FORRESTER
WAVE
LEADER 2023
Cybersecurity Skills
And Training Platforms

IMMERSIVELABS

Assess, Build, and Prove Cyber Workforce Resilience

The Value of Immersive Labs

Welcome

We measure human performance in many facets of life, from sports to university exams and professional certifications. We have become adept at understanding and quantifying an individual's ability in many areas, but there is a blind spot that has often eluded precise measurement: how well a team works together.

Cybersecurity resilience is now a Board-level concern. Directors are increasingly being held accountable for security alongside other types of business-level risks. This has led to increasing scrutiny as **Board members are demanding visibility into cybersecurity risks** and organizational capabilities and readiness.

This spotlight has led to the uncomfortable truth that current approaches aren't working. Tools and technology are not enough to ensure resilience; the capabilities of individuals and teams are just as important. At the same time, **the current approach to people-centric cybersecurity isn't up to the task**. Certifications are failing us. Cybersecurity professionals spend hours obtaining credits to maintain their certifications, which do nothing to improve their hands-on skills. Traditional methods of training are unable to upskill talent at all levels, leaving us with a skills gap that is growing exponentially. CISOs don't know how their teams will respond to a real-life crisis and are left holding the bag when a breach occurs. We need to approach team cybersecurity capabilities and performance with an entirely new level of rigor.

Advanced analytics are now pervading professional sports as statisticians attempt to compute each individual's contribution to team performance. It's time for a similar revolution in cybersecurity. We need to use realistic exercises that span from executives down to the most technical teams to unlock new levels of real-world performance measurement. We need to **know** how our teams will respond to an incident or breach.

If you are ready to assess, build, and prove cyber resilience for teams at all levels of your organization, Immersive Labs can be the strategic partner that can help you on this journey.

James Hadley
CEO, Immersive Labs

The human element continues to drive breaches. **This year 74% of breaches involved the human element.** Whether it is the use of stolen credentials, phishing, misuse, or simply an error, people continue to play a very large role in incidents and breaches alike.

Introduction

Immersive Labs is the leader in people-centric cybersecurity. We are pioneering an entirely new approach to assessing, building, and proving an organization's ability to effectively respond to the latest cyber threats - **Cyber Workforce Resilience**. Trusted by world's largest organizations and governments, our approach improves the cybersecurity capabilities of the entire workforce, facilitating a fundamental shift in how organizations think about team performance and risk reduction.

Customers tell us that "check-the-box" solutions like point-in-time training and certifications don't satisfy their need for tangible results. They struggle to fully understand the cybersecurity capabilities of their cybersecurity professionals, software developers, and the organization as a whole. Existing solutions can't provide them with the confidence that their teams are able to respond to the latest threats - and when they do feel prepared, they don't have the data to prove it to their Boards, customers, and regulators.

We believe that an organization's cyber resilience should be continuously measured, compared with industry benchmarks, and improved using real-world scenarios and realistic simulations. Gaps must be identified, invested in, closed, and re-evaluated. Teams should have the opportunity to continuously exercise their skills to ensure they are prepared to respond to the latest threats. As organizations adopt this data-driven approach, they are better able to mature their cybersecurity programs to achieve their business goals around risk reduction and cyber resilience.

Cyber Workforce Resilience Benefits

Cyber Workforce Resilience helps you move past legacy training and tabletop exercises to hyper-realistic labs and simulations that measurably improve - and prove - your cyber resilience. It's a challenge today to truly understand the capabilities of your people and teams and to know how they will perform in a crisis.

By partnering with Immersive Labs, you can understand and prove the cybersecurity capabilities your teams require to respond to today's threats. We can help you hire, train, and retain your cybersecurity talent.

Cyber Workforce Resilience prepares your defensive and offensive cybersecurity teams, cloud and application security practitioners, developers, and more.

Measurably Increase Resilience

Partnering with Immersive Labs leads to continuous improvements in cyber threat preparedness. The 2023 IBM Cost of a Data Breach report shows the average cost difference of breaches at organizations with these cost-influencing factors compared to the mean cost of a data breach of USD $4.45 million. Immersive Labs helps organizations with several of the most impactful factors that can **lower the average total cost of a breach by $1,069,674**:[1]

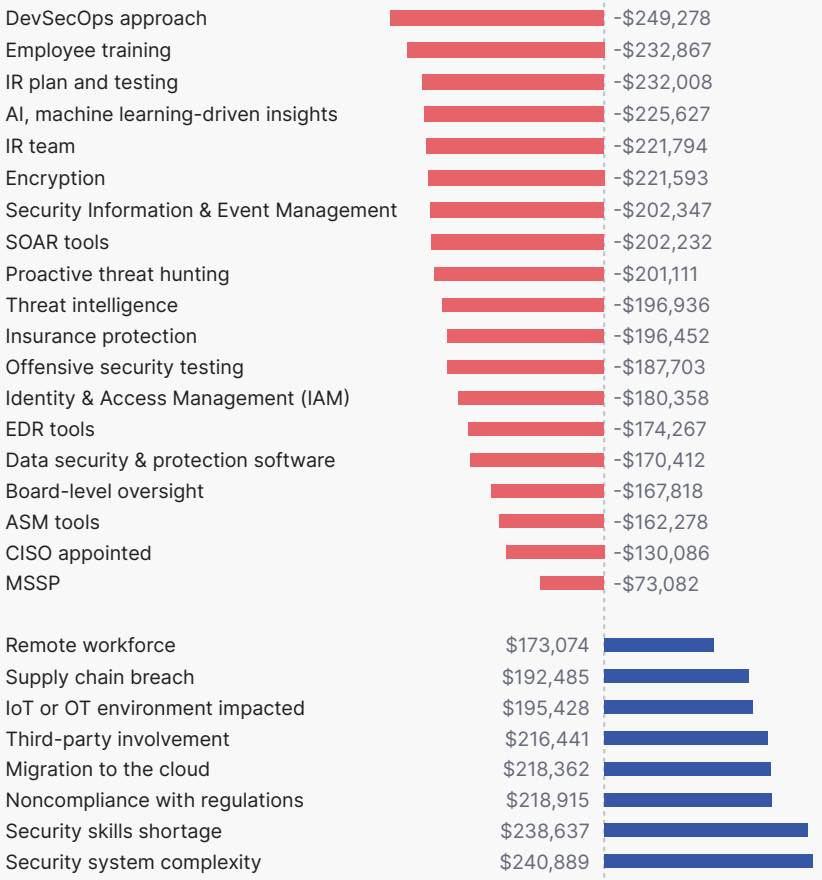
- **DevSecOps Approach ($249,278 reduction).** Prepare your Application Security teams and Developers to “shift left” - embedding security into the development process early.
- **Employee Training ($232,867 reduction).** Provide hands-on cybersecurity training for the entire workforce.
- **Extensive tests of the IR Plan ($232,008 reduction).** Immersive Labs Crisis and Team Simulations bring next-generation tabletop exercises to a distributed workforce - with measurable insights.
- **Board Level Oversight ($167,818 reduction).** Detailed reporting empowers Directors to make informed decisions about cyber resilience.
- **Red Team Testing ($187,703 reduction).** Build offensive capabilities in-house with advanced Labs, Simulations, and Cyber Ranges.

In addition, Immersive Labs can help avoid or mitigate an additional $465,136 in costs:

- **Security Skills Shortage ($238,637).** Identify talent in unexpected places with Candidate Screening
- **Compliance Failures ($218,915).** Identify and close gaps in people-centric cybersecurity.

[1] IBM, “2023 Cost of a Data Breach”

Impact of key features[1]



The Value of Immersive Labs

Immersive Labs helps customers achieve a measurable impact on improving resilience in the face of cyber threats. From identifying skill gaps to improving incident response times, Immersive Labs enables you to gain visibility into your current people-centric cybersecurity posture and measure improvement over time.

Business Outcomes

Immersive Labs drives three primary business objectives:

Reduce cyber risk

Build cyber capabilities to improve incident decision-making and response times.

Prove operational resilience

Use performance data to demonstrate cyber capabilities according to industry frameworks.

Facilitate compliance

Demonstrate cyber readyness to meet regulatory and other compliance requirements.

Key Value Factors

Immersive Labs helps our customers achieve their business objectives with a series of clearly-defined cybersecurity benefits:

Cybersecurity Benefits	Immersive Labs Value
Report on and prove current levels of cyber capability across the organization aligned to security frameworks	
Understand human cyber capabilities	Gain the visibility needed to identify gaps and areas of strength by comparing individual and team performance to industry frameworks and benchmarks. Extensive reporting at both the individual and team level enables cybersecurity leaders to identify and reduce specific organizational risks and vulnerabilities, such as gaps in coverage within the MITRE ATT&CK framework.
Measure progress using credible, well-understood metrics	Track both individual and team improvement using a combination of crisis and technical team simulations and individual training labs. Measure capabilities against baselines to document progress against goals.
Improve speed and quality of response to emerging threats	
Reduce incident response times while improving decision-making	Respond faster to cyber incidents with pressure-tested teams that regularly practice responding to real-world crisis scenarios. Improve technical defensive cybersecurity abilities to reduce the time to detect vulnerabilities, threats, and incidents of all types. The faster incidents are detected, the more risk and the cost of a breach are reduced. Incident response labs train individuals and teams on the latest techniques, including exercises and simulations on AI risks for all roles. With the development of incident response skills, the mean time to respond (MTTR) to incidents will decrease, reducing the breach severity and costs.
Reduce time to capability vs. emerging threats	Rapidly gain hands-on experience responding to emerging threats. The dedicated Immersive Labs response team produces exercises and simulations within hours of a new threat going live to help our customers prove their ability to stay current. For example, content for Log4Shell, Gitlab, UAParser, Apache, OMIGod, and Less.js was released in less than one business day.

Detect more threats	Threat Hunting labs provide practical, hands-on training specifically focused on improving individual and team abilities to identify threats. Labs range from Threat Hunting fundamentals to detailed analyses of the latest CVEs.
Effectively deal with cyber crises	Quickly and effectively dealing with a crisis can significantly reduce damage to the organization, resulting in quantifiable cost savings. The Immersive Labs Crisis Simulator enables teams across the entire organization to assess how they would perform in a cyber crisis using realistic, dynamic, challenging and engaging scenarios. Participating teams may include executives, cybersecurity, operations, and more - working together to respond to a crisis. Crisis simulations exercise and improve judgment, teamwork, and communications - ultimately improving crisis outcomes.

Increase efficacy in recruitment, retention and promotion

Identify and hire top-quality cybersecurity talent while reducing recruiting costs	Immersive Labs' Candidate Screening enables hiring managers to test for real-world cybersecurity capabilities, surfacing high-quality candidates who might otherwise have been overlooked by legacy application processes and certification requirements. This approach reduces bias in the hiring process and can lead to more diverse applicant pools. By assessing the cyber capabilities of each candidate entering into the recruitment process and ruleing out unsuitable candidates prior to the interview stage, organizations can reduce wasted time by recruiting teams and hiring managers.
Retain existing cybersecurity talent	Retaining skilled cybersecurity talent is a challenge with demand (and compensation) soaring. The opportunity to continuously develop in a role leads to greater job satisfaction, reducing turnover.

Reduce cloud and application vulnerabilities early and across the SDLC

Reduce vulnerabilities early and across the SDLC	Identify and address application security vulnerabilities and flaws with hands-on AppSec and DevSecOps labs. Labs include secure coding fundamentals, a deep-dive on the OWASP Top 10, Cryptography, TLS, and more.
Reduce cloud security vulnerabilities	Identify and address cloud security vulnerabilities and weaknesses with CloudSec labs, which provide hands-on training on Amazon Web Services (S3, EC2, SSM, etc.), NIST Guidelines on Public Cloud Computing, NIST Guidelines on Public Cloud Computing, the UK National Cyber Security Centre Cloud Security Guidance, DevSecOps fundamentals, and more.

Reduce cybersecurity costs and improve investment decisions

Consolidate cybersecurity training and capability management

Companies enjoy significant administrative and cost benefits when they can consolidate solutions. Immersive Labs provides people-centric security requirements for the entire organization, including defensive cybersecurity professionals, red team experts, application and cloud security practitioners, developers, and more. Organizations no longer have to manage point solutions for each aspect of their cybersecurity program. Everything is covered under one powerful platform with all of the data, management, and reporting available as a single point of reference.

Immersive Labs can replace in-person security training, as well as solutions focused only on areas such as application and cloud security.

Reduce reliance on third-party staffing and consultants

Third-party consultants are typically brought into an organization to fill a skills gap or support understaffed teams. By developing staff internally, the skill gap can be closed and security teams can be appropriately staffed, reducing or eliminating the need for expensive consultants.

Make informed, risk-based cybersecurity investment decisions

Focus investments according to risk that is based on evidence of capabilities, not opinions. The Immersive Labs platform provides management, executives, and Boards with the data they need to make more informed (evidence-based) decisions on investment in cybersecurity capabilities.

Reduce risk of regulatory fines

Immersive Labs provides management and organizational leadership with the confidence that their workforce can act in a risk-aware and a legally and regulatory compliant fashion. Unlike typical check-box training, Immersive Labs can provide the evidence that your workforce hasve the knowledge, skills, and judgment necessary to demonstrate compliance with various legal and regulatory requirements.

Measuring cyber capabilities across the organization, identifying and addressing vulnerabilities in your application or cloud security through to preparing your executives on how to respond to cybersecurity threats supports regulatory compliance and reduces the risk of potential fines.

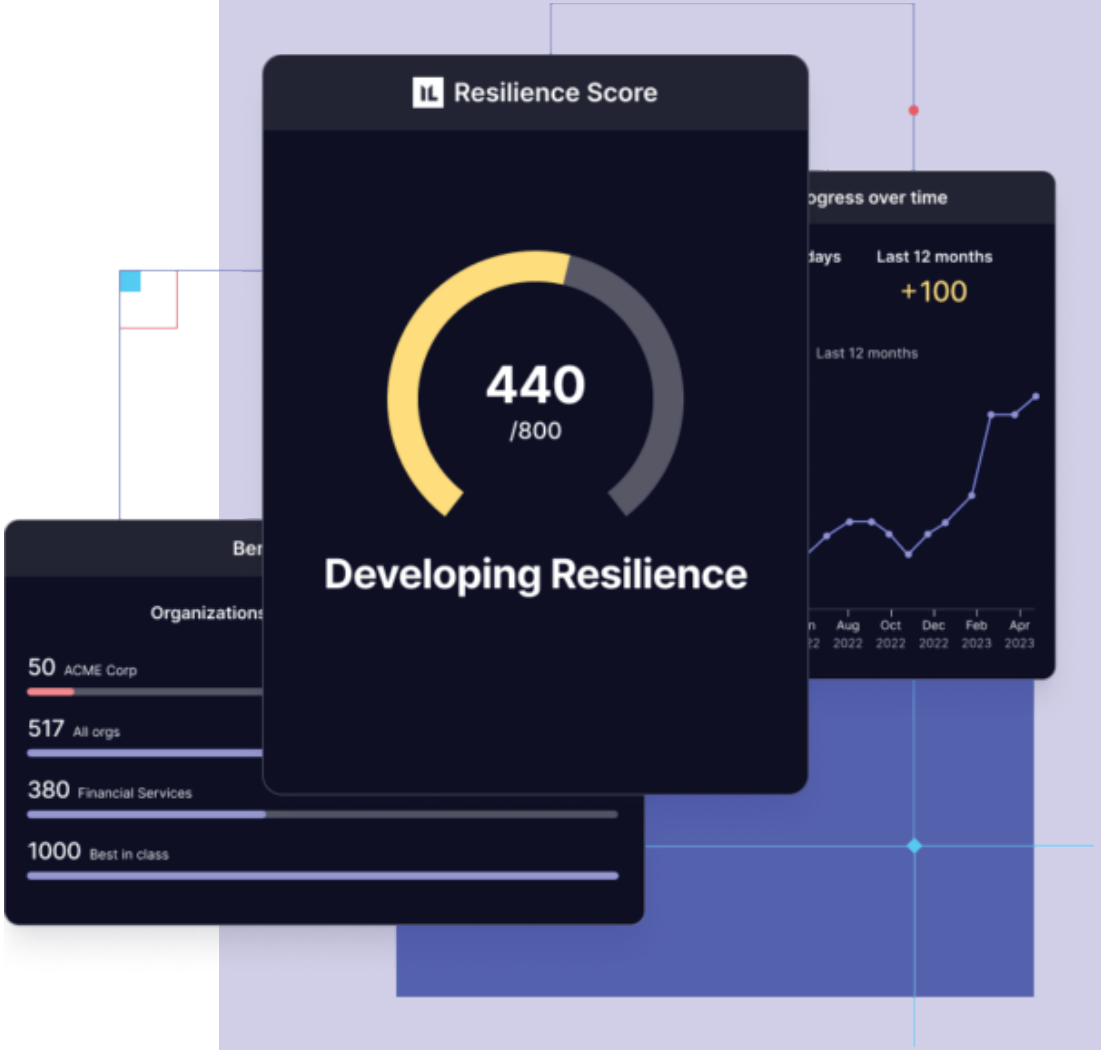
The Immersive Labs Resilience Score

How do you know your organization will be resilient in the face of ever-increasing and more sophisticated cyber attacks? The Immersive Labs Resilience Score uses advanced statistical techniques to demonstrate that resilience can be assessed, benchmarked, improved, and proven in a clear, data-driven way.

Confidence quantified

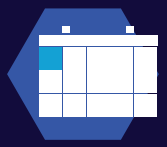
The Resilience Score is a single value that an organization can use to measure its overall cyber workforce resilience. The algorithm evaluates multiple factors using performance data from across the platform and enables organizations to understand:

- Their overall cyber resilience
- Trends and progress
- Comparisons to industry and best in-class benchmarks



Cyber Resilience Snapshot

Insights from the Immersive Labs 2023 Cyber Workforce Benchmark. We assessed teams like yours under real-world conditions. Here are the most eye-opening discoveries we made.



12
Months

1.1 million
Exercises and hands-on labs

Organizations continue to accelerate response times to threats.

Organizations' median response time to emerging threats improved by one third, indicating a significant increase in the speed of response and continued progress compared to the year prior. Enterprises have enhanced their knowledge about newly discovered threats and vulnerabilities, enabling them to respond more rapidly than ever before. The Log4j crisis, for example, was a watershed moment that could well have been a catalyst for this urgency given its catastrophic impact on organizations around the world.

Organizations aren't preparing their workforces enough for after-incident responses.

To effectively reduce risk, organizations must be prepared both before, and after, an incident. While organizations are ensuring that cyber resilience activities span the MITRE ATT&CK® framework, we observed a notable bias towards the earliest stages of the attack lifecycle, suggesting cyber leaders have room for improvement and are potentially leaving their organizations exposed to after-incident risk.

IMMERSIVELABS

Immersive Labs is the leader in people-centric cyber resilience. We help organizations continuously assess, build, and prove their cyber workforce resilience for teams across the entire organization, from front-line cybersecurity and development teams to Board-level executives. We provide realistic simulations and hands-on cybersecurity labs to evaluate individual and team capabilities and decision-making against the latest threats. Organizations can now prove their cyber resilience by measuring their readiness compared to industry benchmarks, building team capabilities, and demonstrating risk reduction and compliance with data-backed evidence.

Immersive Labs is trusted by the world's largest organizations and governments, including Citi, Pfizer, Humana, Atos, T. Rowe Price, and the UK National Health Service. We are backed by Goldman Sachs Asset Management, Summit Partners, Insight Partners, Citi Ventures, and Menlo Ventures.

Learn more | www.immersivelabs.com/
Book a demo | www.immersivelabs.com/demo/
Our blog | www.immersivelabs.com/blog/