Take Control of Your Cyber Security Defenses

Disney Cheng
Principal Security Engineer – APAC
Tenable Inc.

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

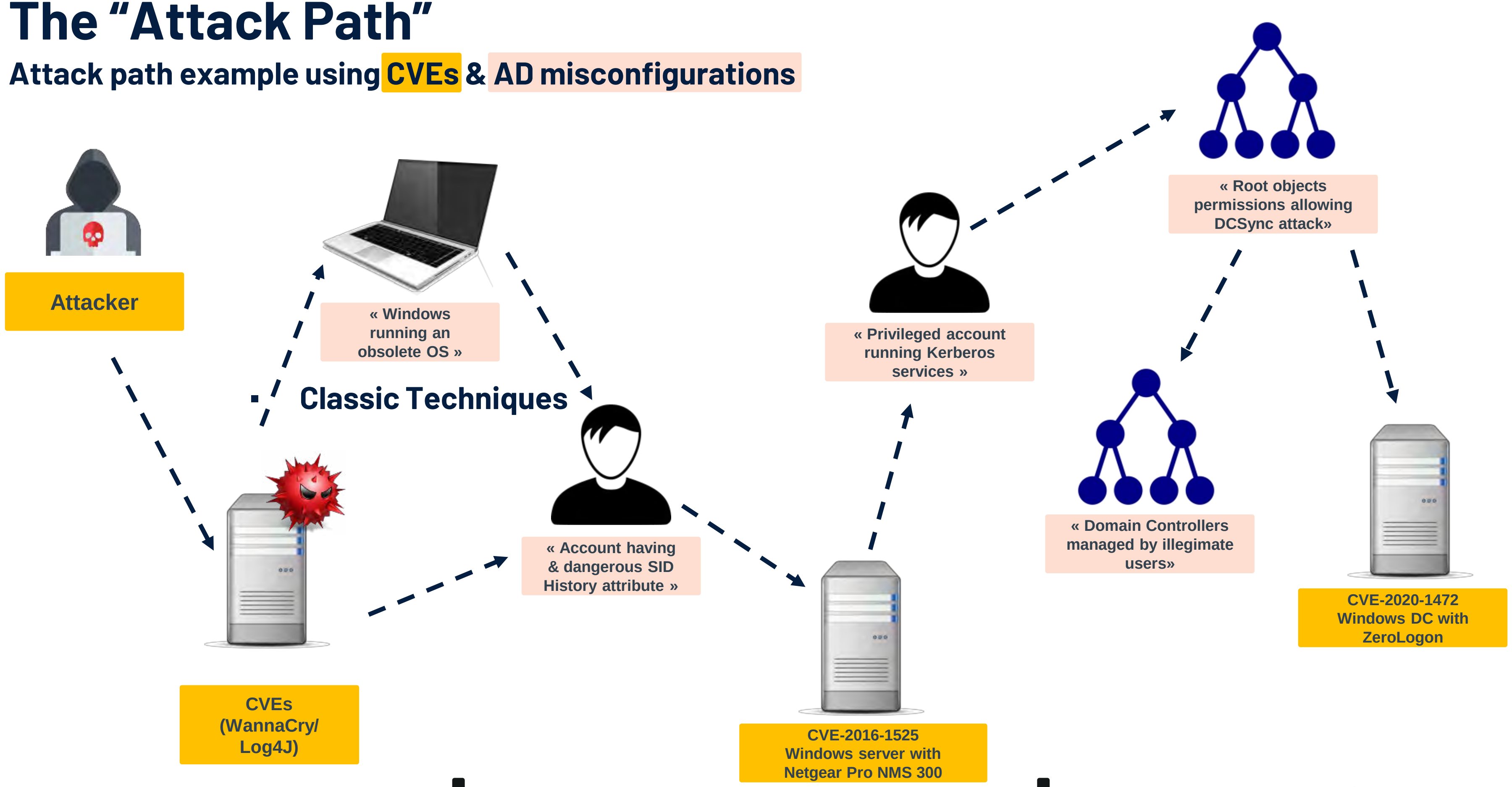
Named CNAPP & Active Directory Defense vendor

Gartner

tenable

The “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 »

« Privileged account running Kerberos services »

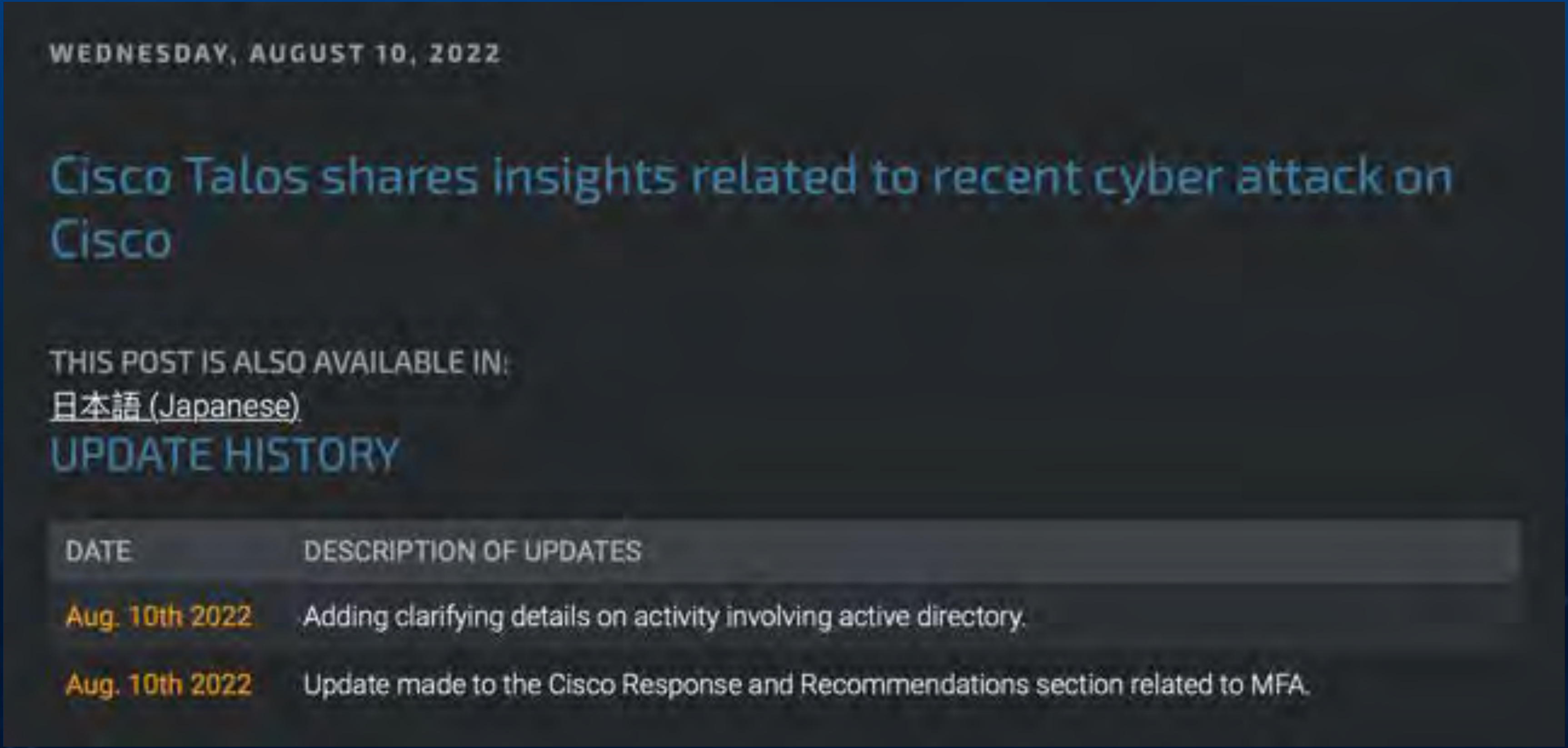
CVE-2016-1525 Windows server with Netgear Pro NMS 300

« 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



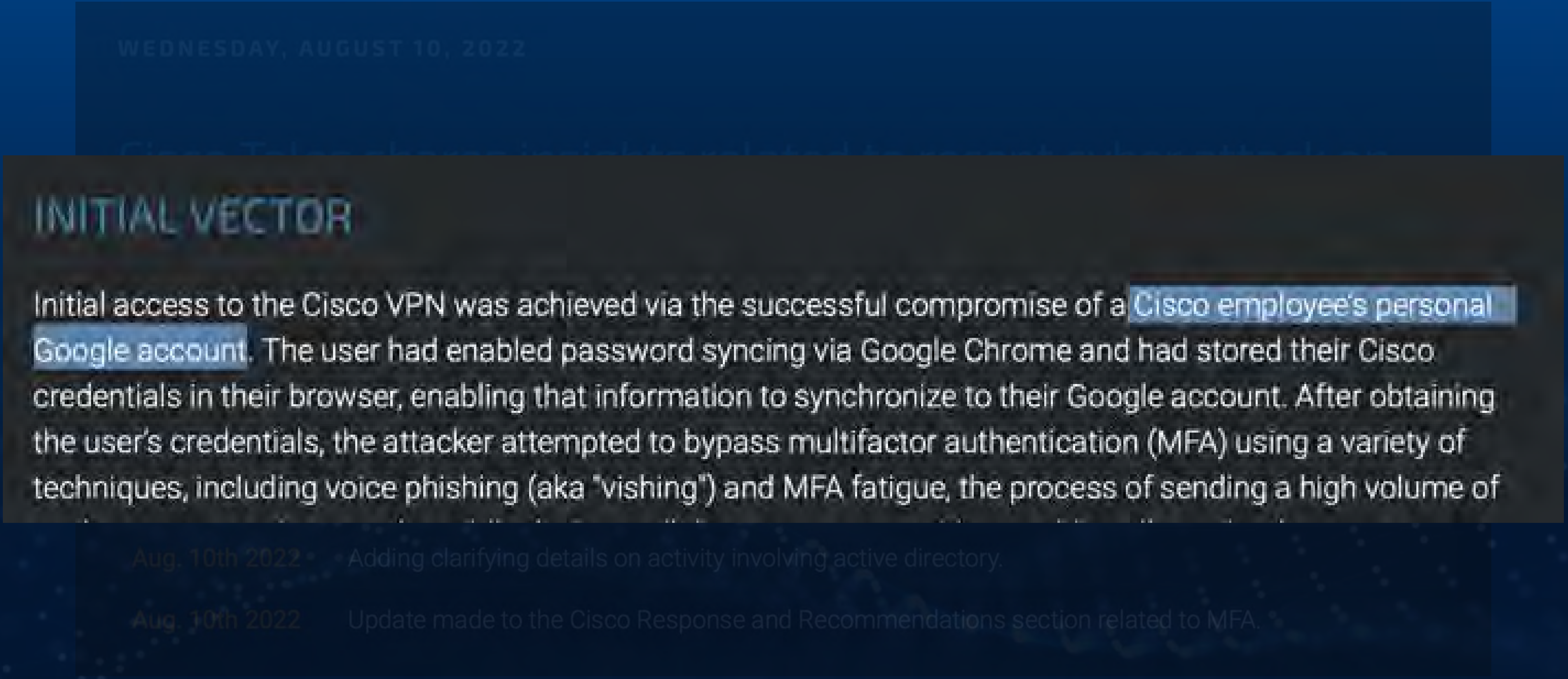
WEDNESDAY, AUGUST 10, 2022

Cisco Talos shares insights related to recent cyber attack on Cisco

THIS POST IS ALSO AVAILABLE IN:
日本語 (Japanese)

UPDATE HISTORY

DATE	DESCRIPTION OF UPDATES
Aug. 10th 2022	Adding clarifying details on activity involving active directory.
Aug. 10th 2022	Update made to the Cisco Response and Recommendations section related to MFA.

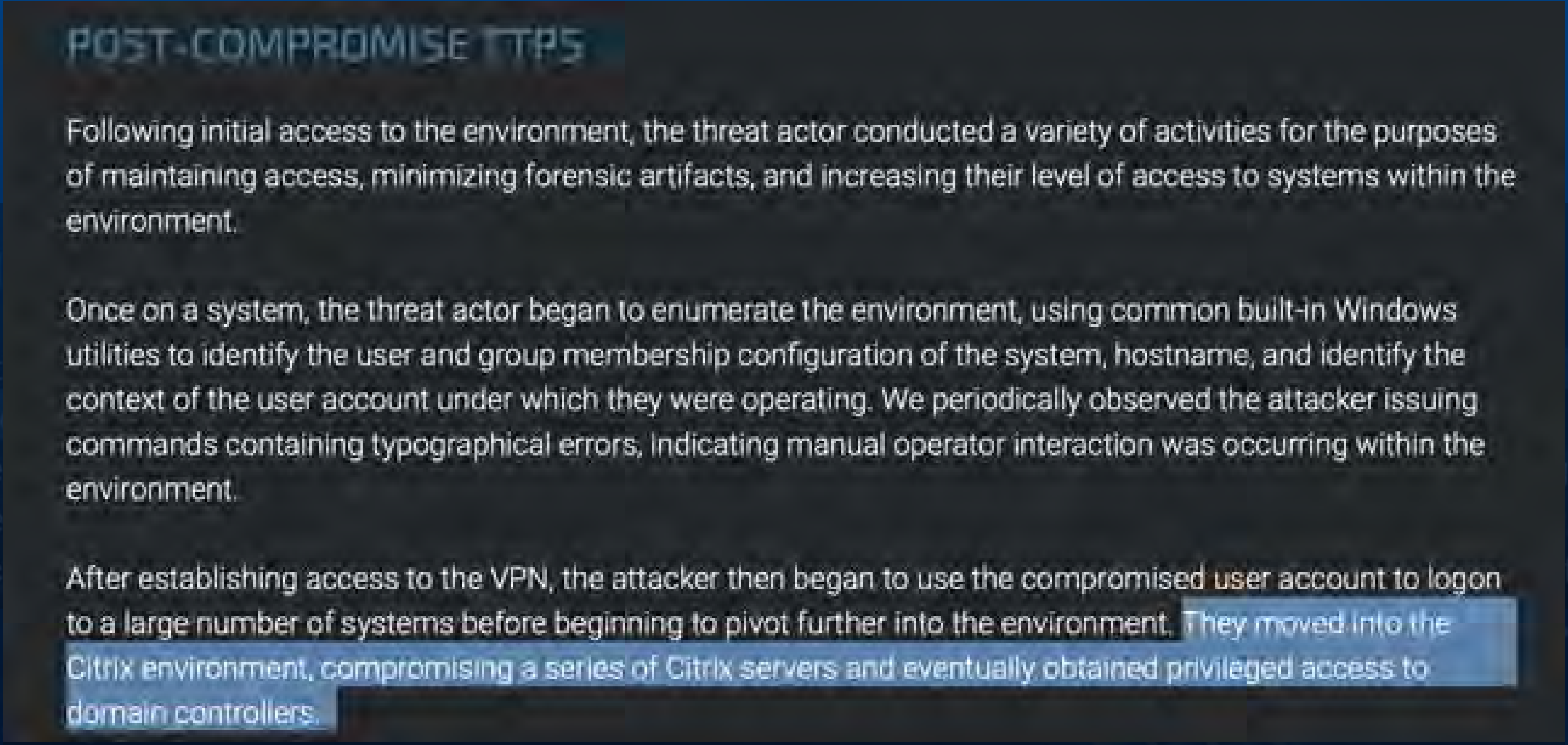


WEDNESDAY, AUGUST 10, 2022

INITIAL VECTOR

Initial access to the Cisco VPN was achieved via the successful compromise of a Cisco employee's personal Google account. The user had enabled password syncing via Google Chrome and had stored their Cisco credentials in their browser, enabling that information to synchronize to their Google account. After obtaining the user's credentials, the attacker attempted to bypass multifactor authentication (MFA) using a variety of techniques, including voice phishing (aka "vishing") and MFA fatigue, the process of sending a high volume of

Aug. 10th 2022	Adding clarifying details on activity involving active directory.
Aug. 10th 2022	Update made to the Cisco Response and Recommendations section related to MFA.

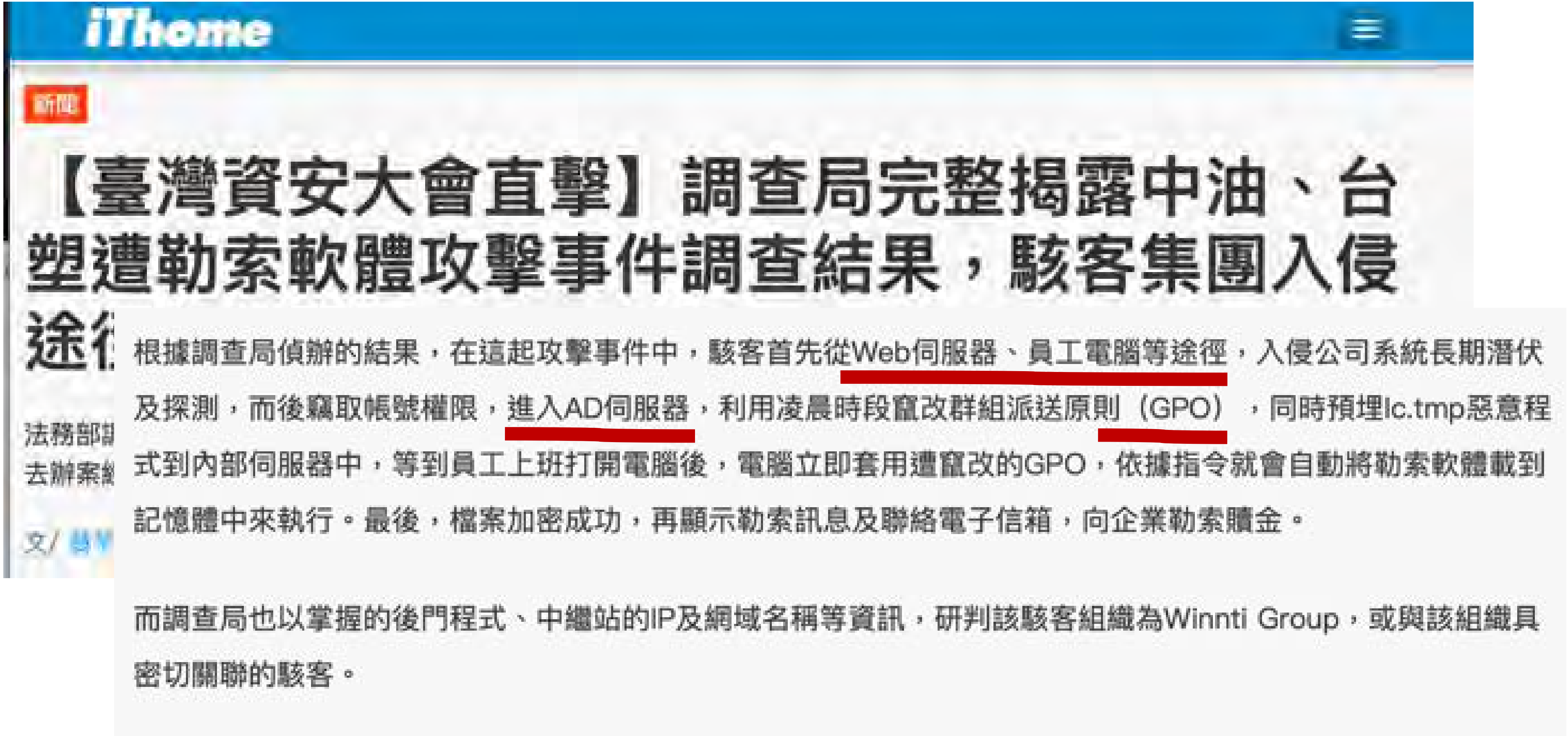


POST-COMPROMISE TTPS

Following initial access to the environment, the threat actor conducted a variety of activities for the purposes of maintaining access, minimizing forensic artifacts, and increasing their level of access to systems within the environment.

Once on a system, the threat actor began to enumerate the environment, using common built-in Windows utilities to identify the user and group membership configuration of the system, hostname, and identify the context of the user account under which they were operating. We periodically observed the attacker issuing commands containing typographical errors, indicating manual operator interaction was occurring within the environment.

After establishing access to the VPN, the attacker then began to use the compromised user account to logon to a large number of systems before beginning to pivot further into the environment. They moved into the Citrix environment, compromising a series of Citrix servers and eventually obtained privileged access to domain controllers.



【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

法務部

去辦案

文/

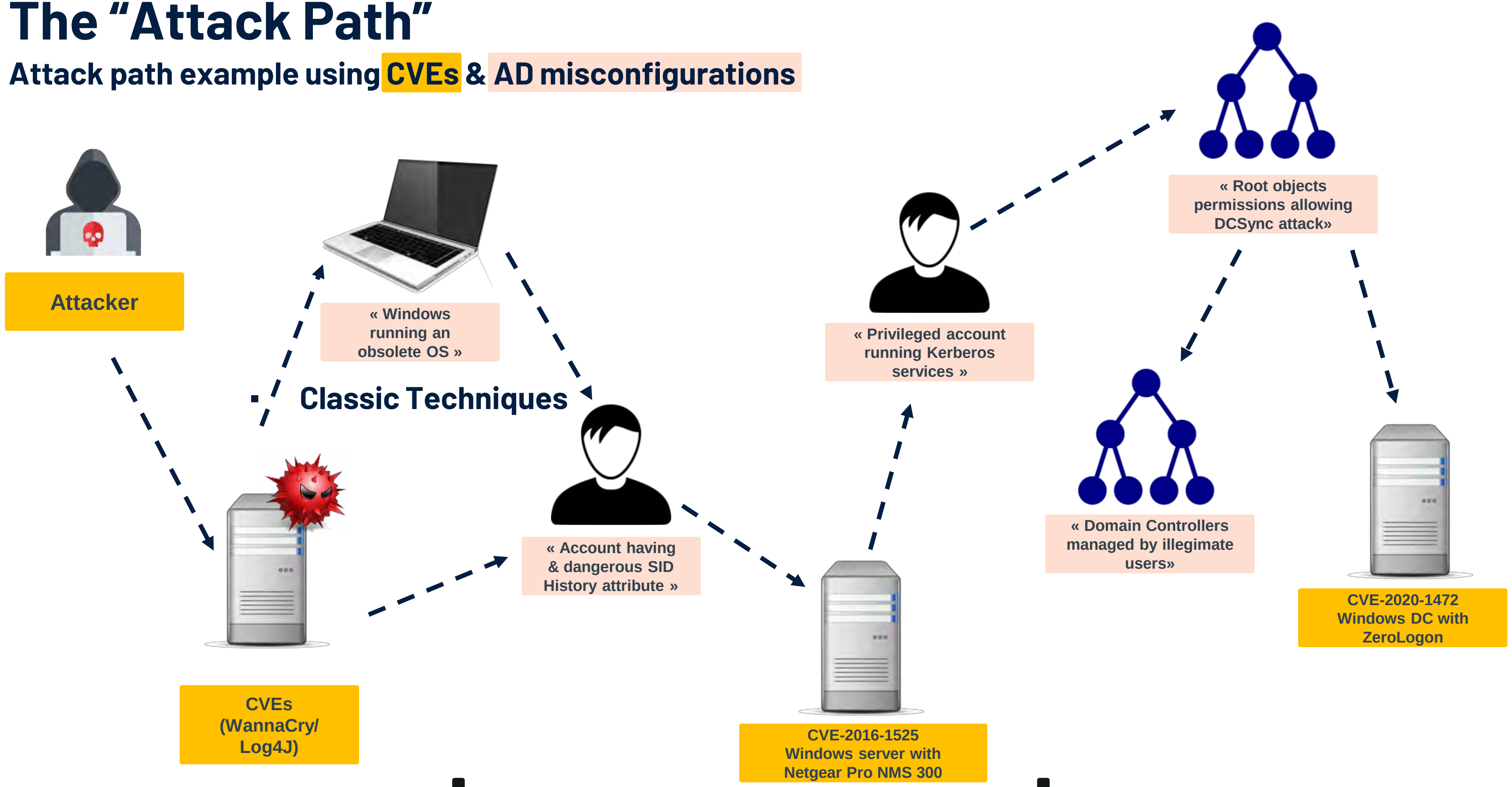
根據調查局偵辦的結果，在這起攻擊事件中，駭客首先從Web伺服器、員工電腦等途徑，入侵公司系統長期潛伏及探測，而後竊取帳號權限，進入AD伺服器，利用凌晨時段竄改群組派送原則（GPO），同時預埋lc.tmp惡意程式到內部伺服器中，等到員工上班打開電腦後，電腦立即套用遭竄改的GPO，依據指令就會自動將勒索軟體載到記憶體中來執行。最後，檔案加密成功，再顯示勒索訊息及聯絡電子信箱，向企業勒索贖金。

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

CVEs (WannaCry/ Log4J)

« Windows running an obsolete OS »

Classic Techniques

« 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»

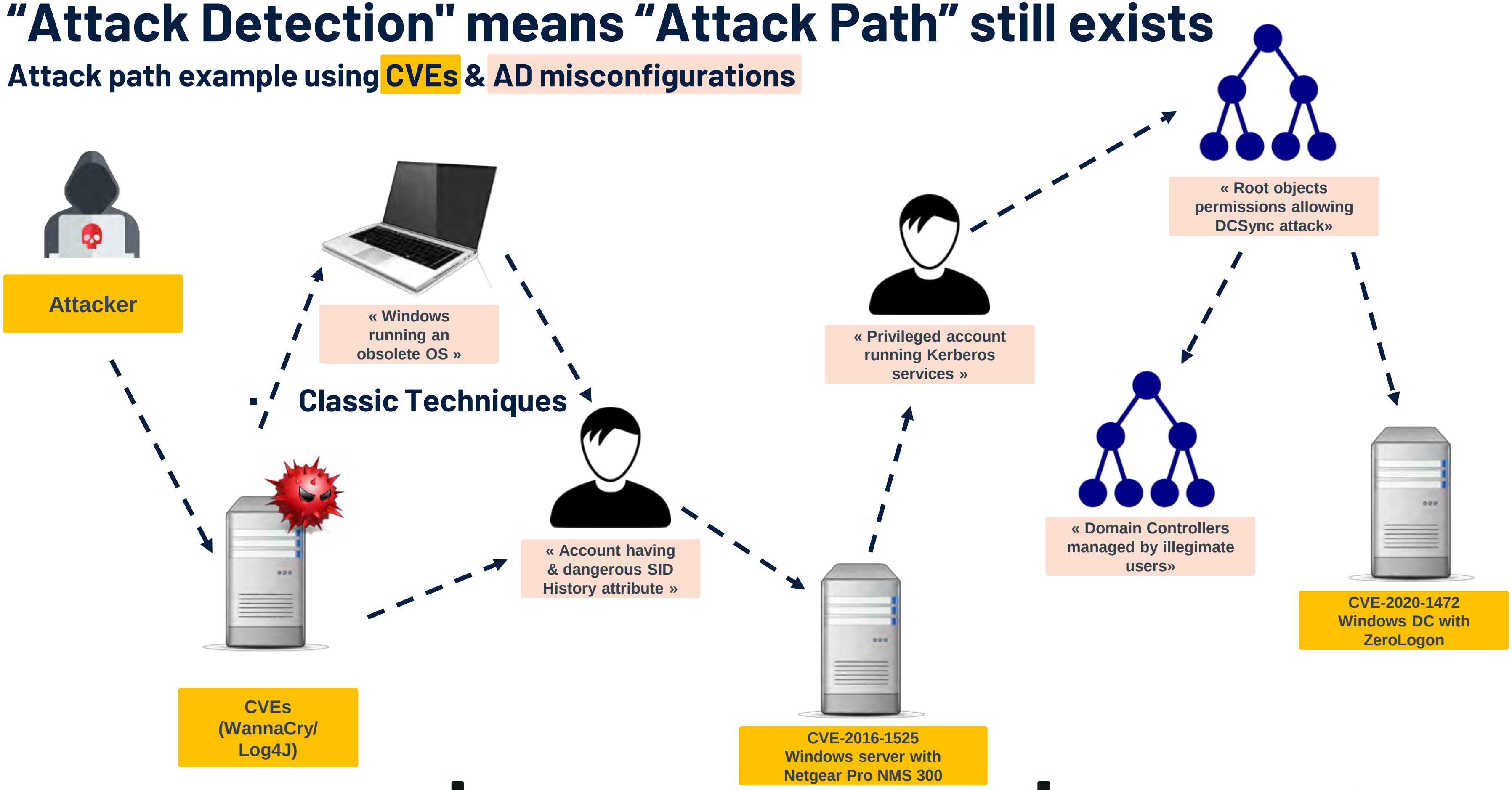
« Domain Controllers managed by illegimate users»

CVE-2020-1472 Windows DC with ZeroLogon

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

“Attack Detection" means “Attack Path” still exists

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»

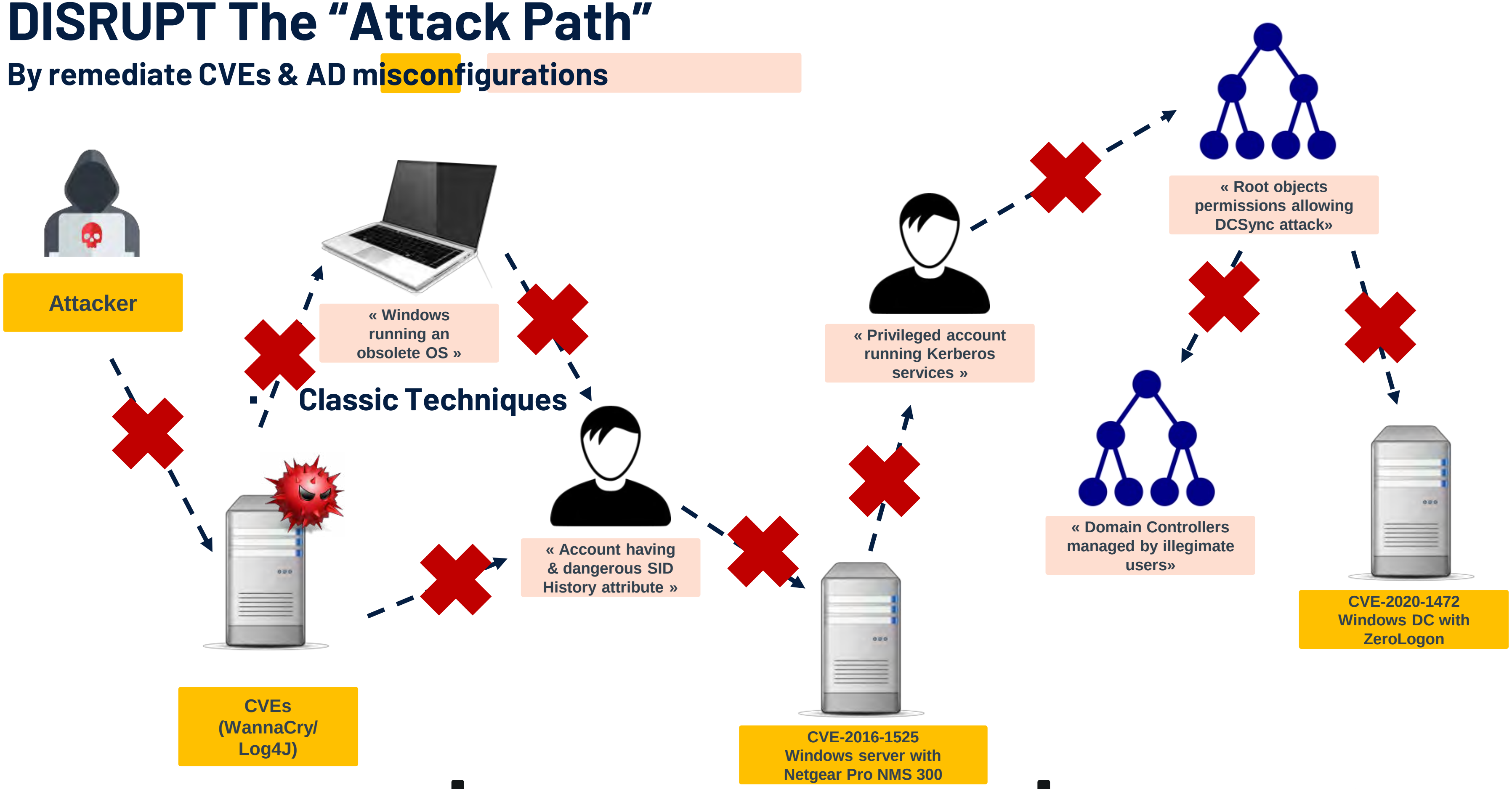
CVE-2020-1472 Windows DC with ZeroLogon

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

Take Control of Your Cyber Security Defenses by DISRUPT The "Attack Path"

DISRUPT The “Attack Path”

By remediate CVEs & AD misconfigurations



Attacker

« Windows running an obsolete OS »

Classic Techniques

CVEs (WannaCry/ Log4J)

« Account having & dangerous SID History attribute »

« Privileged account running Kerberos services »

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

« Root objects permissions allowing DCSync attack»

« Domain Controllers managed by illegimate users»

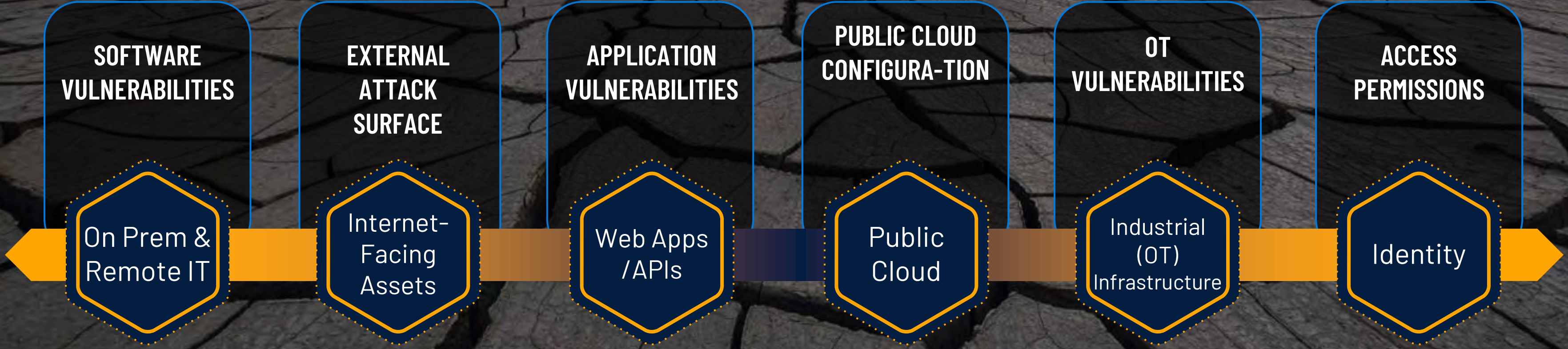
CVE-2020-1472 Windows DC with ZeroLogon

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

MANAGING EXPOSURES ACROSS THE MODERN ATTACK SURFACE

EXPOSURE MANAGEMENT

Visibility across the modern attack surface with intelligence to prioritize preventative actions and communicate risk to all levels of the organization.



SOFTWARE VULNERABILITIES

On Prem & Remote IT

EXTERNAL ATTACK SURFACE

Internet-Facing Assets

APPLICATION VULNERABILITIES

Web Apps /APIs

PUBLIC CLOUD CONFIGURA-TION

Public Cloud

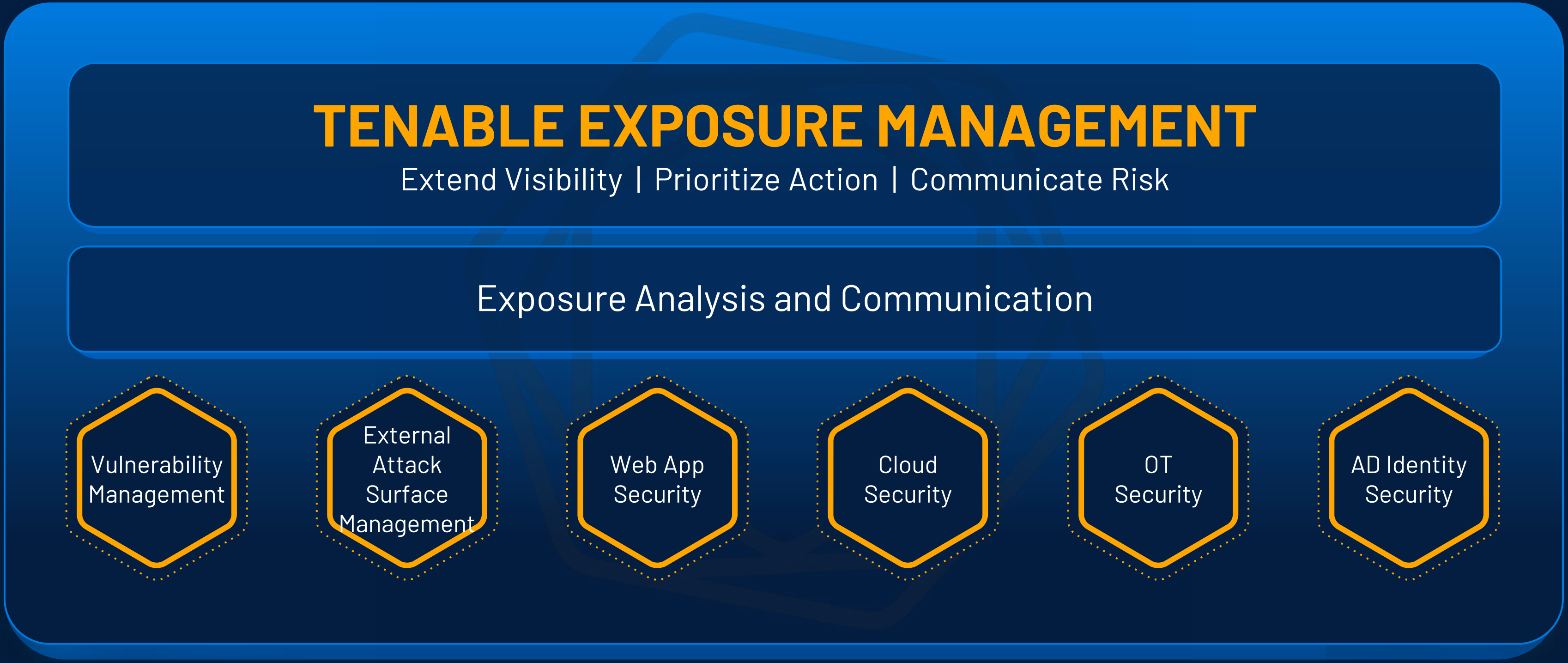
OT VULNERABILITIES

Industrial (OT) Infrastructure

ACCESS PERMISSIONS

Identity

THE TENABLE PORTFOLIO



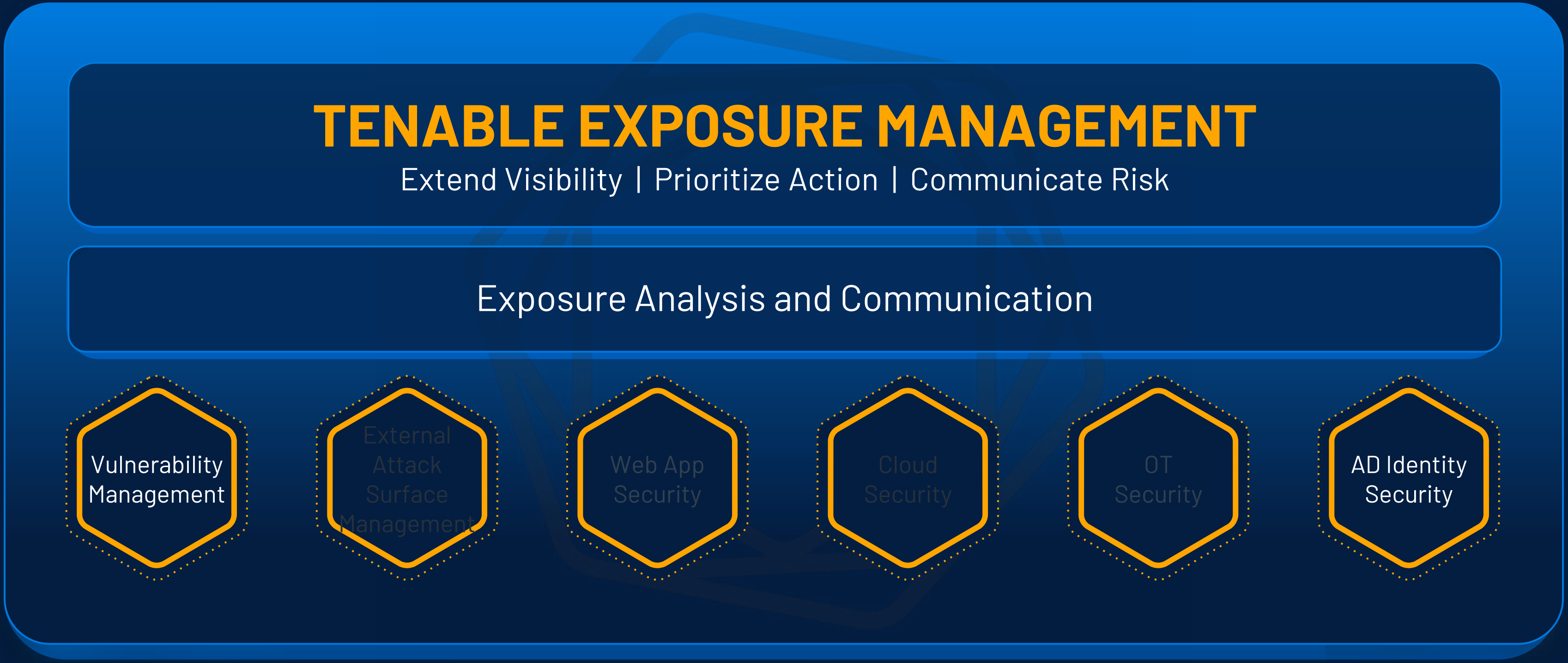
TENABLE EXPOSURE MANAGEMENT

Extend Visibility | Prioritize Action | Communicate Risk

Exposure Analysis and Communication

- Vulnerability Management
- External Attack Surface Management
- Web App Security
- Cloud Security
- OT Security
- AD Identity Security

THE TENABLE PORTFOLIO



TENABLE EXPOSURE MANAGEMENT

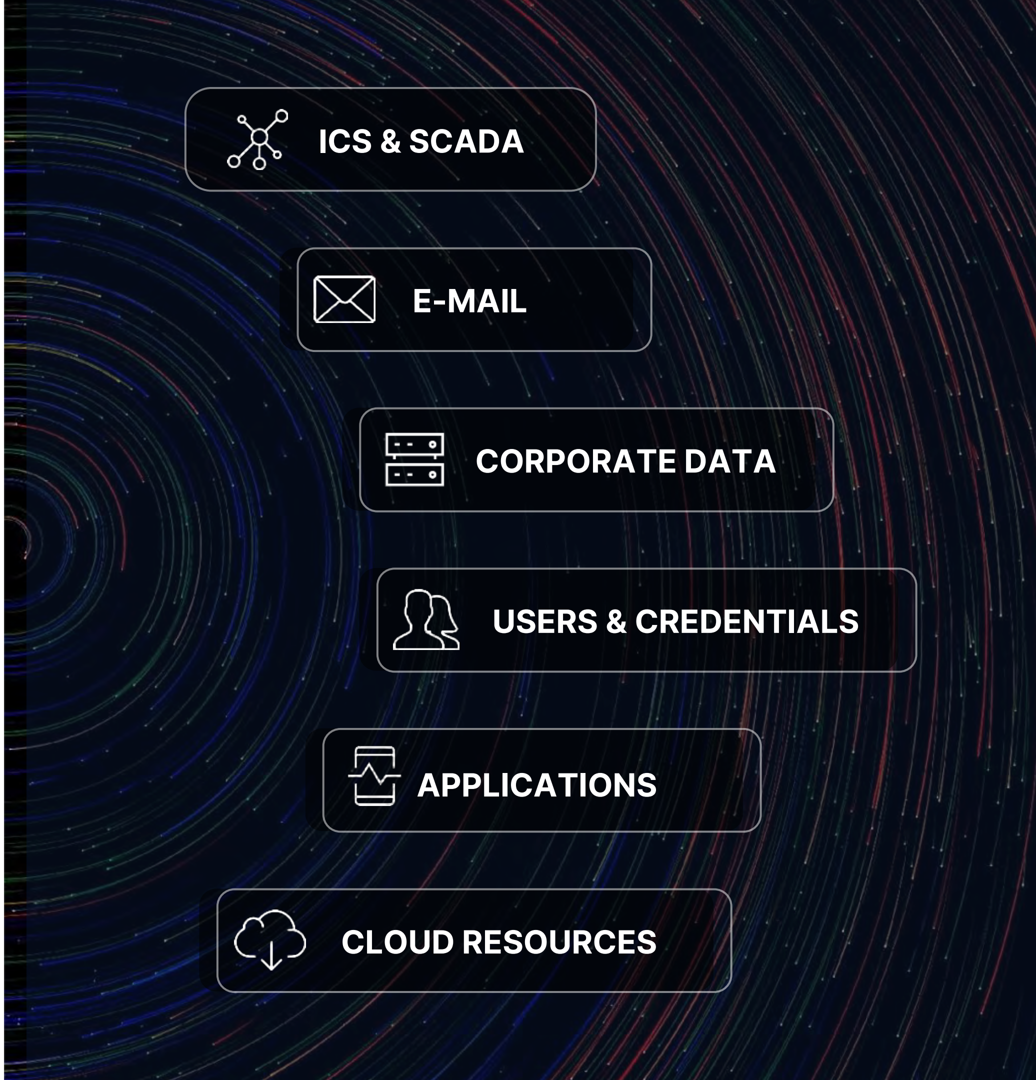
Extend Visibility | Prioritize Action | Communicate Risk

Exposure Analysis and Communication

- Vulnerability Management
- External Attack Surface Management
- Web App Security
- Cloud Security
- OT Security
- AD Identity Security

Active Directory holds the **keys to everything**

- Governs authentication, holds all passwords
- Manages access rights to every vital asset
- A complex, evolving architecture that becomes unmanageable over time



ICS & SCADA

E-MAIL

CORPORATE DATA

USERS & CREDENTIALS

APPLICATIONS

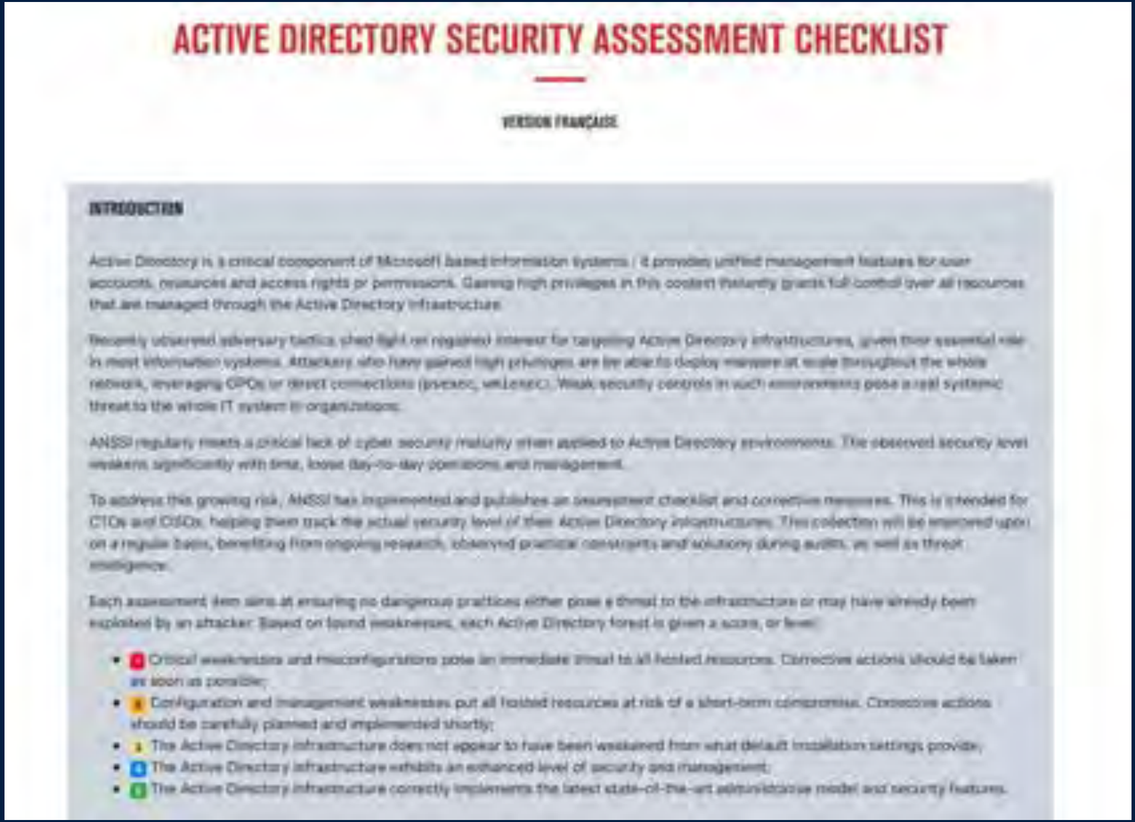
CLOUD RESOURCES

How old is your AD?

Active Directory Security?

- Currently Most organization still review Active Directory Security Manually – twice to once a year.

- A very good public resources is ACTIVE DIRECTORY SECURITY ASSESSMENT CHECKLIST by ANSSI (French National Cybersecurity Agency)



ACTIVE DIRECTORY SECURITY ASSESSMENT CHECKLIST

VERSION FRANÇAISE

INTRODUCTION

Active Directory is a critical component of Microsoft based information systems : it provides unified management features for user accounts, resources and access rights or permissions. Gaining high privileges in this context instantly grants full control over all resources that are managed through the Active Directory infrastructure.

Recently observed adversary tactics shed light on regained interest for targeting Active Directory infrastructures, given their essential role in most information systems. Attackers who have gained high privileges are be able to deploy malware at scale throughout the whole network, leveraging GPOs or direct connections (psexec, wmiexec). Weak security controls in such environments pose a real systemic threat to the whole IT system in organizations.

ANSSI regularly meets a critical lack of cyber security maturity when applied to Active Directory environments. The observed security level weakens significantly with time, loose day-to-day operations and management.

To address this growing risk, ANSSI has implemented and publishes an assessment checklist and corrective measures. This is intended for CTOs and CISOs, helping them track the actual security level of their Active Directory infrastructures. This collection will be improved upon on a regular basis, benefiting from ongoing research, observed practical constraints and solutions during audits, as well as threat intelligence.

Each assessment item aims at ensuring no dangerous practices either pose a threat to the infrastructure or may have already been exploited by an attacker. Based on found weaknesses, each Active Directory forest is given a score, or level:

- 1 Critical weaknesses and misconfigurations pose an immediate threat to all hosted resources. Corrective actions should be taken as soon as possible;
- 2 Configuration and management weaknesses put all hosted resources at risk of a short-term compromise. Corrective actions should be carefully planned and implemented shortly;
- 3 The Active Directory infrastructure does not appear to have been weakened from what default installation settings provide;
- 4 The Active Directory infrastructure exhibits an enhanced level of security and management;
- 5 The Active Directory infrastructure correctly implements the latest state-of-the-art administrative model and security features.

https://www.cert.ssi.gouv.fr/uploads/guide-ad.html

tenable

Tenable Automate Active Directory Security Monitoring

tenable.ad™

- Discover the underlying issues affecting your Active Directory
- Identify dangerous trust relationships
- Catch every change in your AD
- Make the link between AD changes and malicious actions
- Analyze and Detect in-depth details of attacks
- Explore MITRE ATT&CK descriptions directly from incident detail

NO AGENTS

NO PRIVILEGES

AD-NATIVE

NEAR-INSTANT VALUE

SECURE YOUR ACTIVE DIRECTORY AND **DISRUPT** ATTACK PATHS

MITIGATE EXISTING THREATS

- Immediately discover, map, and score existing weaknesses
- Follow step-by-step remediation tactics and prevent attacks

MAINTAIN HARDENED SECURITY

- Continuously identify new vulnerabilities and misconfigurations
- Break attack pathways and keep your threat exposure in check

DETECT ADVANCED ATTACKS IN REAL TIME

- Get alerts and actionable remediation plans on AD attacks
- Help your SOC team visualize notifications & alerts in your SIEM

Tenable Revolution Vulnerability Prioritization

tenable

CVSS is Heavily Flawed

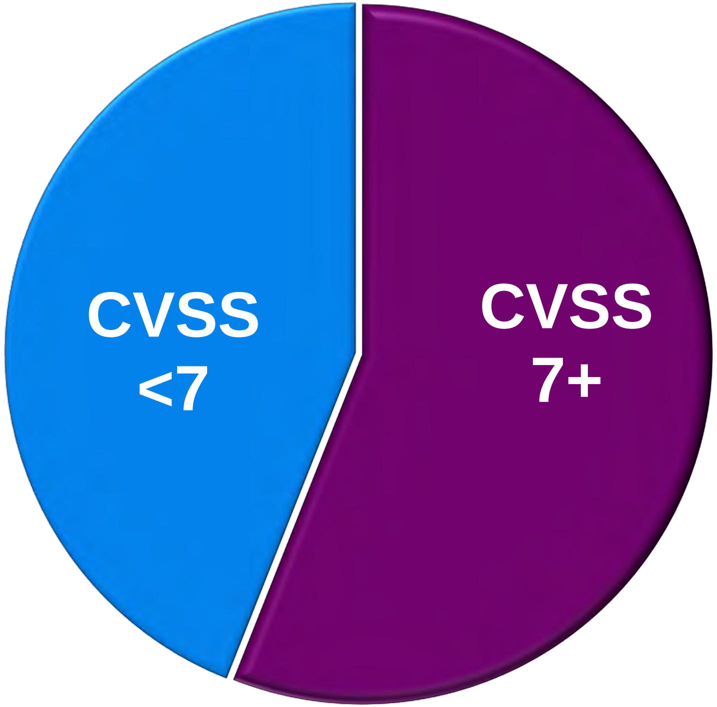
"CVSS is designed to identify the technical severity of a vulnerability. What people seem to want to know, instead, is the risk a vulnerability or flaw poses to them, or ***how quickly they should respond to a vulnerability***."

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

If Everything is a Priority, 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

Machine Learning Powered Prediction

>20M

Aspects of threat data continuously analyzed for prediction

>10

More than 10 threat providers covering over 9000 distinct threat sources

>55K

More than 55,000 vulnerabilities tracked and prioritized nightly

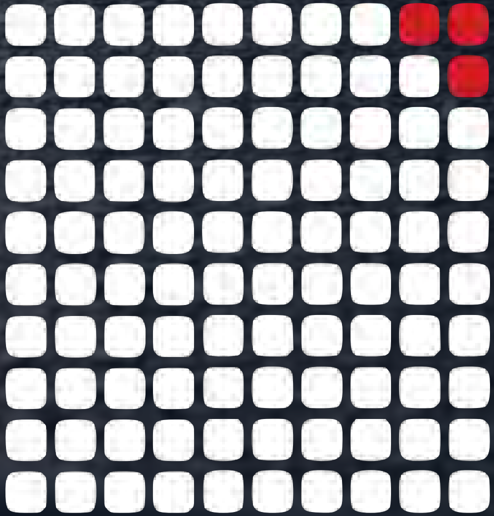
>20 TRILLION

threat, vulnerability, and asset data points continuously assessed

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

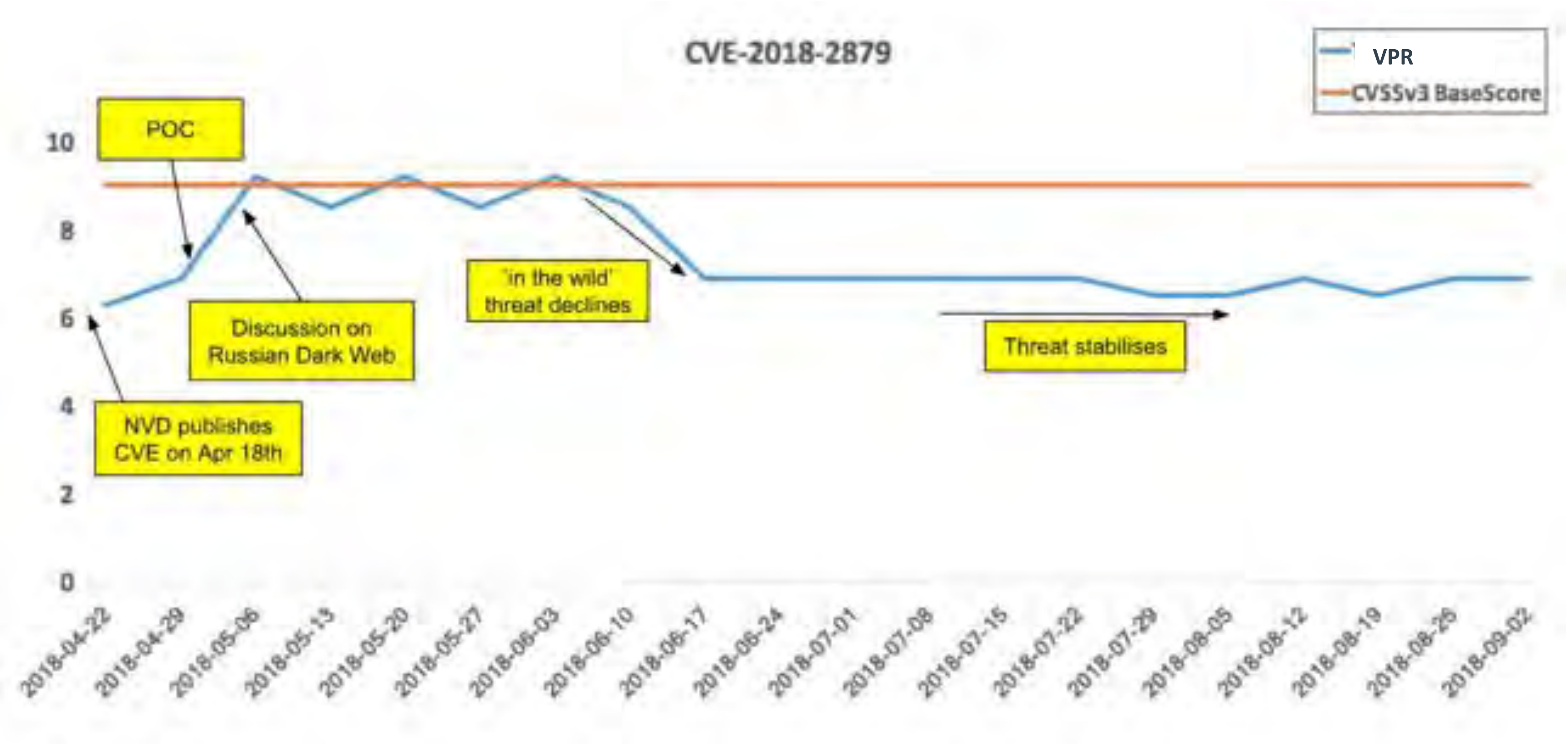
<3%

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



tenable

VPR can sometimes tell you things aren't so bad



tenable RESEARCH

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

>412

Zero Days disclosed by Tenable Research since January 2019

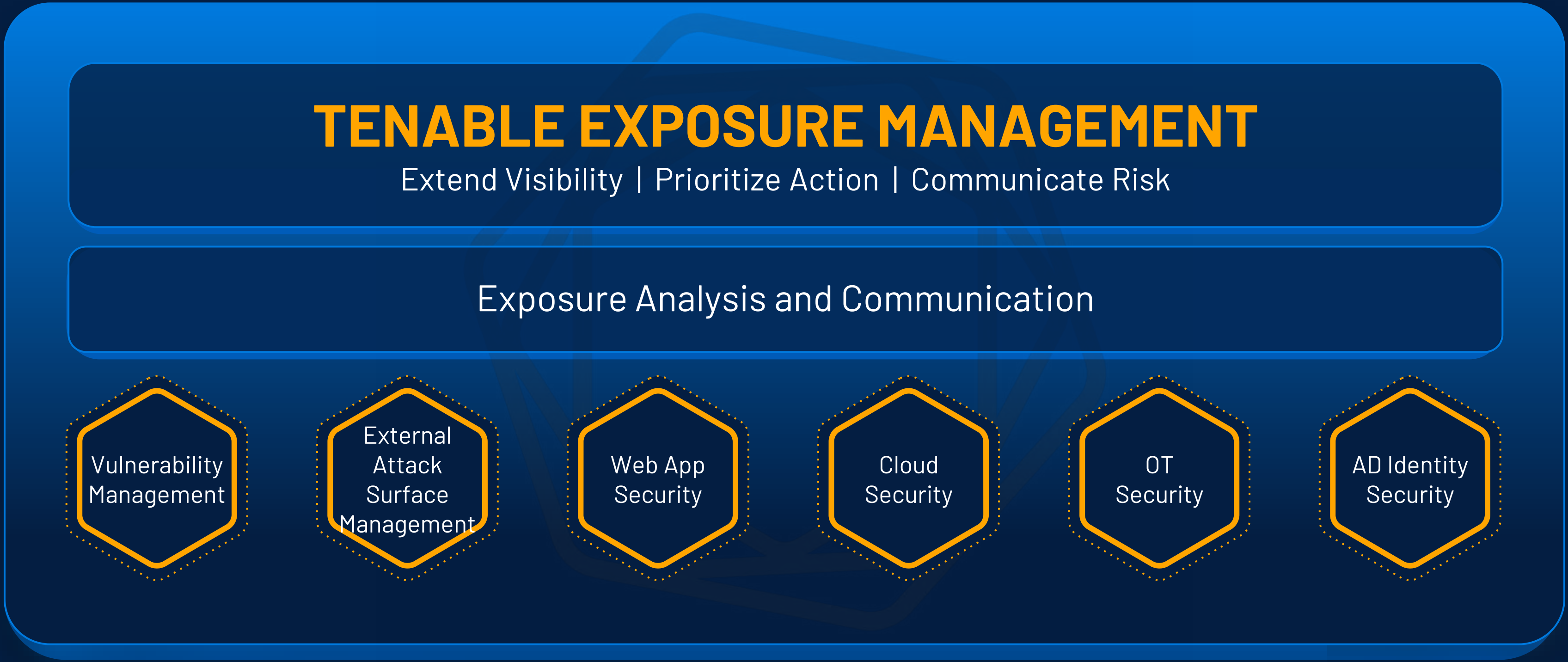
>71K

Vulnerabilities assessed with 174,000+ Plugins

<24h

Median time for coverage of high-profile issues

THE TENABLE PORTFOLIO



TENABLE EXPOSURE MANAGEMENT

Extend Visibility | Prioritize Action | Communicate Risk

Exposure Analysis and Communication

- Vulnerability Management
- External Attack Surface Management
- Web App Security
- Cloud Security
- OT Security
- AD Identity Security

tenable

tenable®

Thank You