GUIDE TO CTEM ADOPTION

Practical Tips for Framework Implementation

PENTERA

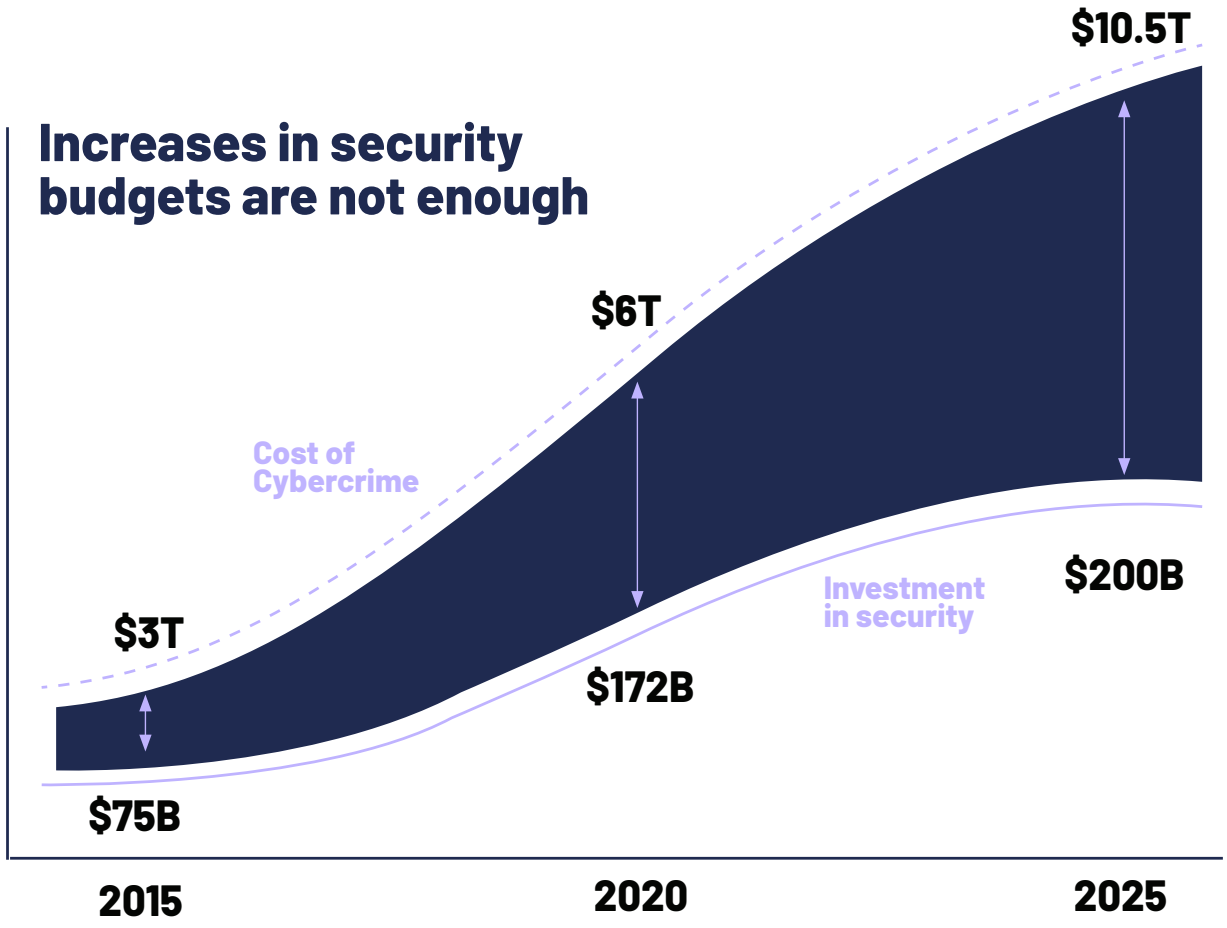
GUIDE TO CTEM ADOPTION

Table of contents

estment in defensive cybersecu tinues to increase, yet breache on the rise.

The paradox: Bigger budgets, yet still bigger breaches

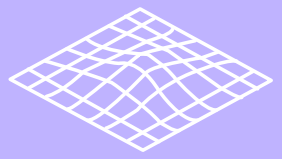
In 2020 investment in cybersecurity was at $172 billion, and yet the cost of cybercrime was at $6 trillion. By 2025, the cost of global cybercrime is expected to be $10.5 trillion, where spending will be $200 billion. Although companies invest more in their organizational security posture, there is no sign that this is successfully slowing the rate in which they are breached.



Source: Cybersecurity Ventures - 2023, Global cybercrime damage costs, Cobalt - 2023, Top cybersecurity statistics for 2024

This gap highlights a critical issue: **conventional cybersecurity measures are falling short.**

A few possible reasons for this:



Constantly morphing attack surface

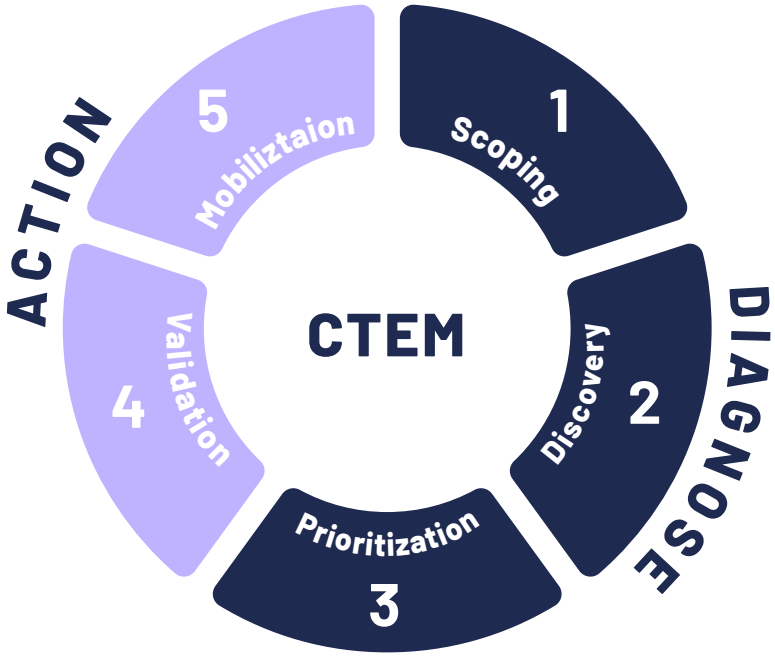
Rapidly changing network infrastructure

Attackers are constantly innovating their techniques with new malware ingenuities

All of these reasons indicate that a broader, more dynamic approach to managing cybersecurity is necessary.

What is CTEM?

CTEM (Continuous Threat Exposure Management) is a proactive security framework that integrates people, tools and processes to reduce risk and actively mitigate exposures across IT infrastructure.
It provides a **continuous and comprehensive** view of the attack surface and the vulnerabilities that may lead to exposure. It tests whether security controls effectively block the potential exploitation of exposures, prioritize exposures according to business risk, and identify the most effective mitigation tactic. It then streamlines the mobilization process towards remediating those vulnerabilities. This approach helps organizations maintain a high level of readiness and resilience.

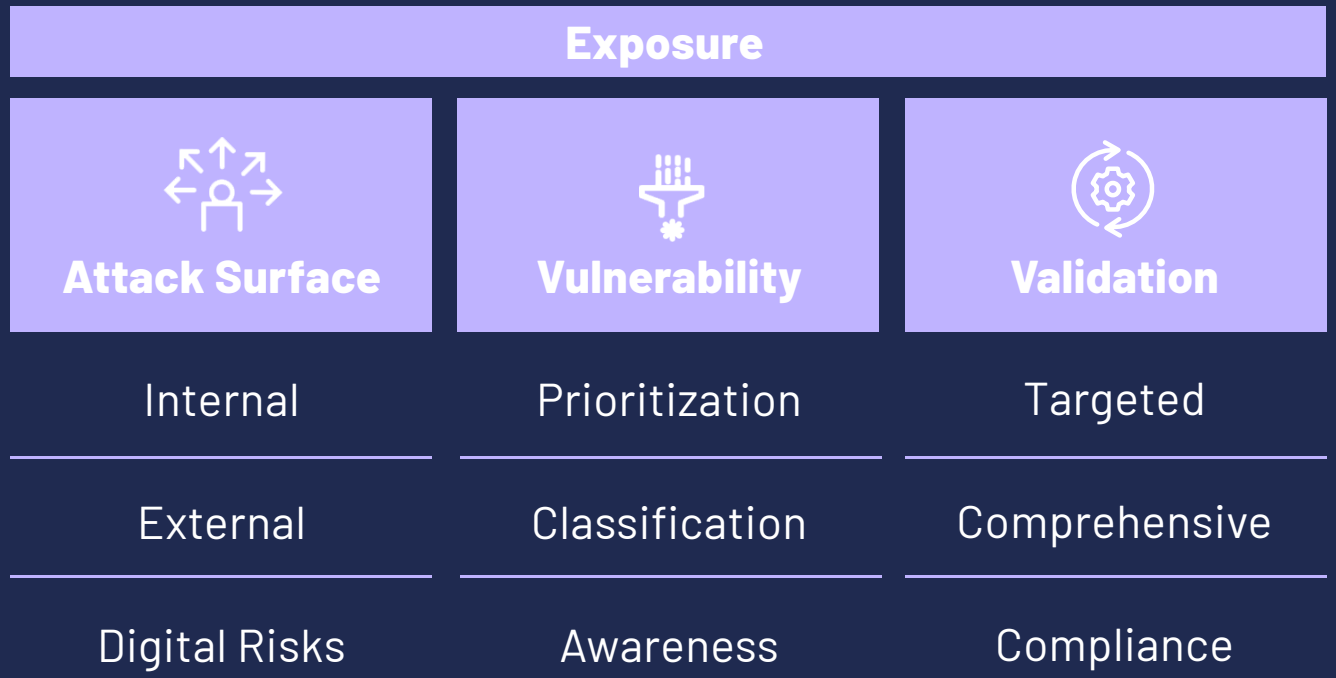


Adopting CTEM naturally implies the orchestration of many moving parts; pulling together digital assets, workloads, networks, identities, and data across the enterprise. We have broken down the pillars of CTEM to provide helpful steps to guide you through this process of system-wide orchestration.

The Three Key Pillars of CTEM

Adopting an effective CTEM strategy puts you in a structurally better security posture to weather a breach.

Components of Exposure Management



Gartner

By 2026, organizations prioritizing their security investments, based on a continuous threat exposure management program, will realize a two-third reduction in breaches.

"Top Strategic Technology Trends for 2024: Continuous Threat Exposure Management"' Oct 2023

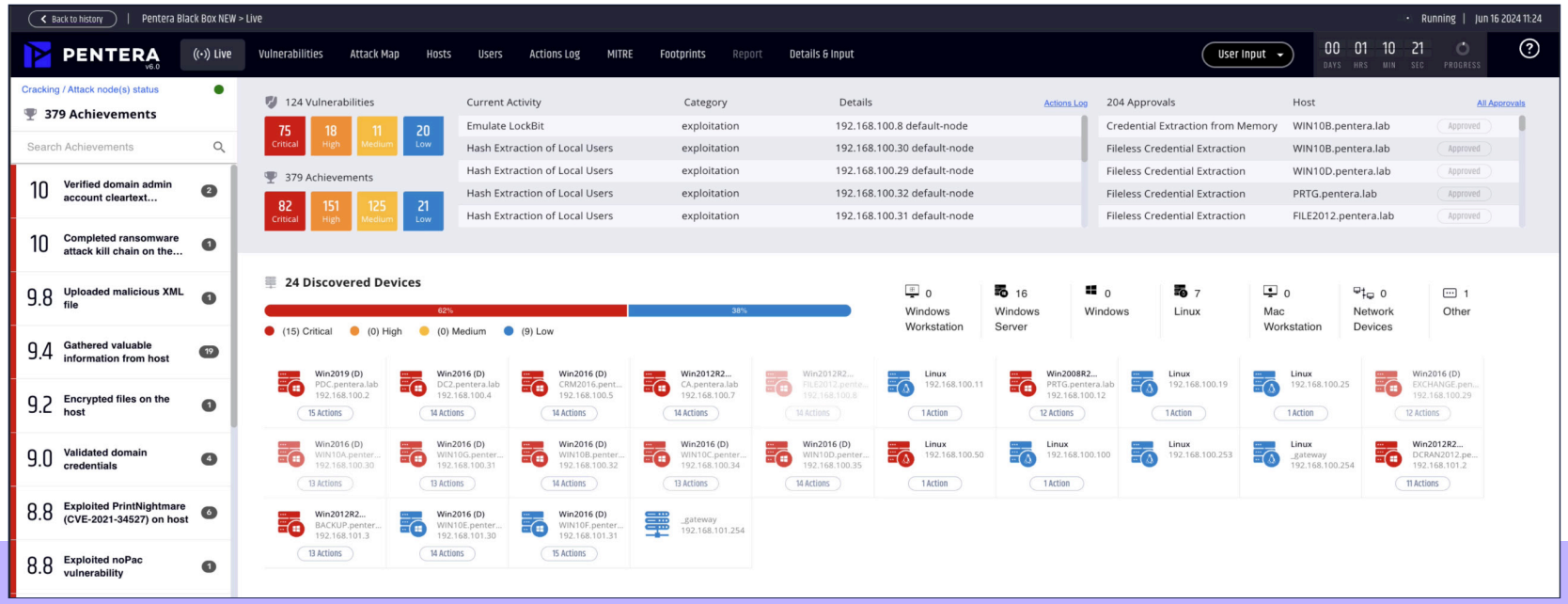
Pillar #1:

Attack Surface

Adopt an attacker's mindset for asset analysis

Asset management is an essential step at scoping the entire environment and getting a full inventory of digital assets and their relative sensitivity. However, the ability to understand each asset's exposure profile remains a challenge.

Organizations adopting CTEM gain a more realistic view of the exposure profile of each digital asset. **CTEM imposes an attacker's mindset, where the aim is identifying how an attacker could compromise the availability, integrity, and confidentiality** of the organization's valuable digital assets.



Scope the entire environment for digital assets and their associated attack surfaces. Considering the enormity of this task, it is recommended to do this in stages.

First, identify an initial manageable set of assets. There are two good candidates for a pilot program:

Internal attack surface

Find the most critical parts of your internal network that if compromised, give attackers access to your "crown jewels".

External attack surface

Internet-connected assets, which are typically protected by a large ecosystem of security tools and controls, are certainly not impervious to attack. Malicious actors are constantly scanning and probing to find cracks in network perimeters.

This initial scope should be accompanied with a plan of how it will expand as the program evolves and the IT environment changes and grows.

At a second stage, consider expanding the scope to additional sources of exposure:

Digital identity compromise. This includes exposure due to weak or leaked credentials, insufficient access controls, overly permissive accounts, and privilege escalation attacks.

SaaS tooling-which lends itself to easier internal communication about risks, as SaaS solutions tend to host critical data.

Integrating dark and deep web sources-identify potential threats to critical assets and provide contextual information on threat actors and their tactics.

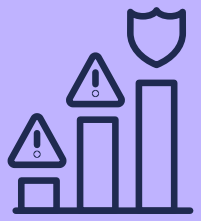
Finally, once you've defined the scope of assets and attack surfaces, you can begin the process of evaluating and addressing risk exposure within that scope.

A comprehensive discovery of exposures should start with high value assets identified in the scoping process.

It's important to remember that CTEM is an ongoing and agile process. By **continuously assessing and validating** exposures across the attack surface, organizations can keep up with constant changes to IT infrastructure. It also means that it becomes possible to assess the risk of digital assets in the face of a constantly evolving threat landscape.

Automation helps to drive this continuous process, which ensures that exposure management is both comprehensive and adaptive.

Pillar #2:



Vulnerability

Vulnerability Management has long been the cornerstone of many organizations' cybersecurity strategies, focusing on identifying and patching against known CVEs. However, with the growing complexity of the IT environment and the enhanced capabilities of threat actors, Vulnerability Management is becoming increasingly insufficient at maintaining the cybersecurity posture of the enterprise.

The ideal of being “patch-perfect” becomes a dangerous and misleading aspiration within a Vulnerability Management program. Security admins are constantly inundated with security patches that need to be applied, distracting them from their core responsibilities of protecting the IT environment.

2023 had 29,085 published CVEs of which only 2-7% of these are ever seen to be exploited in the wild.*

In a reality where not all CVEs (or even a majority of them) are ever going to get patched, the question that needs to be asked is: should all of them be patched?

*Source: Forum of Incident Response and Security Teams https://www.first.org/epss/model

Non-patchable Vulnerabilities

Under the CTEM framework, vulnerabilities extend to non-patchable vulnerabilities as they also contribute to risk exposure. Gartner predicts that by 2026, non-patchable attack surfaces will grow to include more than half of the enterprise. They include vulnerabilities such as:

Stolen and exposed credentials

Active Directory issues

Identity and access management issues

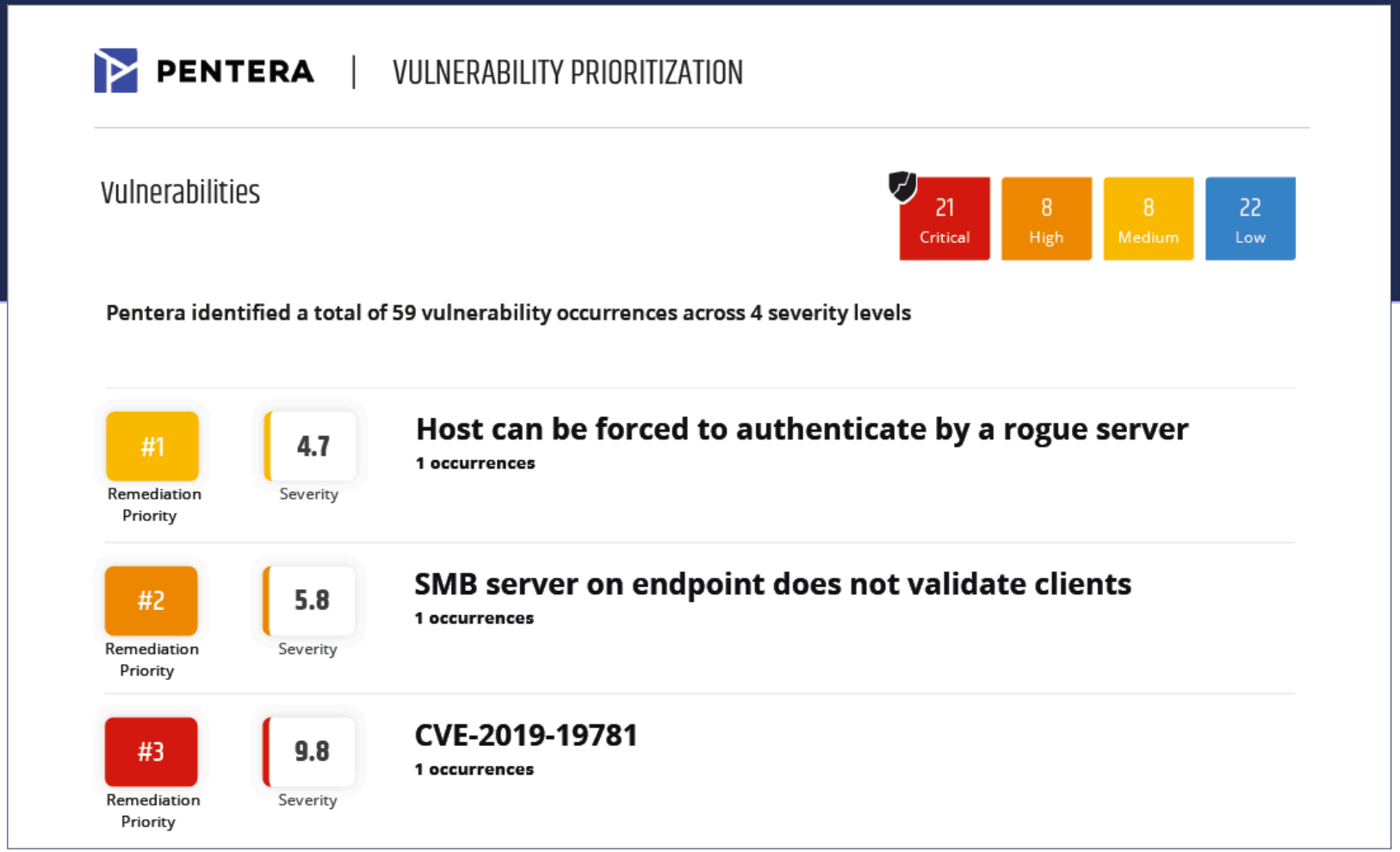
Poorly designed network architecture

Misconfigurations

Unsupported, legacy third-party software

CTEM shifts the focus to prioritize exposures based on their exploitability and the risk impact on critical assets.

Conventional Vulnerability Management methods for prioritizing exposures are based on CVSS scores, chronology, or vendor scoring and cannot keep up with the growth of the non-patchable attack surface. In contrast, CTEM ensures that the most sensitive digital assets to the organization's continuity and objectives are addressed first.



Pillar #3:

Validation

Validation transitions CTEM from theory to proven strategy

While CTEM widens the scope of discovery and prioritization under the Attack Surface and Vulnerability pillars, it's the incorporation of Validation that transforms the value of CTEM from a theoretical data-generating exercise into a focused, actionable strategy.

IT security teams need to validate that any proposed security measures will work to effectively block security gaps, building confidence that they are not only identifying and prioritizing risks but can show proof of how they are effectively mitigating them.

To ensure the ongoing efficacy of security controls, the validation must meet three critical criteria:

1. Continuous and based on automation, to drive efficiency with minimal effort.
2. Covering the full attack surface, and able to map the entire sequence of an attack path.
3. Providing hard evidence of exposure by emulating attacker methods and full attack kill-chains.

Top Priority

There are four strategies for testing your environment like an attacker, each mirroring the techniques employed by adversaries:

Think in Graphs

Attackers think in graphs, mapping out the relationships and pathways between various components of the network.

Validate Real Attack Paths

Attackers do not focus on isolated vulnerabilities; they consider the entire attack path, from initial access to exploited impact.

Automate Tests

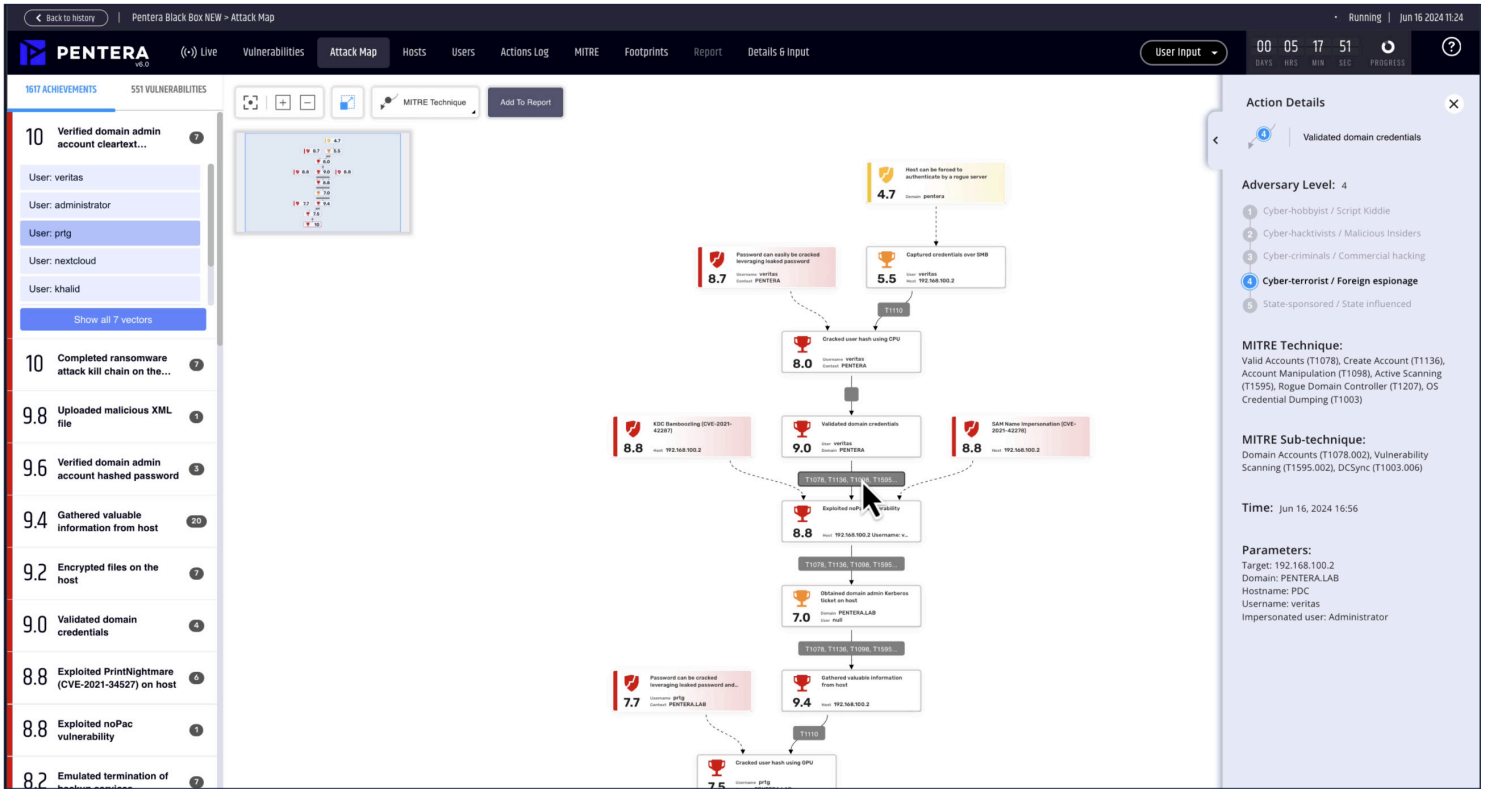
Attackers leverage automation to execute attacks swiftly, efficiently and at scale, giving them the advantage of speed, sophistication and volume.

Test Continuously

Attackers work in short iterative cycles to find security gaps, this gives them a continuous 'pulse' of the network.

Accelerate your Exposure Validation Strategy with Pentera

Pentera is uniquely positioned to support the validation pillar of your CTEM strategy by supporting you to take an adversary mindset to cybersecurity. Pentera allows you to safely attack your own live environments, mimicking the way a potential attacker would see your IT assets and search for weaknesses. It then displays the full attack chain, showing how attackers would be able to initially breach your network, and move laterally across it.

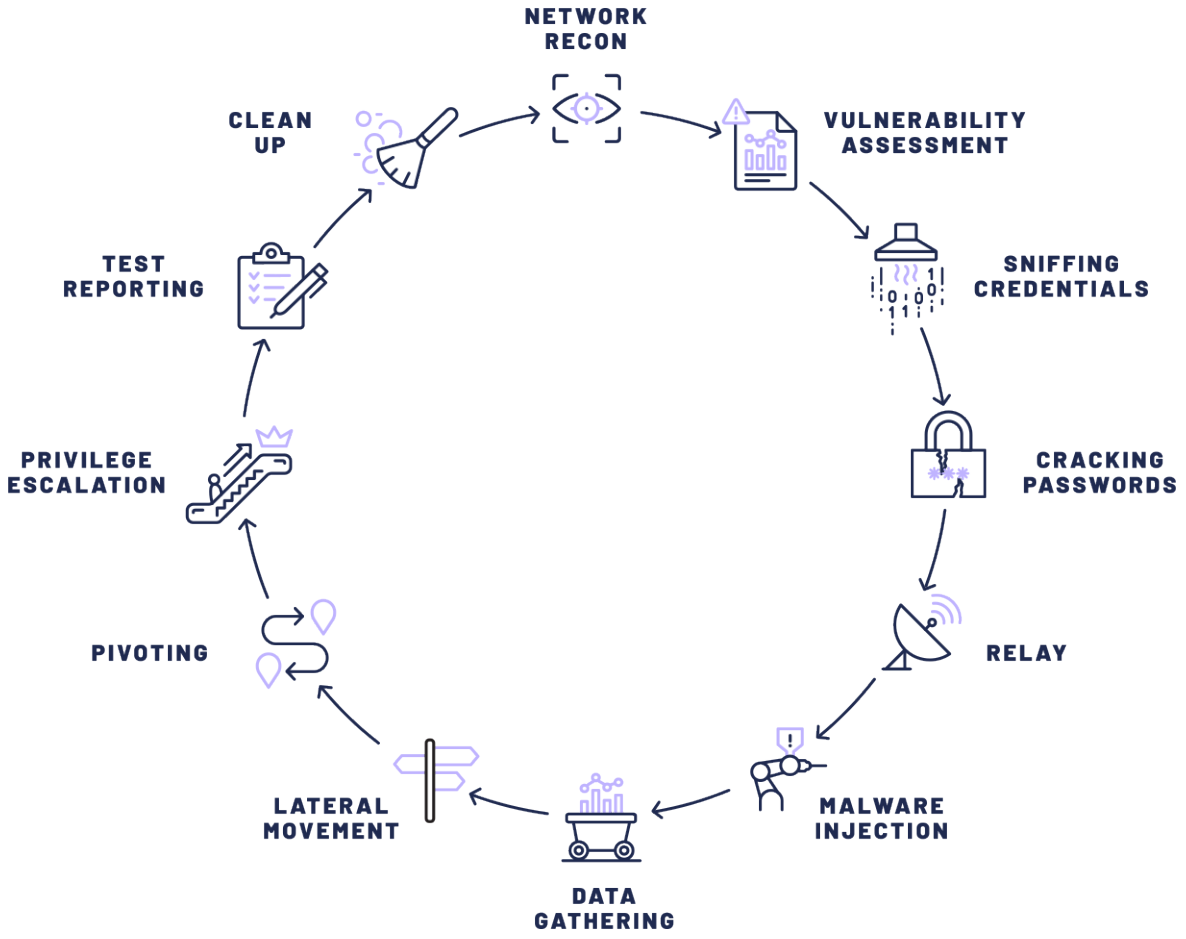


Pentera gives you this visibility across all network environments, for example across on-prem to cloud and vice versa. This is graphically mapped to root vulnerabilities that, if mitigated, mitigate the entire attack path.

Exploits Used in Pentera's Attack Kill Chain

To attempt a complete attack kill chain, Pentera reverse engineers highly stealthy and evasive malware to create benign versions. Pentera safely attempts a wide range of exploits, from remote code execution to privilege escalation and data exfiltration.

In this process of stress-testing the environment, the platform tests the effectiveness of defensive security controls deployed in the environment, such as XDRs, EPPs, Firewalls, and WAFs. Results from these tests give security teams a clear understanding of how their defense systems stand up against modern attacks.



With Pentera, you can perform continuous security validation tests as frequently as needed - monthly, weekly, or even daily. Addressing gaps as they are identified, security teams can confirm that applied fixes have effectively eliminated exposures and account for continual change.

Without leaving anything to chance, prioritizing validation closes the loop in your exposure management strategy, allowing you to assess the success that remediations are working as intended.

3 Key Steps Towards CTEM Implementation

With all the different elements of people, processes, and tools in a CTEM strategy, it's easy to get overwhelmed. It's helpful to keep a few things in mind:

1 You're not starting from scratch. You already have your asset management and your vulnerability management systems in place, the focus here is to simply extend their scope. Make sure your tools are comprehensively covering your IT environment's entire attack surface and they are continually updated with the pace of change.

2 Consider this a process of continual refinement. Implementing the CTEM framework becomes an agile cycle of discovery, mitigation, and validation. The job is never truly done. As your enterprise grows and matures, so does your IT infrastructure. It therefore needs a process that keeps it adaptive to of constant change.

3 Put validation at the center of your CTEM strategy. This gives you the confidence to know that your security operations will stand up when put to the test. At any point in time, you should know where you stand. Perhaps everything checks out, which is great. Alternatively, a gap might be identified, but now you can fill that gap, fully aware of what the downstream impact will be.

ABOUT PENTERA

Pentera is the global leader in Automated Security Validation, trusted by cybersecurity professionals in over 1000 organizations and service providers across more than 60 countries. Pentera's platform empowers organizations to proactively test their complete attack surface against the latest cyber attacks and guides remediation priorities based on true and proven risk. Pentera provides the centerpiece of Continuous Threat Exposure Management (CTEM) operations at any scale. With Pentera, enterprises can effectively identify and reduce security exposure and improve their security teams' efficiency.

For more info, visit: pentera.io

PENTERA