HORIZON3.ai

~~TRUST BUT~~ VERIFY

WHITE PAPER

From War Room to Board Room

How Operationalized Pentesting Reduces Exploitable Risk and Strengthens Your Security Narrative

WAR ROOM

The Most Dangerous Window in Cybersecurity

The most dangerous time for a CIO or CISO isn't when a breach occurs—it's the window between discovering an exploitable weakness and verifying it's fixed. If attackers strike during that "window of opportunity", the board won't ask about tooling or telemetry—they'll ask one thing:

Why wasn't it fixed faster?

A decade ago, security leaders could plead ignorance. Today, that excuse is off the table. Regulatory bodies, shareholders, and the SEC have established a **Duty to Know** expectation. Leadership is accountable not just for what they knew, but for what they *should have known*—and what they did about it.

Most security programs don't fail at identifying issues—they fail at acting quickly to fix and verify remediation. Traditional pentests surface risks but often result in static reports that sit untouched. Worse, they offer only a snapshot in time, while the environment continues to change. To truly reduce exposure, organizations must shift to an **operationalized pentesting model**—one where each finding becomes a trigger for cross-functional action, and progress is assessed continuously to determine whether security posture is improving over time.

This shift doesn't just reduce your attack surface—it gives you the metrics, insights, and credibility needed to communicate risk effectively to the board.

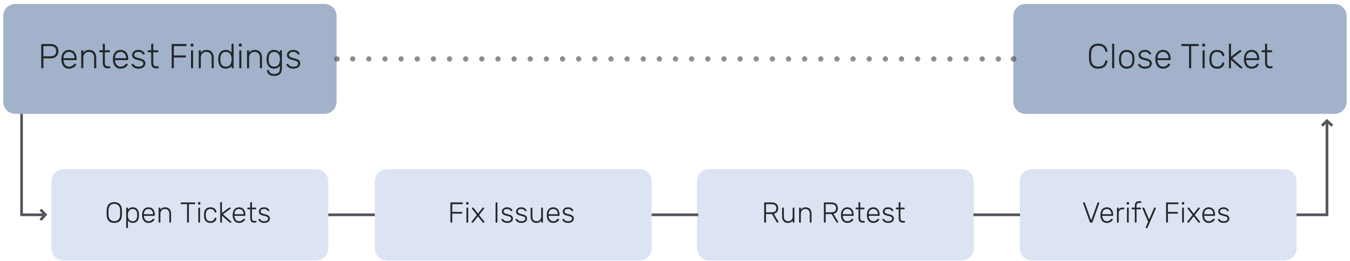


Image 1: Operationalize Pentesting: Test + Remediation Loop

The most dangerous time for a CISO is between finding an exploitable vulnerability and remediating it.

From Static Reports to Action: The War Room Approach

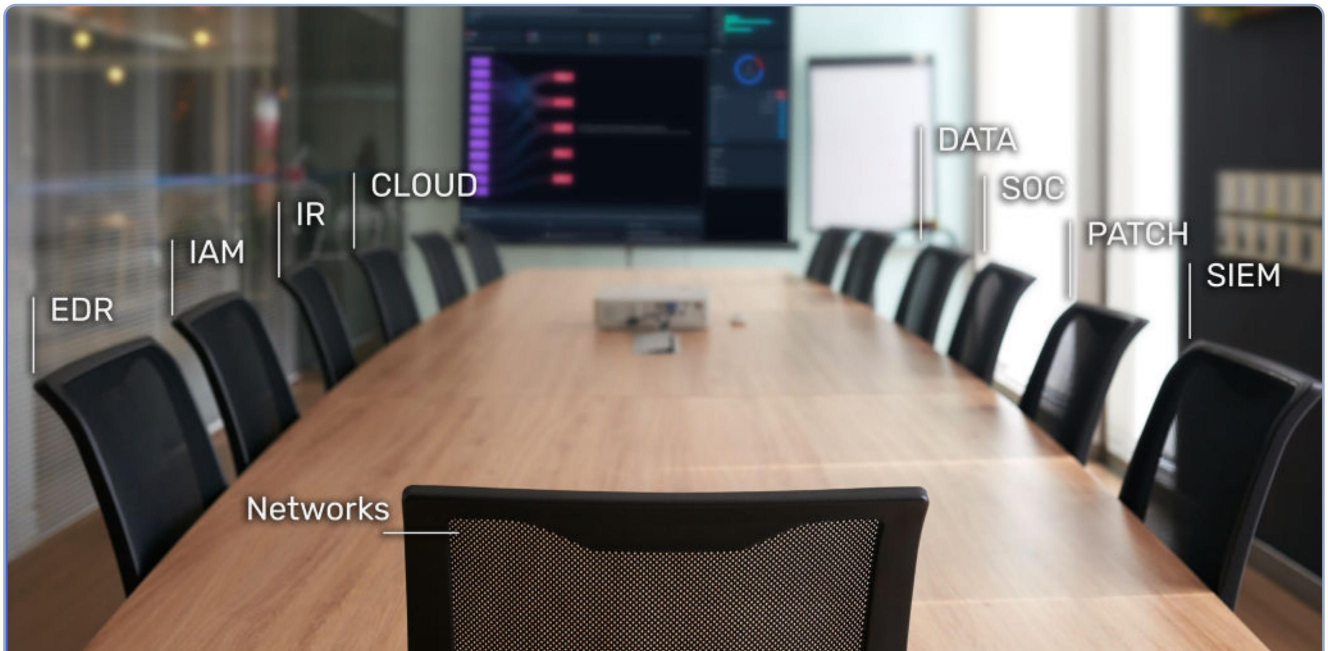
Once a pentest proves a critical attack path, every second counts. The response shouldn't be a PDF report—it should be a **War Room**: a focused, cross-functional initiative to understand the findings, drive remediation, verify fixes, and tune defenses.

1. Assemble the Right Stakeholders

The War Room isn't a meeting—it's an operational command center.
It should bring together:

- **SIEM Engineers** – Confirm which attack paths triggered detections and which went unnoticed.
- **EDR Analysts** – Validate endpoint defense capabilities.
- **Incident Response Leads** – Rehearse containment procedures for proven attack paths.
- **Network & Infrastructure Teams** – Address segmentation gaps and lateral movement opportunities.
- **IAM Owners** – Eliminate credential weaknesses and excessive privileges.
- **Patch & Application Teams** – Prioritize urgent fixes and coordinate rollout.
- **SOC Operators** – Tune alert logic and reduce detection blind spots.
- **Cloud & Data Teams** – Identify at-risk assets across hybrid environments.

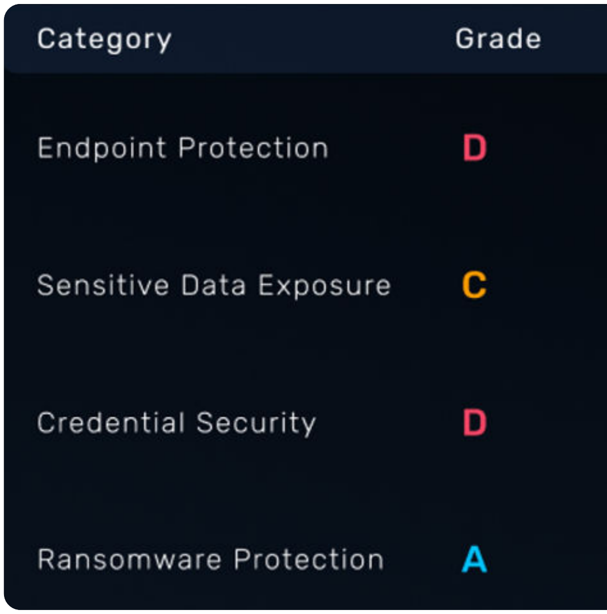
Image 2: The War Room



2. Deconstruct the Exploitable Attack Surface

The War Room's job is to treat every proven attack path like it's been exploited in the wild:

- **What was detected:** Did existing security controls trigger alerts on attack paths?
- **What was missed:** Were there silent failures in SIEM, EDR, or logging configurations?
- **What's the business impact:** How severe is the risk associated with each finding?
- **What are our mitigation options:** Can we remediate immediately, or do we need compensating controls?
- **Who owns the fix, and what's the timeline:** Can we define clear action items, owners, and timelines?



Category	Grade
Endpoint Protection	D
Sensitive Data Exposure	C
Credential Security	D
Ransomware Protection	A

Image 3: Security Category vs. Grading System

This isn't just about fixing vulnerabilities. It's about improving detection, reducing response time, and building institutional muscle memory.

What weaknesses should I fix first?

Why didn't my EDR block the RAT?

What logs can I add to my SIEM to improve MTTD?

Are there any "band aids" I can apply to buy me time?

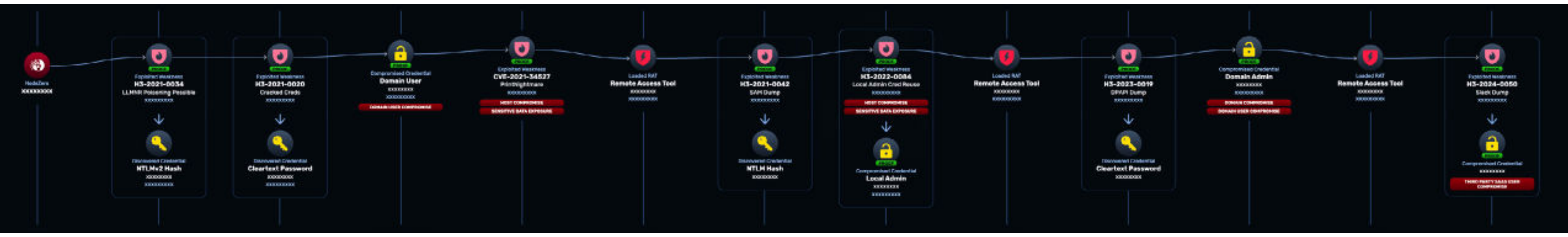


Image 4: Example of a NodeZero® Attack Patch with Multiple Vulnerabilities and Weaknesses

3. Deploy Honey Tokens and Validate Response Readiness

As part of your security validation efforts, honey tokens can be strategically deployed along confirmed attack paths. These decoys serve as early-warning signals—if an adversary retraces those steps during or after an engagement, alerts will trigger, but only if your security operations center (SOC) is prepared to detect and respond. The incident response (IR) and SOC teams should ensure:

- Each honey token is explicitly mapped to a known attack path.
- Tabletop exercises are conducted regularly to validate containment strategies.
- Alerting pipelines are configured to surface honey token activity immediately within SIEM and SOAR platforms.

This proactive approach transforms the SOC from a passive monitor into an active defense function—reducing both Mean Time to Detect (MTTD) and Mean Time to Contain (MTTC).

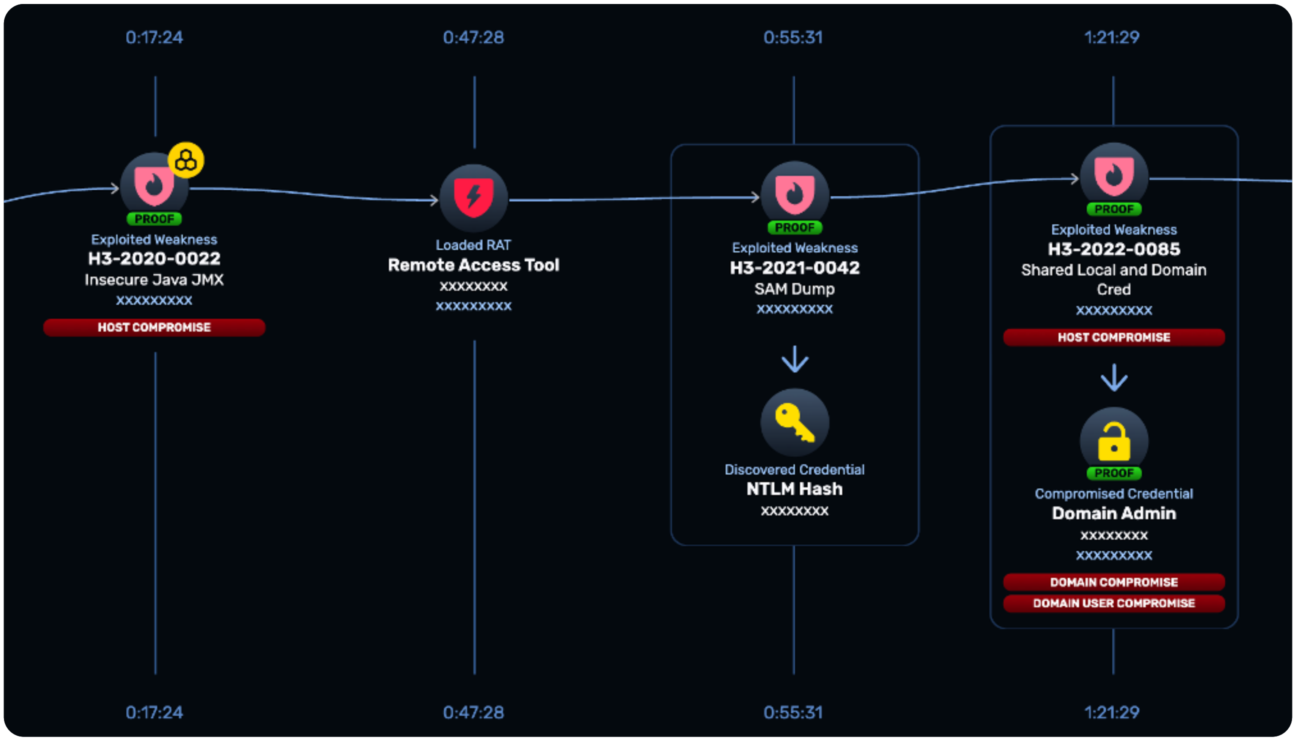


Image 5: Example of NodeZero Tripwires™ Integrated into Incident Response Processes

Deploy NodeZero Tripwires

Direct Tripwires to place decoys onto specific assets.

Configure NodeZero Alerts

Send Tripwire alerts to SOC team and push to SIEM.

Build Incident Response Process

Verify internal IR processes are operational for each Tripwire.

4. Fix Fast. Then Verify.

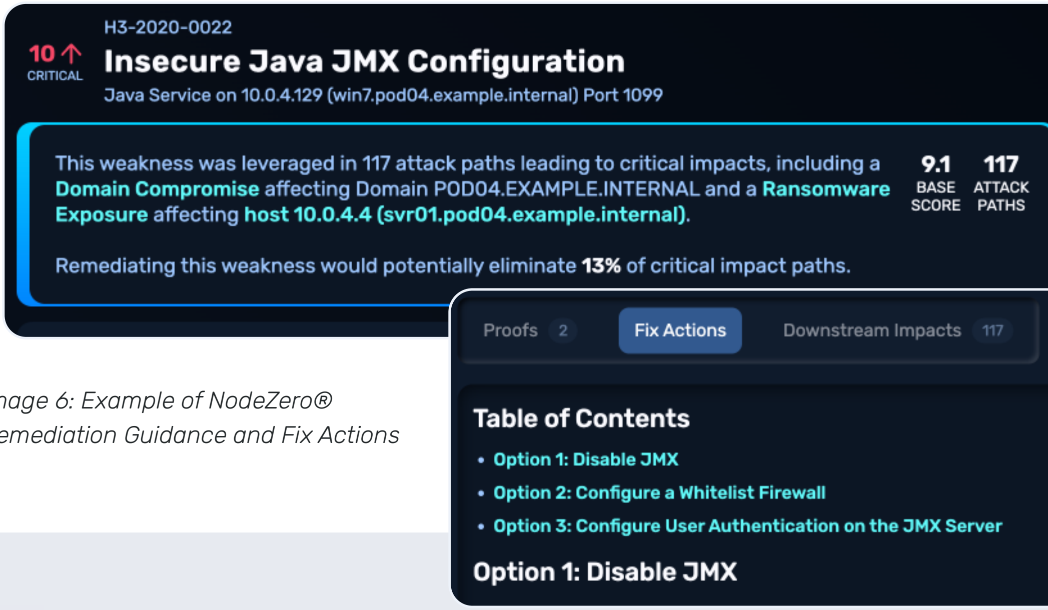
Discovery is only the beginning. What matters most is how quickly you can remediate—and prove the issue is truly resolved.

Hold daily standups to track open issues, assign clear ownership, and identify blockers.

Use targeted retesting tools to validate that fixes are effective in real time.

Set service-level agreements that reflect the urgency of the risk: critical paths should be verified within hours, not weeks.

Validation isn't optional—it's the only way to ensure that remediation efforts actually reduce risk.



10 ↑ CRITICAL

H3-2020-0022

Insecure Java JMX Configuration

Java Service on 10.0.4.129 (win7.pod04.example.internal) Port 1099

This weakness was leveraged in 117 attack paths leading to critical impacts, including a **Domain Compromise** affecting Domain POD04.EXAMPLE.INTERNAL and a **Ransomware Exposure** affecting **host 10.0.4.4 (svr01.pod04.example.internal)**.

Remediating this weakness would potentially eliminate **13%** of critical impact paths.

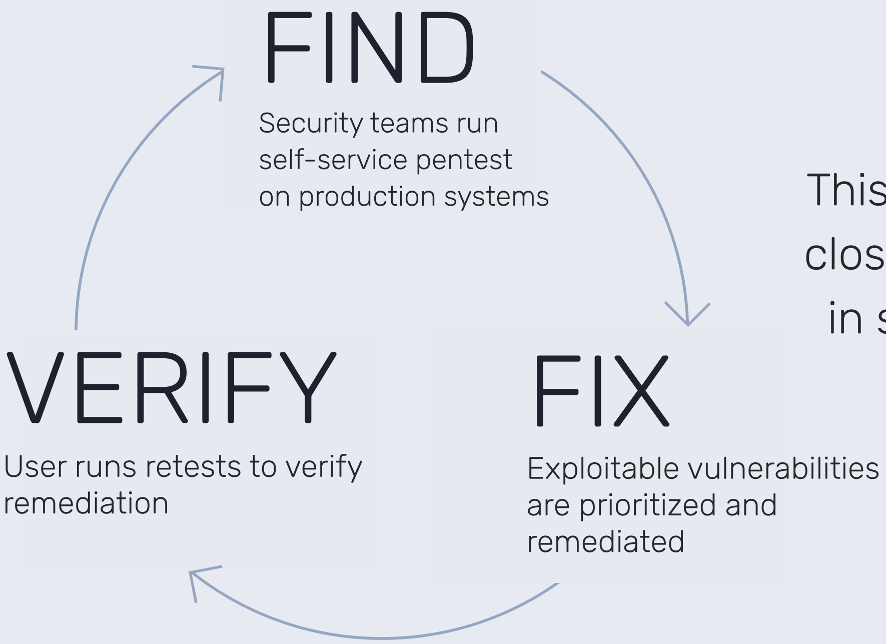
9.1	117
BASE SCORE	ATTACK PATHS

Table of Contents

- Option 1: Disable JMX
- Option 2: Configure a Whitelist Firewall
- Option 3: Configure User Authentication on the JMX Server

Option 1: Disable JMX

Image 6: Example of NodeZero® Remediation Guidance and Fix Actions



FIND

Security teams run self-service pentest on production systems

FIX

Exploitable vulnerabilities are prioritized and remediated

VERIFY

User runs retests to verify remediation

Image 7: Find, Fix, Verify Loop

This tight loop—*find, fix, verify*—closes the most dangerous gap in security: the time between knowledge and action.

HORIZON3.ai

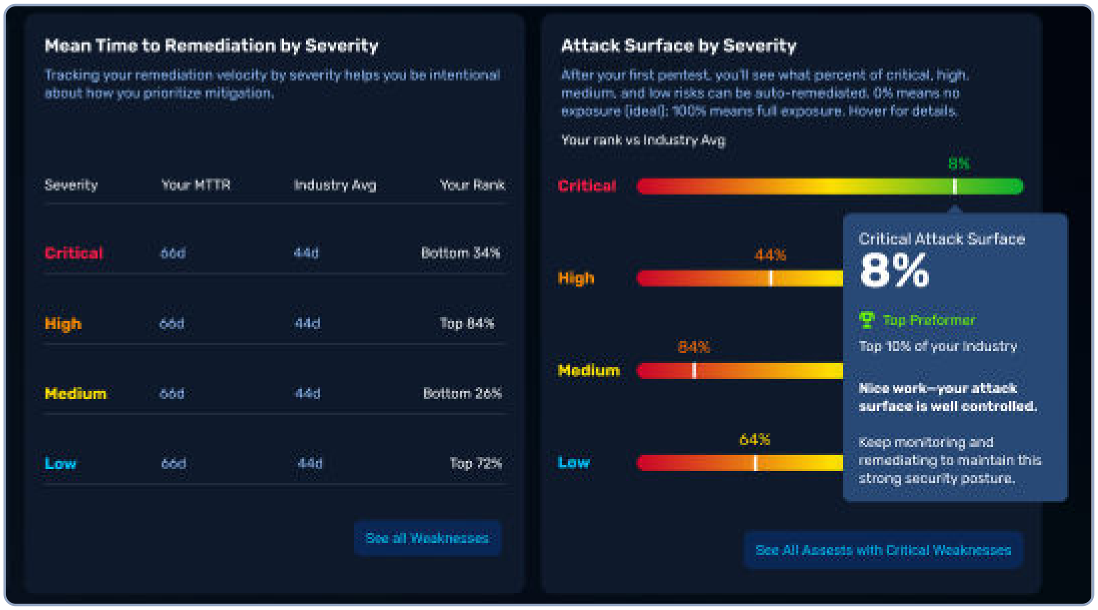
~~TRUST BUT~~ VERIFY

Peer Comparisons and Budget Justification: A Data-Driven Approach Centered on MTTR

In today's risk-averse environment, numbers speak louder than words—especially when justifying cybersecurity investments to the board. Among the most powerful metrics is Mean Time to Remediation (MTTR), which measures how quickly your organization can find, fix, and verify the remediation of exploitable weaknesses—while simultaneously confirming the effectiveness of your SOC's detection and response capabilities.

But MTTR isn't just an internal benchmark—it's a competitive one.

Peer comparison data shows how your MTTR stacks up against similar organizations. This lets you move beyond gut feel or vague metrics, and instead offer a data-driven, defensible case for continued investment in your people, processes, and platforms.



Mean Time to Remediation by Severity

Tracking your remediation velocity by severity helps you be intentional about how you prioritize mitigation.

Severity	Your MTTR	Industry Avg	Your Rank
Critical	66d	44d	Bottom 34%
High	66d	44d	Top 84%
Medium	66d	44d	Bottom 26%
Low	66d	44d	Top 72%

Attack Surface by Severity

After your first pentest, you'll see what percent of critical, high, medium, and low risks can be auto-remediated. 0% means no exposure (ideal); 100% means full exposure. Hover for details.

Your rank vs Industry Avg

Critical Attack Surface

8%

Top Preformer

Top 10% of your industry

Nice work—your attack surface is well controlled.

Keep monitoring and remediating to maintain this strong security posture.

Image 8: Example of NodeZero Insights™ Peer Comparison

> "Our MTTR is now 40% better than the industry average. That translates into faster remediation, less exposure time, and a tangible reduction in operational risk."

Whether you're defending your current budget or requesting more resources, peer-based MTTR benchmarking creates a clear link between technical execution and business value. It reframes cybersecurity as an area of measured performance improvement, not just expense.

Using MTTR to Justify, Communicate, and Prove

1. Justify Investment

When paired with peer data, MTTR becomes a board-ready metric.

> “We reduced MTTR by 60% over two quarters. That means faster remediation, tighter risk windows, and greater ROI on our security stack.”

2. Communicate Risk in Leadership Terms

Executives may not understand CVEs or kill chains, but they grasp time and exposure.

> “We’re now mitigating exploitable issues 40% faster than our peers—giving us a clear operational advantage.”

3. Prove Progress Over Time

MTTR provides a measurable way to track security maturity.

> “Quarter over quarter, MTTR is improving. That proves our War Room model and operational investments are working.”

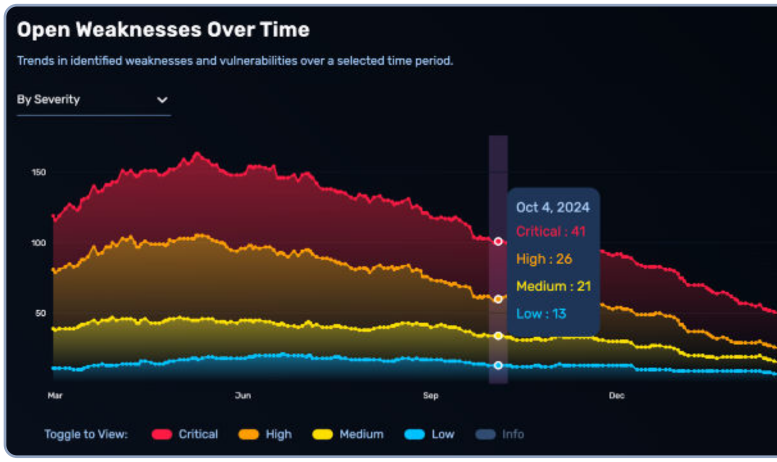
Boardroom Takeaways: Turning Ops Into Narrative

At the executive level, cybersecurity must be framed as a business risk—not a technical exercise. It’s the responsibility of the teams who oversee pentests to equip the CIO and CISO with clear, data-driven insights that translate security outcomes into credible board-level narratives.

Key Takeaways Should Include:

- **Exploitability Reduction**
  "We've gone from 11 critical attack paths to 3— all monitored by honey tokens now deployed."
- **SOC Performance**
  "MTTD improved from 12 hours to 2. MTTR dropped from 4 days to 10 hours."
- **Risk Ownership Transparency**
  "Five gaps remain. Without resourcing, they stay exploitable—and that's a risk the board must explicitly accept or fund us to mitigate."

These takeaways shift the conversation from technical noise to business risk management—and clarify where accountability truly sits.



Open Weaknesses Over Time

Trends in identified weaknesses and vulnerabilities over a selected time period.

By Severity

Image 9: Example of NodeZero Insights™: Open Weaknesses Over Time

Conclusion: Collapse the Gap. Own the Narrative.

Cybersecurity success depends on your ability to collapse the gap between knowing and doing. By operationalizing pentest findings through a War Room model, organizations can:

- Shrink their exploitable attack surface
- Tune SOC detections and incident response
- Prove real-world improvements in MTTD and MTTR
- Communicate a credible risk narrative to leadership

This is what separates mature security programs from those that fail under scrutiny.

It's not about whether you test. It's about how fast you act on the results.

That's the new standard. That's what leadership expects.

Many of the images in this paper come from Horizon3.ai's NodeZero® Platform, NodeZero Tripwires™, and NodeZero Insights™.

@Horizon3ai ✉ info@horizon3.ai www.horizon3.ai