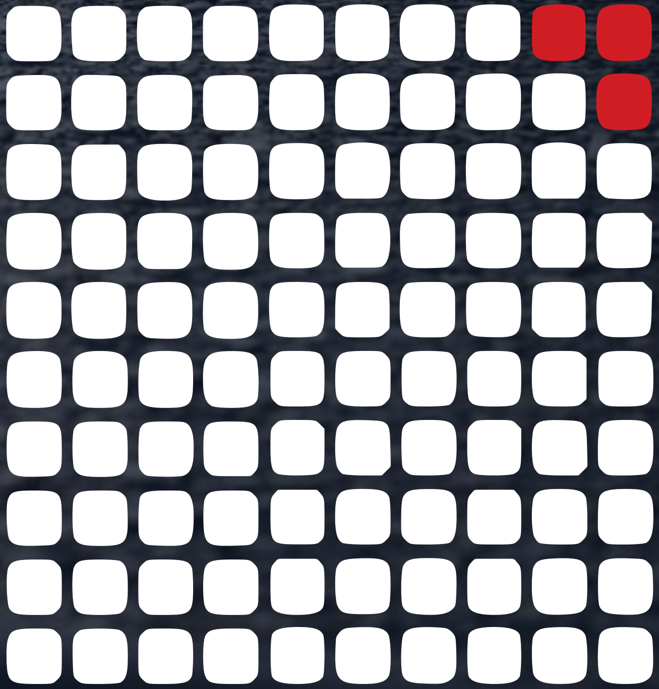
- Wastes 76% of the security team’s time
- Leaves 44% of risky vulns in your environment

Source: Tenable Research

YOU’VE GOT **99 FLAWS** BUT ALL THEY NEED IS **ONE**

<3%

OF VULNERABILITIES HAVE A HIGH PROBABILITY OF BEING **LEVERAGED IN ATTACKS**



Low	Medium	High	Critical
(0.0-3.9)	(4.0-6.9)	(7.0-8.9)	(9.0-10)

VPR

VULNERABILITY PRIORITY RATING

Leverages supervised machine learning algorithms to calculate the priority of a vulnerability based on the real threat posed.
Key Drivers include

Threat Recency

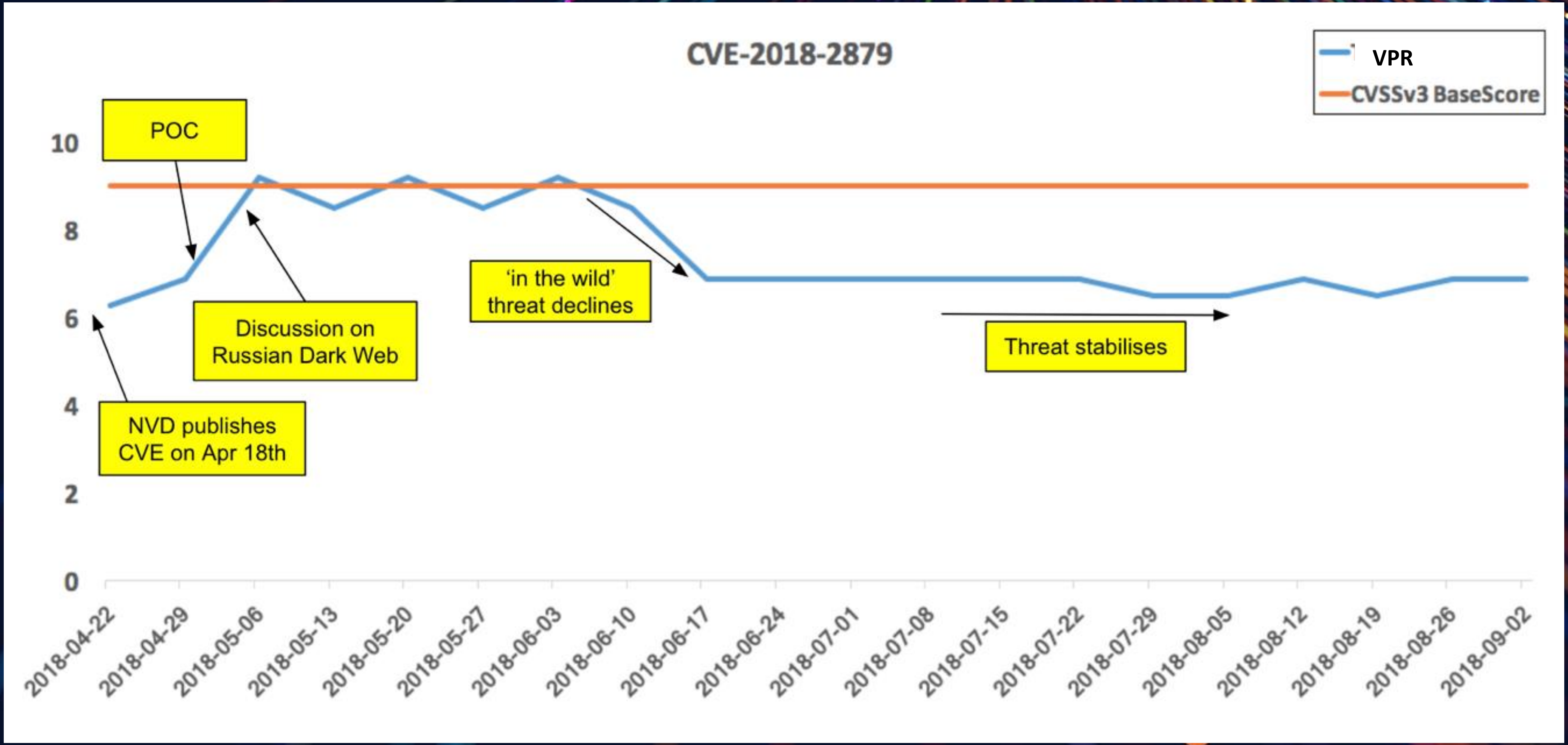
Threat Intensity

Exploitability

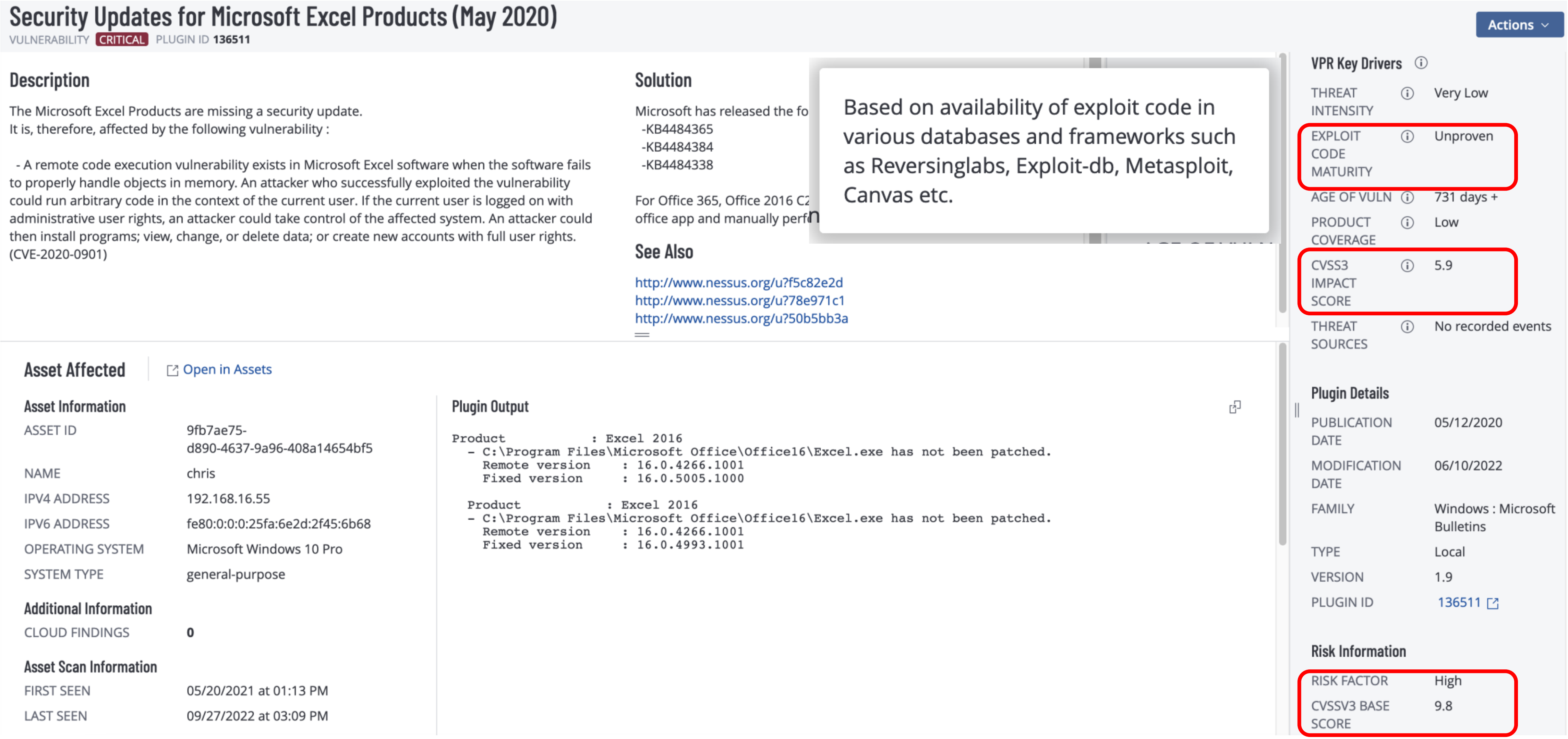
Vulnerability Age

Threat Sources

VPR can sometimes tell you things aren’t so bad



Example of VPR with CVSS score



Security Updates for Microsoft Excel Products (May 2020)

VULNERABILITY CRITICAL PLUGIN ID **136511**

Description

The Microsoft Excel Products are missing a security update.
It is, therefore, affected by the following vulnerability :

- A remote code execution vulnerability exists in Microsoft Excel software when the software fails to properly handle objects in memory. An attacker who successfully exploited the vulnerability could run arbitrary code in the context of the current user. If the current user is logged on with administrative user rights, an attacker could take control of the affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. (CVE-2020-0901)

Solution

Microsoft has released the fo
-KB4484365
-KB4484384
-KB4484338

For Office 365, Office 2016 C2
office app and manually perf

Based on availability of exploit code in various databases and frameworks such as Reversinglabs, Exploit-db, Metasploit, Canvas etc.

See Also

http://www.nessus.org/u?f5c82e2d
http://www.nessus.org/u?78e971c1
http://www.nessus.org/u?50b5bb3a

VPR Key Drivers

THREAT INTENSITY	Very Low
EXPLOIT CODE MATURITY	Unproven
AGE OF VULN	731 days +
PRODUCT COVERAGE	Low
CVSS3 IMPACT SCORE	5.9
THREAT SOURCES	No recorded events

Asset Affected

Open in Assets

Asset Information

ASSET ID	9fb7ae75-d890-4637-9a96-408a14654bf5
NAME	chris
IPV4 ADDRESS	192.168.16.55
IPV6 ADDRESS	fe80:0:0:0:25fa:6e2d:2f45:6b68
OPERATING SYSTEM	Microsoft Windows 10 Pro
SYSTEM TYPE	general-purpose

Additional Information

CLOUD FINDINGS	**0**

Asset Scan Information

FIRST SEEN	05/20/2021 at 01:13 PM
LAST SEEN	09/27/2022 at 03:09 PM

Plugin Output

```
Product            : Excel 2016
  - C:\Program Files\Microsoft Office\Office16\Excel.exe has not been patched.
    Remote version     : 16.0.4266.1001
    Fixed version      : 16.0.5005.1000

  Product            : Excel 2016
  - C:\Program Files\Microsoft Office\Office16\Excel.exe has not been patched.
    Remote version     : 16.0.4266.1001
    Fixed version      : 16.0.4993.1001
```

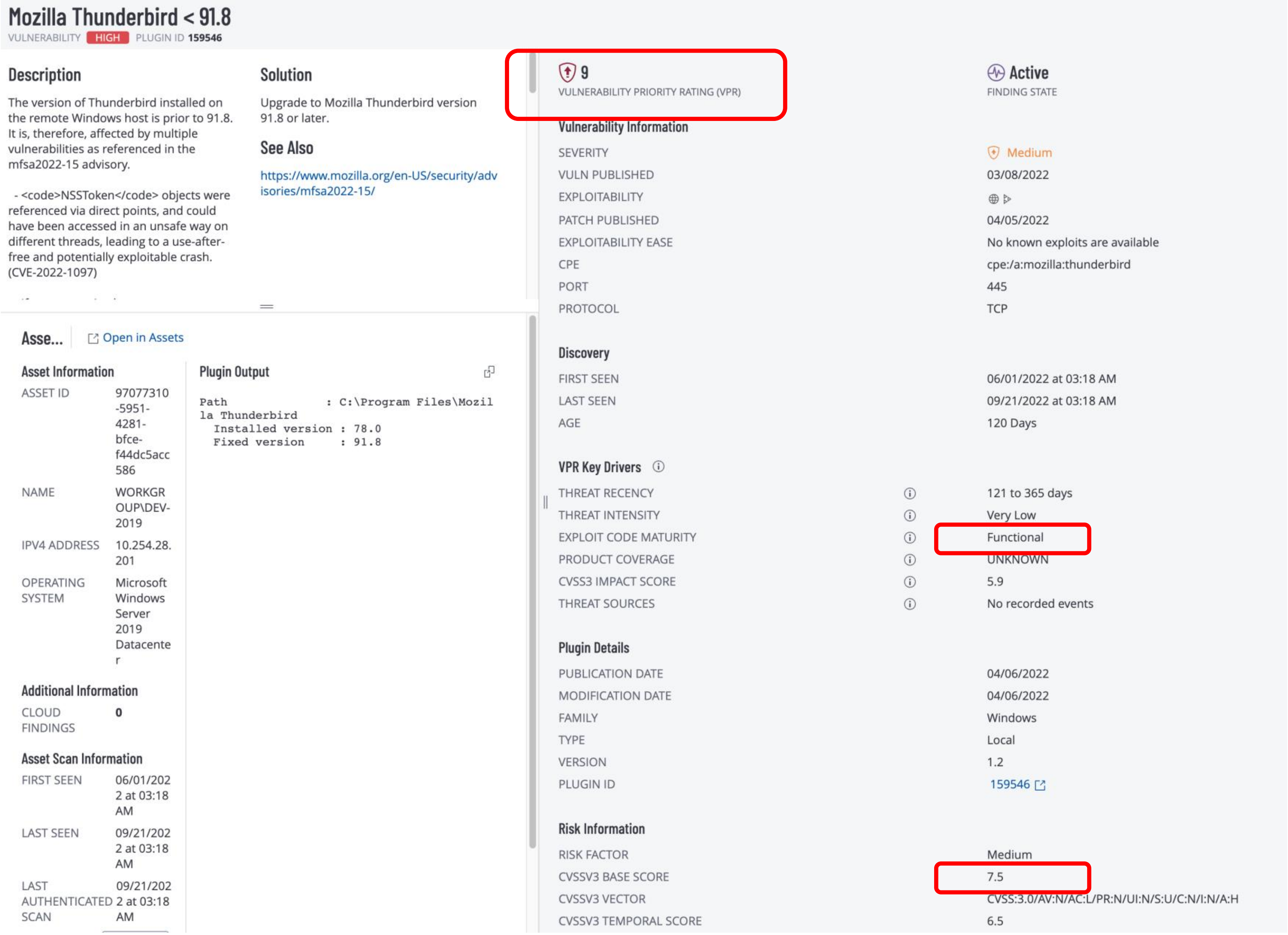
Plugin Details

PUBLICATION DATE	05/12/2020
MODIFICATION DATE	06/10/2022
FAMILY	Windows : Microsoft Bulletins
TYPE	Local
VERSION	1.9
PLUGIN ID	136511

Risk Information

RISK FACTOR	High
CVSSV3 BASE SCORE	9.8

Example of VPR with CVSS score



Mozilla Thunderbird < 91.8

VULNERABILITY HIGH PLUGIN ID **159546**

Description

The version of Thunderbird installed on the remote Windows host is prior to 91.8. It is, therefore, affected by multiple vulnerabilities as referenced in the mfsa2022-15 advisory.

- <code>NSSToken</code> objects were referenced via direct points, and could have been accessed in an unsafe way on different threads, leading to a use-after-free and potentially exploitable crash. (CVE-2022-1097)

Solution

Upgrade to Mozilla Thunderbird version 91.8 or later.

See Also

https://www.mozilla.org/en-US/security/advisories/mfsa2022-15/

Asse...

Open in Assets

Asset Information

ASSET ID	97077310-5951-4281-bfce-f44dc5acc586
NAME	WORKGROUP\DEV-2019
IPV4 ADDRESS	10.254.28.201
OPERATING SYSTEM	Microsoft Windows Server 2019 Datacenter

Additional Information

CLOUD FINDINGS	**0**

Asset Scan Information

FIRST SEEN	06/01/2022 at 03:18 AM
LAST SEEN	09/21/2022 at 03:18 AM
LAST AUTHENTICATED SCAN	09/21/2022 at 03:18 AM

Plugin Output

```
Path              : C:\Program Files\Mozil
la Thunderbird
  Installed version : 78.0
  Fixed version     : 91.8
```

9
VULNERABILITY PRIORITY RATING (VPR)

Active
FINDING STATE

Vulnerability Information

SEVERITY	Medium
VULN PUBLISHED	03/08/2022
EXPLOITABILITY	
PATCH PUBLISHED	04/05/2022
EXPLOITABILITY EASE	No known exploits are available
CPE	cpe:/a:mozilla:thunderbird
PORT	445
PROTOCOL	TCP

Discovery

FIRST SEEN	06/01/2022 at 03:18 AM
LAST SEEN	09/21/2022 at 03:18 AM
AGE	120 Days

VPR Key Drivers

THREAT RECENCY	121 to 365 days
THREAT INTENSITY	Very Low
EXPLOIT CODE MATURITY	Functional
PRODUCT COVERAGE	UNKNOWN
CVSS3 IMPACT SCORE	5.9
THREAT SOURCES	No recorded events

Plugin Details

PUBLICATION DATE	04/06/2022
MODIFICATION DATE	04/06/2022
FAMILY	Windows
TYPE	Local
VERSION	1.2
PLUGIN ID	159546

Risk Information

RISK FACTOR	Medium
CVSSV3 BASE SCORE	7.5
CVSSV3 VECTOR	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H
CVSSV3 TEMPORAL SCORE	6.5

Picking the right tool for the job

nessus Professional

Nessus Professional is Tenable’s Vulnerability Assessment tool, born in 1998, the technology has been refined over 23 years and remains at the core of all our products.

#1 in Accuracy

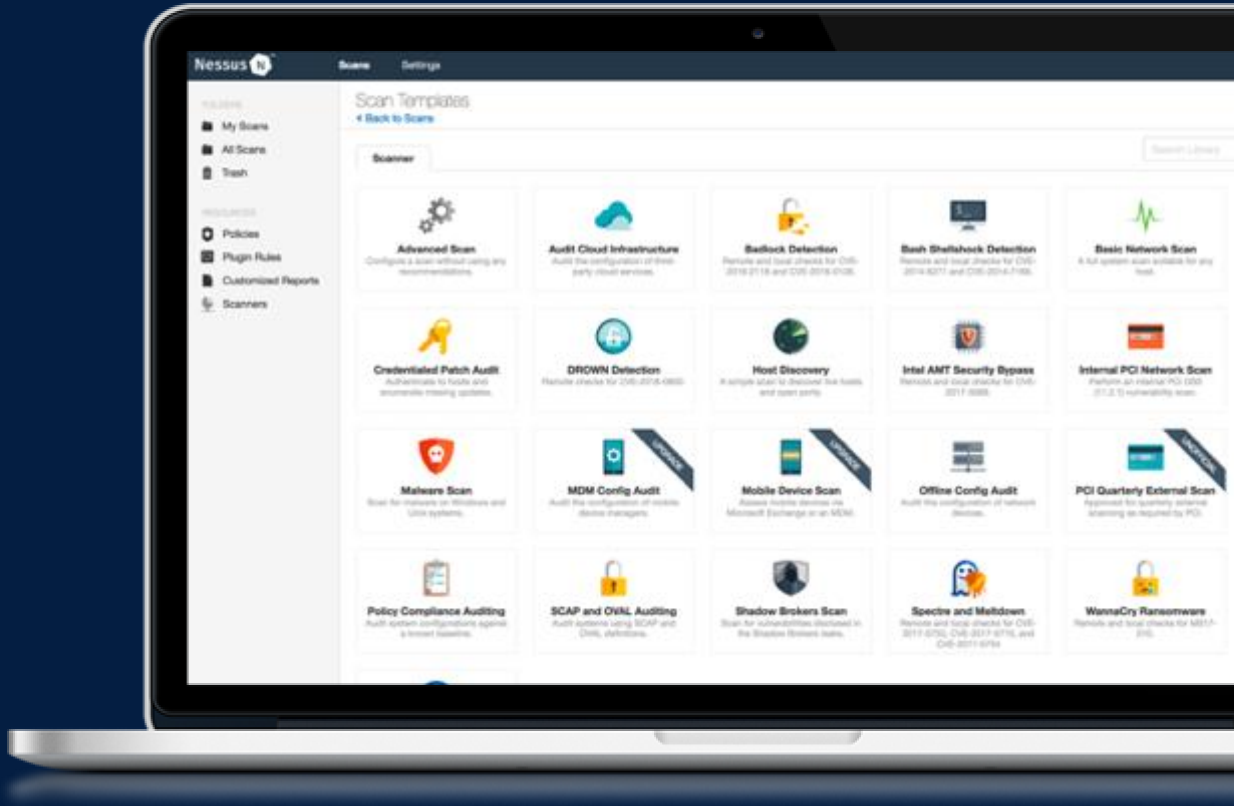
- Nessus has the industry’s lowest false positive rate with six-sigma accuracy

#1 in Coverage

- 160,000 plugins, more than 70,000 CVE and over 100 new plugins released weekly within 24 hours of vulnerability disclosure.

#1 in Adoption

- Nessus is trusted by more than 30,000 organizations globally, including 2 million downloads.



Who is Nessus for

Nessus is designed to conduct point-in-time assessments of the traditional IT environment to gain visibility of the assets within your network, understand the threat exposure and to audit for compliance.

SMB security Practitioner

Security consultant / service provider

Asset discovery

Discover all assets within your network, check their configuration and find anomalies

Penetration test

Using the powerful Nessus engine, discover and report on all the vulnerabilities in a network

Compliance audit

Use pre-built templates in the Nessus library to easily meet the needs of a variety of regulatory requirements

Expanding the Aperture: The **Modern Attack Surface**

1. Traditional IT Assets

What we've known up to this point

- Desktops
- Workstations
- Networking equipment
- On-prem servers
- Etc.

2. Infrastructure as Code (IaC)

Unknown security issues as part of the Software Development Lifecycle (SDLC)

Extremely disruptive and costly to fix vulns when code is deployed

- Vuln in code
- Vuln in code
- Vuln in code

3. Attack Surface Mgmt. (ASM)

"What internet connected assets are out there that we don't know of?"

- dev.acme.com
- temp.acme.com
- staging5.acme.com

tenable

tenable RESEARCH

#1

IN **COVERAGE, ACCURACY** AND **ZERO DAY RESEARCH**

>402

Zero Days disclosed by Tenable Research since January 2019

>69K

Vulnerabilities assessed with 167,000+ Plugins

<24h

Median time for coverage of high-profile issues

Nessus Feature Comparison

	Nessus Essentials	Nessus Professional	Nessus Expert
IT	• Scan 16 IPs • Pre-built Policies & Templates ○ No Compliance scans • Reporting	• Unlimited Assessments • Pre-built Policies & Templates ○ Includes Compliance scans Reporting	• Unlimited Assessments • Pre-built Policies & Templates ○ Includes Compliance scans Reporting
IaC	• Use Terrascan via Command Line Interface	• Use Terrascan via Command Line Interface	• Terrascan with built in User Interface
EASM	• Not Available	• Not Available	• 5 Domain Discovery Scans (per 90 days) • Data Provided: ○ Sub-domains ○ Port Info ○ SSL Info ○ DNS Info

Nessus Comparison (High Level)

	Nessus Essentials	Nessus Professional	Nessus Expert
Use Case	Use Nessus for small home and educational environments	Use Nessus to assess and audit IT networks and cloud environments.	Use Nessus to discover, assess and audit IT, cloud environments and including Internet-connected assets
Target	• Educators • Students • Individuals starting careers in Cyber	• Consultants • Pen Testers • Security Practitioners	• Consultants • Pen Testers • Security Practitioners
Coverage	• IT Assets • IaC Installer Integration	• IT Assets • IaC Installer Integration	• IT Assets • IaC (No Runtime) • EASM (2 Domains)

Summary

VISIBILITY

- Know yourself
  - Inventory list
  - Vulnerability list
- Know your enemy
  - What they want?
  - What they use?
- Use the right tool: Nessus
- Prioritize with dynamic rating

THANK YOU

Nessus Essentials download URL

https://www.tenable.com/products/nessus/nessus-essentials