Integrity360

your **security** in mind

CTEM as a Service

Continuous Threat Exposure Management (CTEM)

CTEM as a Service

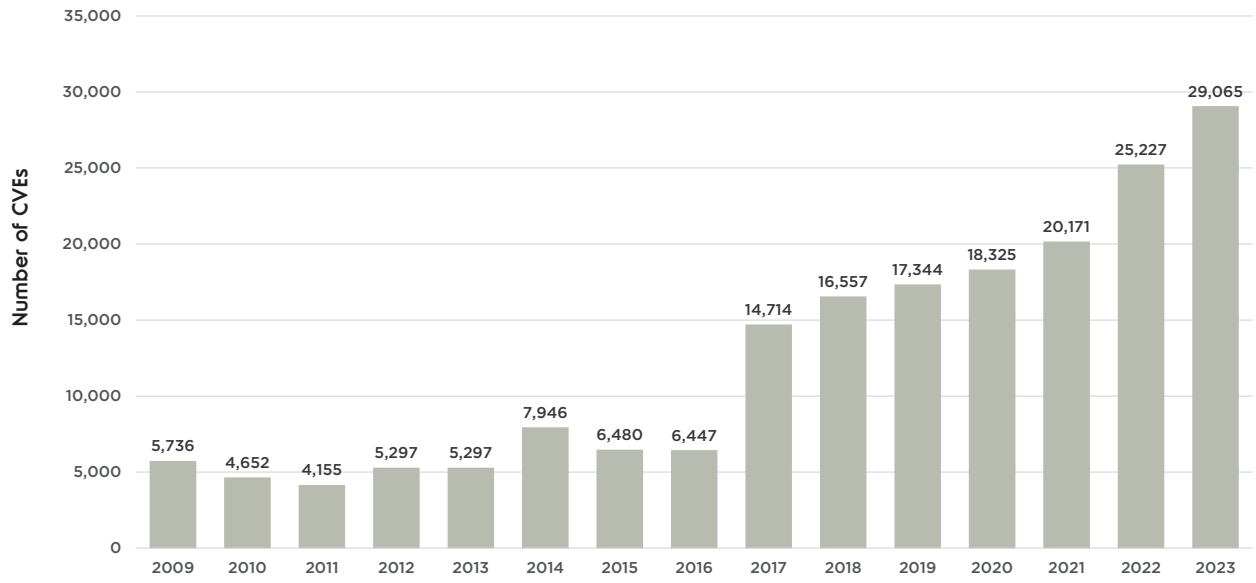
Every year, the world discovers thousands of new vulnerabilities, creating a growing challenge for organisations to stay secure. In addition, they also face many other types of exposures that put their critical assets at risk. It is not enough to simply identify these risks – businesses need a strategy to prioritise and remediate them effectively before they escalate. This is where Integrity360's Continuous Threat Exposure Management (CTEM) as a Service steps in, offering a proactive solution to protect your organisation.

Integrity360's CTEM as a Service offering, based upon the XM Cyber Continuous Exposure Management (CEM) Platform, is designed to help organisations implement CTEM - providing a real-time, holistic view of their exposures and equipping them with the tools to address those that present the greatest risk, proactively and on an ongoing and continuous basis.

"By 2026, organisations that prioritise their security investments based on a continuous exposure management program will be 3x less likely to suffer a breach"

- Gartner

Vulnerabilities (CVEs) identified by year



Source: Statista.com

"A continuous threat exposure management (CTEM) programme is an integrated, iterative approach to prioritising potential treatments and continually refining security posture improvements"

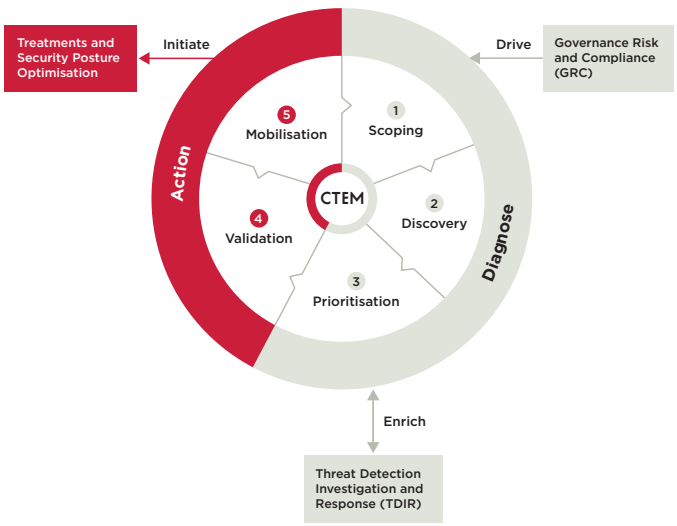
What is Continuous Threat Exposure Management (CTEM)?

CTEM refers to an organisational programme involving an integrated, iterative approach to prioritising the response to identified exposures and continually refining security posture improvements. Rather than focusing solely on periodic scans and assessments and long lists of CVEs, CTEM operates continuously, scoping, discovering, prioritising, validating, and mobilising the treatment of exposures on an ongoing basis.

This method allows businesses to stay ahead of evolving threats and avoid the gaps in security that can arise from relying on outdated, reactive models. CTEM ensures that your organisation is not just responding to incidents but preventing them by focussing on treating the exposures that present the most risk.

The key components of CTEM:

- **Scoping:** Understanding the scope of potential exposure to encompass the full attack surface, whether on-prem assets, cloud, identity permissions configurations, and more. Adopting the attacker's view is critical here.
- **Discovery:** Discovering assets and risk profiles within the identified scope, going beyond just vulnerabilities to also include misconfigurations, ineffective security controls, and more – anything that can be exploited by a threat actor to achieve their goals.
- **Prioritisation:** Prioritising the treatment of exposures based on the risks they present overall rather than just in isolation. Key considerations include how threat actors could exploit exposures to compromise critical assets.
- **Validation:** Understanding how an attacker could actually exploit an identified exposure and how security controls might react with and without proposed treatments, to quantify potential impact.
- **Mobilisation:** Operationalising the CTEM programme findings by reducing friction in approval, implementation processes and mitigations and compensating controls across all involved stakeholder and resolver groups.



"Even taking a risk-based vulnerability management (RBVM) approach might not be sufficient. Fixing every known vulnerability has always been operationally infeasible."

- Gartner

Integrity360's CTEM as a Service

Integrity360's full CTEM as a Service includes the following elements:

- Setup and Operational Management of the XM Cyber Continuous Exposure Management Platform
- Exposure Detection and Prioritisation
- Exposure Remediation Prioritisation
- Optional Exposure Remediation Management
- Optional Remediation Resource Augmentation

Integrity360 delivers the service in a continuous and cyclical manner, ensuring constant improvement of security posture and maintenance of that posture in the face of new exploits and exposures emerging in the environment.

The technical scope coverage of the service can include any of on-premises workstations and servers, Active Directory, and Cloud platforms and workloads.

The objectives of Integrity360's CTEM as a Service

The objectives of Integrity360's CTEM as a Service are as follows:

1. Risk reduction

Attackers chain exposures to build attack paths. By identifying those exposures that mostly contribute towards attack paths from breach points to critical assets, the service identifies for the customer which exposure remediations will give the biggest return in terms of choking off those attack paths. The resultant outcome is heavily prioritised and much more focussed organisational alignment on what they need to remediate first, and for what reason. This can also provide much-needed alignment between Security and IT teams.

2. Remediation prioritisation

Given that organisations struggle to deal with the number of vulnerabilities and exposures they do have, the service aims to provide practical and targeted recommendations for what to remediate first to eliminate the highest exposure risks from the environment.

3. Remediation Value Delivery

Through ongoing support for the execution of the remediation process through internal and external teams, the service ensures value delivery into the end customer and takes a load off security teams to manage and track the implementation of critical remediations identified by the service.

Attackers chain exposures to build attack paths

Two levels of service: Tailored to your needs

Integrity360's CTEM as a Service offers two service levels, each designed to meet your organisation's needs. Whether you need just exposure detection and prioritisation or full remediation management, we have the right solution for you.

1. Continuous Threat Exposure Prioritisation

This foundational level provides a comprehensive approach to identifying and prioritising exposures. It includes the setup, configuration, and ongoing management of the XM Cyber platform, as well as continuous detection of security exposures. Through sophisticated attack scenarios and attack path analysis, we help you understand which exposures pose the greatest risk to your critical assets. By offering prioritised remediation recommendations, we ensure that you focus your security efforts on the areas that will have the biggest impact.

2. Continuous Threat Exposure Management

For organisations that require more hands-on support with remediation management, this level includes all the features of Continuous Threat Exposure Prioritisation, with the added benefit of full Exposure Remediation Management. This service integrates with your existing ticketing systems (such as Jira or ServiceNow) and works closely with your resolver stakeholder groups, including IT and DevOps teams. We manage the entire remediation process, tracking the progress of remediating identified exposures. In addition, we provide weekly KPI reporting to keep you informed of progress and ensure accountability.

3. Optional Professional Services and Resource Augmentation

For organisations facing resource limitations, Integrity360 also offers professional services and CyberConnect360, our resource augmentation service to fill the gaps in your team to remediate your exposures. Whether you need temporary assistance or long-term support, CyberConnect360 provides expert remediation specialists to supplement your in-house teams, ensuring that your risk levels remain manageable even during periods of high demand, or to assist with clearance of a major backlog.

With these two service tiers and optional resource augmentation, Integrity360 ensures that your organisation has the flexibility and expertise needed to proactively and continuously maintain a high level security posture.

CTEM as a Service benefits

Risk reduction:

CTEM helps reduce (3X) the risk exposures resulting in a breach or negative outcome

Enhanced resilience:

CTEM makes organisation more resilient against attack

Response preparedness:

Knowledge gained from CTEM can assist security teams detect and respond to threats more effectively

Improved prioritisation:

Enables focus on business-critical threats, vulnerabilities & exposures

Cost optimisation:

CTEM allows biggest return on investment on mitigation activities

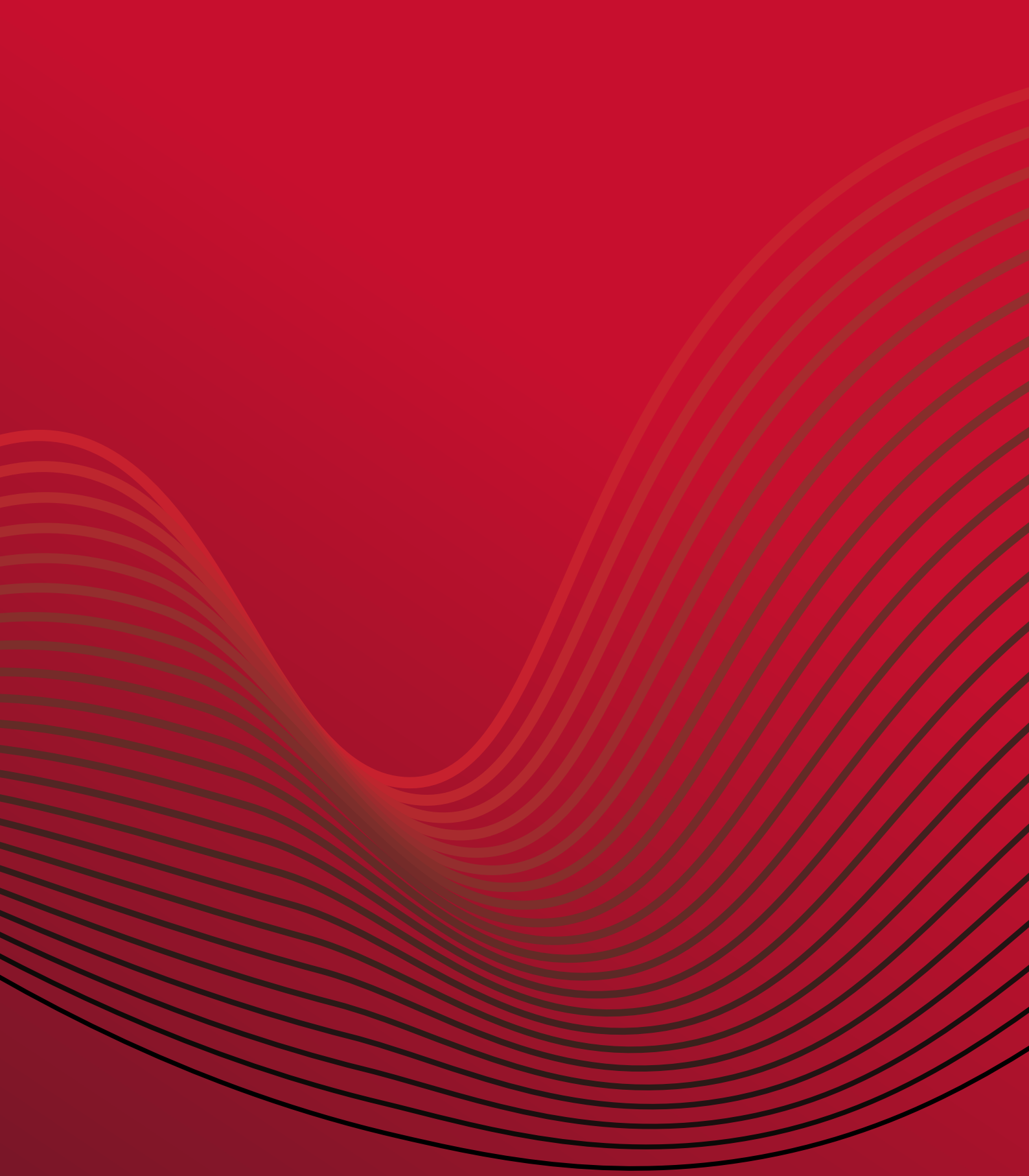
Continuous improvement:

CTEM adopts a continuous process of monitoring, evaluating & enhancing the mitigation of threat exposures

Why choose Integrity360?

Choosing a cyber security provider is a critical decision for any business. Here are just a few reasons why you should choose Integrity360:

- **Experience:** With over 320 security consultants, engineers, and analysts, we have the global experience and expertise to safeguard your business from even the most complex and evolving threats.
- **Reputation:** We have earned the trust of over 550 global companies and have a strong reputation in the industry, built upon by exceptional technical expertise, a client-first attitude, and a proven track record on complex security projects.
- **Customised Solutions:** We take a personalised approach to cyber security, partnering closely with each client to understand their unique needs and recommend the most effective security solutions.
- **Passion and Commitment:** We are passionate about cyber security and committed to delivering the best possible protection for our clients' businesses.
- **Certifications:** Greatest level of technical certifications and capability.
- **Partnerships:** Strongest vendor partnerships and support arrangements.
- **Recognition:** Recognised by Gartner in four market guides.
- **Five Security Operation Centres (SOC)** located in Ireland, Italy, Sweden, Bulgaria and South Africa.



integrity360.com
info@integrity360.com

London, UK
+44 20 3397 3414

Dublin, Ireland
+353 01 293 4027

Stockholm, Sweden
+46 8 514 832 00

Sofia, Bulgaria
+359 2 491 0110

Kyiv, Ukraine
+38 0 504 701 125

Madrid, Spain
+34 910 767 092

Cape Town, South Africa
+27 21 100 3774

Naples, Italy

Vilnius, Lithuania