

WHY CTEM MATTERS:

Moving Beyond Finding Vulnerabilities to Understanding Exposure

Modern security teams face an ever-growing list of vulnerabilities. But not every vulnerability presents the same level of risk. We explore Continuous Threat Exposure Management, how it differs from traditional vulnerability management, and how penetration testing can help validate real-world exposure and attack paths.

A CUSTOMER FOCUSED APPROACH TO PENTESTING

Whether it's a one off or 300 tests a year, you, the customer, are at the heart of our approach to pentesting. iSTORM® offer a fully managed service, real time reporting and a dedicated team of specialist testers so you can focus on the day job.

OUR MISSION IS SIMPLE

To combine the best possible customer experience, with market leading delivery for every client, every time.

Overview

Cyber security is no longer about finding vulnerabilities and fixing them when you have time.

In today's cyber landscape, companies face ever-evolving attack methods and vulnerabilities, and the challenges are becoming increasingly sophisticated. Cyber security teams have also never had more visibility into their vulnerabilities, yet there is still a problem:

**Finding vulnerabilities isn't the issue anymore.
Identifying the vulnerabilities that matter is.**

A vulnerability on its own doesn't necessarily tell you how likely an attack is, whether an attacker can actually reach it, what systems it could lead to, or what the potential business impact could be.

This is where Continuous Threat Exposure Management (CTEM) changes the conversation. Rather than simply asking "What vulnerabilities do we have?", CTEM asks a much more valuable question: "Which exposures could realistically lead to a business-impacting incident, and what should we address first?"

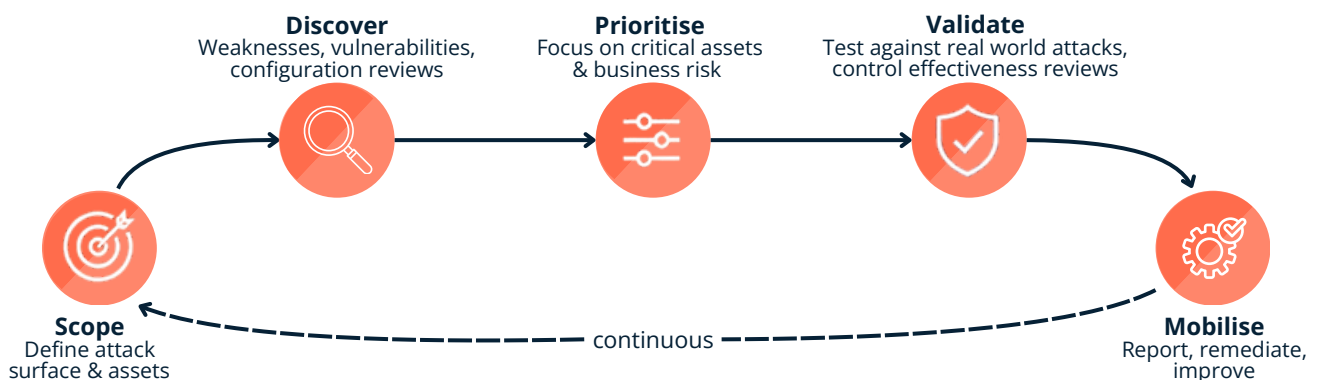
What is CTEM?

CTEM is a structured framework designed to reduce an organisation's cyber security exposure*.

This is done by:

- 🔍 Continuously identifying vulnerabilities and attack paths
- 🔍 Prioritising risks based on their potential impact on critical assets
- 🔍 Validating security measures to ensure effectiveness
- 🔍 Systematically remediating threats in a coordinated and iterative manner

CTEM Model



The five stages of a CTEM approach

Rather than treating security testing as a series of isolated activities, CTEM creates a continuous cycle of understanding what matters, finding exposures, determining which ones present the greatest risk, validating those risks and then taking action.

The result is a shift from simply producing a list of vulnerabilities to actively reducing the attack paths and exposures that matter most to the organisation.

The CTEM model consists of five stages:

1. Scoping: Understanding what matters

The first stage of the CTEM approach is scoping:

- 🌀 Identifying critical assets and their importance to the business.
- 🌀 Understanding the organisation's attack surface, including on-premises, cloud, and hybrid environments.
- 🌀 Defining key objectives and metrics for success.*

3. Prioritisation: Identifying what matters

This stage is where CTEM moves beyond traditional vulnerability management. Instead of prioritising vulnerabilities based solely on severity ratings, additional factors are considered. This stage focuses on:

- 🌀 Ranking risks based on factors such as exploitability, business impact, and existing security controls.
- 🌀 Using a threat-centric approach to address the most critical vulnerabilities first.*

5. Mobilisation: Turning insight into action

Mobilisation is about turning security findings into action by assigning ownership, coordinating remediation and tracking progress. This includes:

- Addressing prioritised threats.
- Implementing patches, configuration updates, or new security controls.
- Monitoring improvements to ensure continuous progress.

2. Discovery: Finding the exposures

Organisations next need to understand exposure. This could include misconfigurations, exposed services, weak authentication, and attack paths between systems. This phase consists of:

- 🌀 Conducting asset inventories.
- 🌀 Performing vulnerability assessments.
- 🌀 Identifying misconfigurations and identity risks.
- 🌀 Mapping potential attack paths*.

4. Validation: Proving the risk

Validation helps determine whether identified weaknesses represent a genuine and exploitable threat and ensures that security controls can target them effectively.

This stage includes:

- 🌀 Simulating attacks through red teaming or penetration testing.
- 🌀 Testing response plans and mitigation strategies.
- 🌀 Verifying the effectiveness of implemented controls.*

The objective isn't simply to close tickets. It's to reduce exposure.

*Reference: <https://ctem.org/>

Why finding vulnerabilities isn't enough

Traditional vulnerability management remains an important part of a strong cyber security programme. It helps organisations identify known software vulnerabilities, manage patching and maintain visibility across their technology estate.

But technical severity isn't the same as business risk.

Consider two vulnerabilities:

- 🌀 A critical vulnerability exists on a system that isn't externally accessible, is heavily isolated and has strong compensating controls.
- 🌀 A lower-severity vulnerability exists on an internet-facing system that provides a potential route towards sensitive information or a critical business application.

Which one represents the greater risk?

The answer isn't necessarily the vulnerability with the highest CVSS score. CTEM looks beyond the individual vulnerability and considers factors such as exploitability, reachability, business criticality, attack paths and existing security controls. This means organisations can focus on the exposures most likely to result in a meaningful security incident.

CTEM vs traditional vulnerability management

CTEM isn't designed to replace vulnerability management.

Vulnerability management remains a fundamental component of cyber security. The difference is the objective and outcome. Traditional vulnerability management identifies risks and manages vulnerabilities, while CTEM takes a broader approach and considers the real, actionable risk, rather than just the CVSS score.

Where penetration testing fits into CTEM

Penetration testing is about understanding security from an attacker's perspective. That makes it a natural component of a CTEM approach.

Penetration testing validates whether specific vulnerabilities or attacks are genuinely exploitable within your environment. CTEM ensures that exposure management is continuous between testing engagements.

At iSTORM, this is an important part of how we approach security testing: not simply identifying weaknesses but helping organisations understand their significance and mitigate risks.

iSTORM's approach

CTEM is a programme, not simply another security tool.

It brings together discovery, prioritisation, validation and remediation to create a continuous approach to reducing exposure.

At iSTORM, our CREST-accredited penetration testing services can help organisations understand how vulnerabilities translate into genuine attack paths and business risk. Our approach focuses on scenario-based testing to understand current external attack surfaces, validate vulnerabilities and strengthen security controls.

We believe cyber security should be practical, proportionate and focused on the risks that matter to your organisation.

Want to understand where your organisation is exposed?

iSTORM can help you assess, validate and prioritise your security risks through CREST-accredited penetration testing and expert security consultancy.

Talk to the iSTORM team to find out how we can support your CTEM journey.

Contact us directly:

info@istormsolutions.co.uk or call +44 (0) 1789 608708



iSTORM Privacy. Security. Pentesting