Meeting the ECB's AI-Enabled Cybersecurity Mandate with NodeZero®

On 7 July 2026, the European Central Bank directed every significant institution to submit a board-level action plan addressing AI-accelerated cyber threats. NodeZero maps directly to the six focus areas the ECB requires — with continuous, production-safe proof, not point-in-time assessments.

October 31, 2026
Action plan due to your Joint Supervisory Team

6
ECB focus areas — each mapped to a NodeZero capability below

DORA / NIS2
NodeZero methodology already aligned to existing obligations

The Challenge

AI has compressed the window between vulnerability discovery and exploitation to hours — but most bank security programs still operate on manual, point-in-time testing cycles. Teams are left managing lists of theoretical findings while attackers move on verified attack paths.

The ECB is not asking institutions for more activity, it is asking for evidence that exploitable exposure is being continuously identified, prioritized, and reduced.

Mapping the ECB's Six Focus Areas to NodeZero

Each requirement in Annex 1 of the ECB letter maps to a specific, production-proven NodeZero capability.

1 Protect the Attack Surface

ECB Requires	NodeZero Delivers
Identify ICT assets, including third-party/ open-source components; continuously monitor internet-facing, cloud, and externally exposed assets; prioritize perimeter remediation.	**External Pentesting & Asset Discovery** — Open-source Intelligence (OSINT)–driven enumeration provides continuous visibility into internet-facing assets, enabling organizations to respond faster when critical vulnerabilities emerge. **Cloud & Kubernetes Pentesting** — extends the same view across cloud and containers. **Internal Pentesting** — covers threats originating from inside the network, as the ECB explicitly flags.

2 Accelerate Vulnerability & Patch Management at Scale

ECB Requires	NodeZero Delivers
Prioritized scanning; AI-assisted tooling with safeguards and human oversight; change management that supports faster, risk-based patching.	**Risk-Based Exposure Management** — prioritizes remediations based on proven, exploitable attack paths—not raw CVE volume **1-Click Verify** — instantly re-tests patched vulnerabilities to verify that the fix eliminated the exploit path **Pentest Wednesday® cadence** — recurring autonomous tests validate that Patch Tuesday worked.

3 Enhance Monitoring, Detection & AI-Enabled Defense

ECB Requires

Strengthened monitoring of logs, network traffic, and access to catch indicators of compromise and attempted exploitation faster.

NodeZero Delivers

NodeZero Tripwires™ — deception decoys (honeytokens) placed along the exact high-risk attack paths NodeZero identified during testing.

Rapid Response — early alerts and pre-built exploits for emerging zero- and n-day threats.

Threat Actor Intelligence — maps findings to threat-actor TTPs relevant to financial services.

4 Strengthen Governance, Funding, Training & Supply Chain Assurance

ECB Requires

ICT budgets/staffing matched to threat pace; third-party ICT provider accountability; risk-appropriate awareness training.

NodeZero Delivers

NodeZero Insights™ — generates executive and JST-ready posture reports detailing security trends and Mean Time to Remediation (MTTR) over time.

Third-Party Risk Management (TPRM) — safely verifies third-party security posture with autonomous pentesting across your supply chain—without agents, integrations, or relying on self-attestations.

High-Value Targeting & Advanced Data Pilfering™ — demonstrates business impact to justify security investments to the board.

5 Reinforce Defense-in-Depth & Modernize Infrastructure

ECB Requires

Assume perimeter breach; adopt zero- trust/micro-segmentation; modernize or retire legacy/end-of-life systems; security-by-design.

NodeZero Delivers

AD Password Audit & Identity Security Validation — tests the Active Directory and credential hygiene that zero-trust depends on.

Network Segmentation Testing — proves controls actually contain an attacker lateral movement.

Endpoint & Security Control Validation — flags legacy or misconfigured systems before attackers do.

6 Improve Operational Resilience & Information-Sharing

ECB Requires

Crisis management, incident response, and recovery aligned to DORA; testing against high-speed, high-volume attack scenarios; trusted information-sharing.

NodeZero Delivers

Full attack-chain emulation — safely exercises domain compromise and lateral movement scenarios.

1-Click Verify retesting — validates fixes during and after IR drills.

Regulatory evidence generation — automatically formats test data to double as regulatory compliance proof for DORA and NIS2 audits.

Proven in Financial Services

A tier-1 financial services organization's first autonomous internal pentest illustrates the shift from point-in-time compliance testing to continuous, evidence-based resilience.

Rapid Deployment

3 full domain compromise pathways and 586 previously undiscovered critical impacts found in less than 14hrs.

7.2M

Files found to be accessible to any domain user.

117

Hosts NodeZero obtained admin rights to by abusing domain user privileges.

Why Horizon3

250,000+

Production-safe autonomous pentests executed

5,500+

Global environments tested

4 of 10

Top Fortune 10 companies trust NodeZero

Zero

Downtime across all production tests to date

Key Takeaway

AI-enabled attackers are compressing the time from vulnerability discovery to exploitation, but the fundamentals of the ECB's expectation are clear: **what matters now is which vulnerabilities are actually exploitable, how they chain together, and what impact they can create.**

NodeZero gives significant institutions the evidence to answer that question continuously, so your action plan submitted to the JST is grounded in proof of real exposure and validated resilience, not point-in-time assumptions.

Build your ECB action plan backed by evidence.

Schedule a demo with Horizon3 or sign up for our webinars.

© 2026 Horizon3.ai