



HORIZON3

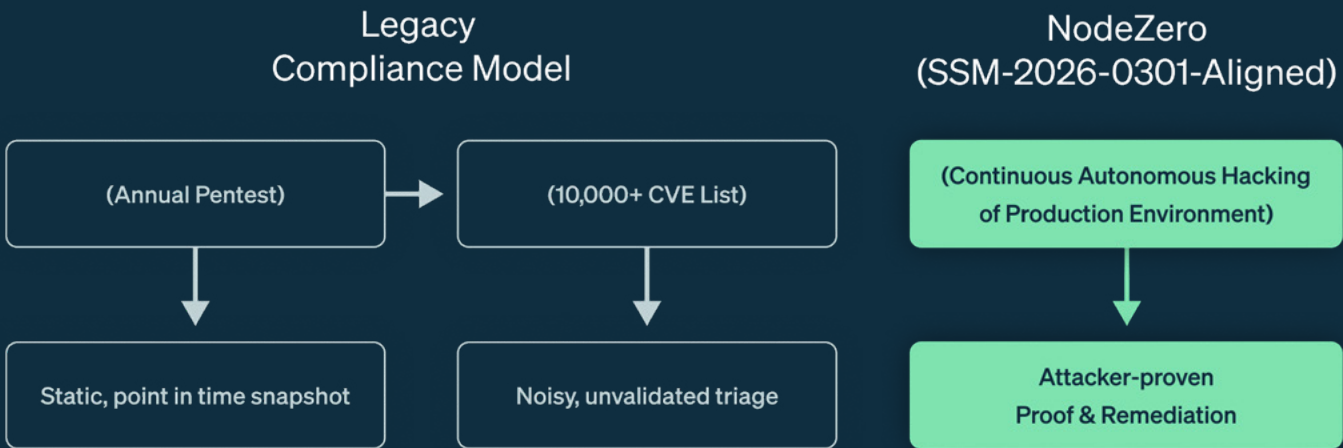
Meeting the ECB's AI-Enabled Cybersecurity Supervisory Recommendations with NodeZero[®]

Context and the Shift in Threat Speed

On 7 July 2026, European Central Bank (ECB) Supervisory Board Chair Claudia Buch issued supervisory letter **SSM-2026-0301** to the CEOs of approximately 110 significant institutions under direct ECB supervision. The message is clear: frontier AI models now automate software vulnerability discovery and weaponized exploit generation. This compresses the timeline between vulnerability discovery and exploitation from weeks to hours.

The letter directs institutions to evaluate this threat shift immediately and submit a comprehensive Action Plan to their Joint Supervisory Team (JST) by 31 October 2026.

Annex 1 details expectations across six core focus areas. While foundational security controls such as patch management, monitoring, governance, and resilience testing all align with DORA and NIS2 frameworks, the ECB has shifted the standard from attested compliance to demonstrated proof.



Static self-assessments, raw vulnerability scans, or annual point-in-time compliance reports are not enough. Banks must demonstrate through empirical proof that exploitable exposures are continuously identified, prioritized, and eliminated. This proof must withstand JST reviews and upcoming cross-sector horizontal analyses.

ECB's Six Focus Areas

1. **Protect the attack surface.**
2. **Accelerate vulnerability and patch management.**
3. **Enhance monitoring, detection and AI-enabled defense.**
4. **Strengthen governance and supply chain assurance.**
5. **Reinforce defense-in-depth cyber hygiene.**
6. **Improve operational resilience and recovery.**

Solution Overview: NodeZero Autonomous Testing

NodeZero by Horizon3 is an autonomous penetration testing platform that continuously finds, validates, and proves exploitable risk across your entire attack surface. NodeZero executes real attack vectors across infrastructure, cloud, identity, and applications. It continuously chains misconfigurations, weak credentials, and software vulnerabilities into full, multi-stage attack paths.

NodeZero now extends this testing across web applications as well as infrastructure, cloud, and identity; a single exposed application is tested not in isolation, but as the first step in the same attack chain a real adversary would follow.

NodeZero shifts your security strategy from managing raw vulnerability volume to validating actual risk reduction. Every test generates actionable proof:

- **Production-Safe Autonomous Exploitation:** Executes real-world attack techniques (remote code execution, credential dumping, lateral movement) without agents or system downtime, operating within strict, built-in guardrails.
- **Proof-of-Concept Evidence:** Captures verifiable proof of exploitation (such as domain admin escalation or accessible database tables) so engineering teams fix confirmed attack paths.
- **Continuous Loop Verification:** Retests remediation with a single click (1-Click Verify) to confirm that an applied fix closes the attack path.

NodeZero Attack Path in Action

“We moved beyond point-in-time testing to continuously validate real exposure. NodeZero gave us clearer priorities, faster response, and better visibility into what actually matters. Security is now an ongoing discipline — not just a once-a-year exercise.”

ICT Infrastructure Engineer,
UK public-sector organization

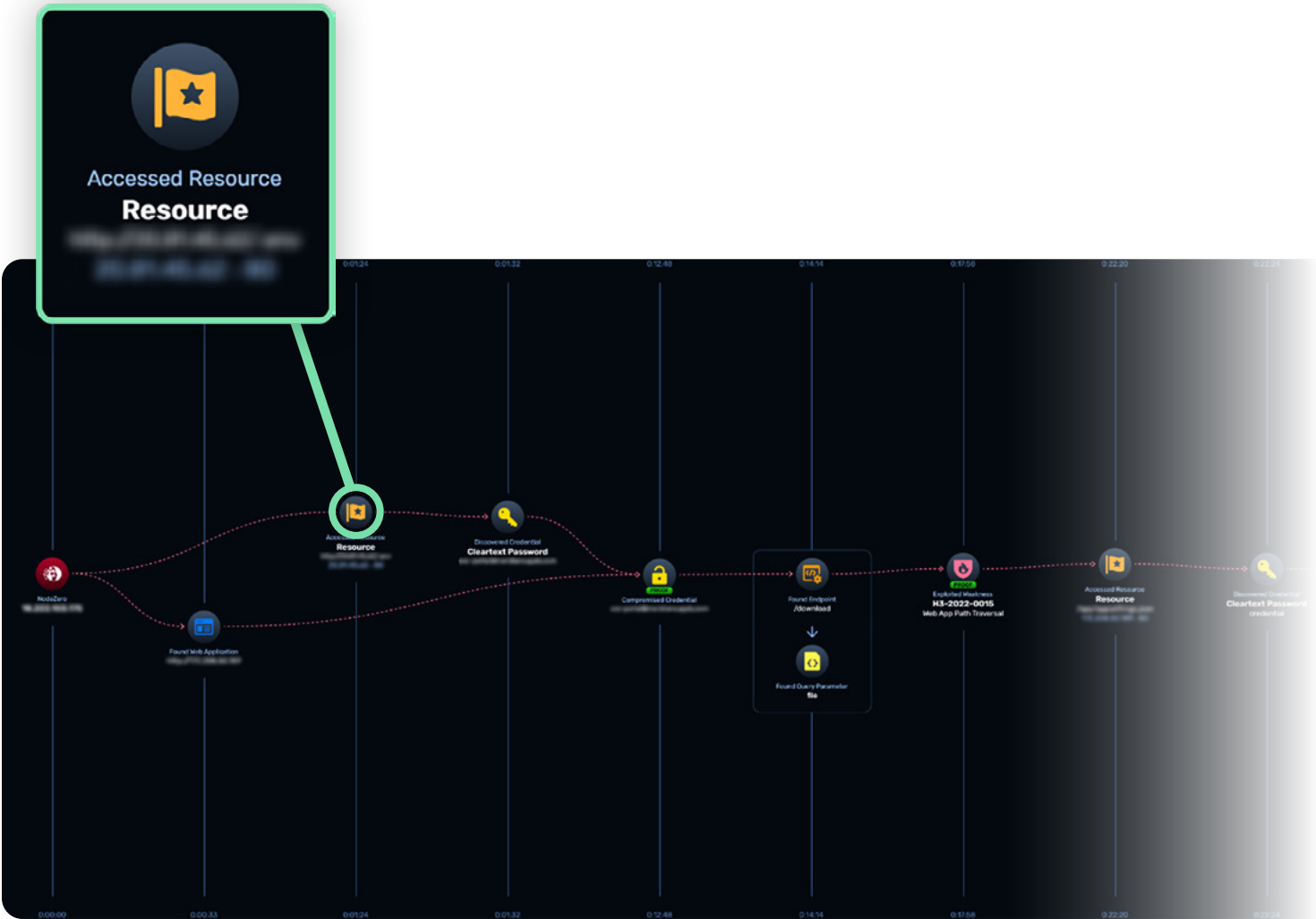
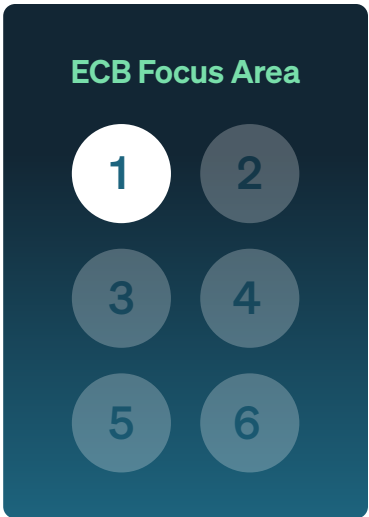
Annex 1 asks banks to prove exploitable exposure is found, prioritized, and closed across the perimeter, the patch cycle, detection, identity, and infrastructure. NodeZero doesn't prove this with six disconnected tools. It proves it with one continuous, autonomous attack chain. The following example walks through a demonstrated attack path to illustrate exactly how the resulting evidence maps to the ECB's six focus areas.

External Attack-Surface Discovery

Area 1: Protect the Attack Surface

NodeZero begins by enumerating public-facing web applications without requiring CMDB input. This reconnaissance discovers an internet-facing staging application with an exposed .env file at the web root and identifies a related production application.

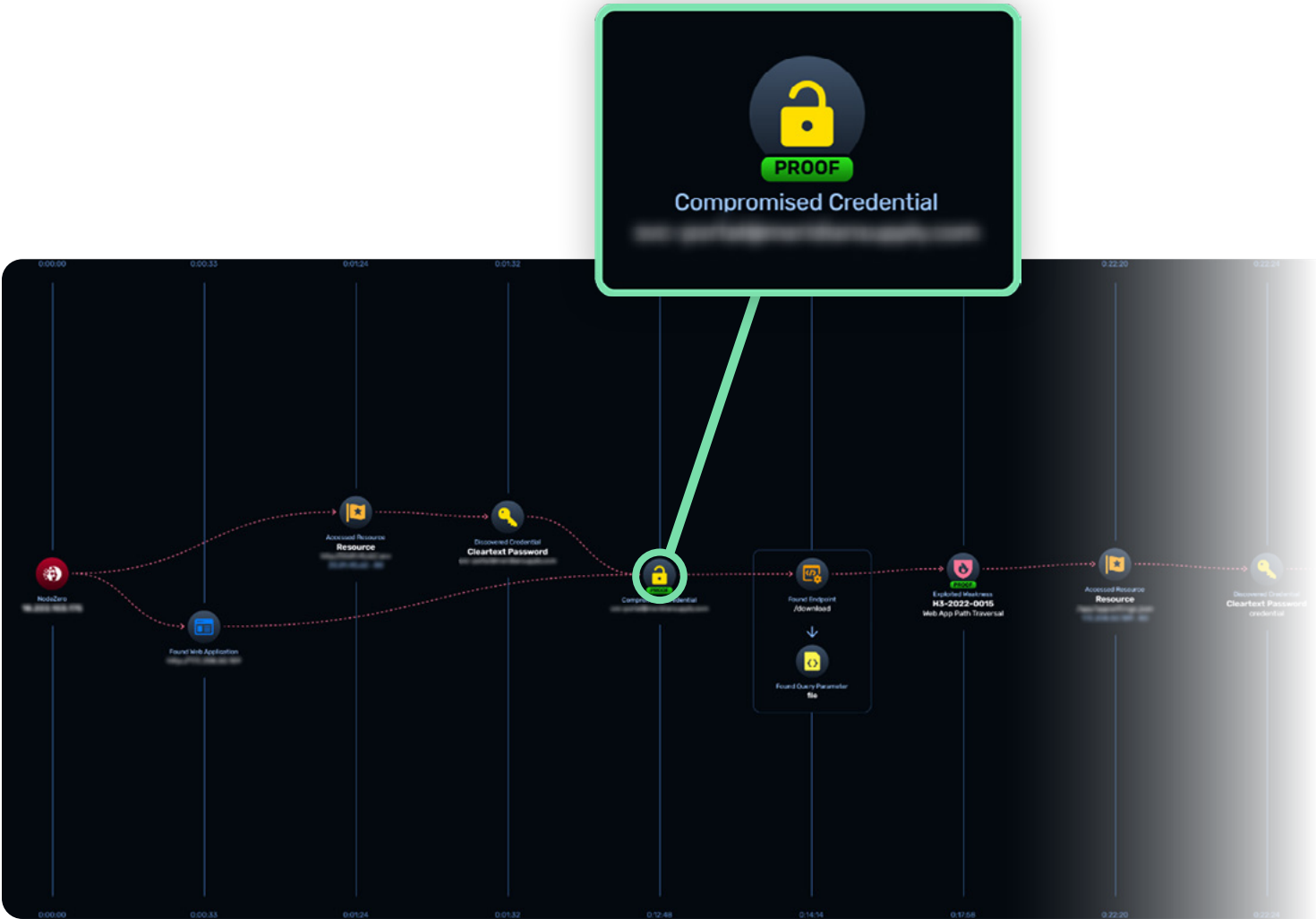
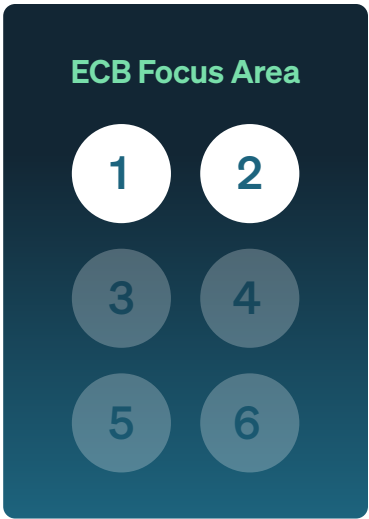
This is an exposed-asset discovery, not yet an application-logic exploit. The finding demonstrates why institutions need accurate visibility into internet-facing assets, including assets that may sit outside the expected inventory, and continuous monitoring of what is actually exposed.



Exposed Configuration to Authenticated Production Access

NodeZero analyzes the exposed file with AI-assisted credential analysis and identifies a hard-coded backend service credential used for routine application maintenance. It tests that credential against the related applications and successfully authenticates into the production web application as a legitimate user.

The credential is not the objective; the access it enables is. Authentication changes what NodeZero can evaluate, including application functionality, endpoints, parameters, permissions, and behavior that are not visible to an unauthenticated scanner.



Authenticated Path Traversal Exposes Cloud Credentials

Now authenticated, NodeZero dynamically crawls the production application and evaluates its exposed routes, endpoints, and parameters. It discovers an authenticated path-traversal vulnerability in the custom application.

NodeZero safely exploits that weakness to read the application's configuration from disk, where it finds hard-coded Azure credentials. The path has now crossed an organizational boundary: a weakness in the web application has exposed a cloud identity.

This is not a generic CVE in an off-the-shelf product. It is a custom-application weakness that makes the secure-by-design and risk-based remediation expectations in the ECB letter concrete.

ECB Focus Area

1

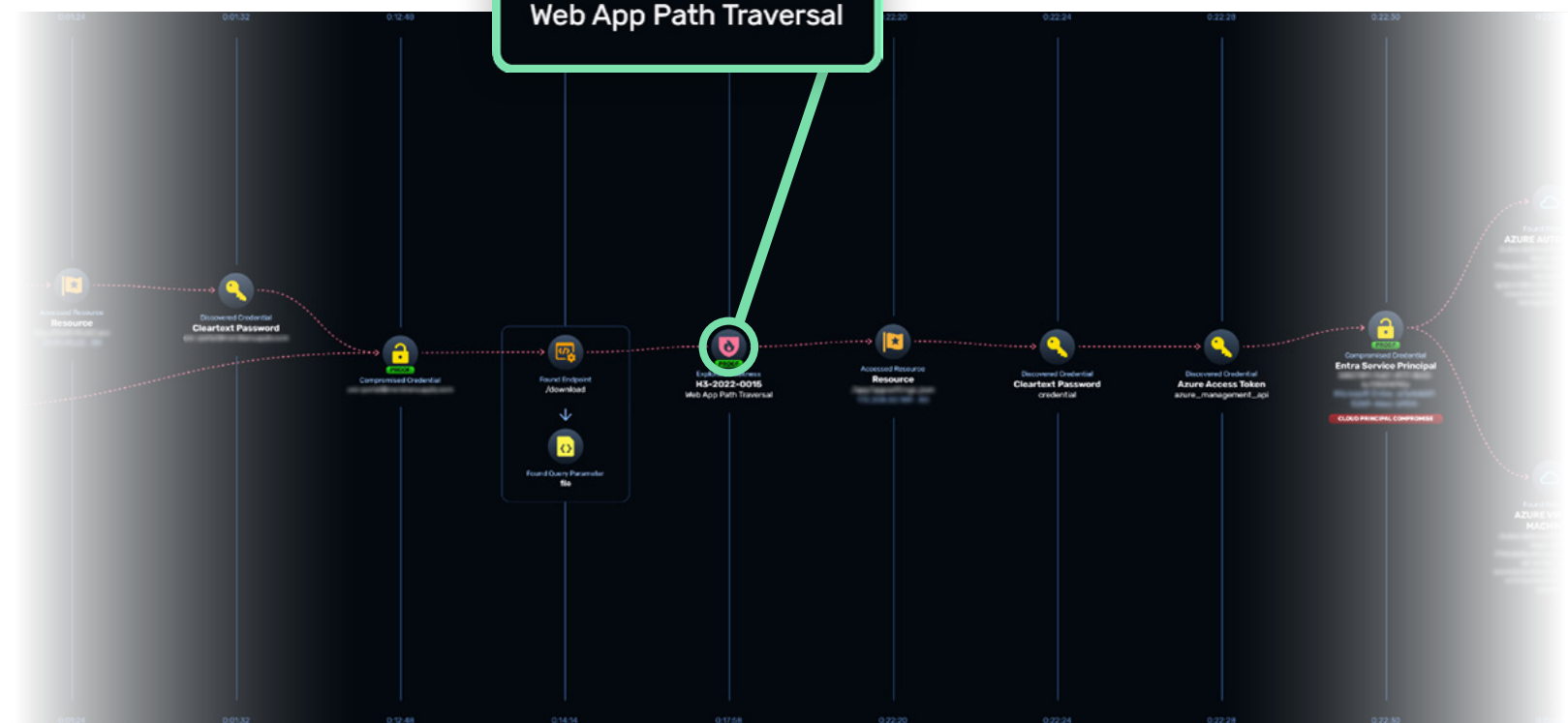
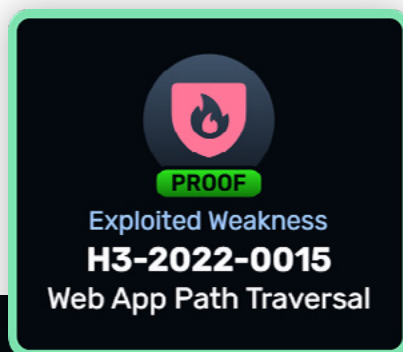
2

3

4

5

6

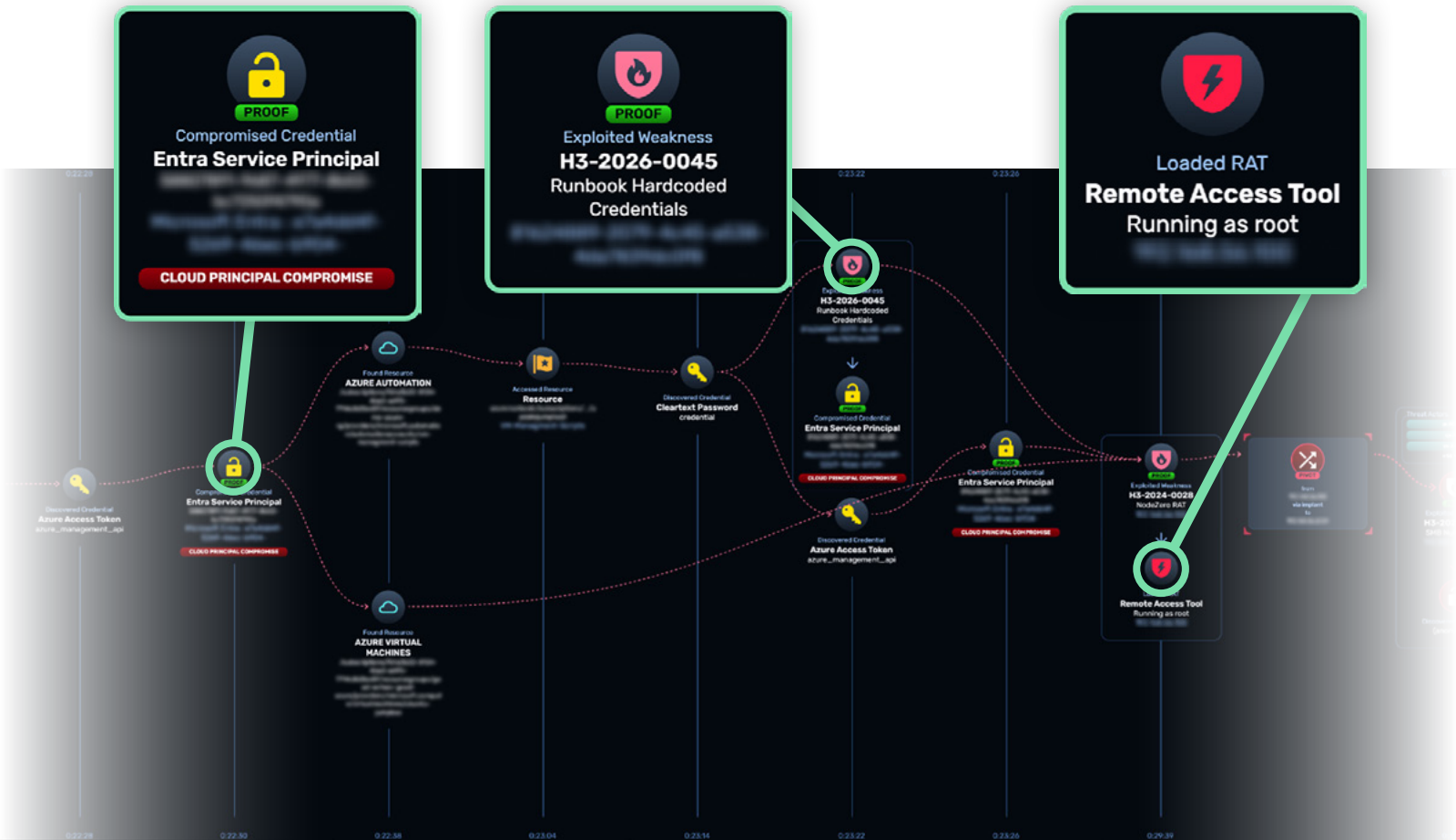
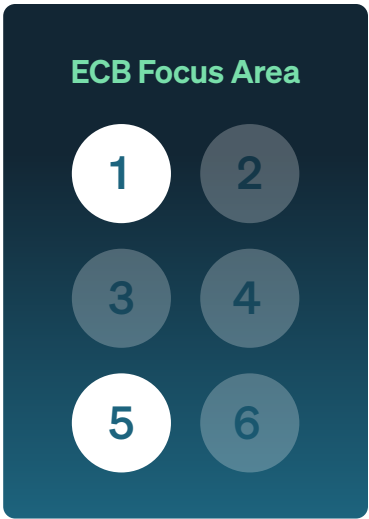


Read-Only Cloud Access Becomes Infrastructure Control

The initial Azure identity provides read-only access. NodeZero uses that visibility to enumerate available Azure resources and discovers an Automation Account containing a runbook. The runbook contains a second hard-coded credential with greater privilege and the ability to execute commands on virtual machines.

NodeZero uses the newly discovered credential and Azure Run Command to execute code on an internal host and install its production-safe remote-access component. From that implanted host, it establishes a tunnel to resources that are not directly reachable from the internet and begins internal reconnaissance.

This sequence is more precise than describing the first cloud identity as already privileged: the escalation comes from cloud enumeration, cleartext credential exposure in the runbook, and excessive command-execution rights.

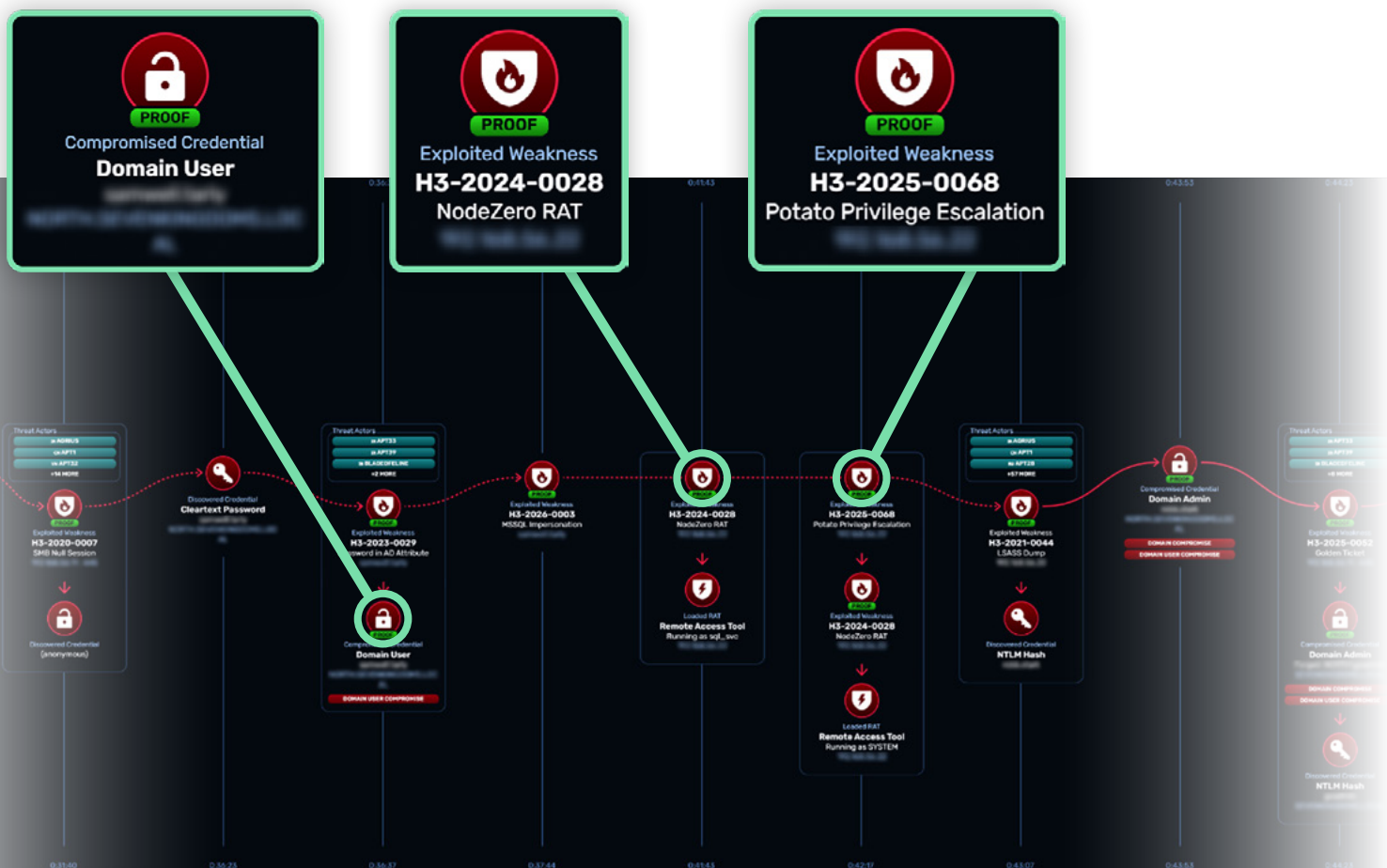
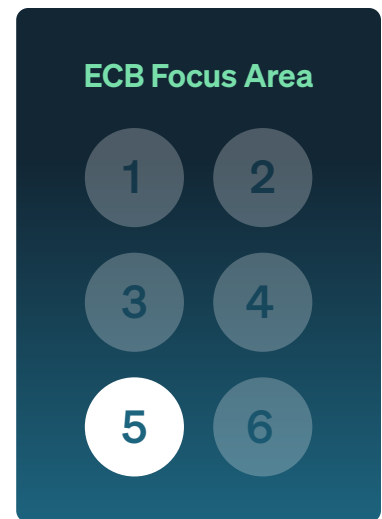


Internal Identity and Infrastructure Pivot: Defense-in-Depth

During internal reconnaissance, NodeZero identifies a domain-user credential exposed in Active Directory. It retrieves the credential and successfully authenticates as the domain user, expanding the systems, relationships, and permissions it can evaluate.

NodeZero then evaluates the internal attack graph and discovers that the compromised domain user has access to SQL Server. It abuses that access to execute code and implant on another host, then performs local privilege escalation to reach SYSTEM.

The path demonstrates why perimeter protection alone is insufficient. Continuous verification of identities, service accounts, access rights, segmentation, remote execution paths, and internal systems is required after an initial foothold is established.

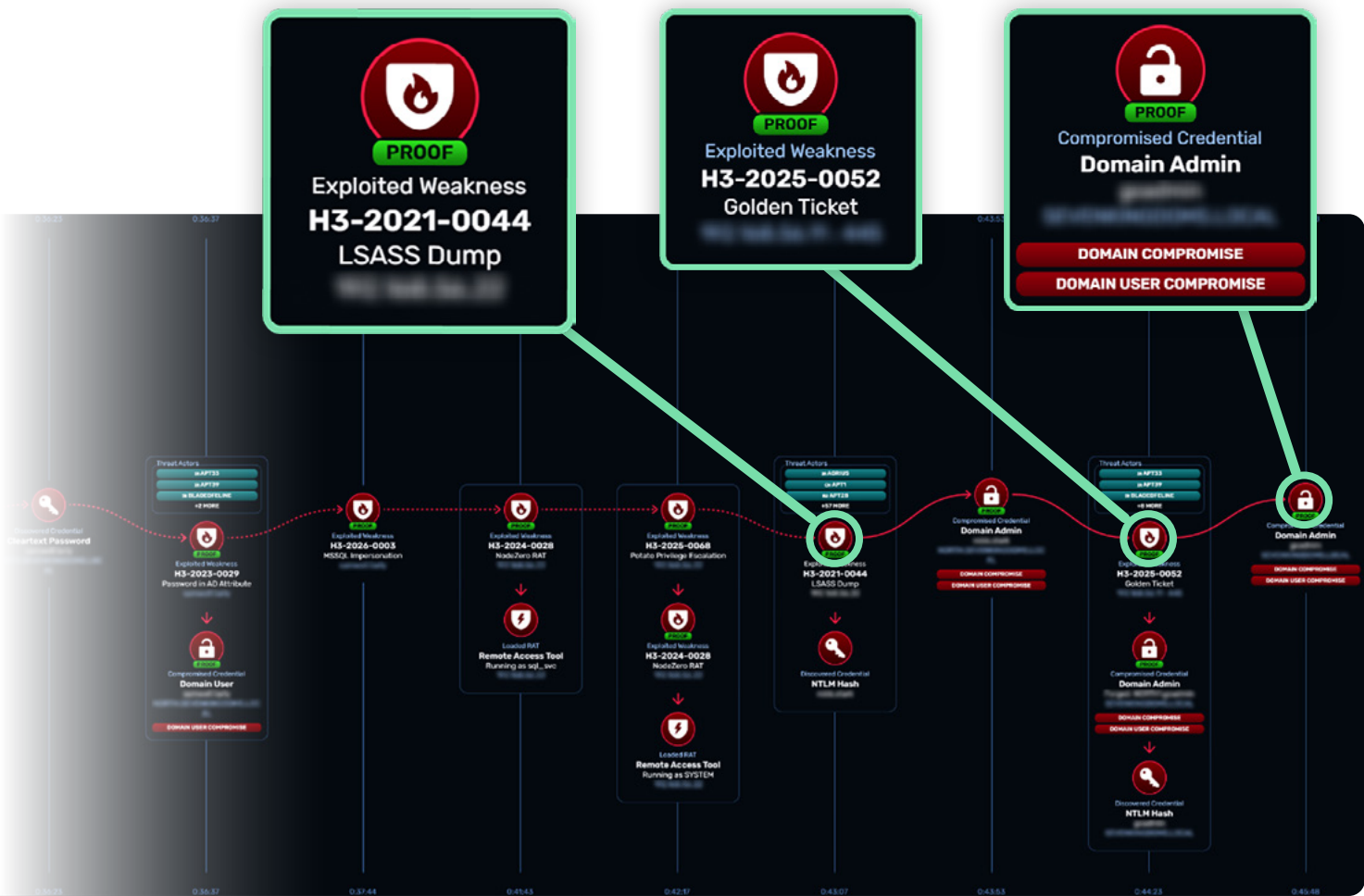
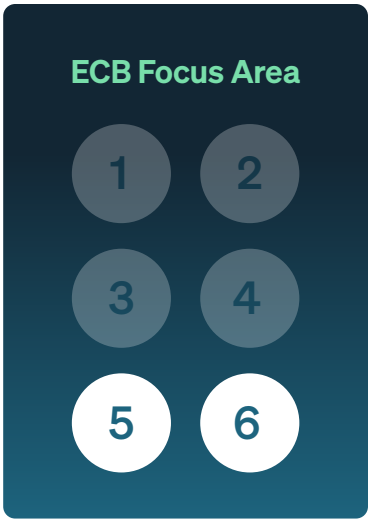


Active Directory Compromise and Ransomware Exposure

From SYSTEM-level access, NodeZero safely accesses LSASS and finds credentials belonging to a domain administrator. It uses those credentials to compromise the first domain, north.sevenkingdoms.local.

NodeZero then uses the compromised domain-administrator access to execute a golden-ticket attack, compromising the parent domain, sevenkingdoms.com. In the demonstrated environment, the path proves enterprise-wide domain compromise and ransomware exposure.

The important point is that the route emerged as the environment revealed new opportunities: an exposed file, a service credential, an authenticated application weakness, a cloud identity, a privileged Azure runbook, an internal implant, a domain credential, SQL access, SYSTEM privileges, and domain-administrator access.

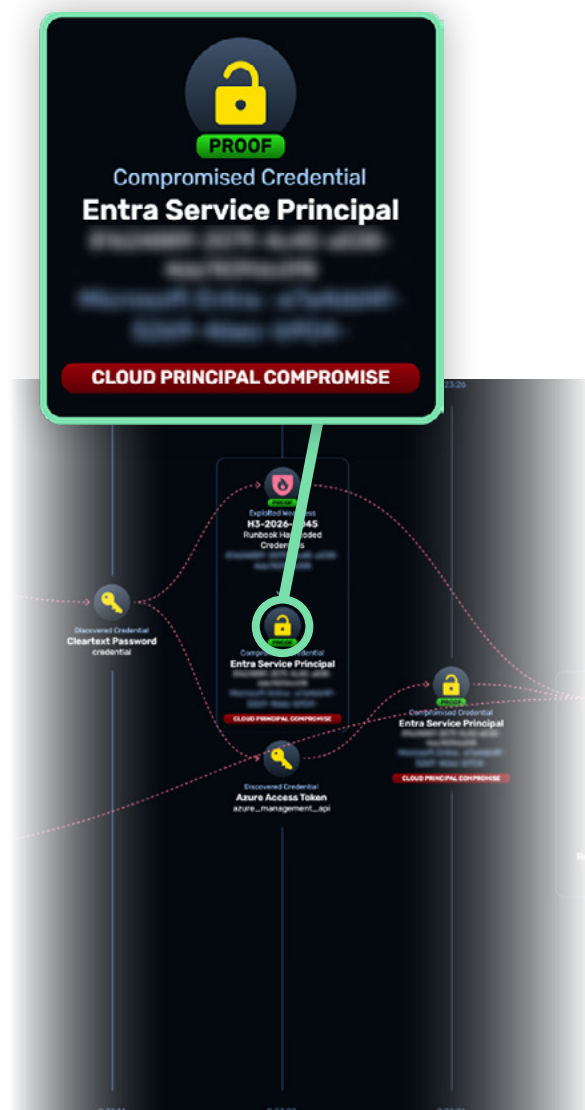
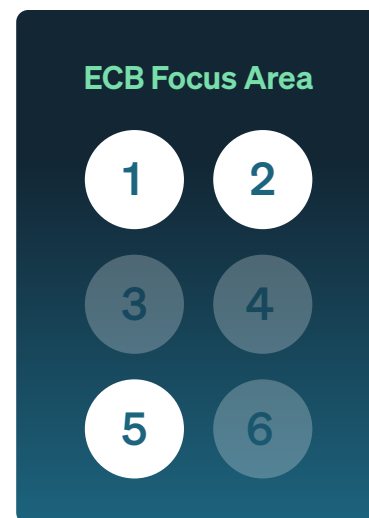


Prioritizing Remediation

Showing the attack is only half the value. The attack graph also shows where different teams can reduce risk and how to sequence remediation.

The exposed .env file should be removed immediately. The authenticated path-traversal vulnerability requires a code-level fix. The cloud credentials exposed in the application configuration and Azure runbook should be rotated and removed from clear text. The Active Directory credential exposure should be corrected, and SQL permissions and remote-execution paths should be constrained.

There is not always one universally correct place to start. The initial-access weakness may require an emergency fix, while the downstream identity, privilege, and segmentation weaknesses represent critical defense-in-depth work. Closing the first door matters; removing the conditions that allow an attacker to cascade through the environment matters too.



Why this matters for your Oct 31 submission

A single validated attack path can give institutions concrete evidence for the parts of the ECB Action Plan that concern exposed assets, exploitable application and identity weaknesses, cloud and internal reachability, least privilege, segmentation, and risk-based remediation. It should be combined with separate evidence for monitoring and detection, management oversight, third-party assurance, incident response, recovery, and information sharing.

Why Horizon3 (not a point solution)

NodeZero is the only platform that autonomously chains web application, identity, cloud, and infrastructure into one validated attack path. That path is production-safe, replayable, and verified closed, and the same evidence powers what your leadership and regulators actually need to see.

Closing the Remaining Gaps

The following capabilities round out a defensible Oct 31 submission:

Risk-Based Exposure Management (RBEM) + Vulnerability Prioritization (VP):

Re-score scanner findings against validated attack paths so teams can distinguish theoretical volume from weaknesses that create a credible route to material impact. In this demonstration, the custom path-traversal weakness and the credentials that enabled cloud and internal access are higher-value remediation points than an undifferentiated list of findings.

Remediation verification:

Retest the code fix, credential rotation, runbook change, AD correction, SQL-permission change, and remote-execution restriction to confirm that the relevant path is closed or materially reduced.

Recurring validation:

A recurring cadence can create continuity beyond a point-in-time assessment.

Detection and response validation:

Use the demonstrated chain as a scenario for testing application, access, cloud, network, endpoint, and identity telemetry.

Quantifiable Impact and Real-World Validation

Proven Results in Tier-1 Financial Institutions

During an initial autonomous internal test at a Tier-1 global financial services organization, NodeZero operated for less than 14 hours and identified:

- 3 unmanaged Domain Compromise paths leading to full administrative control.
- 586 critical business-impact exposures, including over 7.2 million files accessible through improperly scoped global permissions.
- 117 hosts where administrative rights were acquired by abusing standard domain user credentials.

INSTITUTIONAL TRACK RECORD

330,000+

production-safe autonomous penetration tests completed globally.

7,000+

corporate and banking networks continuously tested.

4 of the Fortune 10

trust NodeZero

Zero

production downtime across autonomous penetration tests

Next Steps for Technical Teams and JST Alignment

As significant institutions build their 31 October 2026 Action Plan, replacing theoretical compliance checks with continuous, proof-based exposure management provides a defensible posture for JST reviews and horizontal ECB audits.

- Request a Demonstration: Speak to a Horizon3 representative to discuss how you can plan your response.
- Access Technical Research: Review the technical paper, Hacking the Hackers: Can You Still Deceive an AI Attacker?, for AI deception benchmarks.
- Watch the Briefing: Access Decoding the ECB's AI Cyber Letter for Banks, featuring former ECB Executive Board member Yves Mersch.