



cyber futurists

Continuous Threat Exposure Management (CTEM) Market in Europe






Continuous Threat Exposure Management (CTEM) Market in Europe

1. Introduction: The Business Case for CTEM

Geopolitics, digital sovereignty, and supply chain fragility have all converged to make cybersecurity a boardroom issue in Europe. The EU's push for greater autonomy, both economically and digitally, isn't just about technology independence. It's about resilience. And that includes resilience against increasingly sophisticated and persistent cyber threats.

As part of this broader agenda, Continuous Threat Exposure Management (CTEM) is gaining traction. The logic is simple: if your attack surface is constantly changing, your defense posture can't be static. While CTEM is another new acronym, it reflects an actual shift toward operationalizing continuous risk reduction, aligning security strategy with critical infrastructure protection, compliance mandates, and the EU's digital agenda.

As the European Union pushes for greater digital autonomy and "Made in Europe" solutions, there is an emerging imperative to cultivate a robust, independent CTEM ecosystem. This push aligns cybersecurity innovation with broader macroeconomic and geopolitical objectives, including strengthening critical infrastructure and reducing reliance on non-European vendors.



1.1 The Growing Need for CTEM

Hybrid cloud, remote work, shadow IT, and thousands of unsecured IoT devices have created an attack surface that defies traditional mapping.

Add to that the growing sophistication of attackers, some of them nation-state backed, many of them now using AI and automation, and the problem becomes clear: periodic security checks and once-a-quarter vulnerability scans are no longer enough to keep pace with dynamic threats. CTEM poses the question, "What is currently exploitable, by whom, and to what extent?"

This shift is being accelerated by four forces:

- AI-powered adversaries: Attackers now automate reconnaissance and exploit chaining at scale.
- Expanding compliance demands: NIS2, DORA, and GDPR don't just require you to be secure—they expect you to prove it continuously.
- Economic efficiency pressures: CTEM promises smarter prioritization and faster remediation; CISOs must do more with less.
- Geopolitical tensions and digital sovereignty goals: Governments and enterprises are under pressure to reduce reliance on foreign technology stacks and to build sovereign cybersecurity capabilities. CTEM aligns with this goal by reinforcing operational control and autonomy.

Of course, this assumes CTEM tools are integrated, data is normalized, and teams have the resources to act. However, this is not always fully the case. Adoption is still uneven, and implementation maturity varies widely across sectors. But the direction of travel is clear: exposure management is moving from project to process, from periodic to continuous.






1.2 Regulatory & Compliance Drivers in Europe

Europe has some of the world's most stringent cybersecurity regulations, compelling organizations to implement proactive security measures. The introduction of the General Data Protection Regulation (GDPR) has already mandated organizations to safeguard sensitive data, with severe penalties for non-compliance.

- NIS2 extends cybersecurity mandates beyond traditional critical infrastructure to include digital services, cloud providers, and managed service providers.
- DORA focuses on financial entities, mandating comprehensive ICT risk frameworks, testing, and incident reporting.

These regulatory frameworks emphasize the need for continuous security assessment and risk-based prioritization, aligning closely with the principles of CTEM. Organizations that fail to implement continuous exposure management risk regulatory fines and expose themselves to operational disruptions, reputational damage, and financial losses due to cyberattacks.

All of these regulations share a theme: static defenses won't cut it. Regulators are pushing for continuous risk assessment, evidence-based controls, and more transparency in how threats are managed. That plays directly into CTEM's core promise.



1.3 The Shift to Continuous Security Monitoring

Traditional security approaches such as annual penetration testing and periodic vulnerability scanning provide only a snapshot of an organization's risk posture at a given moment. However, modern threats evolve rapidly, rendering point-in-time assessments ineffective.

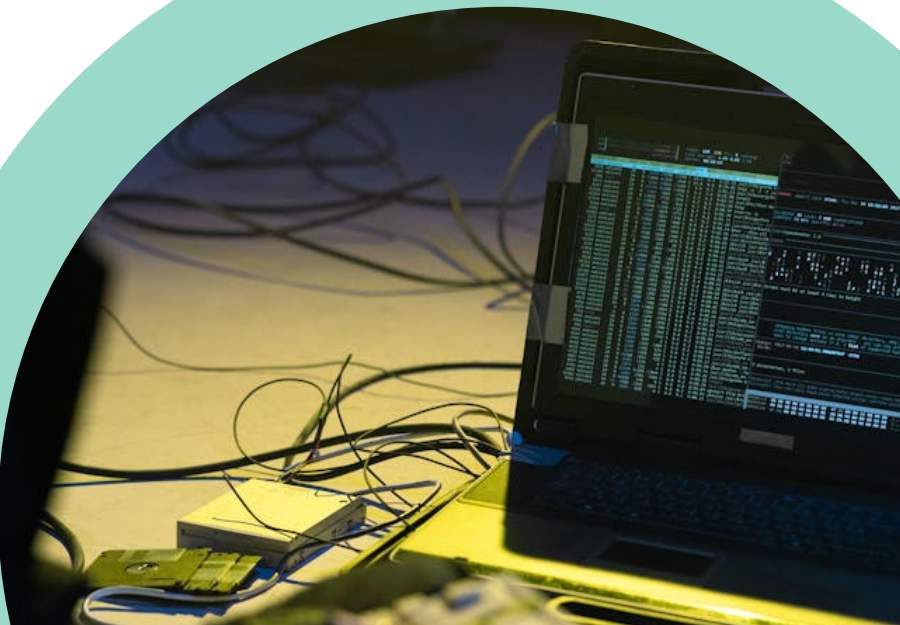
Continuous Threat Exposure Management (CTEM) represents a shift in security operations, emphasizing real-time threat detection, contextual risk analysis, and automated remediation. CTEM reflects a necessary evolution: from point-in-time testing to real-time posture management.

Increasingly CTEM leverages AI and automation to provide real-time visibility into security exposures. The theory is that by continuously monitoring and analyzing their attack surfaces, organizations can identify security weaknesses before they are exploited, enabling proactive mitigation strategies. Additionally, CTEM integrates seamlessly with Security Information and Event Management (SIEM) systems, Security Orchestration, Automation, and Response (SOAR) platforms, and Extended Detection and Response (XDR) solutions, enabling a holistic approach to cybersecurity.

It combines:

- Continuous asset discovery across hybrid environments
- Threat-informed risk prioritization, not just CVSS scores
- Validation through BAS, red teaming, and attack simulation
- Automation and orchestration to scale remediation
- Feedback loops and machine learning to adapt as threats evolve

CTEM is no silver bullet. Nothing ever is. But it's the current best practice for security teams to keep up with dynamic threats.





2. What Makes a Good CTEM Program?

2.1 CTEM is a Capability Set, not a Category

One of the biggest misconceptions about CTEM is that it's a product. It's not. No single vendor currently offers a complete, turnkey CTEM solution. Instead, CTEM is stitched together from a combination of capabilities, discovery, prioritization, validation, automation, across multiple tools.

Most organizations implementing CTEM today are integrating:

- External Attack Surface Management (EASM) for asset discovery
- Vulnerability and risk-based prioritization tools
- Breach and attack simulation (BAS) or red teaming for validation
- SOAR and ITSM tools for orchestration and ticketing
- Threat intel feeds and asset inventory platforms for context

This composability is both a strength and a weakness. It gives buyers flexibility, but it also places a high integration burden on security teams and requires careful architecture planning.

2.2 Core Components of CTEM Program

A robust CTEM program requires a systematic approach that integrates security insights, automation, and contextual intelligence. Unlike traditional vulnerability management, CTEM is an iterative and dynamic process that continuously assesses, validates, and mitigates threats in real time. The framework consists of key components that work together to reduce risk exposure and strengthen cyber resilience.

The table below outlines the five fundamental components of an effective CTEM program. Together, these elements create a comprehensive lifecycle that ensures organizations can continuously identify, assess, and remediate threats in a cohesive and strategic manner. and their respective functions:

Component	Function
Discovery	Ongoing asset discovery across cloud, hybrid, and on-prem. Finds shadow IT, misconfigurations, and unmanaged assets.
Prioritization	Context-aware risk scoring using business impact, exploitability, threat intel, and attack path analysis.
Validation	Simulates attacks using BAS, red teaming, and adversary emulation. Confirms whether issues are exploitable in practice.
Mobilization	Triggers action. Uses Security Automation, SOAR, SIEM, and EDR workflows to automate response—patching, segmentation, or isolation.
Continuous Improvement	Learns from outcomes. Refines detection logic and prioritization models using feedback loops and ML.

Each of these components contributes to a more proactive security strategy that enables organizations to detect and mitigate threats before they escalate into incidents.





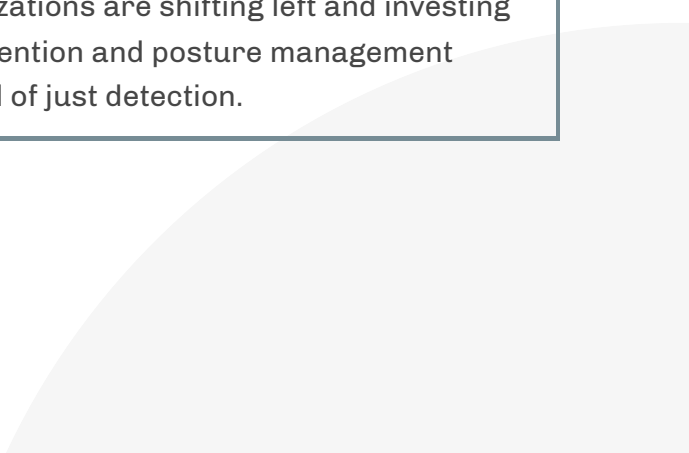
3. European Businesses and CTEM Adoption

3.1 CTEM Adoption Trends in Europe

European businesses are increasingly recognizing the value of Continuous Threat Exposure Management (CTEM). Organizations across multiple industries are adopting CTEM practices to mitigate risk, optimize security investment, and comply with evolving regulatory requirements.

The following key trends illustrate the adoption of CTEM in Europe:

Trend	Description
Large Enterprises Leading	Multinational firms are adopting CTEM first due to regulatory pressure and complex attack surfaces.
Mid-Market Catching Up	Cloud-native CTEM tools are lowering barriers for mid-sized firms to participate.
Regulated Sectors First	Finance, healthcare, and energy sectors are early adopters due to NIS2 and DORA requirements.
Cyber Insurance Pressures	Insurers increasingly demand proof of proactive security practices, driving interest in CTEM.
From Reactive to Proactive	Organizations are shifting left and investing in prevention and posture management instead of just detection.



3.2 Adoption Challenges for European Organizations

Of course, no transformation is frictionless. While the benefits of CTEM are clear, European organizations face several hurdles when adopting CTEM:

Challenge	Impact on CTEM Adoption
Budget Constraints	Security teams struggle to justify the cost of continuous exposure management solutions compared to traditional vulnerability management.
Fragmentation in Security Tools	Many organizations use disparate security tools that lack integration, making it difficult to implement a seamless CTEM workflow.
Lack of Skilled Personnel	CTEM requires expertise in attack path modeling, automation, and risk-based prioritization, which many organizations lack.
Difficulty in Mapping Threats to Business Risk	Many organizations lack clear frameworks for translating security exposures into measurable business risk.





3.3 European Buyers, Non-European Stack

Despite calls for “Made in Europe” digital infrastructure, most of the CTEM stack is still dominated by U.S. and Israeli vendors. From asset discovery to BAS to prioritization engines, the majority of innovation and market traction lies outside the EU.


This presents a strategic tension. European enterprises are under pressure to reduce reliance on foreign technology vendors, especially in sensitive sectors, but often find limited mature alternatives domestically.

Unless European security vendors begin to consolidate CTEM functionality across the lifecycle, expect ongoing reliance on foreign tooling, albeit increasingly deployed within sovereign cloud environments or managed by local MSSPs.

3.4 The Role of MSSPs and Security Consultancies

Given the complexity of CTEM adoption, many European businesses are turning to Managed Security Service Providers (MSSPs) and security consultancies for implementation support. MSSPs offer managed CTEM services, enabling organizations to leverage expert-driven continuous exposure management without requiring large internal security teams. Consulting firms, on the other hand, provide CTEM maturity assessments, strategic guidance, and integration support to help organizations build in-house CTEM capabilities.

As CTEM adoption continues to grow, the role of MSSPs and consultancies will be critical in helping European businesses navigate implementation challenges and establish effective, scalable exposure management programs.



4. The European CTEM Ecosystem and Landscape


4.1 Key Market Trends in the European CTEM Landscape

The adoption of CTEM in Europe is influenced by multiple factors, including increased cyber threats, regulatory mandates, and the need for improved risk management. These drivers are interrelated: regulatory pressure fuels investment in proactive technologies, while heightened threat awareness accelerates the adoption of advanced exposure management solutions. Together, they create a reinforcing cycle that makes CTEM an operational and strategic necessity.


Adding to this momentum are recent geopolitical pressures, such as the war in Ukraine, global tensions around technology supply chains, and increased cyber activity from state-linked actors, which have underscored the strategic importance of cybersecurity sovereignty. As a result, the EU is placing stronger emphasis on homegrown cybersecurity solutions to reduce dependence on foreign technologies and strengthen digital autonomy. This is driving public-private initiatives, funding programs, and strategic procurement aligned with European CTEM vendors.

The following table highlights key market trends that are shaping the European CTEM landscape:, including increased cyber threats, regulatory mandates, and the need for improved risk management. These drivers are interrelated: regulatory pressure fuels investment in proactive technologies, while heightened threat awareness accelerates the adoption of advanced exposure management solutions. Together, they create a reinforcing cycle that makes CTEM an operational and strategic necessity. The following table highlights key market trends that are shaping the European CTEM landscape:





Trend	Impact on CTEM Adoption
Regulatory Pressure Driving Proactive Security	Compliance requirements such as NIS2 and DORA are pushing organizations to implement continuous risk assessment and remediation strategies.
Rise of AI-Powered Exposure Management	AI-driven analytics and automation are transforming CTEM capabilities, allowing for faster risk detection and response.
Cybersecurity Consolidation & M&A Activity	European cybersecurity firms are increasingly being acquired or merged, consolidating CTEM capabilities into broader security platforms.
Growth of Managed Security Services (MSSP)	Organizations lacking in-house expertise are turning to MSSPs to manage CTEM and security exposure strategies.
Emergence of Local Cybersecurity Startups	Startups specializing in attack surface management, breach attack simulation, and automated remediation are gaining traction.
Geopolitical and Digital Sovereignty Pressures	EU policies and recent conflicts are accelerating demand for European cybersecurity sovereignty and locally headquartered CTEM providers.



4.2 Regional Differences in CTEM Adoption

CTEM adoption varies across different regions in Europe due to differences in regulatory emphasis, industry focus, and cybersecurity maturity. Below is a regional comparison of CTEM adoption:

Region	Characteristics of CTEM Adoption
Western Europe (Germany, UK, France, Netherlands)	Strong regulatory frameworks, advanced cybersecurity infrastructure, high adoption of automated threat exposure management solutions.
Nordics (Sweden, Finland, Denmark, Norway)	High focus on innovation, early adopters of AI-driven CTEM solutions, collaboration with public-private cybersecurity initiatives.
Southern Europe (Spain, Italy, Portugal, Greece)	Growing CTEM adoption driven by increased cyber incidents, reliance on MSSPs due to skill shortages.
Eastern Europe (Poland, Czech Republic, Hungary, Romania)	Emerging CTEM market, rapid digital transformation, increasing focus on cybersecurity resilience, growing number of local cybersecurity vendors.



4.3 Key Players in the European CTEM Market

Continuous Threat Exposure Management (CTEM) – a proactive, continuous program for uncovering and reducing cyber risk – was coined by Gartner in 2022 as an evolution beyond traditional vulnerability management. Several Europe-headquartered security vendors specialize in CTEM, offering platforms and services to continuously assess exposures. Below are key companies, their CTEM offerings, differentiators, and notable recognition:

BreachLock (Netherlands)

breachlock.com

- Offerings: Unified CTEM & Pen-Testing-as-a-Service platform covering external attack-surface discovery, automated & manual pentesting, dark-web monitoring and continuous retesting—all delivered through a single portal.
- Differentiators: “See-External-Threats” (SET) spin-up in <1 hour, evidence-backed findings, asset discovery plus DNS & API scanning, and automated ticketing workflows accelerate MTTR.
- Industry Recognition: Gold winner in the 2025 Cybersecurity Excellence Awards (CTEM category) and cited as a Sample Vendor in Gartner’s 2025 Emerging-Tech Impact Radar for Threat Exposure Management.
- Market Presence & Clients: Dual HQ in Amsterdam (BreachLock NL B.V.) and New York; serves 600+ enterprises across EU, US and APAC via global red-team operations.

CyberCyte (United Kingdom)

cybercyte.com

- Offerings: CyberCyte X-CTEM is an AI-driven risk- and threat-exposure-management platform that unifies vulnerability, mis-configuration, hardening and inventory data in a single SaaS/OEM console, mapping findings to compliance frameworks and automating diagnostics and one-click remediation across the full five CTEM stages.
- Differentiators: Integrated risk-prioritisation that correlates asset, threat and hardening data; automated Security-Control Assessment (ASCA) to spot control-drift; and generative-AI assistants that cut deployment and operational overhead.
- Industry Recognition: Public case-studies with a Tier-1 energy distributor, a global retailer and a multi-national bank validate the platform’s maturity in highly regulated environments.
- Market Presence & Clients: Head-quartered in Reading (UK) and registered since 2019, CyberCyte serves large energy, retail, finance and conglomerate clients across EMEA.

Edgescan (Ireland)

edgescan.com

- Offerings: CTEM platform combining validated DAST, Network, ASM and PTaaS. Validation & prioritisation via combination of cyber analytics, AI and human expertise. Conducts continuous vulnerability detection across web applications, networks, cloud workloads, and APIs, augmented by Penetration Testing as a Service (PTaaS). ASM used to discover assets and add to vulnerability lifecycle. AI Insights user to help prioritise and provide tactical advice.
- Differentiators: Hybrid model with automated scanners & cyber analytics plus a team of certified security experts (CREST, OSCP) who validate findings, reducing false positives and improving remediation accuracy. Cloud Integrations to keep pace with change in dynamic environments. ISO27001 & PCI ASV certified.
- Industry Recognition: Winner of SC Awards Europe's Best Vulnerability Management Solution; recognized for innovation in Computing Security Awards.
- Market Presence & Clients: Serves global enterprises across finance, media, SaaS, healthcare, and government. Provides continuous testing and real-time threat intelligence via AI to large multinational and medium organizations.

Hadrian (Netherlands)

hadrian.io

- Offerings: AI-driven offensive-security platform combining automated penetration testing, continuous attack-surface management and threat-exposure management with built-in remediation workflows.
- Differentiators: Agentless cloud deployment in minutes, AI-guided ethical-hacker techniques, business-context risk scoring and collaboration tools that cut red-team costs by 30 % and MTTR by 80 %.
- Industry Recognition: Leader in GigaOm's 2024 & 2025 Radar for Attack Surface Management and recipient of Frost & Sullivan's New-Product Innovation Award for EASM.
- Market Presence & Clients: Amsterdam HQ with offices in London and Paris; reference customers include London Business School, SHV Energy, Lottomatica and Crédit Agricole.



Intruder (United Kingdom)

intruder.io

- Offerings: Cloud-native exposure-management SaaS combining continuous external & internal vulnerability scanning, attack-surface discovery and automated alerting, tightly integrated with AWS, Azure and CI/CD pipelines.
- Differentiators: Change-triggered “scan-on-discover,” multi-scanner coverage, ML-driven exploitability scoring and automatic certificate/port/service drift detection keep noise low and context high.
- Industry Recognition: Selected for GCHQ’s Cyber Accelerator, listed on Deloitte UK Tech Fast 50 (2023) and boasts >3,000 paying customers worldwide.
- Market Presence & Clients: London-based Intruder Systems Ltd. (Reg. No. 09529593) focuses on SMB and mid-market organisations and is SOC 2 & ISO 27001 compliant.

Nanitor (Iceland/Europe)

nanitor.com

- Offerings: Natively built and authentic CTEM platform focused on security configuration auditing, vulnerability management, and patch remediation, offering real-time continuous visibility into misconfigurations and vulnerabilities.
- Differentiators: Strong focus on continuous improvement & fundamental cyber hygiene, offering a what-is-most-at-risk streamlined approach to CTEM at a lower cost compared to enterprise alternatives. Only 24 hrs to complete onboarding.
- Industry Recognition: Listed as an emerging CTEM alternative in Gartner Peer Insights; strong early adopter feedback.
- Market Presence & Clients: Primarily serving Europe, gaining traction among elite MSPs and MSSPs seeking scalable, automation-driven cybersecurity and growing interest from compliance-driven industries.

Nothreat (United Kingdom)

nothreat.io

- Offerings: Nothreat Platform (CTEM) delivers autonomous, self-learning AI defence that merges edge firewalling, deception (CyberEcho traps) and AI-driven analytics to protect web, IoT/OT and cloud assets in real time.
- Differentiators: <12-minute model-training to 97 % accuracy, adaptive neural networks that avoid catastrophic forgetting, and vendor-agnostic “one-line-config” integration with existing NGFW/WAF/SIEM/EDR stacks.
- Industry Recognition: Proprietary technology backed by peer-reviewed research (Springer) and protected by US & EU patents; valued at £40 M in its May 2025 Crowdcube round.
nothreat.io
- Market Presence & Clients: London HQ with deployments in telecom, infrastructure and elite sports; reference partners include Lenovo, ISD Dubai Sports City, Qarabağ FK and Pafos FC.

Orange Cyberdefense (France)

www.orangecyberdefense.com/global/offering/managed-services/continuous-threat-exposure-management

- Offerings: CTEM managed services, including continuous vulnerability scanning, configuration audits, threat intelligence integration, and validation via controlled attack simulations.
- Differentiators: Operates Europe's first private CERT with 140+ security experts monitoring global threats, integrating MSSP and incident response capabilities into CTEM services.
- Industry Recognition: A leading MSSP in Europe, frequently ranked among top global cybersecurity service providers.
- Market Presence & Clients: Global operations with a strong European base, providing CTEM services to large enterprises, critical infrastructure providers, and government agencies.

A decorative graphic at the bottom of the page featuring overlapping circles in dark blue, teal, and black. The word "Security" is visible in a blurred, glowing font within the black circle.

Outpost24 (Sweden)

outpost24.com

- Offerings: Outpost24 Exposure Management Platform, a unified CTEM solution providing continuous visibility across on-prem, cloud, and external attack surfaces. It consolidates asset inventory, automated vulnerability scanning, external attack surface management, and threat intelligence into one cloud-based platform.
- Differentiators: Covers all five CTEM phases as defined by Gartner, enabling organizations to continuously monitor and remediate what matters most. Prioritization goes beyond CVSS scores by factoring in exploitability and business impact, integrating automated red-team validation for critical exposures.
- Industry Recognition: Highlighted by Gartner as aligning with top security trends, recognized for its modular approach allowing tailored CTEM programs on a single platform.
- Market Presence & Clients: Large European footprint (Sweden, UK, Netherlands, Belgium, Denmark, France, Spain) with expansion into North America. Trusted by enterprises and MSSPs globally.

Patrowl (France)

patrowl.io

- Offerings: Patrowl CTEM is an all-in-one SaaS offering that blends external attack-surface discovery, continuous automated pentesting (CART + PTaaS) and risk-insight dashboards with ITSM-integrated remediation and retest automation.
- Differentiators: Zero-false-positive pledge, contextual EPSS-enhanced prioritisation, multi-tenant architecture and one-click PDF pentest reporting appeal to MSSPs and regulated sectors.
- Industry Recognition: Winner of the 2025 FIC Europe Grand Prix Start-up Award; multiple innovation prizes at CyberNight 2023 and Les Assises 2023/2024; FinTech of the Year 2024.
- Market Presence & Clients: Paris-based (6 Rue du Général de Larminat) with European banking, health-care and public-sector customers; supports DORA, NIS 2 and CyberScore programmes.

Picus Security

picussecurity.com

- Offerings: Picus Security Validation Platform is a modular SaaS/on-prem solution unifying breach-&-attack simulation, automated pen-testing and detection-rule validation to deliver CTEM-aligned visibility across on-prem, cloud and external attack surfaces.
- Differentiators: Daily-updated threat library with a 24-hour SLA and a mitigation library of 80 k+ vendor-specific signatures enable one-click fixes; the open platform correlates exploitability and control effectiveness across MITRE ATT&CK-mapped modules.
- Industry Recognition: Gartner Peer Insights™ 2024 Customers' Choice for BAS, CRN 2025 Five-Star Vendor, and positioned as a leader in Frost & Sullivan's 2022 BAS Radar.
- Market Presence & Clients: Serves ~500 customers through offices in Ankara, Delaware/Tampa, San Francisco, London and Singapore, with reference clients including Mastercard, VMware, Vodafone, Palo Alto Networks, Turkish Airlines and ING.

Quorum Cyber (United Kingdom)

quorumcyber.com

- Offerings: CTEM as a Service, integrated with Microsoft security tools. Uses Defender Threat Protection, Defender EASM, and custom threat intelligence to continuously scan and prioritize exposures.
- Differentiators: Microsoft-aligned security specialization, member of Microsoft Intelligent Security Association (MISA), offering deep integration with Microsoft security ecosystems.
- Industry Recognition: Finalist in Microsoft Security Excellence Awards for Security MSSP of the Year and Security Customer Champion.
- Market Presence & Clients: Strong footprint in the UK and EMEA, expanding into North America. Trusted by financial institutions, government bodies, and mid-market enterprises.



Razor Thorn Security (United Kingdom)

razorthorn.com

- Offerings: CTEM as a service, Layering of additional Pentesting options available such as Red Teaming, Continuous Penetration testing, Penetration Testing Deep Dive Credits.
- Differentiators: Human Operators and Penetration Testers validating results, API to integrate with SIEM, Jira or other services, No Crowdsourced testers, additional services layers on to as needed.
- Industry Recognition: Winner 2024 Cyber Security Excellence Awards, VC clients using Razor's Edge to protect their portfolio.
- Market Presence & Clients: Head Quartered in Royal Tunbridge Wells (Kent, UK) registered since 2007. Razorthorn serves all companies of all sizes across Europe and US.

Steadybit (Germany)

steadybit.com

- Offerings: SaaS/on-prem chaos- & resilience-engineering platform that automates failure injection across cloud-native and on-prem targets, providing the "Validation" phase many CTEM programmes lack.
- Differentiators: Drag-and-drop experiment builder, open-source Reliability Hub (200+ actions), RBAC safety-controls and API/CLI integration for CI/CD-driven continuous validation.
- Industry Recognition: Raised \$7.8 M Series-A; featured by SiliconANGLE as a leading chaos-engineering vendor; regular speaker at KubeCon EU, SREcon and Conf42 Chaos Engineering 2025.
- Market Presence & Clients: Hamburg-based Steadybit GmbH serves global e-commerce, fintech and SaaS firms, boasting logos across Europe, North America and MENA.

ThingsRecon (Netherlands)

thingsrecon.com

- Offerings: External Attack Surface Management (EASM) platform focused on continuous asset discovery, risk evaluation, and prioritized remediation recommendations.
- Differentiators: AI-powered attack surface monitoring with built-in expert advisory services for proactive exposure reduction.
- Market Presence: Emerging European startup specializing in digital risk reduction for enterprises and MSSPs.

XM Cyber (Europe/Israel)

xmcyber.com

- Offerings: CTEM platform that continuously identifies security exposures, maps attack paths with XM Cyber's Attack Graph Analysis), and prioritizes remediation efforts based on risk to critical assets.
- Differentiators: Acquired by Schwarz Group, Europe's largest retailer, enhancing resources and market reach. Focuses on continuous security posture improvement using adversary emulation.
- Market Presence: Offices in the UK, Germany, and France, Spain, Nordics, Poland, Americas and APAC serving enterprises across multiple verticals with a strong presence in regulated industries.

5. Future Outlook for the European CTEM Market

As European organizations continue to adapt to an evolving threat landscape, the role of CTEM will become increasingly integral to enterprise security strategies. The following factors will likely shape the future of CTEM in Europe:

- Increased Integration with Security Operations (SecOps): CTEM solutions will become more tightly embedded into broader SecOps workflows. Seamless interoperability with SIEM, SOAR, and XDR systems will enable real-time exposure detection, contextual correlation, and automated mitigation.
- Expansion of Automated Threat Modeling and AI-Powered Simulation: Organizations will rely more heavily on machine learning and AI to model attacker behavior and map likely attack paths. This will move CTEM from static exposure enumeration to dynamic, predictive analysis.
- Adoption of CTEM in Compliance-Driven Sectors: Financial services, healthcare, critical infrastructure, and government sectors will adopt CTEM more rapidly in response to tightening regulations and the need to maintain continuous compliance with frameworks such as NIS2, DORA, and GDPR.
- Maturation of European CTEM Ecosystem: The local vendor ecosystem will mature, with European firms gaining market share through specialization, regional compliance alignment, and geopolitical trust advantages. Public-private collaborations and national cybersecurity initiatives will boost innovation.



FUTURE?

- 
- **Operationalization of CTEM as a Service:** As organizations seek to reduce complexity, CTEM will increasingly be delivered as a managed service (CTEMaaS), especially for mid-sized and resource-constrained enterprises. MSSPs will standardize CTEM offerings into subscription-based models.
 - **Security as a Business Enabler:** CTEM adoption will support broader business objectives, enabling secure digital transformation, protecting customer trust, and reducing cyber insurance premiums. Boards and executive leadership will treat CTEM outcomes as strategic performance indicators.

In this dynamic environment, European organizations must move beyond static security postures and embrace CTEM as an operational discipline. By doing so, they can ensure continuous visibility across attack surfaces, focus on high-impact exposures, and maintain resilience in the face of evolving threats.

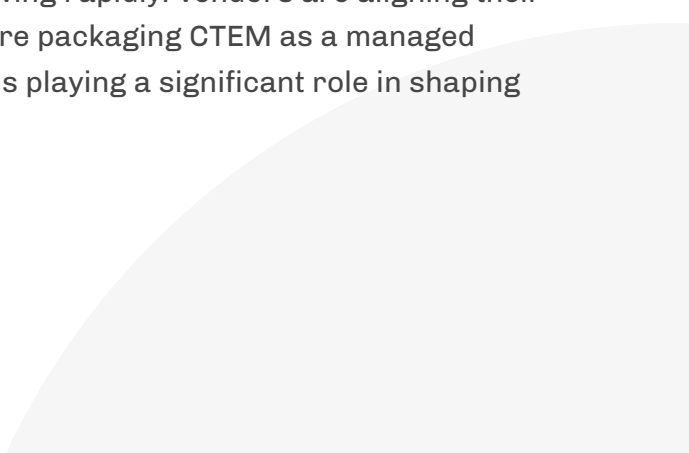
6. Final Words

The urgency to build a sovereign European CTEM ecosystem is growing. As geopolitical tensions rise and supply chain dependencies pose strategic risks, Europe must reduce reliance on external cybersecurity technologies and foster regional innovation. The EU's commitment to "Made in Europe" digital infrastructure presents an opportunity to scale indigenous CTEM capabilities, bolstering both economic and national security.

Continuous Threat Exposure Management (CTEM) represents a fundamental shift in how organizations assess and manage cyber risk. In Europe, this evolution is driven by both necessity and opportunity, rising threat complexity, stringent regulatory expectations, and the need to reduce operational security gaps in real time.

This report highlights that European organizations are embracing CTEM not only as a compliance measure but as a strategic capability. By continuously identifying, validating, and remediating exposures, CTEM enables security teams to focus on what truly matters—protecting critical assets and supporting business resilience.

While CTEM adoption is still maturing, momentum is growing rapidly. Vendors are aligning their solutions with Gartner's CTEM framework, and MSSPs are packaging CTEM as a managed service. The ecosystem is expanding, with European firms playing a significant role in shaping best practices and innovation.



To stay ahead, organizations should:

- Adopt a risk-based mindset grounded in continuous validation and prioritization.
- Invest in CTEM platforms or services that integrate well with their existing tech stack.
- Leverage the growing MSSP ecosystem for scalability and expert support.
- Prepare for regulatory requirements that increasingly mandate continuous exposure visibility.

In an era of continuous threats, only a continuous response will suffice. CTEM offers a blueprint for a more adaptive, proactive, and resilient security posture, and Europe is well-positioned to lead this transformation.

