



LOOKING AHEAD IMMERSIVE ONE / EBOOK / 2026

Training builds skills. Immersive proves them.

A CISO guide to moving from training metrics to measurable cyber resilience.

www.immersivelabs.com



Executive summary

Training still matters. It builds the skills any serious security program requires to succeed. But it is no longer a sufficient proxy for resilience. The gap between activity and proof is now both too wide and too visible. Boards want confidence, regulators want evidence, and critical incidents expose the chasm between training exercises an organization has completed and how it actually performs under the pressure of a real attack.

CISOs need to build role-relevant capability, test performance in realistic conditions, compare progress in context, and explain the result in a language leadership can use.

CISOs need to build role-relevant capability, test performance in realistic conditions, compare progress in context, and explain the result in a language leadership can use.

- Measure performance, not just participation.
- Benchmark scores against peers, roles, and frameworks so the data becomes actionable.
- Report cyber readiness in a format the board, regulator, insurer, and wider business can use.
- Keep exercises aligned to current threats so improvement remains relevant.

“

Immersive One matters because it does not stop at content delivery. It helps a CISO move from activity to proof: building role-relevant capability, testing performance under pressure, benchmarking results in context, and reporting them as evidence that leadership can use. In that sense, resilience begins where training ends.

Eric Johnson,
CRO, Immersive

01 Why training metrics stop short of readiness

Benchmarking matters because it shows where confidence and capability diverge. In the 2025 Cyber Workforce Benchmark Report, Immersive found that while many organizations felt prepared for a cyber crisis, they performed far less effectively when put into controlled simulations. The gap was not marginal. It was structural.

In the study, 94% of organizations said they believed they would be effective in a crisis. Yet in a controlled crisis simulation, average decision accuracy was only 22%. In other words, confidence was high, but performance under pressure was weak, and the data revealed a dangerous readiness gap.

The same disconnect appeared in program maturity. 71% of respondents described their readiness programs as very or extremely mature. Yet resilience scores remained flat and median response times did not improve. The implication is straightforward: many organizations are measuring motion and mistaking it for progress.

What it tells a CISO

- Confidence is not the same as operational readiness.
- Partial or slow engagement is not evidence of fast, coordinated response.
- Maturity language can disguise stagnant capability.



AVERAGE DECISION ACCURACY IN CRISIS SIMULATION **22%**

SAY THEIR READINESS PROGRAM IS VERY OR EXTREMELY MATURE **71%**

SAY DRILL PERFORMANCE MET OR EXCEEDED EXPECTATIONS

85%

AVERAGE COMPLETION AND 29 HOURS TO FINISH THE CRISIS SIMULATION

81%

THE PROBLEM

For a CISO, the real value of benchmarking is that it moves the conversation beyond training activity, self-assessment, and maturity labels, and towards demonstrated performance. It shows whether teams can actually make decisions, coordinate across functions, and improve response over time. It also gives leadership something far more useful than reassurance: an external point of reference for how ready the organization really is.

Benchmarking also points to why progress stalls. Many teams continue to rehearse legacy vulnerabilities and older CVEs rather than the threats shaping today's risk environment. Many programs stop at fundamentals and fail to build intermediate and advanced capability. Non-technical functions such as legal, communications, HR, and executive leadership are often excluded from realistic exercises, even though those groups shape the response to and outcome of a real crisis. And framework alignment too often leans toward checklist compliance rather than the tactics, mitigations, and decisions that matter in the wild.



“ Training is foundational, but it is not sufficient.

Aniket Menon

Chief Product
Officer, Immersive

02 What a readiness program has to deliver

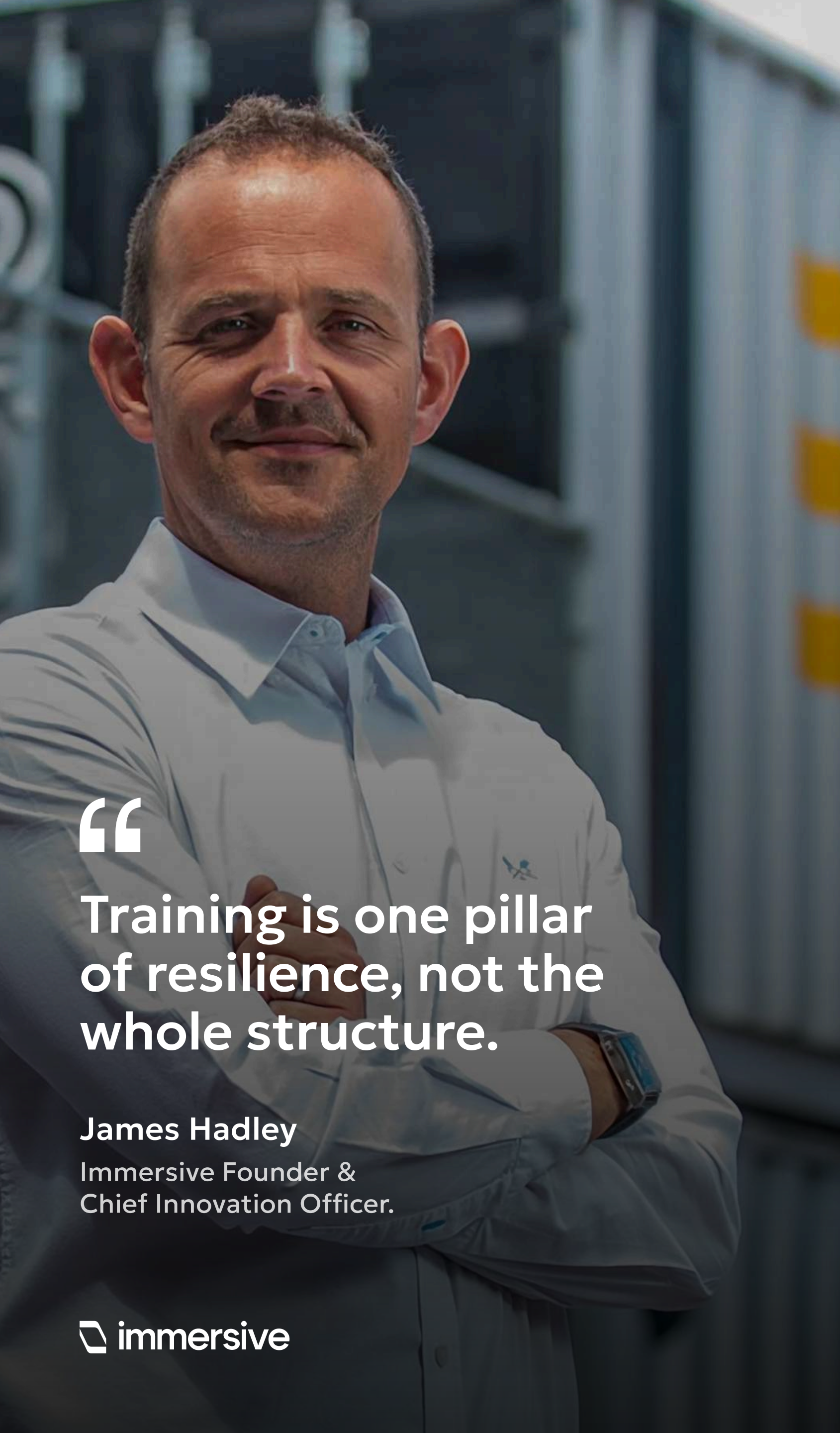
A readiness program cannot stop at skill-building, which is where many organizations still fall short. They run training, measure completions, and assume progress is happening, but they do not always close the loop between capability, performance, context, and evidence. The result is a program that can describe activity without proving readiness.

A stronger model is both simpler and more demanding. A readiness program must build role-relevant skills, prove performance under pressure, benchmark the result in context, and report evidence in a form leadership can use. Each stage strengthens the next.

Training without proving creates false confidence. Proving without benchmarking creates isolated scores. Benchmarking without reporting creates context with no consequence. Reporting without real capability underneath it becomes theater.

This table shows what that closed-loop model looks like in practice, what each stage produces, and why it matters to a CISO.

Stage	Achieved Through	Evidence Generated	Why it matters
Build capability	Hands-on labs, role-based paths, secure coding, cloud, workforce, and AI content develop capability where the organization actually operates.	Mastery signals, uptake, completion by role, and improvement over repeated attempts.	Shows whether the workforce is becoming more capable rather than merely more active.
Prove performance	Crisis simulations, cyber drills, range exercises, and leadership participation test how teams and leaders behave in realistic conditions.	Decision quality, coordination quality, detection and escalation metrics, and after-action observations.	Exposes the gaps that course completion cannot reveal.
Benchmark performance	Peer comparison, resilience scoring, heatmaps, and framework views put results in external and organizational context.	Industry and regional position, team-by-team comparison, trend, and framework coverage.	Answers the question every board member asks: is this good, and where do we need to act?
Report evidence	Executive dashboards, after-action reports, audit-ready outputs, and exports convert raw telemetry into leadership-grade narrative.	Board packs, regulator-ready views, insurer evidence, and traceable improvement stories.	Turns cyber activity into a business decision tool.



“

Training is one pillar of resilience, not the whole structure.

James Hadley
Immersive Founder &
Chief Innovation Officer.



THE MODEL

Training, labs, drills, and programs do more than build capability. They create the performance data a CISO needs to baseline readiness, measure change over time, and show whether investment is reducing risk. That is what turns learning activity into a resilience program.

“ When the board asks, prove it.

Training is just one pillar of resilience. On its own, training can build knowledge and improve technique. What it cannot do is prove whether an organization will perform under pressure, how that performance compares to past or industry peer performance, or what leadership should do next.

That is why readiness has to be run as a program, not just a training activity. The program is the mechanism that connects these stages into one operating model: building capability, testing it in realistic conditions, measuring the result in context, and turning that result into evidence the board, regulator, and business can act on. That is where the platform becomes more than a content engine. It becomes the system through which resilience is developed, tested, benchmarked, and made visible.

The next section explains how Immersive One supports that program model in practice, and how each part of the platform helps a CISO move from skill-building to demonstrable resilience.

13 Why benchmarking is strategically important

What CISOs increasingly need is a way to assess human cyber capability proactively, baseline it, score it today, track it over time, and benchmark it against peers.

That is what gives a resilience score strategic value. Without that context, a number can show movement, but not whether the organization is strong, improving from a weak base, or still lagging behind.

That matters because benchmarking does more than explain performance; it shapes decisions. In the Executive Readiness Pack, recommendations such as increasing MITRE ATT&CK coverage, improving completion of advanced technique paths, and extending exercises beyond cyber teams are not generic program suggestions. They are benchmark-led actions tied to resilience score, comparative standing, and the outcomes the business ultimately cares about. For a CISO, that is the difference between reporting a number and defending a position.

Question leadership asks	What benchmarking adds	Decision it enables
Is our score actually good?	Peer percentiles, industry averages, regional context, and time-series trend.	Whether to hold course, accelerate investment, or reset expectations.
Which team or role is weakest?	Side-by-side comparisons by role, team, and function.	Targeted coaching, path assignment, and scenario design.
Are we aligned to recognized controls and real threats?	Framework mapping across MITRE ATT&CK, NIST, DORA, and other control views.	Where to focus exercises, upskilling, and reporting evidence.



THE MODEL

It also changes the footing of the board conversation. Without benchmarking, the CISO is left defending effort: we ran the program, completed the drills, and improved the metrics. With benchmarking, the argument becomes grounded in strategy: here is how we performed, here is how that compares with organizations like ours, and here is where further action is justified. In a field with few true absolutes, relative position matters. It is what allows a score to become evidence rather than reassurance.

“What we do is wider than training.”

As Immersive CEO Mark Schmitz puts it, “What we do is wider than training. It encompasses benchmarking, reporting, exercising, program-building, and the activity-driven information that sits around all of that.” That is the key point.

Benchmarking is not the end of the story. It is the point at which measurement stops being internal and becomes useful to leadership. The next step is reporting: turning comparative performance into data the board, regulators, insurers, and businesses can actually use.

04 From cyber activity to leadership evidence

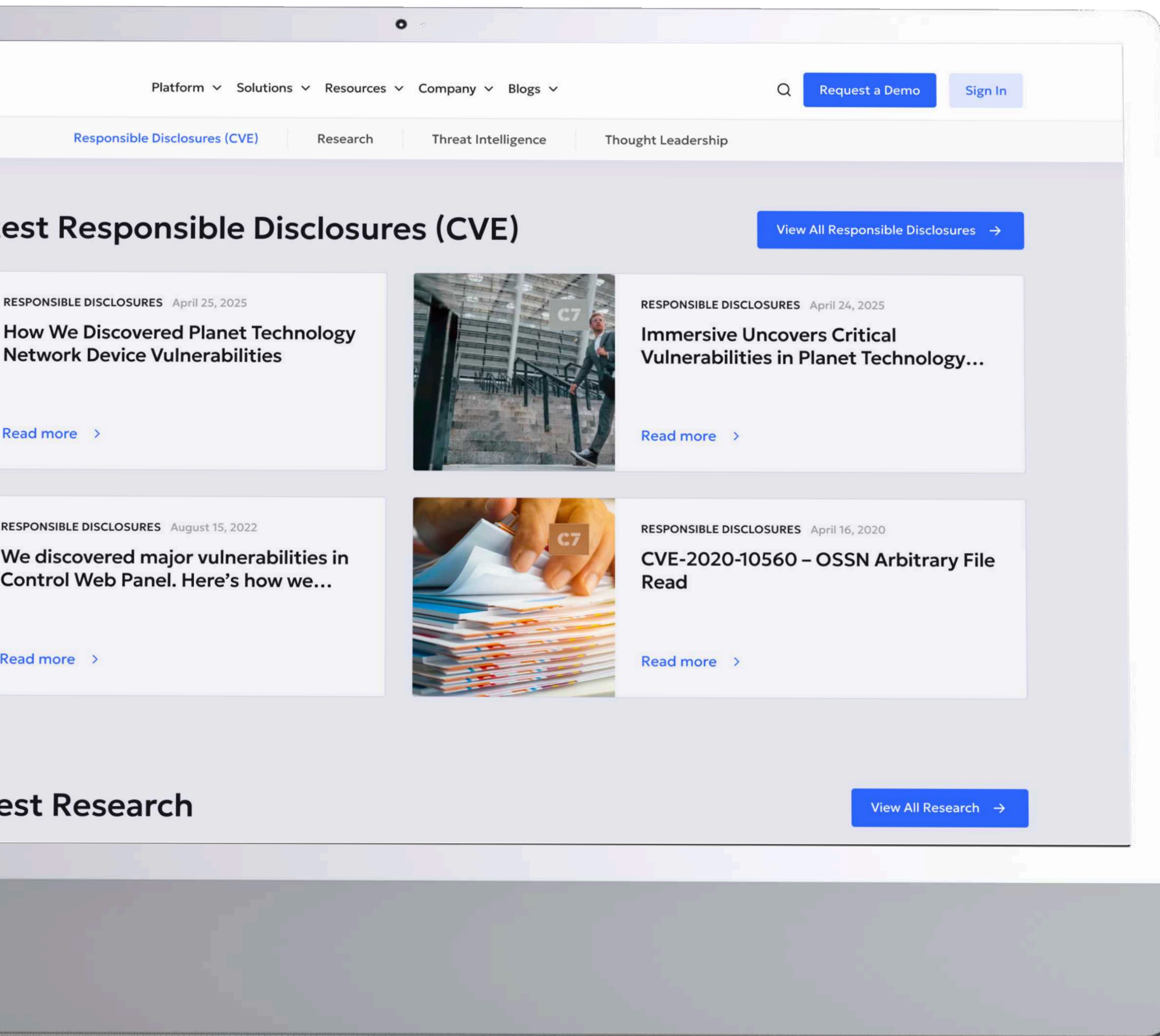
Labs, drills, exercises, and crisis simulations create value in practice. But for a CISO, that value only matters when it can be turned into evidence. Boards, regulators, auditors, and insurers do not need a list of completed activities. They need proof that the organization has a real program for improving resilience over time. Reporting is what turns performance data into that proof: a clear view of posture, movement, exposure, and the actions leadership should take next.

In Immersive One, that means turning performance into a control view leadership can use: resilience scores, benchmark context, framework mappings, after-action findings, role and team gaps, and executive-ready summaries.

The point is not to generate more dashboards. It is to give the buyer a defensible view of readiness and a report the board, regulator, or auditor can actually use.

What matters is not producing one generic report. It is creating the right evidence for the people who need to make decisions from it.

Audience	What they need to see	Typical evidence from Immersive One
Board and CEO	A clear view of current resilience, movement over time, top exposures, and the actions leadership should fund or sponsor.	Resilience score dashboard, trend, board pack, priority actions.
CISO and CRO	Improvement deltas, benchmark position, team gaps, and evidence that investment is changing risk.	Benchmark views, evidence logs, framework mapping, executive dashboard.
SOC and incident leaders	Drill timelines, response metrics, task completion, and decision quality.	After-action reports, timeline replay, MTTD and MTTC views.
Legal and compliance	Continuous evidence mapped to frameworks and disclosures.	Framework heat maps, DORA/ NIST/MITRE mappings, control-gap views.
HR and L&D	Capability gaps by role, path progress, and completion patterns.	Role matrices, assignment uptake, and learning-path views.
Finance and insurer stakeholders	Evidence that resilience is improving and that operational risk is becoming more legible.	Exporter views, risk narrative, and trend metrics.



THREAT CURRENCY

05 Why expertise matters

Reporting shows leadership where readiness stands. Expertise keeps that picture current.

One of the clearest findings from the benchmark is that many teams are still training against the past. When more than 60% of training focuses on older CVEs, teams are practicing for battles already fought. A readiness program only becomes strategically useful when it is fed by current threat intelligence, live vulnerability research, and a clear view of how attacker behavior is changing.

Enter Container 7, Immersive's technical research and threat intelligence team. Its work does not sit on the sidelines as commentary. It feeds the platform itself: new and updated labs, threat-aligned exercises, crisis simulations, and expert insight on emerging threats. In the most recent Forrester Wave™: Cybersecurity Skills And Training Platforms, Q1 2026, Forrester explicitly notes that Immersive's rapid content updates are driven by its in-house research team, with Container 7 research powering new scenarios across current adversary tradecraft and AI attack techniques.

What matters is not producing one generic report. It is creating the right evidence for the people who need to make decisions from it.

06 What a board-ready data actually looks like

The Executive Readiness Pack is where the program becomes visible to leadership. It is not a training transcript and it is not a generic dashboard export. It is the control view of readiness: a leadership-ready document that shows where the organization stands, how it compares, what is driving the result, and what leadership should do next.

A strong readiness pack should show six things clearly:

- | | |
|----|---|
| 01 | Current posture and trends, so leadership can see whether resilience is improving or stalling. |
| 02 | Benchmark context by industry, region, and role, so the board’s first question — is this good? — can be answered with evidence rather than assertion. |
| 03 | Operational performance, including threat response, technical skills, and ATT&CK coverage, so the organization can see whether teams are actually improving where it matters. |
| 04 | Evidence mapped to frameworks and controls, including compliance and secure-code views, so progress is visible in a language regulators and auditors recognize. |
| 05 | Current and emerging threat insight, so the discussion stays anchored in what matters now, not last year’s curriculum. |
| 06 | Specific recommendations and targets for the next period, so the report drives action rather than just observation. |



EXECUTIVE REPORTING

That sequence matters because it mirrors how leadership consumes risk. What is our position? How does it compare? What is driving it? What do we do next? The Executive Readiness Pack turns cyber activity into a clear, defensible view of resilience that can be used with the board, regulators, insurers, and internal leadership alike.

07 What CISOs can achieve with Immersive One

CISOs are responsible for delivering certain outcomes. Counting how much content exists is not one of them. CISO accountability rests on showing which outcomes improve, which gaps remain, and which evidence can be taken into the boardroom.

CISO priorities stem from specific pain points: a response that is too slow, exposure that is too broad, evidence that is too weak, leadership that is underprepared, and a business that keeps adding new risks through AI, suppliers, and modern infrastructure. The role of Immersive One is to help turn those pressures into measurable improvement, defensible evidence, and clearer board-level confidence.

“

What we do is wider than training. It encompasses benchmarking, reporting, exercising, program-building, and the activity-driven information that sits around all of that.

Mark Schmitz
CEO, Immersive

WHAT CISOS CAN ACHIEVE WITH IMMERSIVE ONE

CISO outcome	Why it matters	How Immersive One helps
Faster detection, response, and decision-making	Breach impact is driven by time and decision quality.	Crisis simulations, cyber drills, ranges, and hands-on containment labs expose coordination gaps and create after-action evidence.
Secure the modern enterprise across code, cloud, OT, and identity	The attack surface lives in what teams build and operate every day.	Secure coding, cloud, identity, OT/ICS, and network labs help teams fix real weaknesses and validate improvement in practice.
Enable secure AI adoption and human-agent readiness	AI expands both opportunity and risk; the handoff between agents and people is a new weak point.	AI security labs, AI threat simulations, and role-based pathways test whether teams can deploy, monitor, and challenge AI safely.
Turn compliance into evidence and benchmarks	Boards, regulators, and auditors want proof mapped to recognized frameworks.	Framework mapping, resilience scoring, peer benchmarking, and executive reporting convert exercises into evidence packs.
Build and retain a verifiable cyber-ready workforce	Talent shortages, slow onboarding, and uneven capability leave visible gaps.	Role-based paths, workforce exercises, skills progression, and guided onboarding make capability measurable by role and team.
Strengthen third-party and supply-chain resilience	A vendor event becomes a business event very quickly.	Third-party scenarios and cross-functional crisis simulations test escalation, communications, legal response, and leadership decision-making.



HOW TO START

18 A 90-day plan to prove progress against the right CISO outcomes

The first ninety days are not about launching every capability at once. They are about baselining the six outcomes that matter most, selecting the two or three that matter most to the business this quarter, and producing the first evidence pack that proves movement. Start with the pressure you are under, then work back to the outcome, the exercise plan, and the reporting cadence.

CISO Pressures	Outcome to Work Against	Actions to Take in the First 90 Days	Proof Delivered by Day 90
Board or regulator wants defensible evidence	Transform compliance into evidence and benchmarks	Run one cross-functional crisis simulation, map activity to NIST / MITRE / DORA, and stand up a monthly executive and quarterly board cadence.	First Executive Readiness Pack, framework heat map, benchmark view, and after-action report.
Application, cloud, or identity risk is growing	Secure the modern enterprise	Baseline developer, cloud, and identity roles, assign targeted labs to the biggest gaps, and rerun with current-threat content.	Gap heat map, remediation uplift, and stronger coverage across code, cloud, and ATT&CK views.
The business is pushing AI quickly	Enable secure AI adoption and human-agent readiness	Baseline AI pathways, run one AI or agentic workflow scenario, and define the human review checkpoints that matter.	AI readiness baseline, handoff gaps, and a next-quarter plan for safe adoption.
Hiring is slow and capability is uneven	Build and retain a verifiable cyber-ready workforce	Map roles, assign role-based paths, and measure first-attempt versus latest-attempt improvement for new hires and priority teams.	Skills-gap matrix, onboarding benchmark, and visible progression by role.
Third-party exposure is becoming a board issue	Strengthen third-party and supply-chain resilience	Run one compromised-vendor scenario with legal, comms, HR, and executives; then update escalation and communications protocols.	Third-party after-action report, decision gaps, and an updated response plan leadership can act on.
Response is too slow when it matters	Prove faster detection, response, and decision-making	Run one end-to-end incident and crisis exercise across SOC, IR, communications, and leadership. Baseline detection, escalation, containment, and decision timings, and capture where handoffs break.	After-action report, response-time baseline, escalation gap map, and a prioritised plan to reduce delay next quarter.

A portrait of Aniket Menon, a man with dark hair and a slight smile, wearing a dark blue blazer over a light grey t-shirt. He is standing in front of a blurred background that appears to be an office or library with bookshelves.

“

**Training alone isn't enough...
if you want real organizational
resilience, you need more
capabilities around it.**

Aniket Menon
Chief Product
Officer, Immersive



CONCLUSION

19 Training builds skills. Resilience proves itself.

For a CISO, the implication is straightforward. Training still matters, but it should be treated as the foundation, not the proof. The real question is whether skills are translating into performance, whether that performance is improving in the right areas, and whether the evidence can stand up in the boardroom.

That is where Immersive One is strongest: not as a content library, but as a readiness platform. It helps organizations build role-relevant capability, prove performance under pressure, benchmark results in context, and report evidence in a form leadership can use. That is what connects day-to-day learning to the outcomes a CISO is actually judged on.

That is also why benchmarking, reporting, and expert threat intelligence matter so much. Together, they turn training into something more valuable than activity: proof. Proof of how teams perform, proof of how the organization compares, and proof of what leadership should do next. In the end, that is the shift this whole guide is arguing for. Training builds skills. Resilience proves itself.

Be Ready



Continuously Assess, Build,
and Prove Your Cyber Resilience

Our immersive cybersecurity solutions ensure
your team is prepared to tackle and defend against
the evolving cyber risks of today, and tomorrow.

