Security Validation at the Heart of Exposure Management

Lars Jensen, Regional Director, Pentera

Recent High Profile Breaches

Recent High Profile Breaches

Microsoft

Skeleton key discovered in unprotected storage → Forged 25 authentication tokens to different orgs → Storm-0558 remains under the radar for months

Data Leakage

Privilege Escalation

Lateral Movement

APT

Recent High Profile Breaches

MGM RESORTS INTERNATIONAL®

Spear-vished help desk and abused trust → **Reset OKTA admin user** → **Mass escalation on ESXi hypervisors & ransomware**

Vishing

Privilege Escalation

Lateral Movement

Business Downtime

Software Vulnerability

Data Leakage

Vishing

Supply Chain Attack

Phishing

Stolen Creds

Physical Security Breach

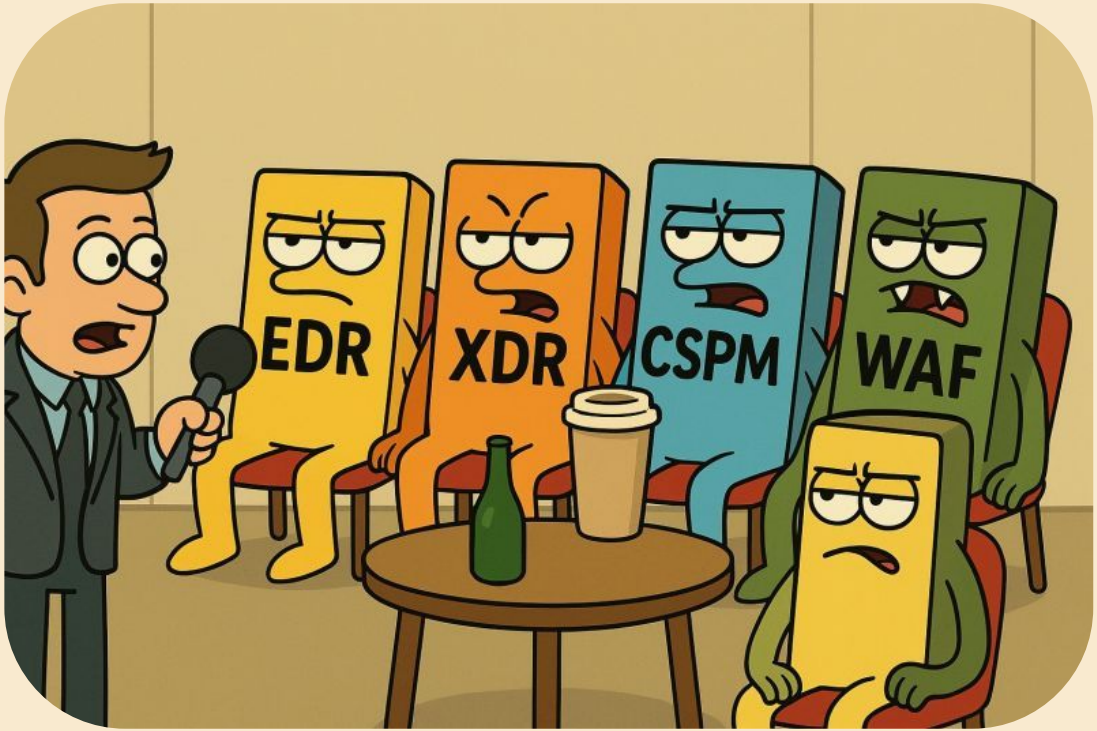
WIFI Breach

Insider Threat

INITIAL ACCESS BECOMES INEVITABLE!!

NOW WHAT?

ASSUME BREACH



BUY THE LATEST TOOLS

How CONFIDENT are you in your security posture?

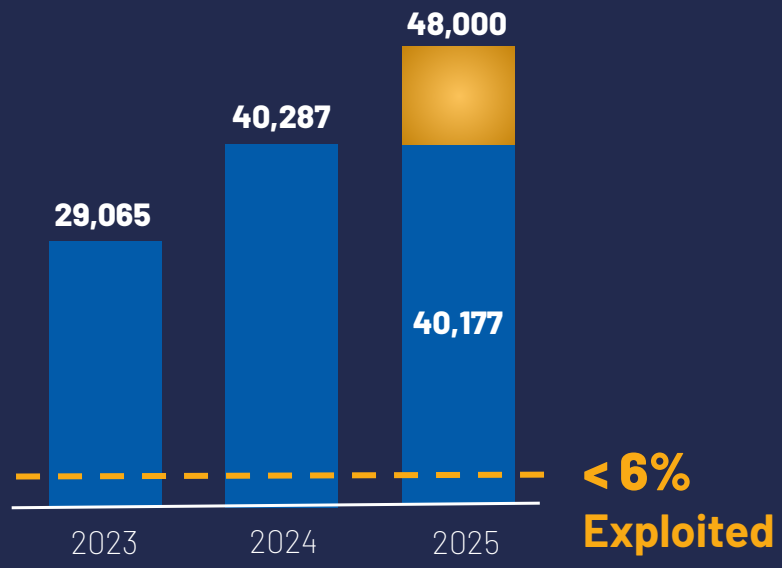
So, can I test my cyber SECURITY DEFENSE?

We Need to Change our

VULNERABILITY-CENTRIC APPROACH

Reality Check - We can never be patch perfect

Vulnerabilities (CVE) Discovered



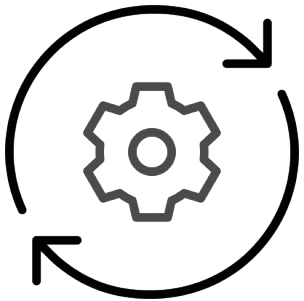
Source: www.cvedetails.com

> Non-patchable attack surfaces will account for **over 50% of enterprise exposure** by 2026.

Source: Gartner: Enterprises Must Expand From Threat to Exposure Management"

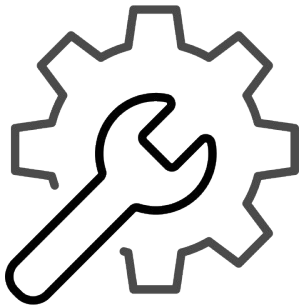
> ...a vulnerability is something I can patch

Patchable vs. Non-Patchable Vulnerabilities



UPDATE...

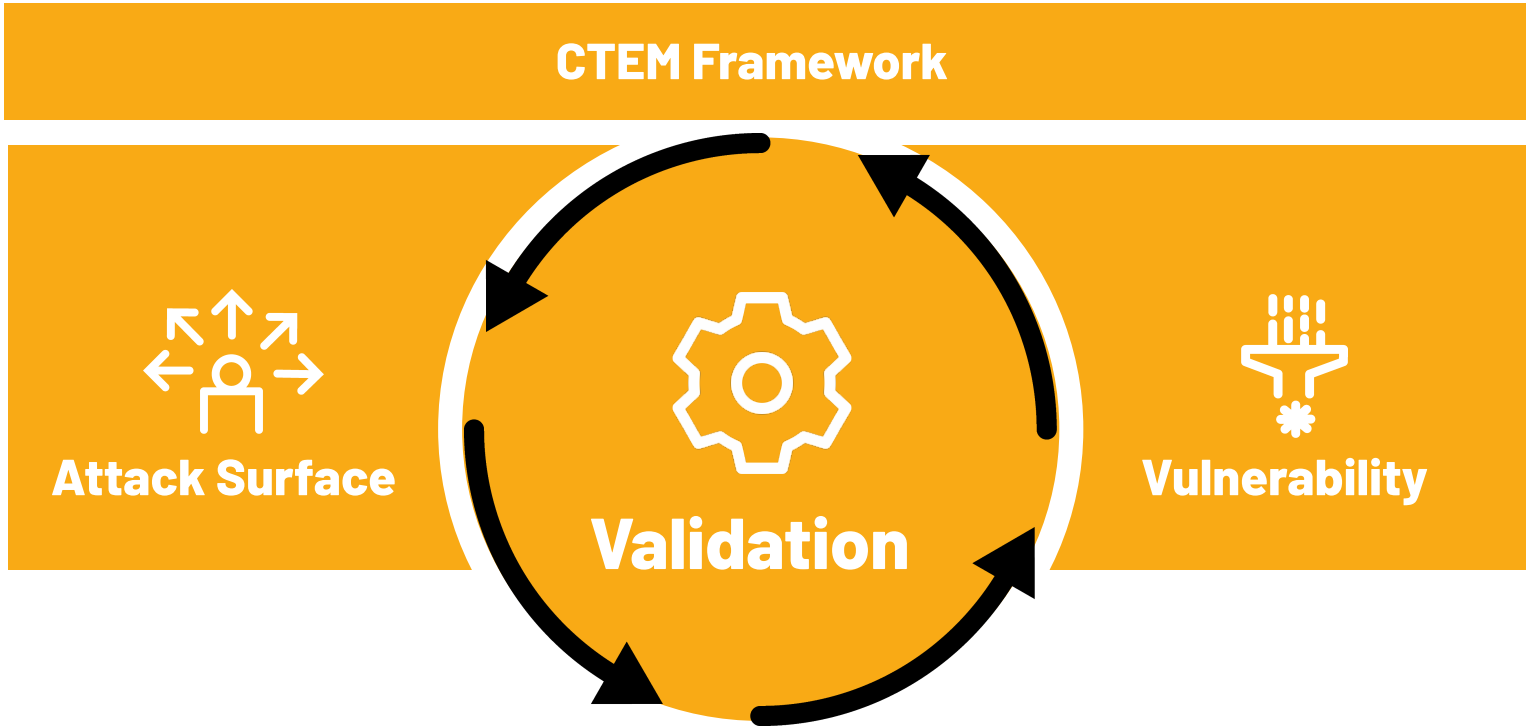
VS.



Introducing EXPOSURE MANAGEMENT

An ongoing process for accounting for and reducing your IT risk.

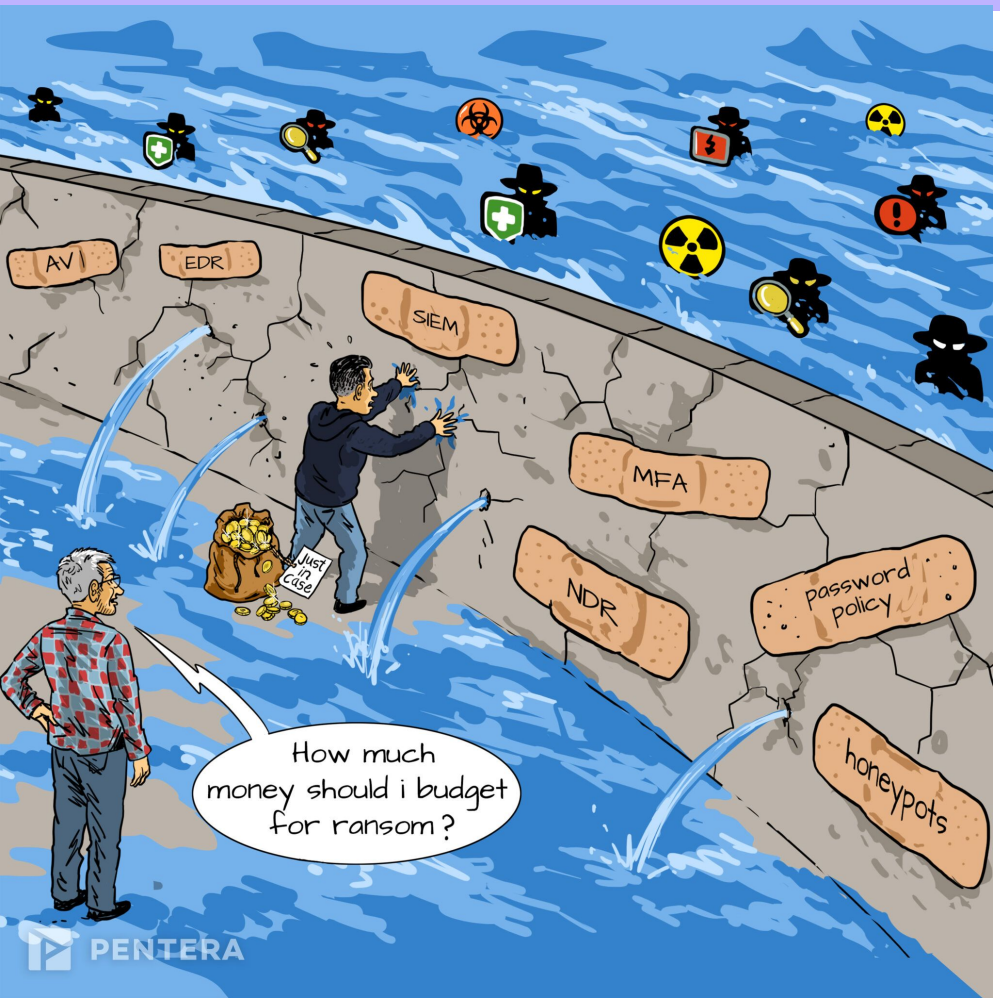
Validation - The Perpetual Engine at the Heart of CTEM



> Exposure management is superseding the vulnerability management practices of today.

60% of Organizations **Pursuing or Considering CTEM**

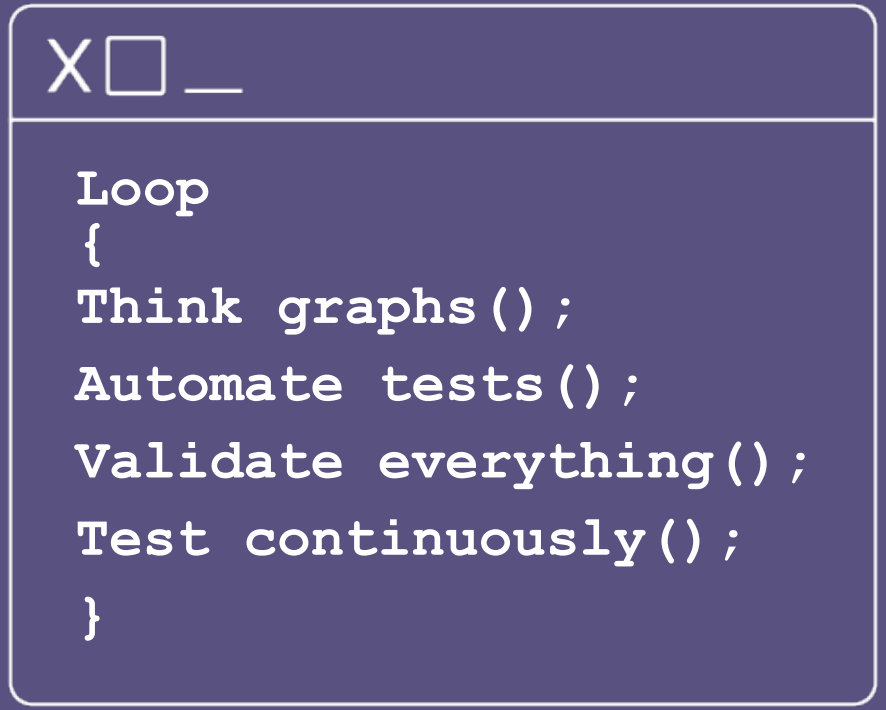
Source: Gartner Strategic Roadmap for CTEM, Aug 2025

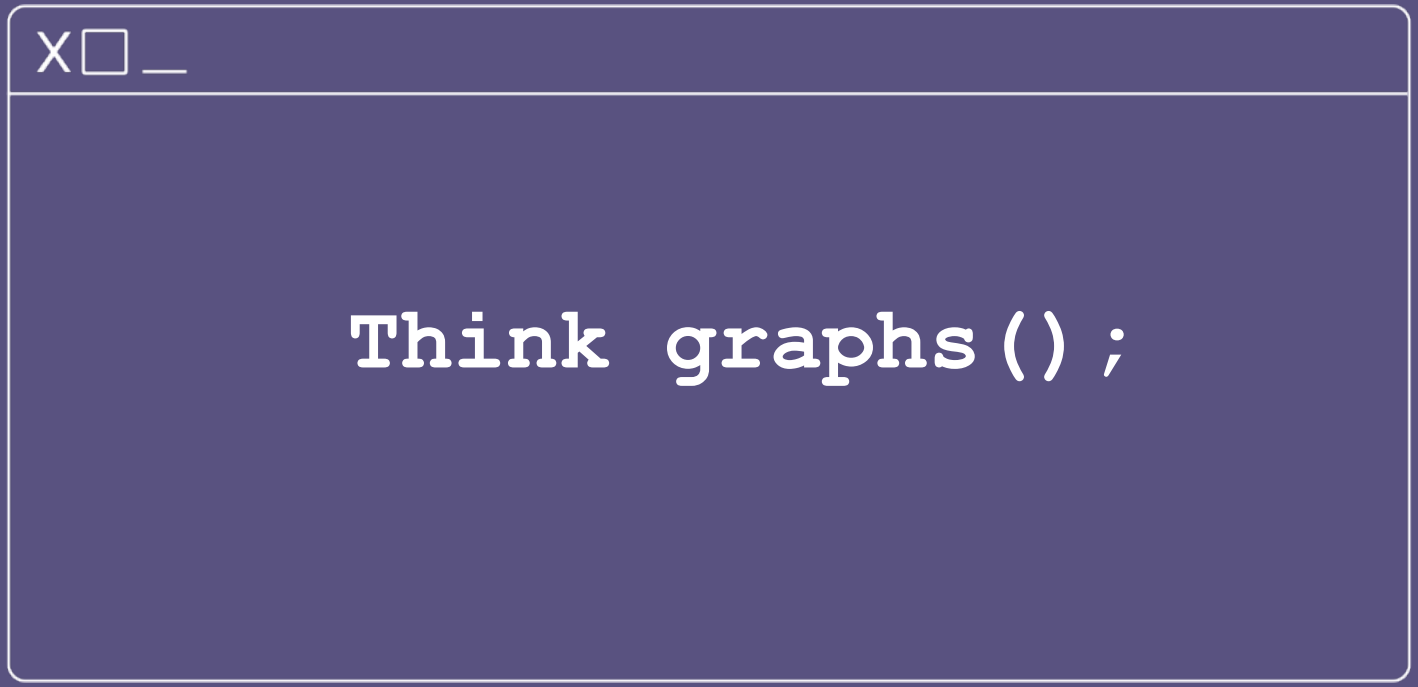


We need to validate like an attacker!

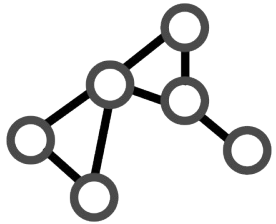
BUT HOW?

4 Pillars to validate like an ATTACKER



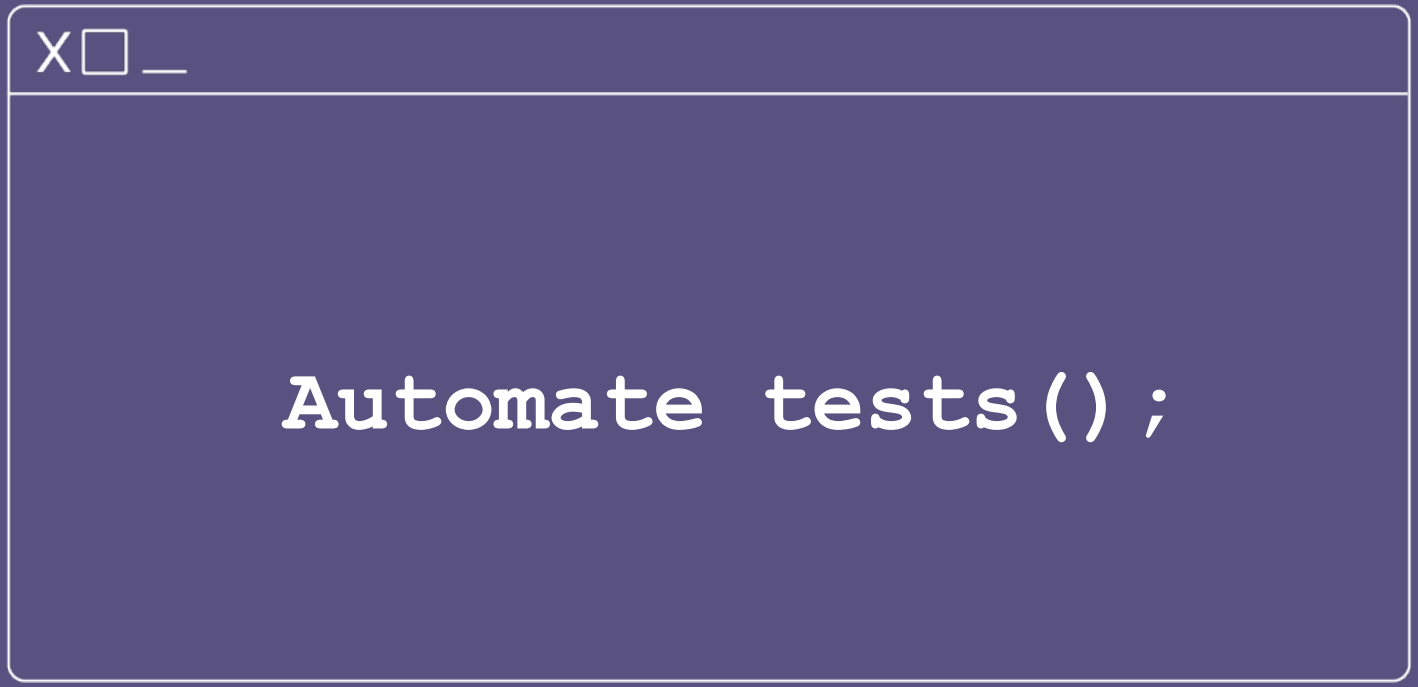

Think graphs();

DEFENDERS
think in lists



ATTACKERS
think in graphs

source: John Lambert, Microsoft


Automate tests();

VS

DEFENDERS
Use Manual Validation

ATTACKERS
Use Automated Attacks

Attackers Automate

APT1

used a batch script to perform a series of discovery techniques and save it to a text file

APT28

used a publicly available tool to gather and compress multiple documents on the DCCC and DNC networks

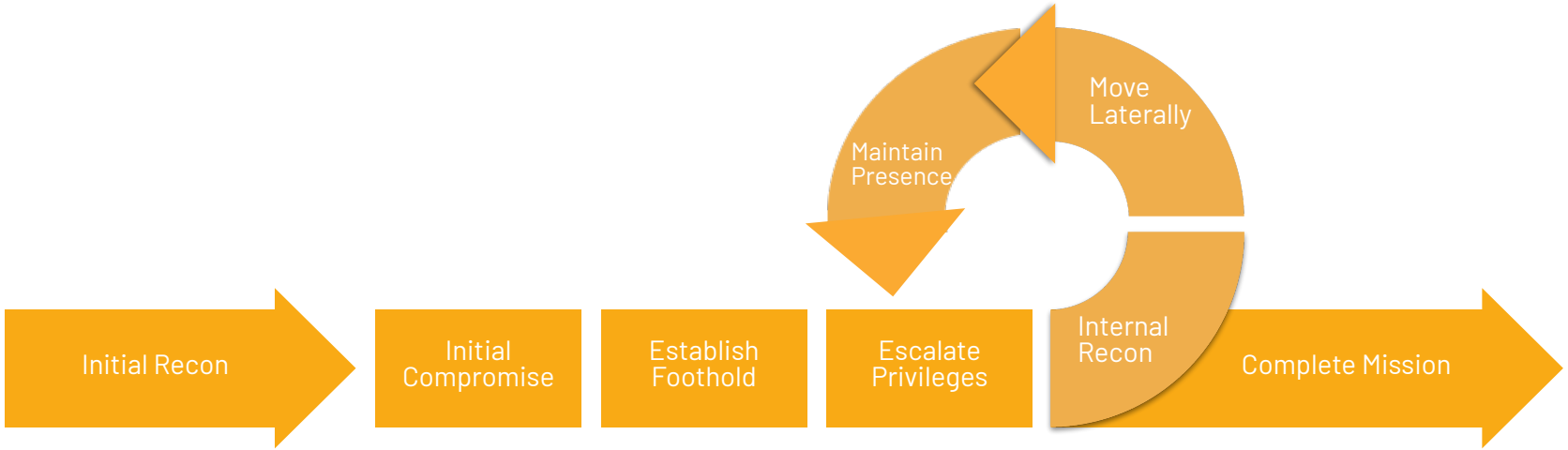
ZEBROCY

scans the system and automatically collects files with specific extensions

FRANKENSTEIN

has enumerated hosts via Empire, gathering the username, domain name, machine name and other system information

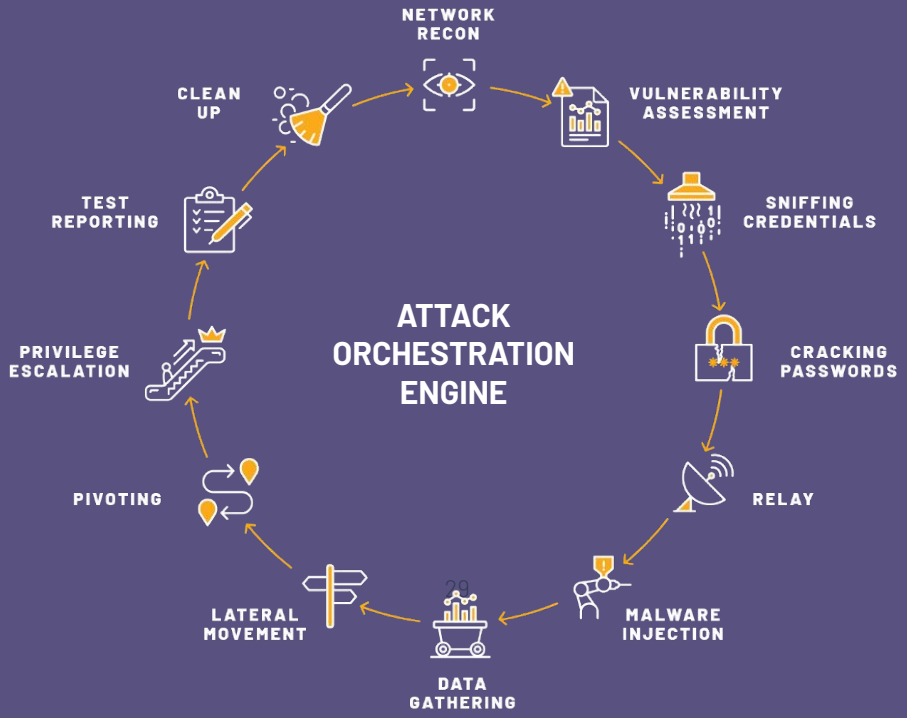
The Automated Attacker Lifecycle



AUTOMATED VALIDATION NEEDS TO GO THROUGH ALL STAGES!

```
Validate everything();
```

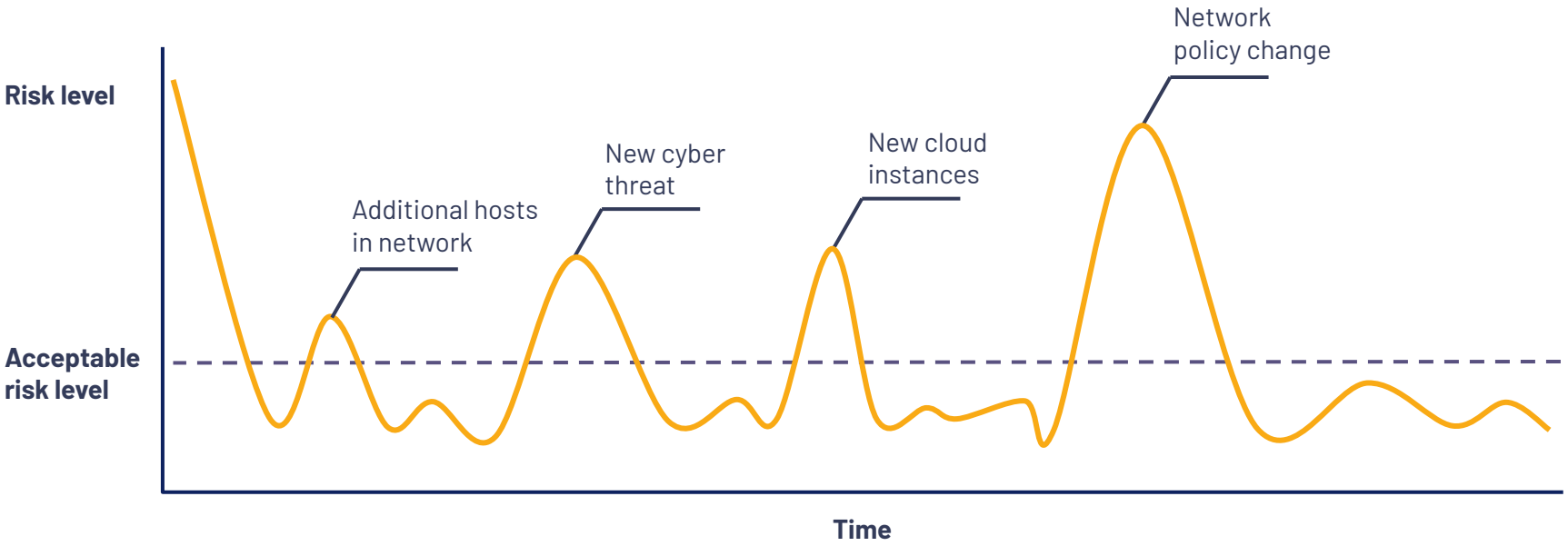
AUTOMATED VALIDATION



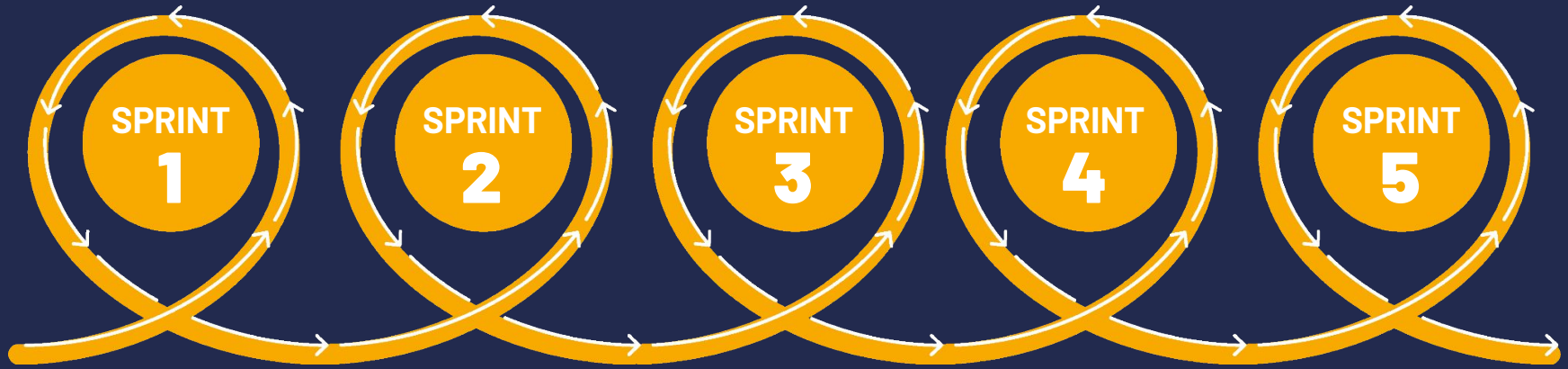
30

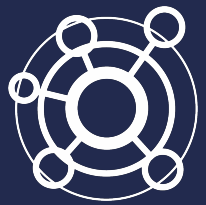
Challenge: Limited Visibility

Accounting for a Constantly Changing Attack Surface



Agile Exposure Management
Monthly/Weekly Remediation “Sprints”





Your exposure management strategy is as good as your security validation capabilities

3 key Takeaways

Assume Breach

3 key Takeaways

Assume Breach

Prioritize remediation according to validated risk and SLA

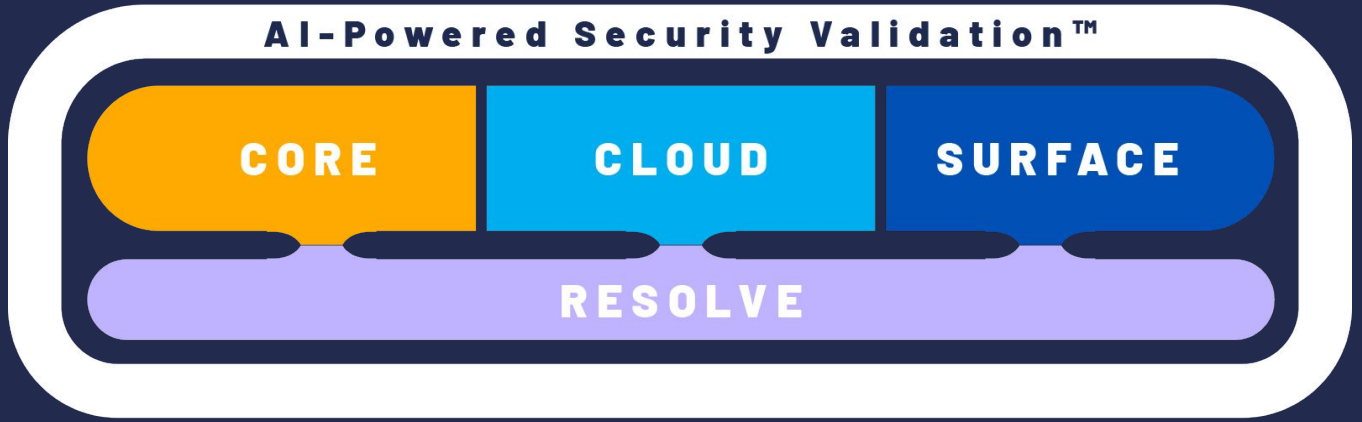
3 key Takeaways

Assume Breach

Prioritize remediation according to validated risk and SLA

Use Automation and AI to Validate

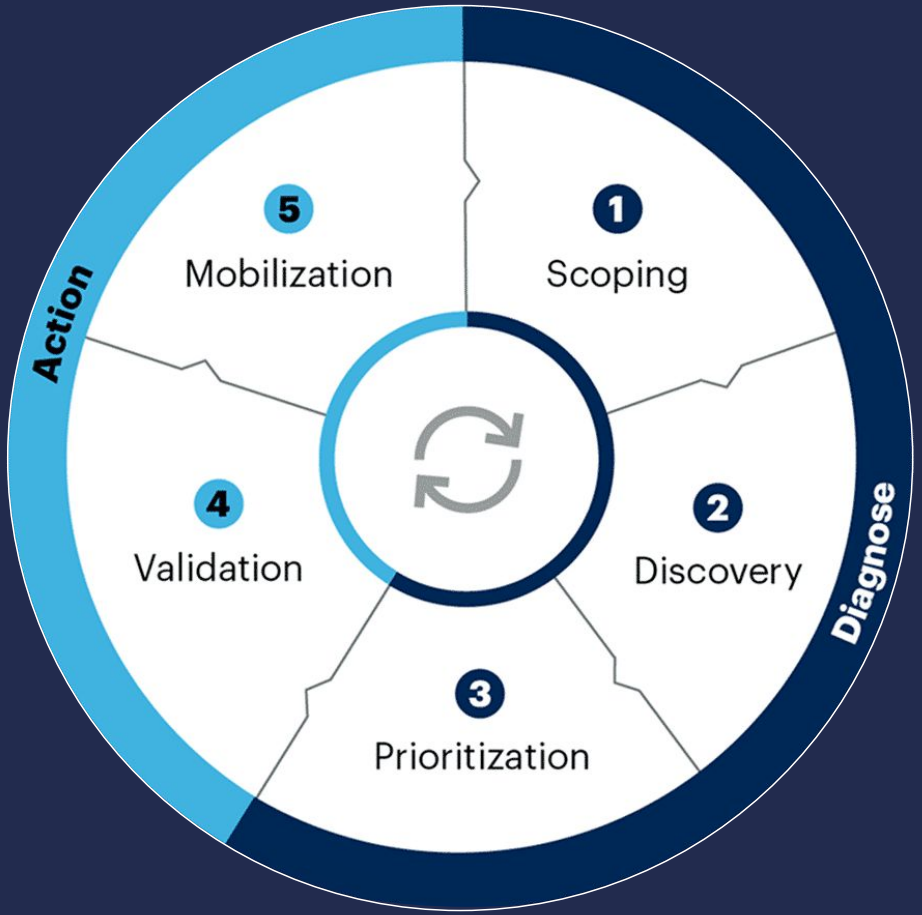
Pentera Platform



A Unified Validation to Remediation Platform

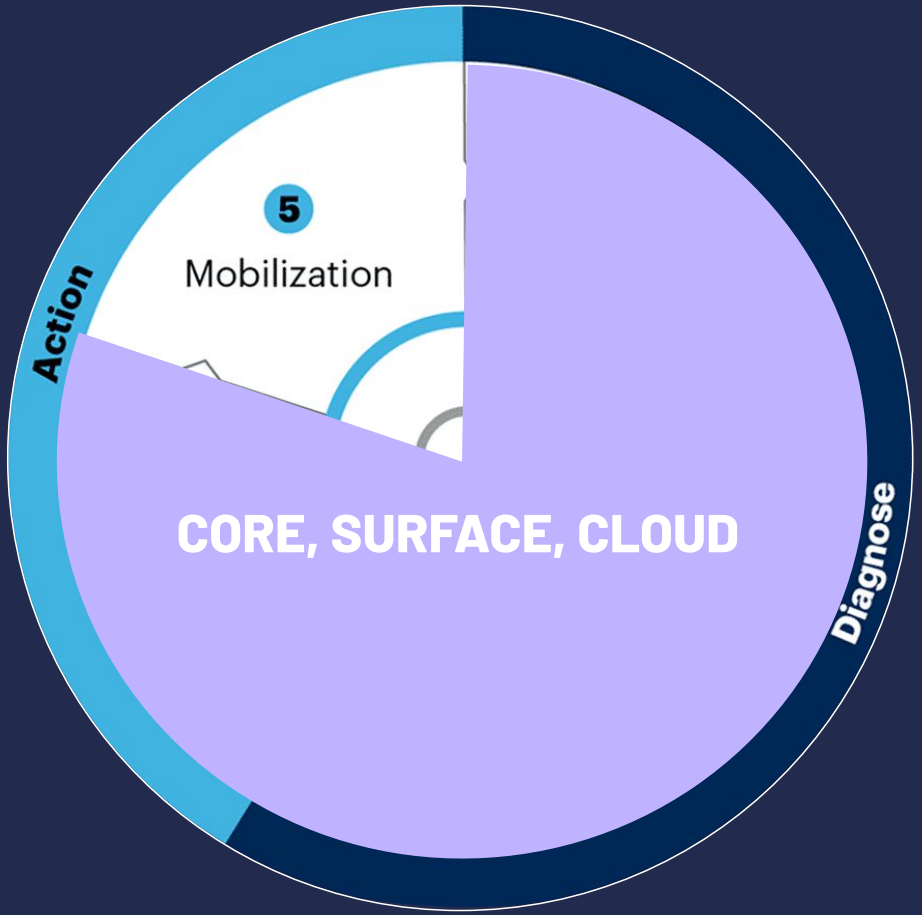
Continuous Threat Exposure Management

Gartner®



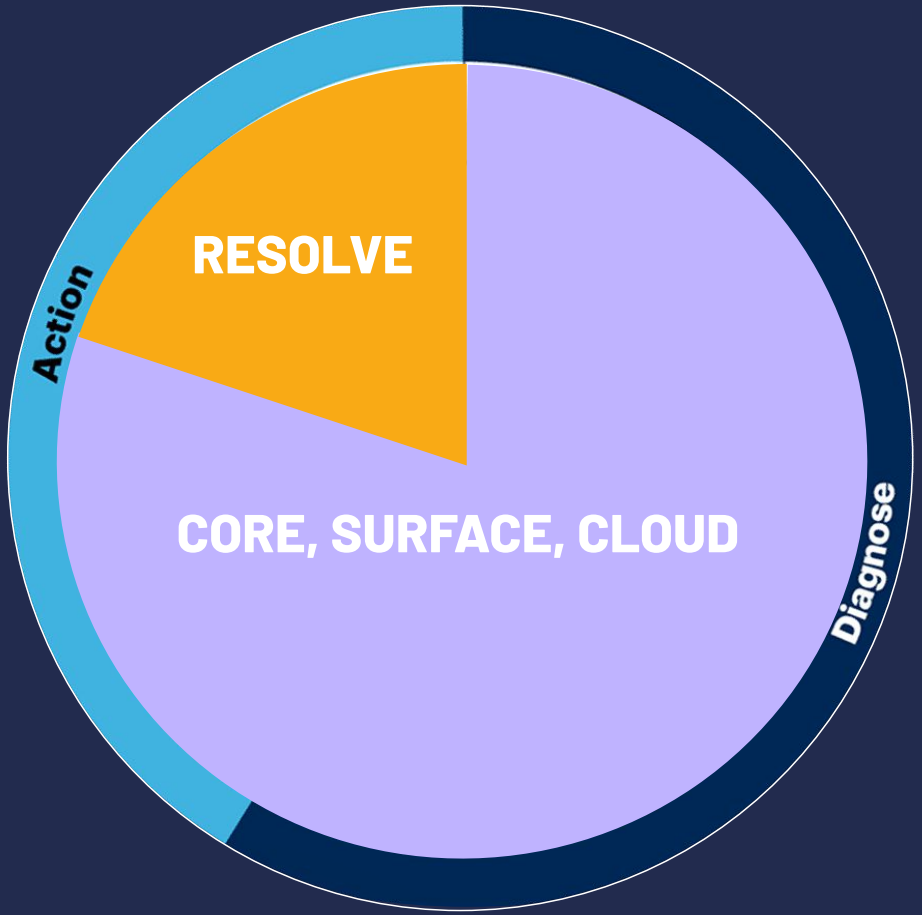
Continuous Threat Exposure Management

Gartner®



Continuous
Threat
Exposure
Management

Gartner®



Questions