immersive

E-Book

Assess, Build, and Prove Cyber Workforce Resilience

The Value of Immersive

Version: 01 | Published: Feb 2025

www.immersivelabs.com

Welcome

> “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.
>
> James Hadley
> Chief Executive Officer - **Immersive**

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 can be the strategic partner that can help you on this journey.

The human element continues to drive breaches. **This year 68% 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.

68%

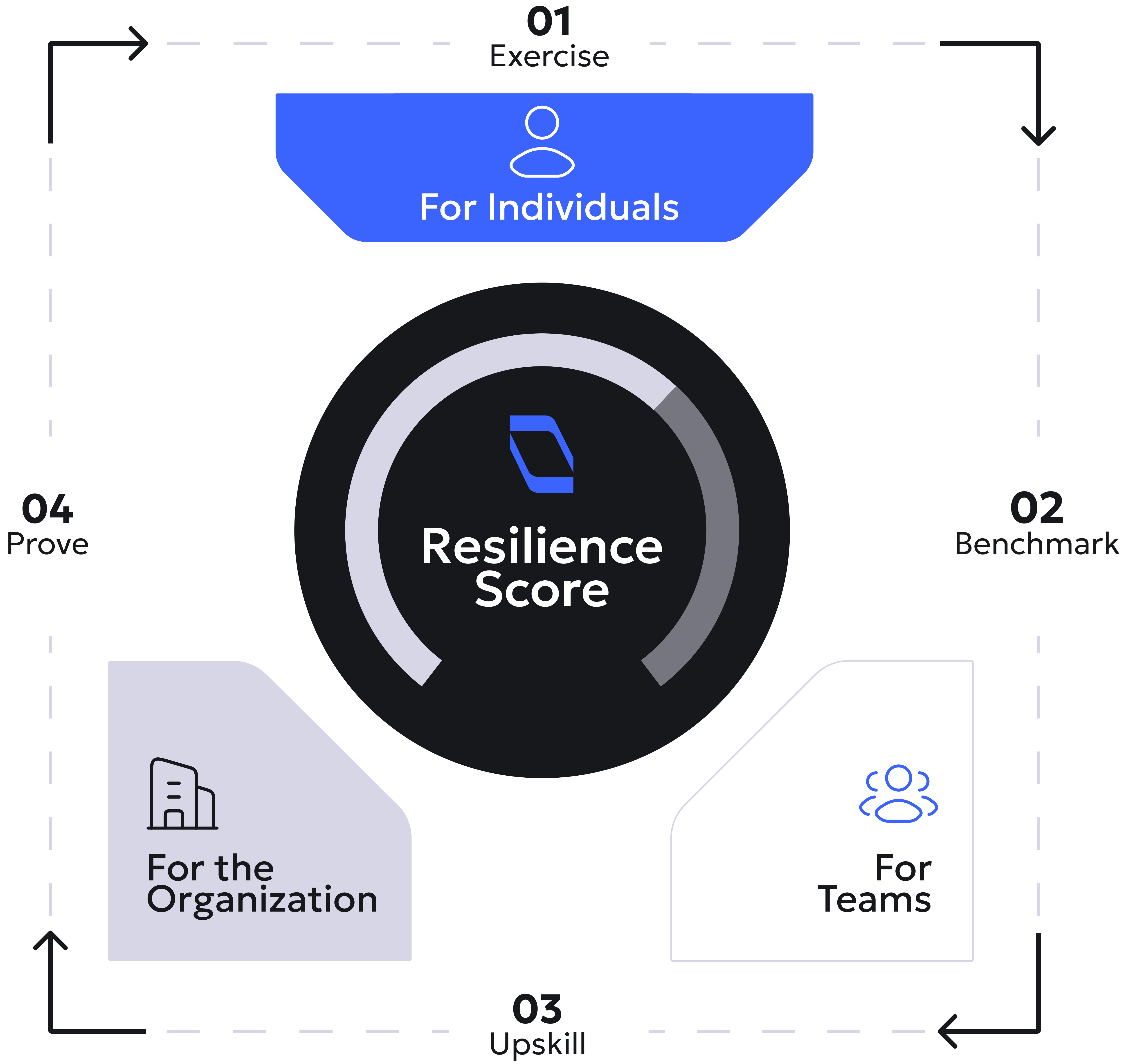
Human Element Involved Breaches

Introduction

Immersive is revolutionizing the way enterprises fortify their defenses by empowering organizations to continuously assess, build, and prove their ability to thwart cyber threats.

In a world where risks evolve at lightning speed, we offer a unified enterprise platform that gives leaders confidence that their people have the knowledge, skills and judgment they need to prepare for, and respond to, cyber attacks.

From the store room to the board room, we deliver tailored, immersive learning experiences that transform your entire workforce into an unbreakable organization.



Cyber Workforce Resilience

Benefits

Empowering Cyber Teams

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

Enhancing Threat Readiness

By partnering with Immersive, 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.

End-to-End Security Training

Cyber Workforce Resilience prepares everyone in every role: defensive and offensive cybersecurity teams, cloud and application security practitioners, developers, high-risk departments...a true store room to board room solution.

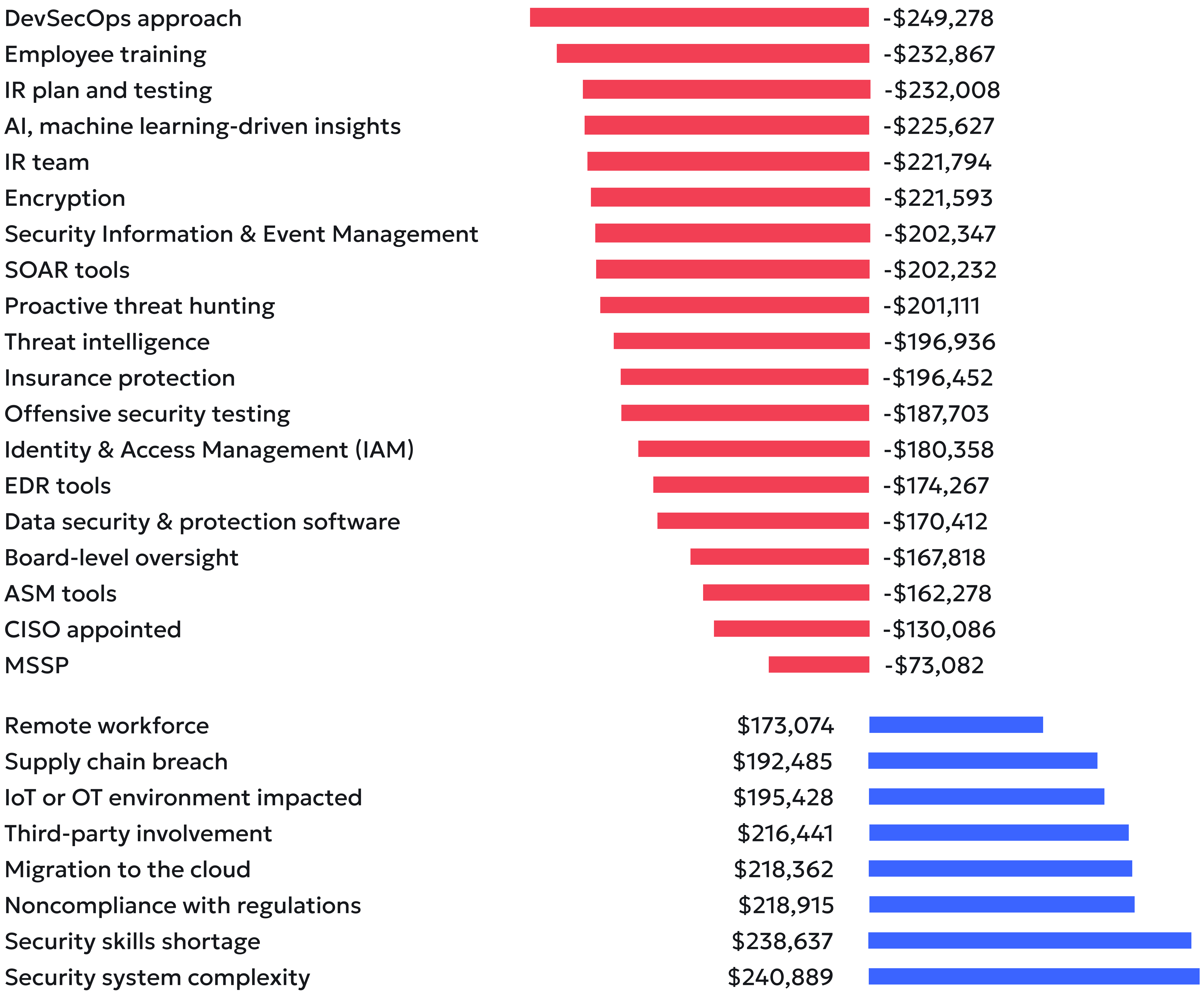
Increased Cyber Resilience

Measure

Partnering with Immersive 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 helps organizations with several of the most impactful factors that can lower the average total cost of a breach by $1,069,674: 1

Impact of key features [1]



Measurably Increase Cyber Resilience cont...

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 Crisis and Cyber Range Exercises 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 can help avoid or mitigate an additional **$457,552** in costs:

$238,637

Security Skills Shortage
Identify talent in unexpected places

$218,915

Compliance Failures
Identify and close gaps in people-centric cybersecurity

The Value of Immersive

With solutions for teams, individuals, and now the entire workforce, the Immersive Platform offers organizations four key benefits and differentiators compared to cyber training options on the market:

01

Proof of Resilience

Gain vital data enabling CISOs and other cyber leaders to be confident that they have a cyber resilient workforce.

02

Complete Organizational Coverage

Drive resilience for everyone in the organization, with unparalleled content tailored to every level of an organization for world-class breadth and depth.

03

Unified Enterprise Platform

Enjoy a seamless and tailored experience across individuals, teams, and the entire workforce in a single platform.

04

AI Ready

Benefit from industry leading advice and content to navigate and leverage the cyber impact of AI on the workforce.

Full Coverage, From the Storeroom to Boardroom

Immersive provides tailored learning experiences through the following solutions that can be run on a regular basis similar to live fire drills:

For the Entire Organization

Workforce Exercising provides broad and targeted learning opportunities for people in every role, filling the gaps left by traditional cybersecurity awareness training and using behavioral science techniques to drive measurable change in your workforce.

For Teams

We provide Crisis Simulations that go beyond typical tabletop exercises and Technical Exercises using sophisticated cyber range technology that can also be combined to take your organization to a new level of cyber readiness. We engage your teams, from Boards and Executives to your most technically skilled personnel in realistic scenarios to enhance their decision-making skills and prepare everyone to stand their ground in the face of cyber risk.

For Individuals

Immersive offers a gamified learning environment, covering the full spectrum of cybersecurity, from offensive and defensive strategies to cloud and application security. These labs equip individuals with the skills and acumen to neutralize them.

Key Differentiators

	Benefits		Value
01	Continuously prove cyber capabilities across the organization, aligned to security frameworks	→	Benchmark and prove readiness to your Board, auditors and insurers
02	Improve organizational response to business risks and emerging threats	→	Reduced breach costs and incident time; industry and corporate risk compliance
03	Increase efficacy in recruitment, retention and career development	→	Reduced recruiting costs and turnover
04	Reduce cloud and application vulnerabilities early and across the SLDC	→	Reduced developer remediation time/cost
05	Reduce cybersecurity costs and improve investment decisions	→	Save money and inform investment

Key Value Factors

Cybersecurity Benefits	Immersive Value
Improve speed and quality of response to emerging threats	
Reduce time to capability vs. emerging threats	Rapidly gain hands-on experience responding to emerging threats. The dedicated Immersive 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.
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.
Fill gaps in organizational knowledge with targeted interventions	Identify high-risk groups exposed to cyber threats, like finance, supply chain, legal and compliance. Arm them with labs covering everything from the basics to advanced theory and practice. Target interventions with on-demand labs based on actionable assessments for maximum impact.
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 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.

Cybersecurity Benefits	Immersive Value
Report on and prove current levels of cyber capability across the organization aligned to security frameworks	
Measure progress using credible, well understood metrics	Track both individual and team improvement using a combination of crisis and technical Cyber Range Exercises and individual training labs. Measure capabilities against baselines to document progress against goals.
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.
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.

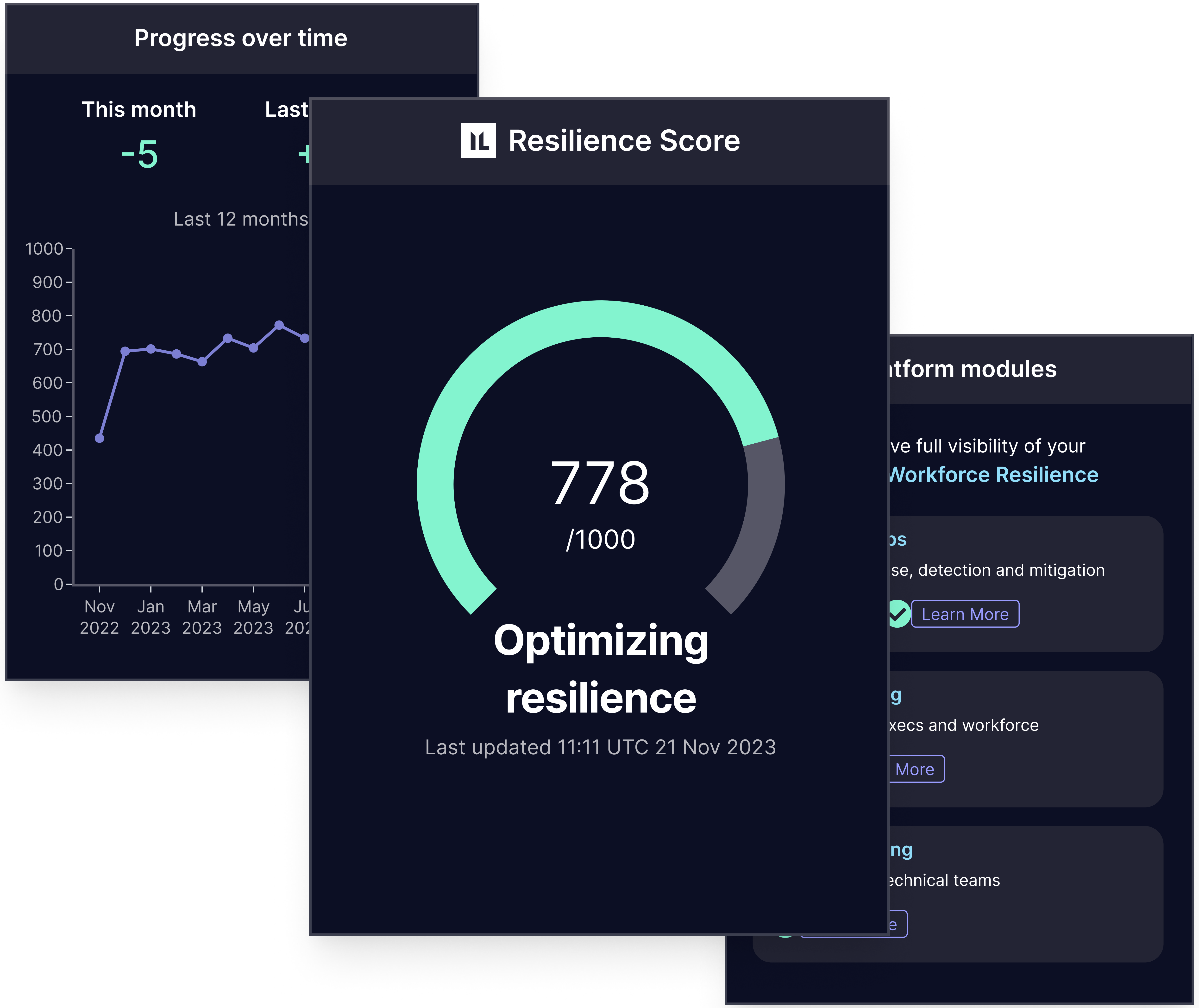
Key Value Factors

Key Value Factors

Cybersecurity Benefits	Immersive Value
Increase efficacy in recruitment, retention and promotion	
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 cybersecurity costs and improve investment decisions	
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 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 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 can provide the evidence that your workforce has 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 Resilience Score

How do you know your organization will be resilient in the face of ever-increasing and more sophisticated cyber attacks? The Immersive 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 2023 Cyber Workforce Benchmark. We assessed teams like yours under real-world conditions. Here are the most eye-opening discoveries we made.

1.1 M

Exercises and hands-on labs in 12 months

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 work forces 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.

Be Ready

immersive

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.