SAFEHILL

Tying CTEM Together

The Whole Is Greater Than The Sum of The Parts

Tying CTEM Together

The Whole Is Greater Than The Sum of The Parts

Executive Summary

Continuous Threat Exposure Management (CTEM) has emerged as one of the most important cybersecurity frameworks for organizations that want to move from reactive defense to proactive resilience. But while many vendors promise “one-size-fits-all” CTEM solutions, the reality is that no single tool can provide the full breadth of capabilities needed to identify, validate, and prioritize cyber risk across today’s complex environments.

A truly mature CTEM program requires a mix of human-led cyber risk services and continuous red teaming solutions—all unified under a Threat Exposure Management (TEM) platform that centralizes visibility, validates findings, and drives prioritized remediation.

This paper argues that SafeHill’s model—combining expert-led penetration testing and adversary simulation with continuous offensive security tooling and a TEM platform—delivers exactly that.

Capoeira: a Martial Arts Analogy

In the old style of cybersecurity, defending an organization was like playing a game of chess—cerebral, deliberate, and measured. Security teams planned moves in advance, executed methodical defenses, and relied on periodic assessments to anticipate threats. Today, the landscape has shifted; the pace and unpredictability of attacks demand something far more fluid. Modern cybersecurity, as embodied by SafeHill’s approach, is closer to champion capoeira—a dance of real-time engagement, where defenders blend instinct, agility, and innate wisdom with lightning-fast reflexes. It’s not about waiting for the opponent to make a move, but about moving continuously with them, adapting mid-step, and turning every attack into an opportunity to strike back in perfect rhythm.

It is a given that all elements must be coordinated and harmonized together, but getting closer to real-time, more integrated and especially in an AI-enabled world that is assisting the attackers, this new way of thinking about cyber conflict has to be brought to the table and is at the heart of doing CTEM right as we see it at SafeHill.

Why a One-Size-Fits-All CTEM Approach Falls Short

Many organizations start their CTEM journey with a single product or scanning tool, expecting it to uncover and manage all exposures. This approach inevitably fails to capture the depth and nuance of the threat landscape because:

- Automated tools often miss complex, chained vulnerabilities that only human researchers detect.
- Point-in-time assessments quickly become outdated as environments evolve.
- Many tools operate in silos, making it difficult to prioritize and correlate risks across domains.

The Gartner CTEM framework stresses that an effective program must continuously perform discov- ery, validation, and prioritization of exposures—something that is best achieved through a hybrid approach.

The Core Components of a Mature CTEM Program

1. Cyber Risk Services (Human-Driven)

Human-led engagements uncover, validate, and contextualize threats in ways automated tooling cannot. These include:

- Penetration Testing (Network, Application, Cloud, Physical)
- Red Team & Purple Team Exercises
- Social Engineering & Deepfake-Enabled Phishing Campaigns
- Tabletop Exercises & Incident Simulation
- Threat Intelligence Research

These services form the foundation for real-world attack path validation—the most critical step in moving from “potential risk” to “proven, exploitable risk.”

2. Red Teaming Solutions (Continuous & Automated)

Continuous offensive security tooling provides breadth and scalability, ensuring that the CTEM loop never stops. Examples include:

- Continuous Penetration Testing Platforms
- Breach & Attack Simulation (e.g., PICUS)
- SaaS & Third-Party Risk Assessments
- External Attack Surface Management (EASM)
- Threat Intelligence Gathering

These solutions extend visibility into external code repositories (GitHub, Bitbucket), social media exposures, cloud misconfigurations, and vulnerable third-party integrations—key sources of expo- sure identified in Gartner’s CTEM guidance.

3. A Central TEM Platform (SafeHill)

The TEM platform is the cornerstone—the unifying element that makes a CTEM program mature. SafeHill's TEM capabilities enable:

- Aggregation of human-led assessment results and automated tool outputs into one dashboard
- Continuous discovery, validation, and risk scoring
- Vulnerability-to-compliance mapping (CMMC, PCI-DSS, HIPAA, ISO 27001, etc.)
- Prioritization of remediation based on business risk, exploitability, and compliance impact
- Future integration with best-in-class third-party solutions (e.g., Obsidian Security, PICUS) for a holistic data set

Why This Mix Matters — Business Rationale

Our consulting approach uses CTEM as a business-aligned framework to ensure that every asset is tested, validated, and prioritized for remediation.

The combination works like this:

1. Cyber risk services get us in the door—identifying high-value attack paths through human-led testing.
2. Red teaming solutions maintain ongoing visibility and breadth of coverage.
3. SafeHill TEM platform aggregates all this intelligence, validates it, and translates it into prioritized remediation plans.
4. Upsell & integration potential—after proving value through services, we expand the engagement by reselling integrated tools and offering SafeHill as the single source of truth for CTEM data.

SafeHill's differentiator: human-validated exposures—ensuring that remediation work is focused on the issues that matter most. Returning to the capoeira analogy, we have to bring it together in a way that is smooth, continuous, integrated and improving. As with any martial art, cyber combat has to learn to fight in defense against an opponent who is determined, graceful and effective in offense.

The Future of CTEM with SafeHill

While SafeHill focuses on its core strengths—EASM, continuous pentesting, threat intelligence gath- ering, vulnerability-to-compliance mapping, and remediation prioritization—our platform is designed for integration. This means customers can plug in best-of-breed products like Obsidian Security or PICUS and still manage everything in one validated, prioritized, business-relevant view.

This is not about doing everything ourselves—it's about delivering the most valuable, validated, and actionable CTEM outcomes possible.

Conclusion

A mature CTEM program is not a single tool, and it's not a single service. It is a living, continuous mix that blends human insight with automation at scale—and brings it all together under a single platform for visibility, validation, and prioritization. This is what you and your team need.

SafeHill enables this maturity by:

- Delivering human-led cyber risk services for real-world validation
- Leveraging continuous offensive security tooling for full-scope discovery
- Centralizing results in a TEM platform that unifies, prioritizes, and drives remediation

In short: If CTEM is the strategy, SafeHill is the operational hub that makes it work, and you are the fighter ready to beat any hostile that comes your way.

About Safehill

Safehill is a cybersecurity startup focused on continuous penetration testing, contextual threat exposure management, and AI-enhanced hybrid service delivery. Leveraging the MITRE ATT&CK framework in innovative ways, Safehill enables organizations to illuminate real attack paths and proactively defend against modern threats.

Learn more at: www.safehill.com