HORIZON3.ai

CASE STUDY

MID DEVON DISTRICT COUNCIL

From Point-in-Time Testing to Continuous, Autonomous Security Validation

Background

Mid Devon District Council delivers essential public services to residents across the region, including housing support, financial assistance, and community safety initiatives. To support these services, the council's ICT team is responsible for maintaining a secure, resilient, and continuously available technology environment.

Like many public sector organisations, Mid Devon operated in a complex and constantly evolving IT landscape, where new risks could emerge between formal assessments and existing controls had to stretch across a broad set of systems and services. The team relied on annual penetration tests, monthly vulnerability scans, and internal monitoring tools to help manage cyber risk. While each of these played an important role, they were fundamentally point-in-time measures.

That created a critical challenge: although the council could identify vulnerabilities and misconfigurations, it was much harder to determine what was actually exploitable in the environment at any given moment.

ABOUT MID DEVON DISTRICT COUNCIL

Champion: Jamie Thornton, ICT Infrastructure Engineer

Industry: Local Government / Public Sector

Employees: ~400

Location: United Kingdom

Solution: Horizon3.ai NodeZero Autonomous Pentesting & Rapid Response

For a lean ICT team supporting essential public services, that distinction mattered. They needed a way to continuously validate real-world exposure, focus effort on the issues that posed the greatest risk, and strengthen security without adding significant operational overhead.

Challenges

Jamie and the team faced several recurring challenges:

Limited visibility between assessments – Annual penetration tests and monthly scans left long periods where newly introduced weaknesses could go undetected, making it difficult to maintain an up-to-date view of real exposure.

Difficulty prioritising remediation – Traditional tools generated extensive lists of vulnerabilities, but those findings did not always indicate which issues could actually be exploited or how they could be chained together by an attacker. As a result, prioritisation was often time-consuming and less precise than the team needed.

Pressure to strengthen identity security – As the council rolled out updated password policies in Active Directory, the team needed a more concrete way to identify weak and compromised credentials and validate whether those changes were meaningfully improving security.

Need to demonstrate progress to leadership and auditors – Internal stakeholders and auditors wanted more than static reports. They needed clear evidence that the council was continuously improving its security posture and reducing real risk over time.

The ICT team needed a practical way to identify, validate, prioritise, and remediate exploitable weaknesses across the environment, without dramatically increasing workload or headcount.

Why Now

The timing for change was driven by a combination of operational need and strategic opportunity.

1. It had become increasingly clear that point-in-time testing was no longer enough. In a dynamic environment with evolving threats, annual penetration tests and periodic scanning could not provide the continuous visibility the team needed.
2. Mid Devon was given the opportunity to participate in an NCSC-led deception technology trial that included Horizon3.ai's NodeZero®. That gave the council hands-on exposure to a modern approach to security validation and a chance to evaluate autonomous pentesting in a real operational context.
3. When a new threat emerged that posed significant risk to the organisation, the team needed more than theoretical vulnerability data. They needed an attacker-style view of whether they were truly exposed, what paths could be exploited, and what actions would reduce risk fastest.

At the same time, the council was actively strengthening identity security through a new Active Directory password policy. To make that initiative effective, the team needed evidence of weak and compromised credentials and a better way to validate that the policy changes were having the intended impact.

Together, these factors made the need for change unmistakable. Waiting for the next annual test was no longer a viable option.

Mid Devon needed a more agile, continuous approach to security validation; one that could keep pace with the environment, support rapid decision-making, and help the team focus on what mattered most.

Solution: Horizon3.ai NodeZero & Rapid Response

Mid Devon's first experience with Horizon3.ai came through the NCSC trial, where the council evaluated NodeZero, Horizon3.ai's autonomous pentesting platform, as part of a proof of concept.

From the beginning, the experience stood out. Deployment was straightforward, the platform required minimal configuration, and the results were immediately useful. Rather than simply surfacing raw vulnerability data, NodeZero showed how weaknesses and misconfigurations could be chained together into real attack paths, helping the team understand what was truly exploitable and what should be addressed first.

Just as important, the platform's reporting made the findings accessible beyond the technical team. The council could clearly communicate risk, explain remediation priorities, and show progress in a way that resonated with both practitioners and leadership.

Following the initial evaluation, Mid Devon adopted NodeZero for regular scheduled pentests as well as on-demand assessments, significantly increasing the frequency and depth of testing without increasing resource requirements.

Key capabilities included:

Autonomous Pentesting – NodeZero continuously discovers attack paths by chaining together exploitable weaknesses, misconfigurations, and identity issues, giving the team a more realistic view of attacker opportunities than traditional point-in-time assessments.

Prioritisation and Remediation Guidance – By focusing on what is actually exploitable, NodeZero helped the team cut through noise and act on the findings that would have the greatest impact on risk reduction. Clear mitigation and remediation guidance made it easier to move quickly and confidently.

Active Directory Password Audit – This capability supported the rollout of the council's new password policy by identifying weak and compromised credentials that required immediate attention, helping strengthen identity security across the environment.

Rapid Response – When an emerging threat created urgent concern, Horizon3.ai's Rapid Response service helped the team quickly assess whether they were exposed, understand the potential impact, and take remediation action faster.

As Mid Devon continues to mature its use of the platform, the team plans to expand coverage to additional environments, including cloud services, helping ensure its security validation strategy evolves alongside its broader technology roadmap.

The Impact: Security at the Speed of Business

Jamie and the team report several meaningful and impactful outcomes from adopting NodeZero across their environment.

Greater visibility into real security exposure: Regular autonomous pentesting has given the council a far clearer and more current view of exploitable risk across the environment than traditional annual testing and periodic scanning alone.

More efficient use of limited resources: By validating what is actually exploitable and pairing findings with actionable remediation guidance, NodeZero has helped the ICT team focus effort where it matters most and reduce time spent working through lower-priority issues.

Stronger identity security: The Active Directory Password Audit played an important role in reinforcing password hygiene during the rollout of the council's updated password policy, and the team sees additional opportunities to strengthen identity defences further over time.

Faster response to emerging threats: With Rapid Response, the council was able to quickly determine its exposure to a serious emerging threat and take action to reduce potential impact without waiting for a traditional assessment cycle.

Improved communication with leadership and auditors: NodeZero's reporting has made it easier to demonstrate continuous improvement, explain risk in business terms, and show that security validation is now an ongoing practice rather than a once-a-year exercise.

Takeaway

Mid Devon recommends autonomous pentesting as a valuable complement to traditional security testing methods, particularly for organisations that need stronger validation, clearer prioritisation, and better operational efficiency. For Mid Devon, NodeZero has helped transform security testing from a periodic compliance activity into a more continuous, practical, and risk-focused discipline.

Mid Devon DISTRICT COUNCIL