Horizon3.AI Europe GmbH

06.08.2025 – 11:10 Uhr

Building Stronger Security by Thinking Like an Attacker

London (ots) -

• Cyber threats in the UK are escalating. Attackers are faster, more automated, and increasingly AI-driven, outpacing traditional defences like firewalls and vulnerability scans.

• Many organisations still rely only on passive, defensive security leaving them uncertain whether their systems would withstand a real attack.

• Proactive, autonomous penetration testing is a key cornerstone of a modern Cyber Security strategy, as part of a Continuous Threat Exposure Management (CTEM) approach.

• Cybersecurity expert Keith Poyser urges regular, attacker-style testing to uncover weaknesses early, fix before exploited, build customer trust, and prepare for stricter regulations.

Cybersecurity has never been more critical in the UK, as organisations face a rapidly evolving threat landscape impacted by geo political tensions in the region, cyber focused organised crime and hybrid conflict. Today's attackers are becoming faster, more automated, and increasingly powered by artificial intelligence, making traditional defensive strategies less effective on their own. At the same time, regulatory pressure is intensifying, with businesses expected to demonstrate measurable risk management. Recent high-profile cyber incidents at multiple flagship retailers have provided a stark reminder that conventional approaches are no longer enough.

While most organisations claim to prioritise security, few put their defences to the test. Too many rely on conventional, passive measures such as checklists, audits, and the assumption that layered systems will hold when challenged. This approach is like installing an elaborate alarm system in a home without ever checking if it will actually trigger during a break-in. What organisations truly need is offensive security: continuous testing that probes every possible entry point to uncover weaknesses before attackers do. Keith Poyser, Vice President for EMEA at cybersecurity company Horizon3.ai, recommends running such a "break-in" at least once a month through regular autonomous penetration testing, to identify any exploitable weaknesses, with prioritised remediation, rather than be left waiting to be exploited. Rather than relying on manual, human penetration testing, which may look at around 5% of a company's attack surface and can take weeks, Horizon3.ai operates an offensive security platform called NodeZero. It delivers 100% coverage, operates 18 times faster than humans, and enables organisations to conduct production-safe cyberattacks on their own IT infrastructure ('penetration tests') to show how to fix, and test the fix, on a continuous basis.

The Escalating Cyber Threat Landscape

With the cyber threat environment becoming more aggressive and complex, attacks are now a constant reality. Today's adversaries are known to take advantage of overlooked system settings, weak login details, and unseen trust paths to quietly expand their reach inside networks. Traditional safeguards—such as firewalls, antivirus software, and occasional vulnerability scans—can no longer keep up with the speed and sophistication of these intrusions. The surge in recent UK breaches is a clear warning, underscoring the urgent need to take decisive steps, though many may be left uncertain about where to begin.

Stress Rising as Cyber Threats Escalate

The latest State of Cyber Risk and Exposure 2025 report from Bitsight* paints a concerning picture of UK cybersecurity readiness. Out of 1,000 cybersecurity and risk professionals surveyed worldwide, only one in five UK organisations rated their cyber risk management as "very mature." Even more troubling, UK security professionals reported higher stress levels than their peers in other regions, reflecting the intense pressure of keeping pace with escalating threats. Security expert Poyser believes the answer lies in a shift of mindset: "Defending passively does not instil lasting confidence. Organisations need to think like attackers, taking a proactive and measurable approach to security. Techniques such as autonomous penetration testing, red teaming, and CTEM reveal exactly how intruders might break in, which defences fail under pressure, how to fix, and how quickly teams can respond."

The Hidden Danger of False Confidence

On the other hand, still too many companies risk falling into a false sense of security. According to Horizon3.ai's Cybersecurity Report UK 2024/25, nearly a quarter of the 150 organisations surveyed admitted they were unaware of any attacks in the past two years, with 8% insisting they had not been targeted at all. Keith Poyser warned that such assumptions are risky: "It's unrealistic to believe that any organisation has been completely overlooked by threat actors for this long. The reality is that many attacks go undetected, and the consequences—ranging from prolonged downtime to severe financial losses or regulatory penalties—can be devastating. Businesses should stop relying on hope and start prioritising proactive, offensive measures to strengthen their security posture."

Pentesting Frequency Is the Key to Cyber Resilience

Findings from Horizon3.ai's Cybersecurity Report UK 2024/25 highlight a mixed picture in how UK organisations currently approach penetration testing. While 60% of respondents reported carrying out pentests, only 13% have adopted automated platforms—widely considered essential for testing at the pace today's threat landscape demands. A further 27% rely on in-house security teams, and 20% bring in external providers to perform tests. Poyser pointed out that manual approaches, whether internal or external, tend to be resource-heavy and therefore less frequent: "The issue isn't just about cost, it's about effectiveness. Automated testing allows companies to test more often, more thoroughly, which is critical when more than 560,000 new cyber threats are identified worldwide every day.** The more efficient and repeatable the process, the stronger the overall security posture."

Ultimately, cybersecurity testing is not just a technical exercise but a cornerstone of business resilience. By embedding regular, proactive testing into their strategy, organisations can move forward with greater confidence, protecting both their operations and their reputation while ensuring they are well-prepared for the escalating challenges.

* https://www.bitsight.com/resources/state-of-cyber-risk-and-exposure-2025

** https://www.statista.com/topics/8338/malware/

About Horizon3.ai and NodeZero: Horizon3.ai provides a cloud-based platform, NodeZero, enabling organisations and public authorities to simulate self-attacks on their IT infrastructure to assess their cyber resilience through penetration testing (pentesting). Thanks to its cloud model, the platform offers affordable, regular pentesting, making it accessible to mid-sized companies. Horizon3.ai continuously monitors the cybercrime landscape to ensure that newly discovered vulnerabilities are swiftly integrated into the cloud system. NodeZero not only identifies security flaws but also offers tailored recommendations for remediation. Through this platform, Horizon3.ai helps organisations meet rising regulatory demands for cyber resilience in Governance, Risk & Compliance (GRC), with guidelines recommending an internal self-attack at least once a week.

Trademark notice: NodeZero is a trademark of Horizon3.ai

Further information:

Horizon3.AI Europe GmbH, Prielmayerstrasse 3, 80335 Munich, Web: www.horizon3.ai

PR Agency: euromarcom public relations GmbH, Tel. +49 611 973150, Web: www.euromarcom.de, E-Mail: team@euromarcom.de

Original content of: Horizon3.AI Europe GmbH, transmitted by news aktuell
Diese Meldung kann unter https://www.presseportal.de/en/pm/163532/6091438 abgerufen werden.