Patching is the tip of the Iceberg

Why most Vulnerability Management programs suffer the fate of the Titanic

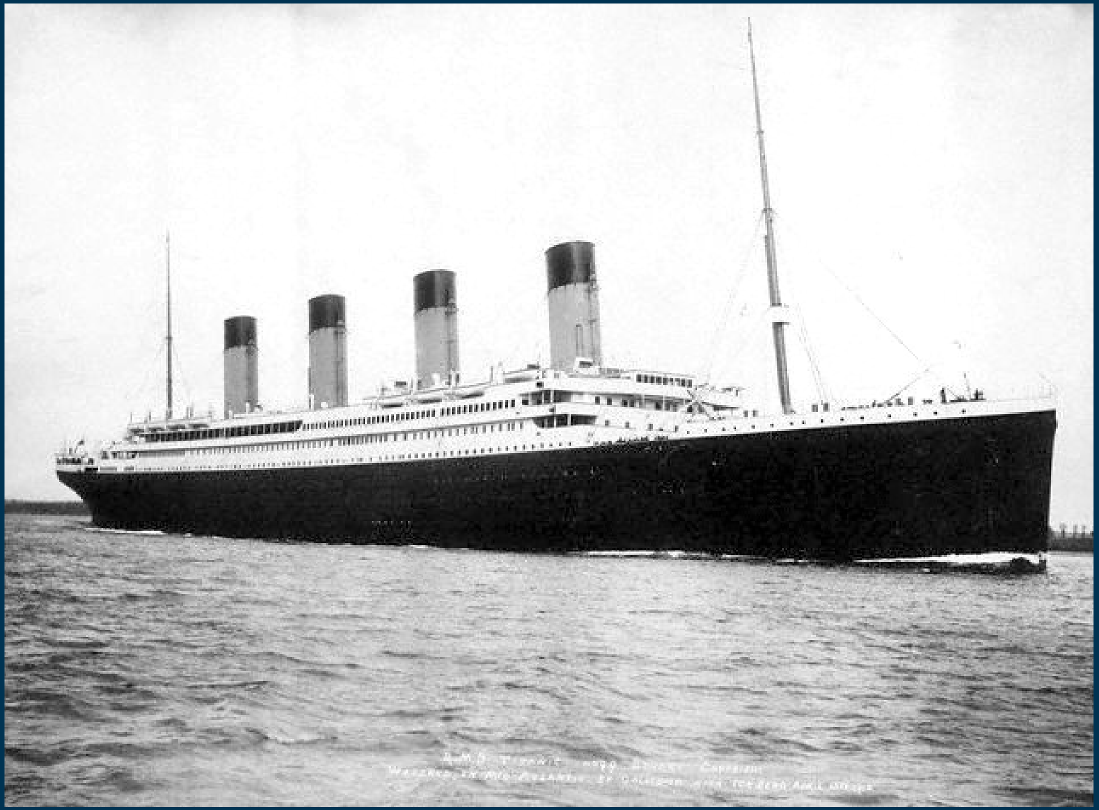
Is this what your Vulnerability Management process looks like?

WHOAMI

- ICT and Cyber professional with 20 years experience
- Recovering Sysadmin
- Continual learner
- Mentor
- Kayaking addict

- Director Cyber Security – Office of Digital Government WA
- Really passionate about Vulnerability Management

SINKING THE UNSINKABLE



- RMS Titanic sunk on 15 April 1912 on its maiden voyage after colliding with an iceberg
- Approximately 1500 died of the 2300 passengers
- The tragedy reshaped Maritime standards still in effect today -> Safety of Life at Sea (SOLAS), 1974

CASCADE OF FAILURES

Before the collision

- Excessive speed
- Long ship design limits manoeuvrability
- Missing binoculars
- Poor training of crew
- Ignored warnings of ice in area
- Insufficient lifeboat capacity
- Iron Plate selection (brittle)

After the collision

- Captain Smith's leadership described as negligent
- Evacuations delayed
- Poor crew internal communication
- Evacuation process favoured 1st/2nd class and crew
- Radio distress were unnoticed by nearby ships
- Lifeboats escaped well below their capacity
- Lifeboats didn't return fast enough to save survivors in the water

AGENDA

- Navigating a sea of vulnerabilities

  (why is VM hard?)

- Do we have enough lifeboats?

  (VM design and processes)

- Should I have engaged the bulkhead doors?

  (why pentests succeed, but VM fails)

- Are there opportunities to modernise vulnerability management?

VM 101

What is a vulnerability?

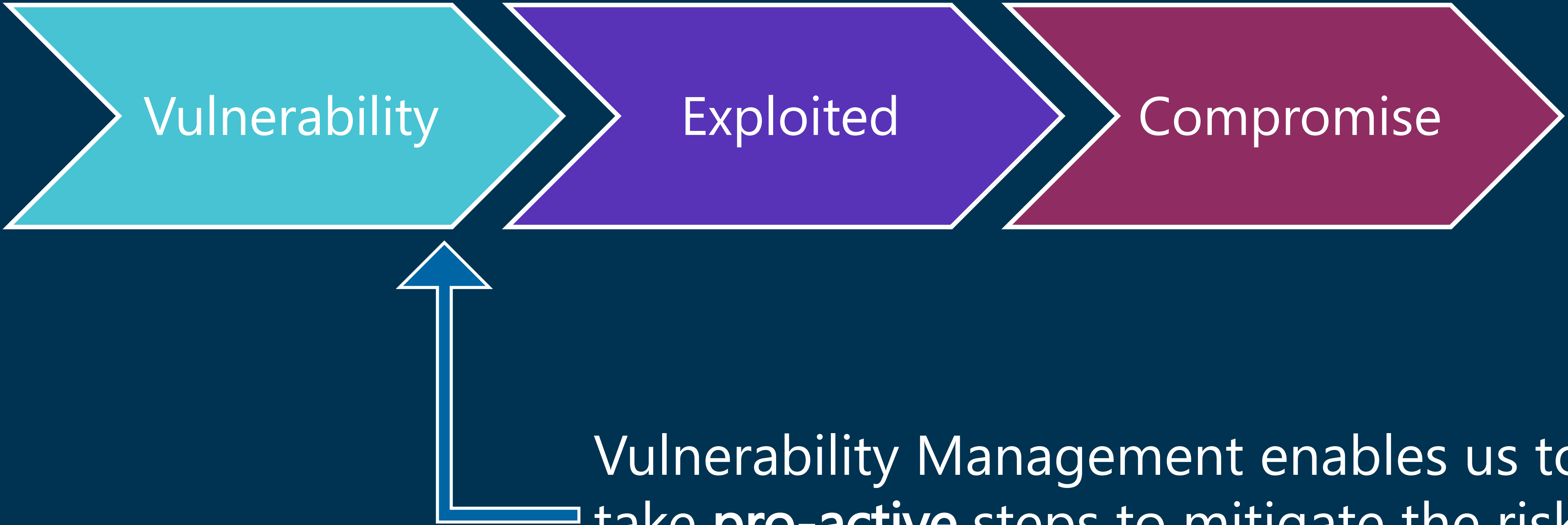
Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source.

Source: NIST Computer Security Resource Center (CSRC)

Cyber Professionals know them as?

- Common Vulnerabilities and Exposures (CVEs)
- 0-Day or Zero-Days
- Findings, Observations and Weaknesses that don’t have a CVE (there are a LOT)

VM 101 – WHY DO IT?

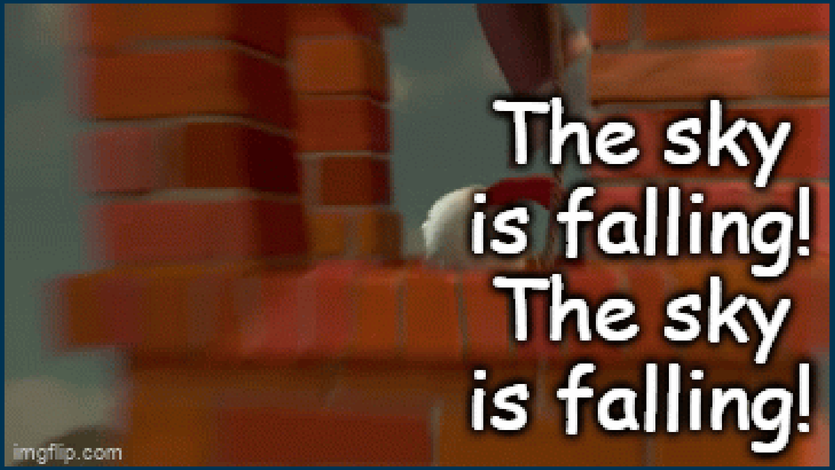


Vulnerability Management enables us to take **pro-active** steps to mitigate the risks of vulnerabilities before they are exploited

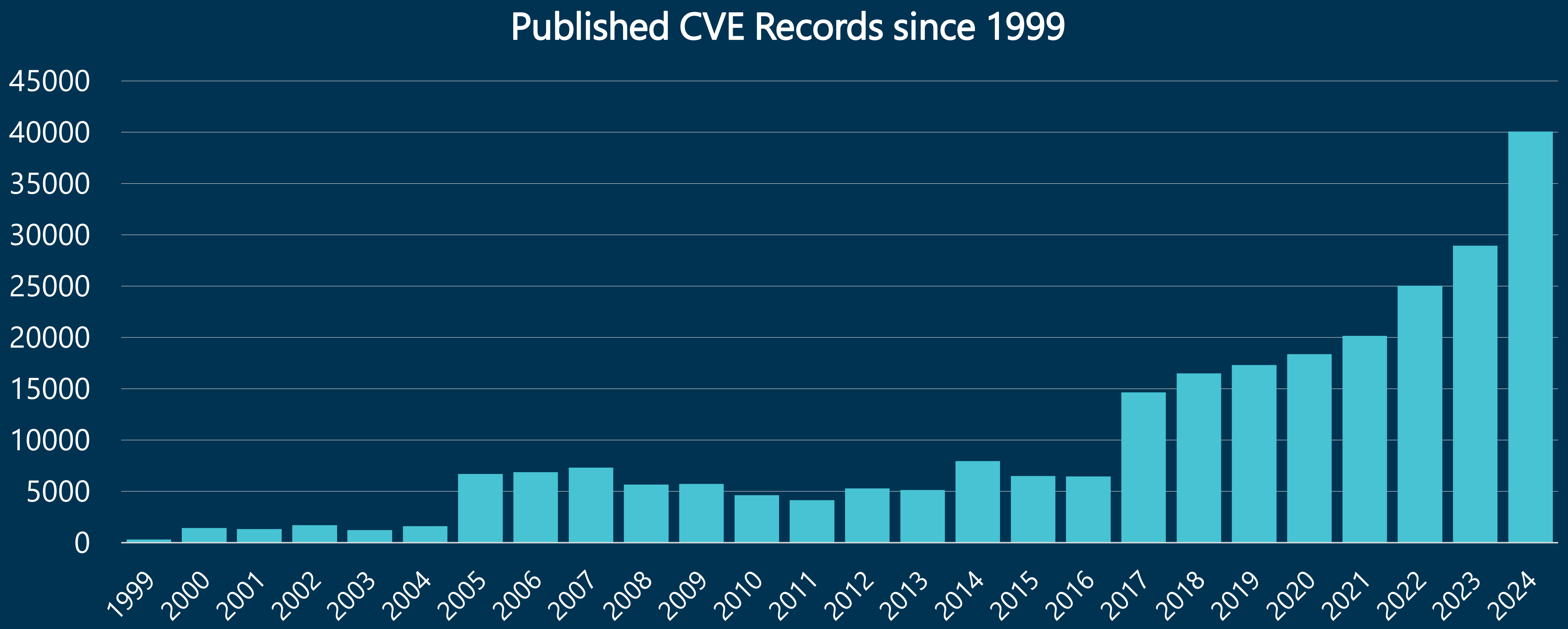
VM RATING/SCORING

Vulnerability scoring is something that SHOULD assist us in understanding the context of a vulnerability and if we should do something about it.

Severity	CVSS v3.x & v4.0 ratings
Critical	9.0-10
High	7.0-8.9
Medium	4.0-6.9
Low	0.1-3.9
None	0.0

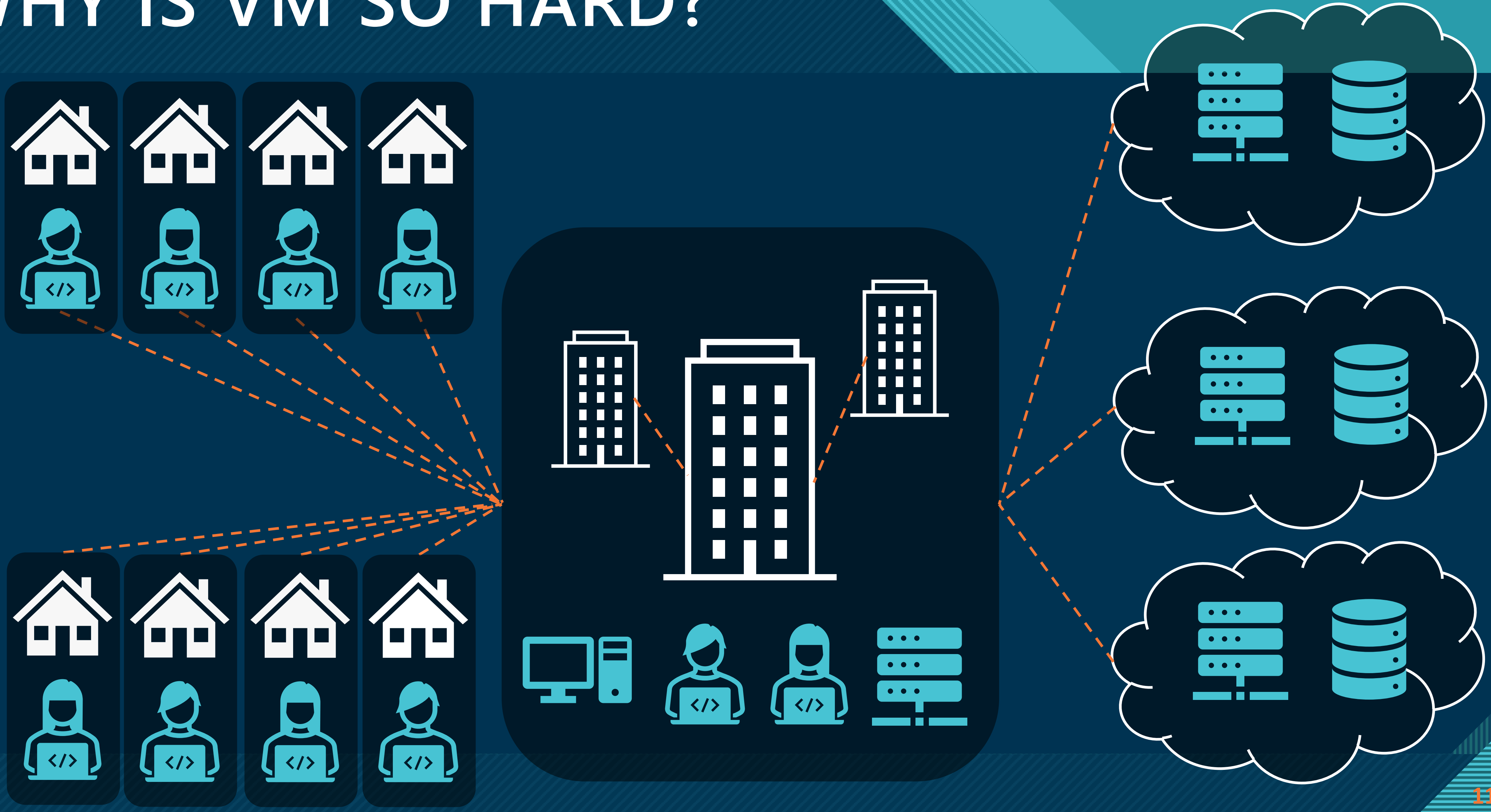


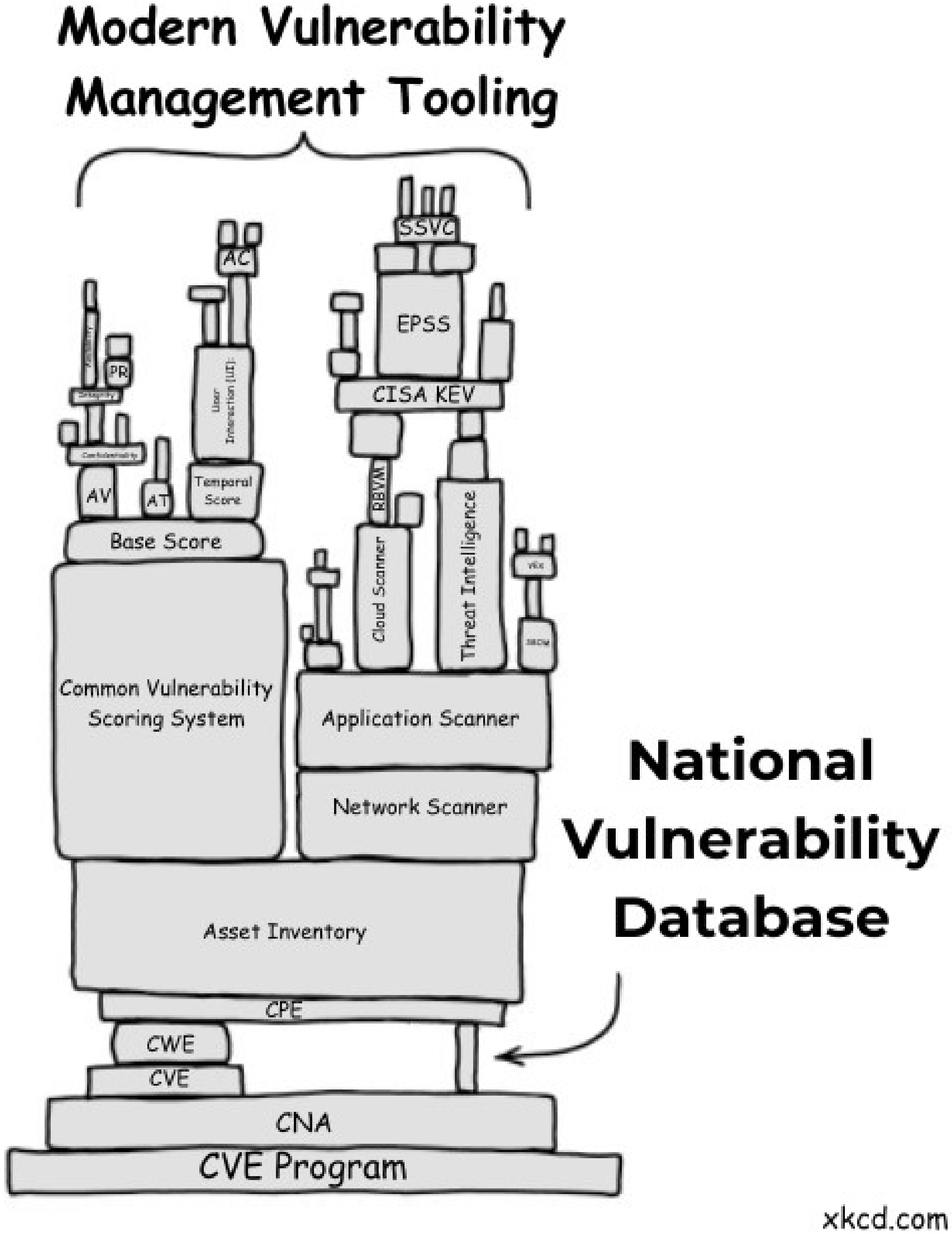
SEA OF VULNERABILITIES



Source: cve.org

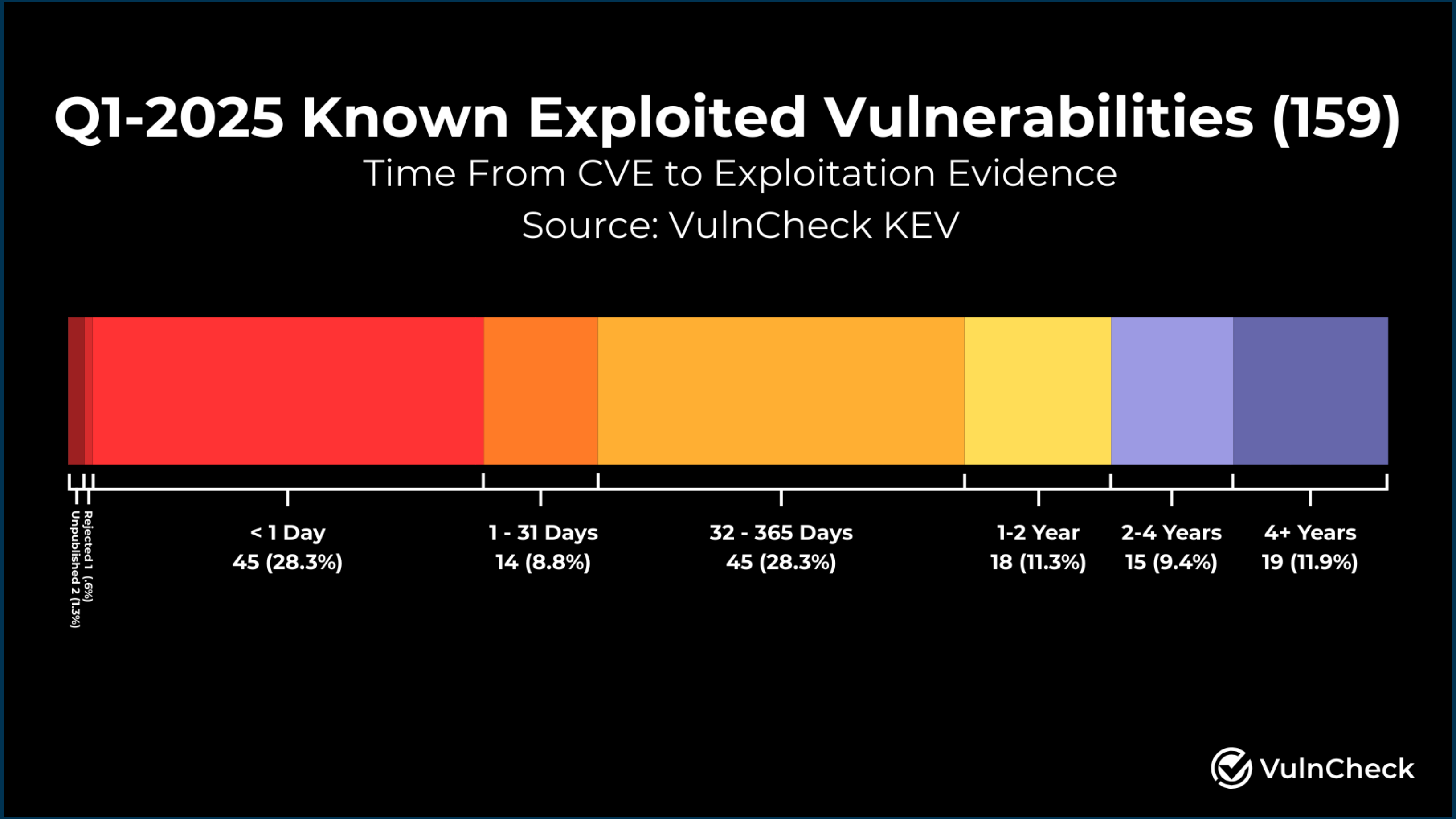
WHY IS VM SO HARD?





National Vulnerability Database

HOW QUICK?



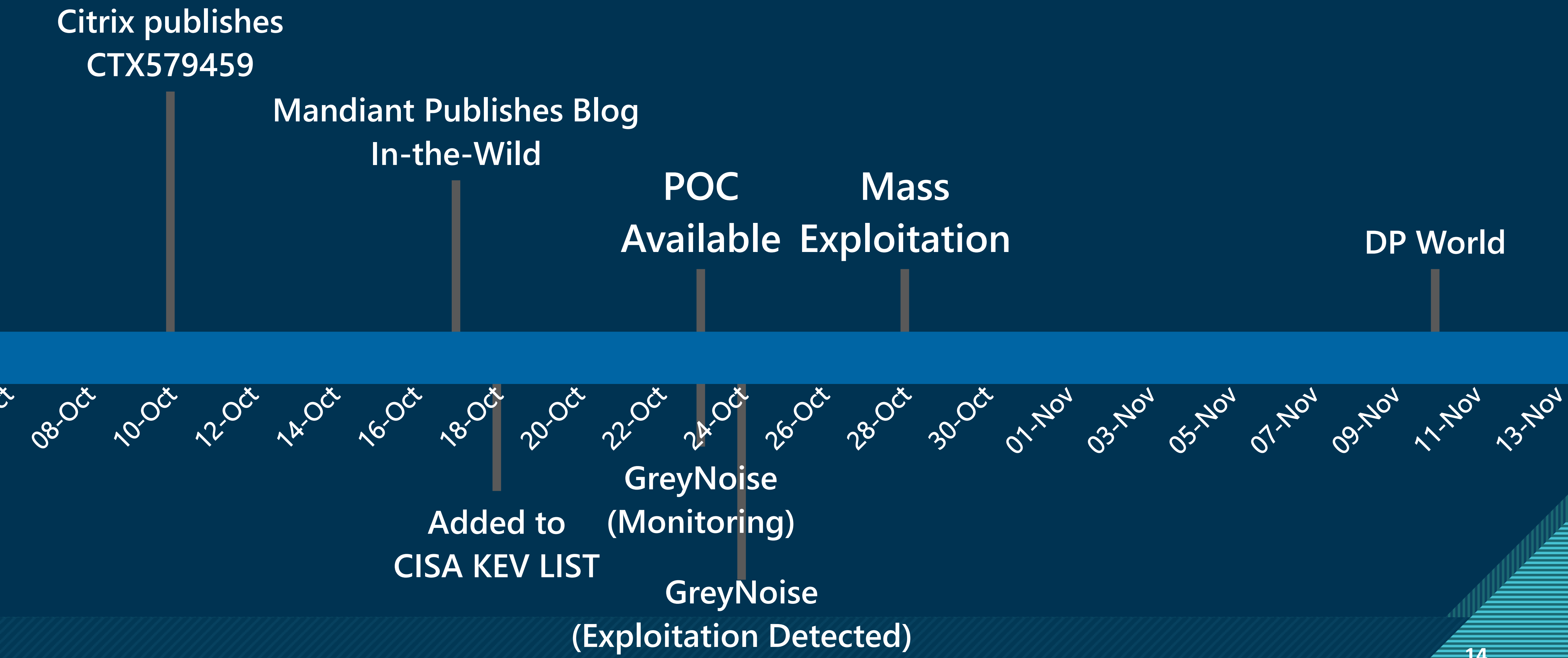
Q1-2025 Known Exploited Vulnerabilities (159)

Time From CVE to Exploitation Evidence

Source: VulnCheck KEV

Source: VulnCheck

CITRIX BLEED SPEED



Citrix publishes CTX579459

Mandiant Publishes Blog In-the-Wild

Added to CISA KEV LIST

POC Available

GreyNoise (Monitoring)

GreyNoise (Exploitation Detected)

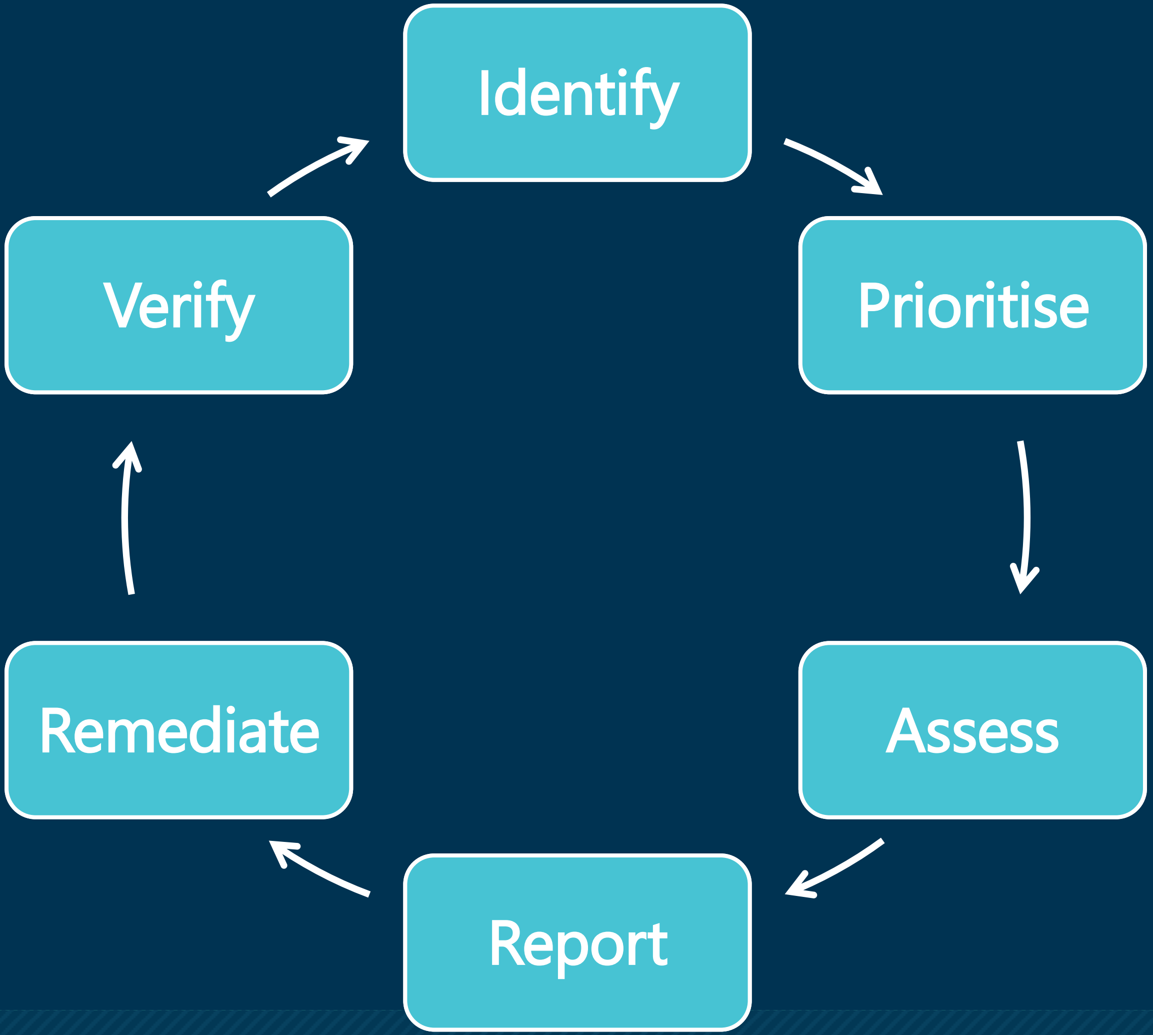
Mass Exploitation

DP World

ENOUGH LIFEBOATS?

- We have a lot of tools to use:
  - Vulnerability Scanners
  - Extended Detection and Response (XDR)
  - Cloud-Native Application Protection Platform (CNAPP)
  - Cloud Security Posture Management (CSPM)
  - External Attack Surface Monitoring (EASM)
  - Static Application Security Testing (SAST)
  - Dynamic Application Security Testing (DAST)
  - And some more….

CLASSIC VM LIFECYCLE



Identify

Prioritise

Assess

Report

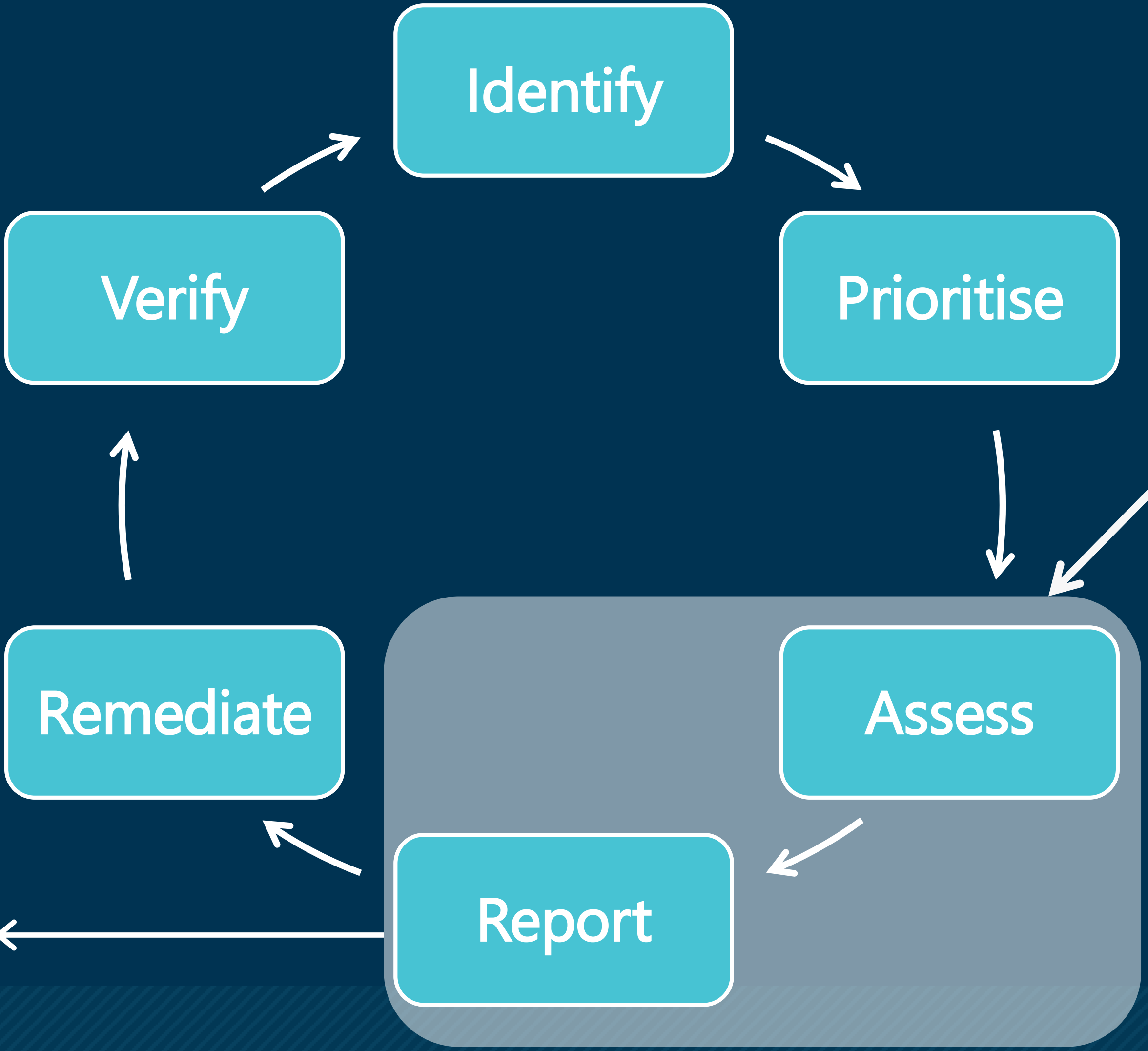
Remediate

Verify

CLASSIC PRIORITISATION

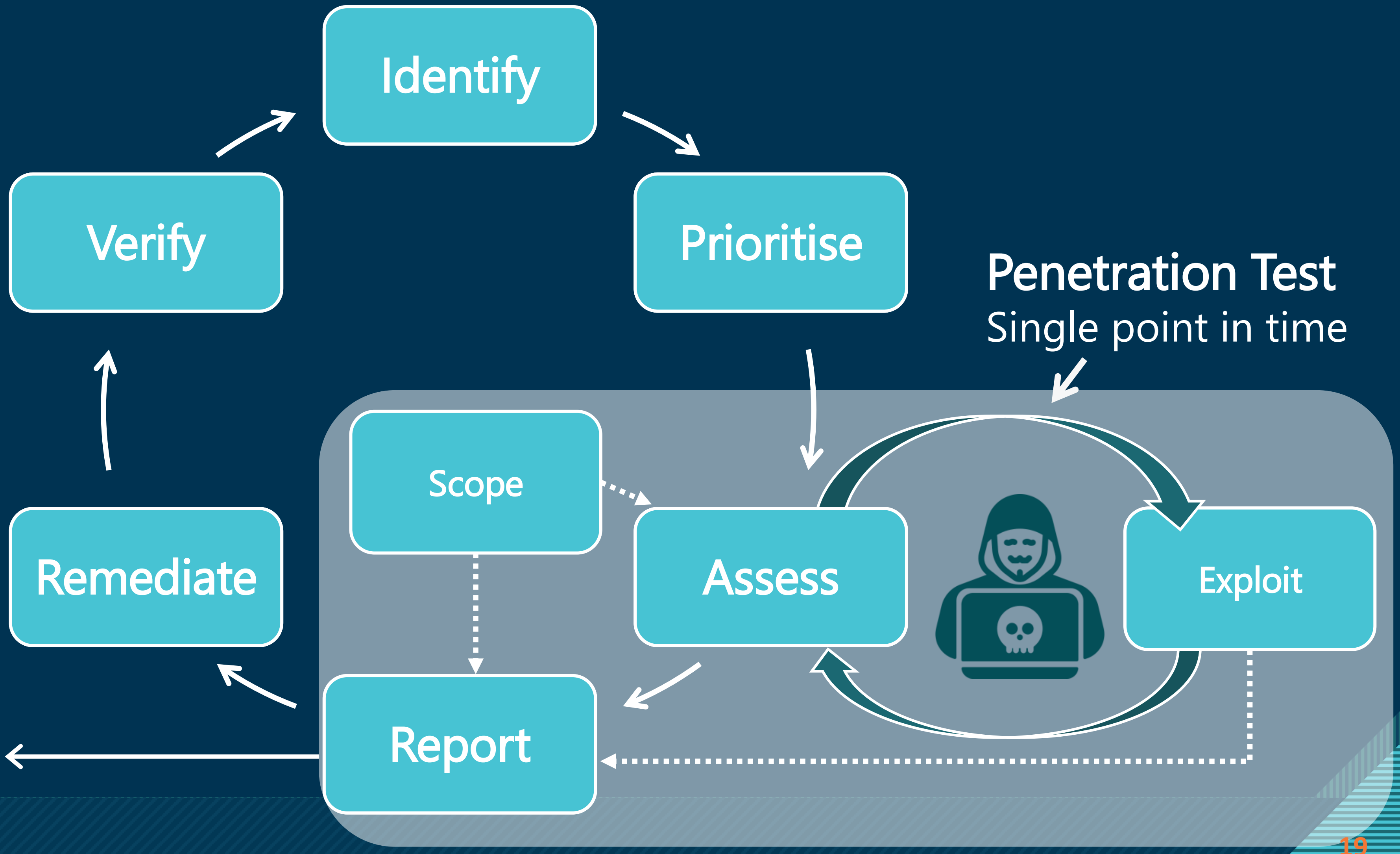
	Vulnerability Assessment Rating (Remediation Target)		
Asset Priority	High	Medium	Low
High	Critical (10 Business Days)	Critical (~~10~~ **30 Business Days**)	High (~~30~~ **60 Business Days**)
Medium	Critical (~~10~~ **30 Business Days**)	High (~~30~~ **90 Business Days**)	Low (~~100 Business days~~ **NEVER**)
Low	High (~~30~~ **180 Business Days**)	Low (~~100 Business days~~ **NEVER**)	Low (~~100 Business days~~ **NEVER**)

CLASSIC VM LIFECYCLE



Vulnerability Assessment
Single point in time

CLASSIC VM LIFECYCLE



Identify

Prioritise

Assess

Report

Remediate

Verify

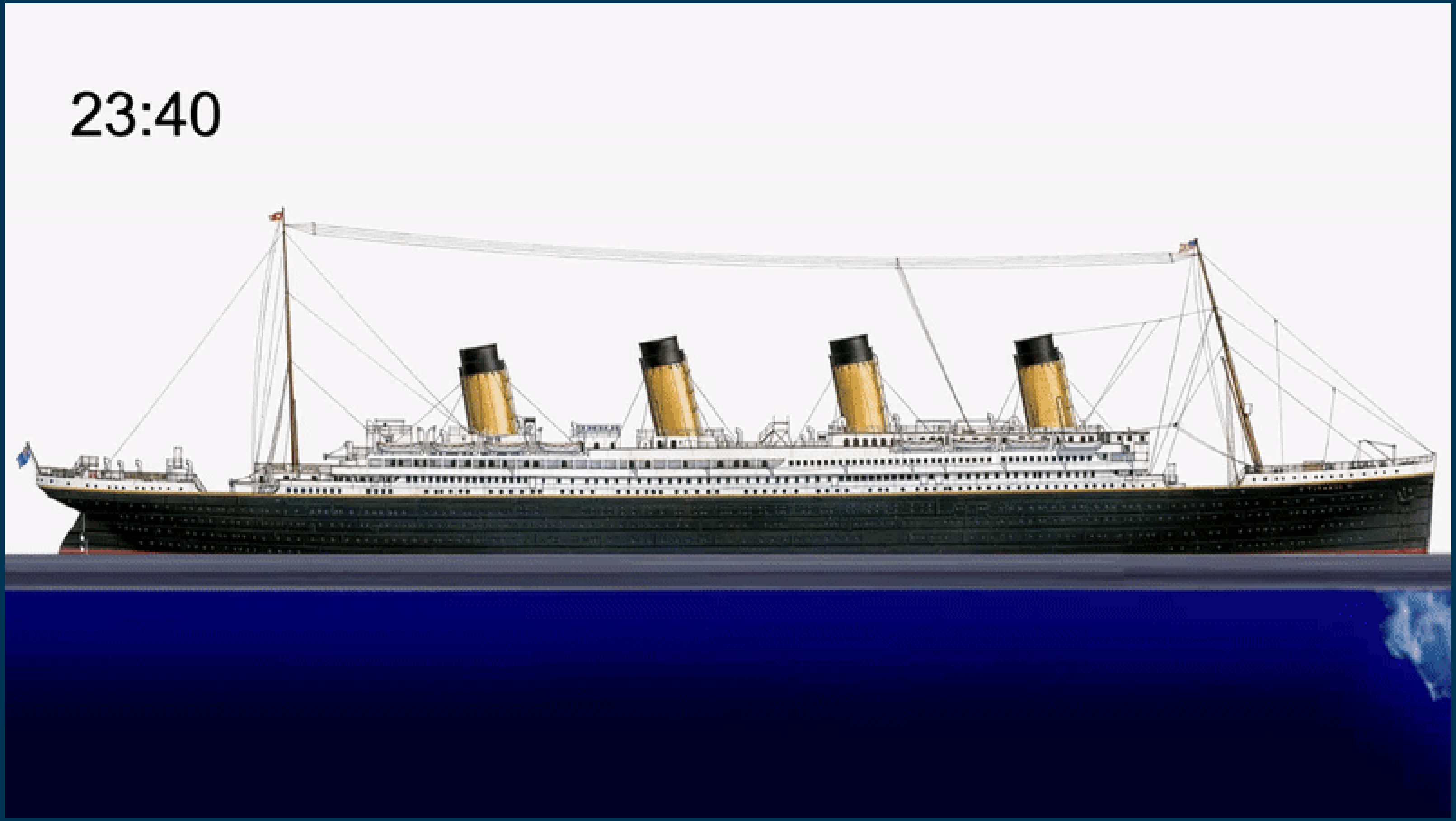
Scope

Exploit

Penetration Test

Single point in time

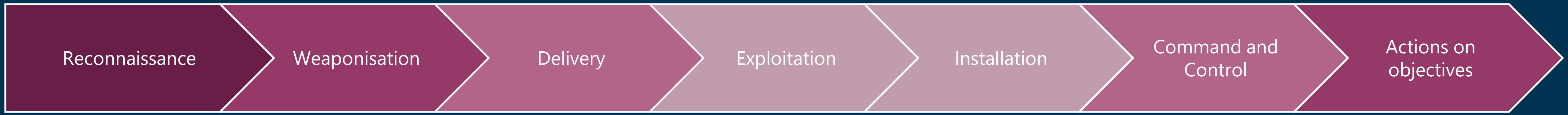
ENGAGING BULKHEADS



VULNERABILITY CHAINING

- Concept where a single vulnerability in isolation is difficult to exploit, however when several vulnerabilities are used in a combination, allows an adversary to have greater impact or gain further

- Traditionally a technique used by Red Team, Penetration testers or Advanced Persistent Threat (APT) groups.



Reconnaissance

Weaponisation

Delivery

Exploitation

Installation

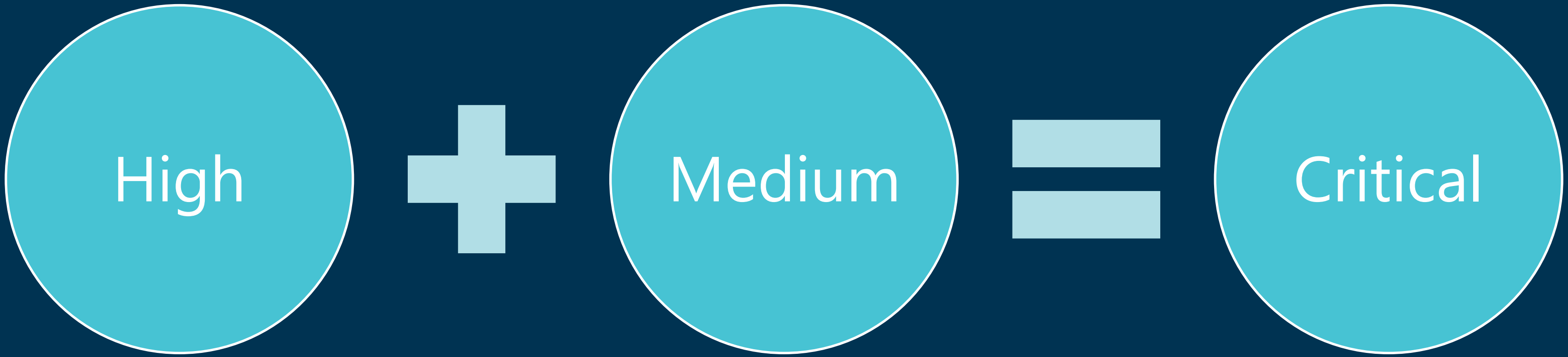
Command and Control

Actions on objectives

Source: Lockheed Martin – Cyber Kill Chain

VULNERABILITY CHAINING

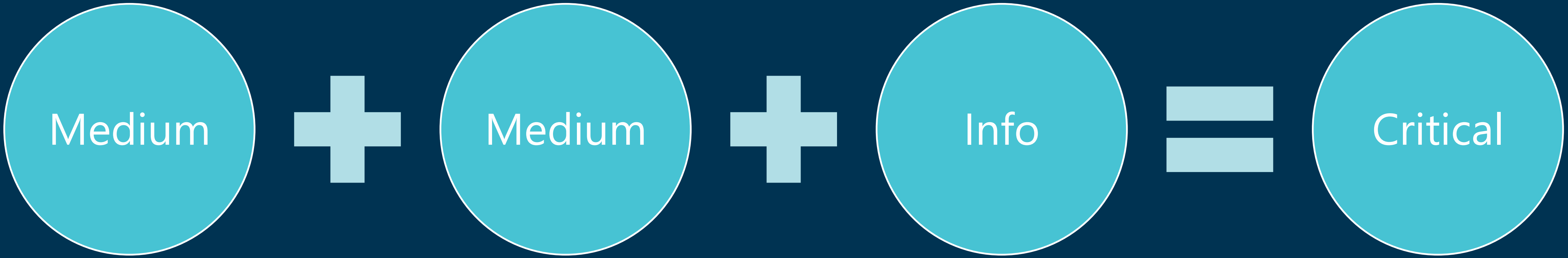
- Ivanti Endpoint Manager Mobile (EPMM)



Severity	Description
High	CVE-2025-4428 Code Injection Vulnerability
Medium	CVE-2025-4427 Authentication Bypass Vulnerability
Critical	Un-authenticated Remote Code Execution

VULNERABILITY CHAINING

- Example from Active Directory



Medium + Medium + Info = Critical

Severity	Description
Medium	LAN Manager authentication level
Medium	SMB Signing not required
Info	Link-Local Multicast Name Resolution (LLMNR)
Critical	Pass-the-Hash Attack

RED/BLUE ASSESSMENTS

CISA Published top 10 Cyber Security Misconfigurations

1. Default configurations of software and applications
2. Improper separation of user/administrator privilege
3. Insufficient internal network monitoring
4. Lack of network segmentation
5. Poor patch management
6. Bypass of system access controls
7. Weak or misconfigured multifactor authentication (MFA) methods
8. Insufficient access control lists (ACLs) on network shares and services
9. Poor credential hygiene
10. Unrestricted code execution

Source: NSA and CISA Red and Blue Teams Share Top Ten Cybersecurity Misconfigurations

SECURE CONFIGURATION

- Security hardening
  - Microsoft Security Compliance Baselines
  - Center for internet Security (CIS) Benchmarks
- On-boarding / Implementation processes
  - Deploy Applications/Software/Services with consistency
  - E.g. Changing default passwords, configure least privilege of access and visibility of services
- Secure-by-default

MODERNISATION OPPORTUNITIES

- Asset Management & Prioritisation

ASSET MANAGEMENT

- Automated discovery
  - What is visible
  - What should be visible (i.e. the gap)

ASSET PRIORITISATION

- Prioritise your assets FIRST

Prioritisation	Asset Group	Assessment Frequency	Remediation Targets (Critical/High/Exploitable)
Highest	Internet Facing Systems	Daily	Critical/Exploitable – 48 Hrs Others – 14 days
	Crown Jewels	Weekly	14 Days
	Authentication and Security Management Software(s)	Weekly	14 days
Medium	Remaining Server Systems	Weekly	OS - 28 days
	Workstations	Weekly	High Risk apps – 14 days OS – 28 Days
Low	Network equipment, Network Printers and Storage Systems	Fortnightly	28 Days
Out of Scope	???	Monthly	N/A

MODERNISATION OPPORTUNITIES

- Asset Management & Prioritisation
- Secure Configuration/Baselines

SECURE CONFIGURATION

- ASD's Blueprint for Secure Cloud
- ACSC’s System Hardening and Administration
- CIS Benchmarks
- Microsoft Security Compliance toolkit
  - Deployable Baselines (GPOs and Documentation)
  - Comparison Tools (PolicyAnalyzer)
- Vendor recommended hardening

MODERNISATION OPPORTUNITIES

- Asset Management & Prioritisation
- Secure Configuration/Baselines
- Continuous Monitoring

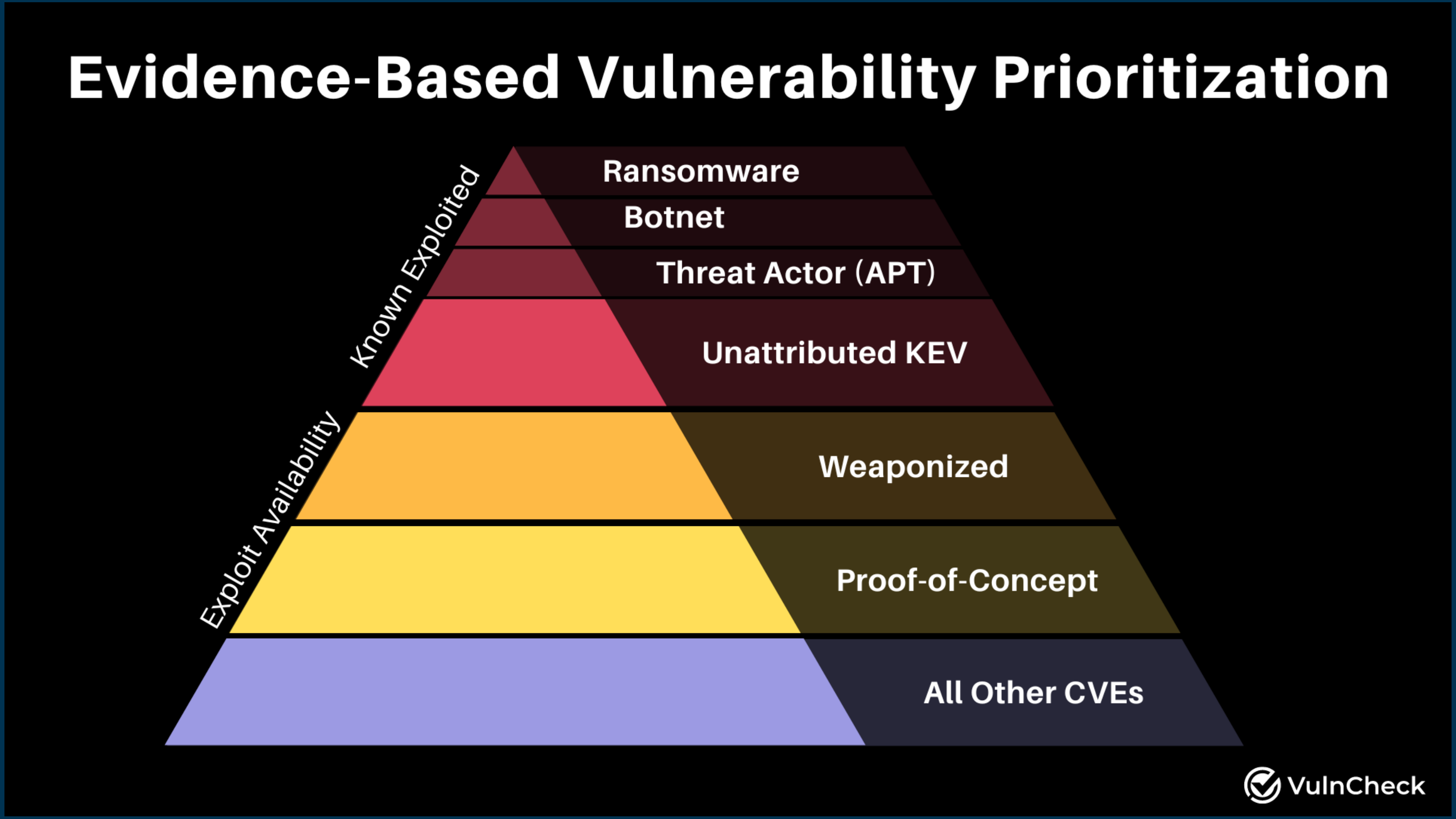
CONTINUOUS MONITORING

- Security Frameworks have it built in:
  - ASD’s ACSC Essential Eight & Information Security Manual (ISM)
  - NIST Cyber Security Framework (CSF) 2.0
  - International Organization for Standardization (ISO) – ISO 27000 Series
  - Center for Internet Security (CIS) Top 18

MODERNISATION OPPORTUNITIES

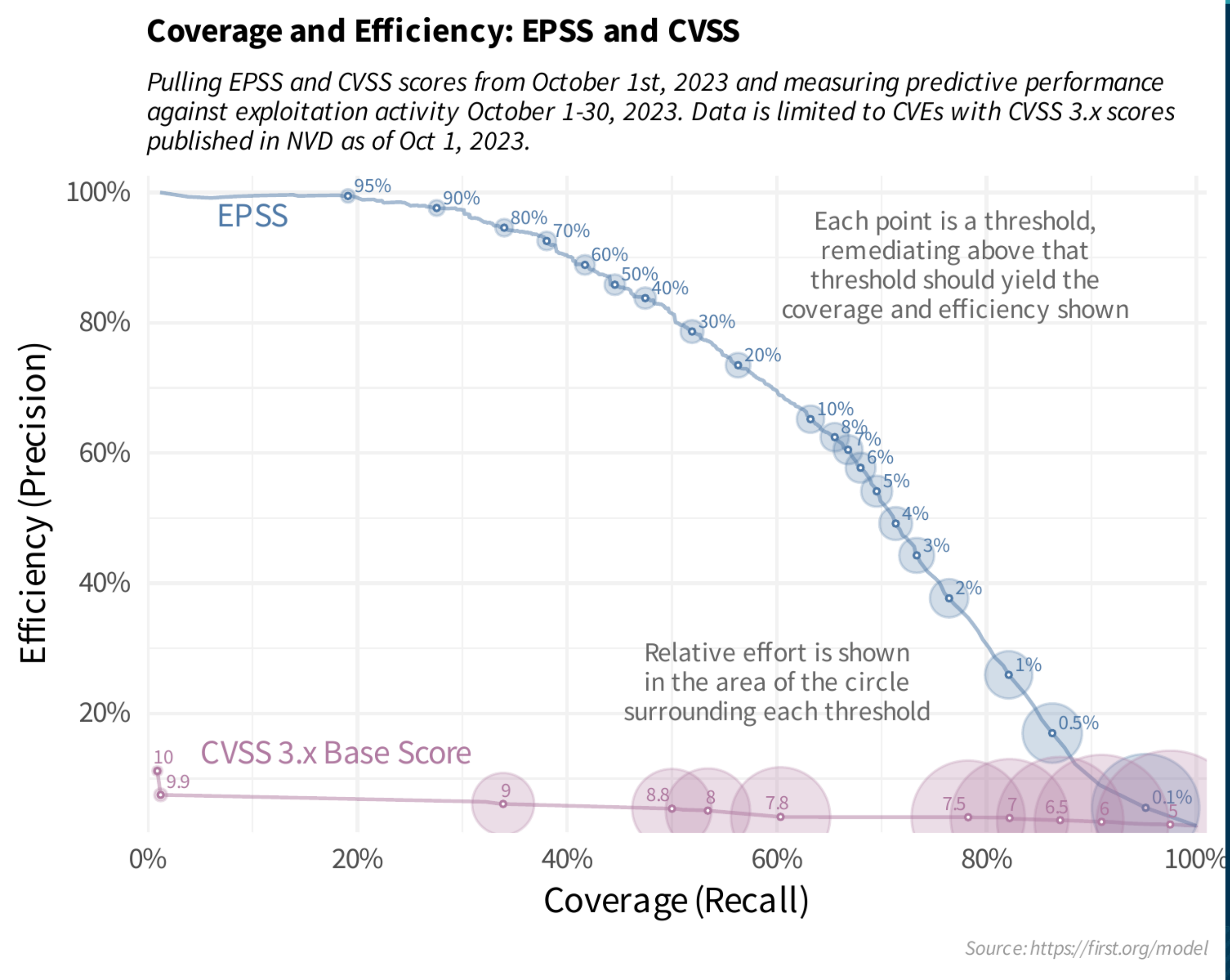
- Asset Management & Prioritisation
- Secure Configuration/Baselines
- Continuous Monitoring
- Threat Informed Prioritisation of Remediation

THREAT INFORMED



Source: Vulncheck

THREAT INFORMED



Coverage and Efficiency: EPSS and CVSS

Pulling EPSS and CVSS scores from October 1st, 2023 and measuring predictive performance against exploitation activity October 1-30, 2023. Data is limited to CVEs with CVSS 3.x scores published in NVD as of Oct 1, 2023.

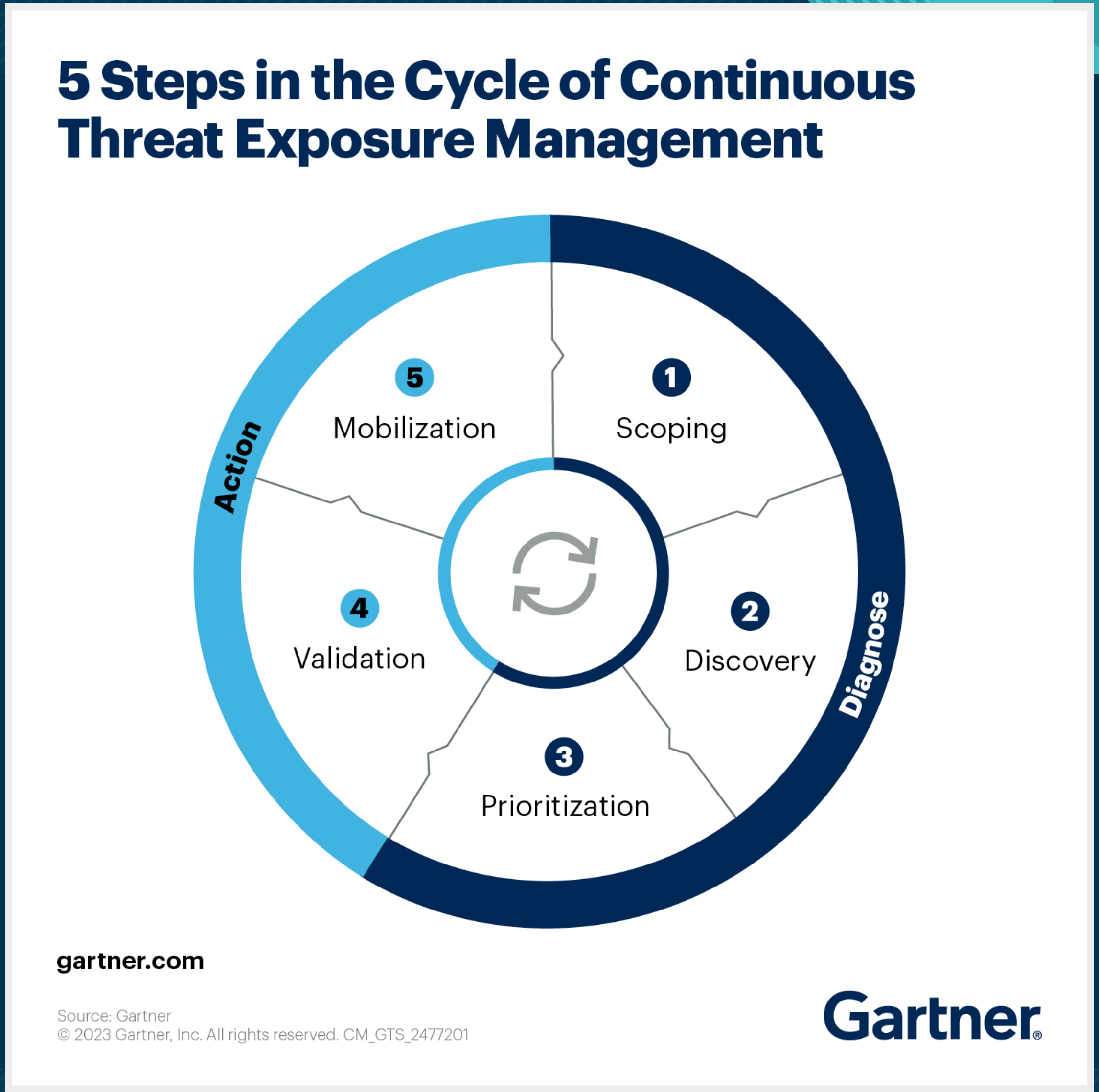
Each point is a threshold, remediating above that threshold should yield the coverage and efficiency shown

Relative effort is shown in the area of the circle surrounding each threshold

Source: https://first.org/model

Source: The EPSS Model (first.org)

CTEM



5 Steps in the Cycle of Continuous Threat Exposure Management

Diagnose

1 Scoping

2 Discovery

3 Prioritization

Action

4 Validation

5 Mobilization

gartner.com

Source: Gartner

Gartner

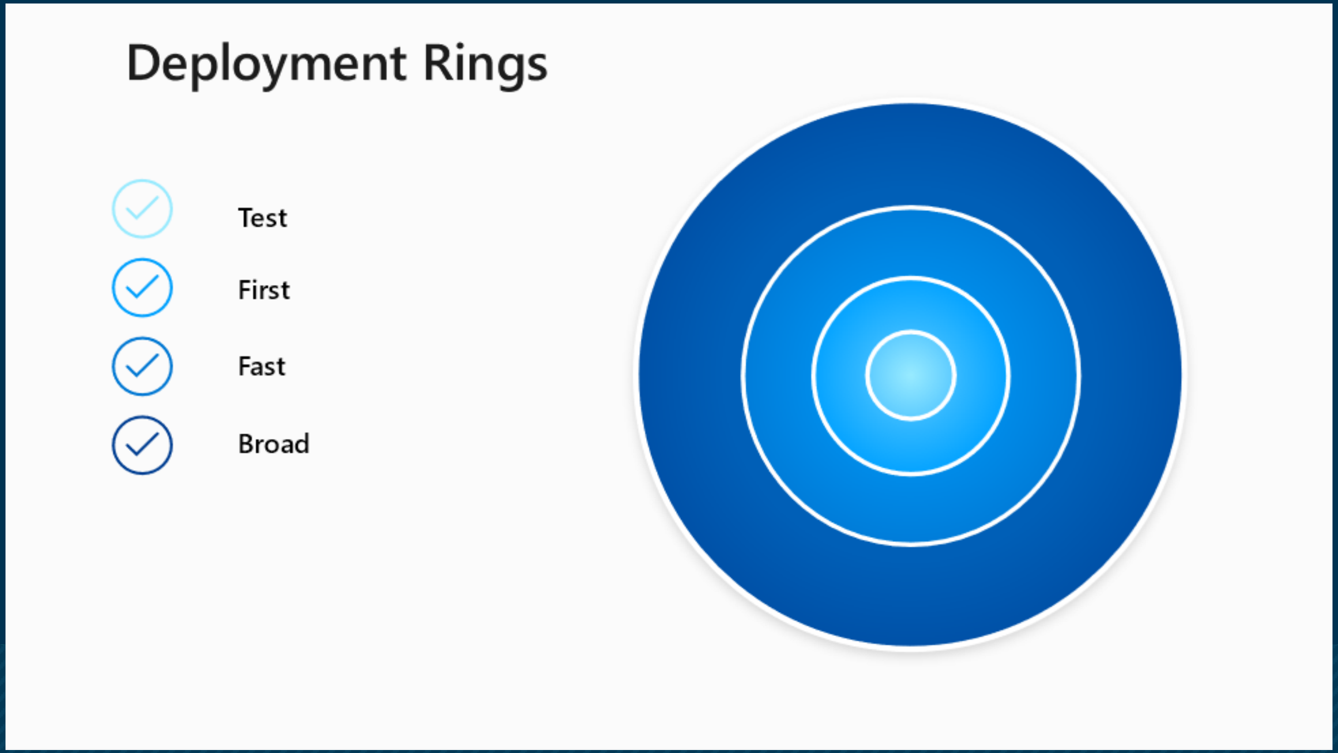
Source: Gartner

MODERNISATION OPPORTUNITIES

- Asset Management & Prioritisation
- Secure Configuration/Baselines
- Continuous Monitoring
- Threat Informed Prioritisation
- Embrace Automation

EMBRACE AUTOMATION

- Follow your Patch release or Change Management Process
- A ringed or staged deployment can minimise harm if negative impacts occur



Deployment Rings

MODERNISATION OPPORTUNITIES

- Asset Management & Prioritisation
- Secure Configuration/Baselines
- Continuous Monitoring
- Threat Informed Prioritisation
- Embrace Automation
- Drive Value Across the Organisation

DRIVE VALUE

Security Team

IT Operations Team

Thank You