

Solution Brief

Build and Prove Cyber Workforce Resilience

Jan 2025







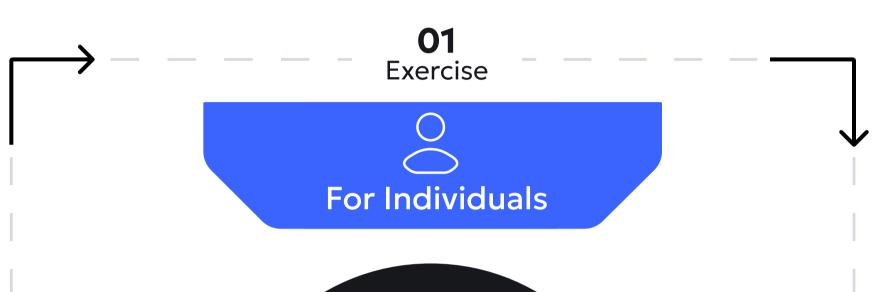


Continuously Build and Prove Your Cyber Workforce Resilience

How do you know your organization will be resilient in the face of ever-increasing and more sophisticated cyber attacks?

All the latest tools and technology are not enough to ensure resilience; people and teams must have the right capabilities and make the right decisions when it counts. We are pioneering an entirely new approach to peoplecentric cybersecurity that enables organizations to assess, build, and prove their ability to effectively prepare for, and respond to, the latest cyber threats.





In a world where risks evolve at lightning speed, true resilience requires people and teams to learn continuously and work together seamlessly.

At the same time, legacy check-box training and paper certifications aren't up to the task.

Trusted by world's largest organizations and governments, our Immersive Exercises and Labs improve the cybersecurity capabilities of the entire workforce, facilitating a fundamental shift in how organizations prove team performance and reduce risk, from the store room to the board room.



ForIndividuals

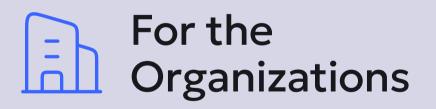
Hands-on labs offer engaging, gamified learning environments

- Defensive Cybersecurity Professionals
- Penetration Testers Developers



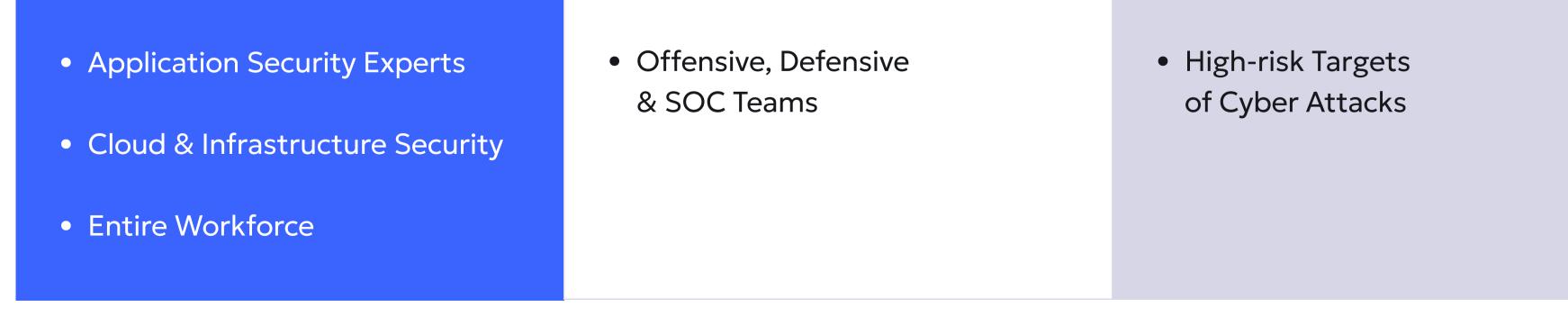
Team-based simulations from the store room to the board room

- Executive Teams
- Crisis Management & Incident Response Teams



Skills development exercises that drive transformative behavioral change

- Senior Leaders
- Front-line Employees





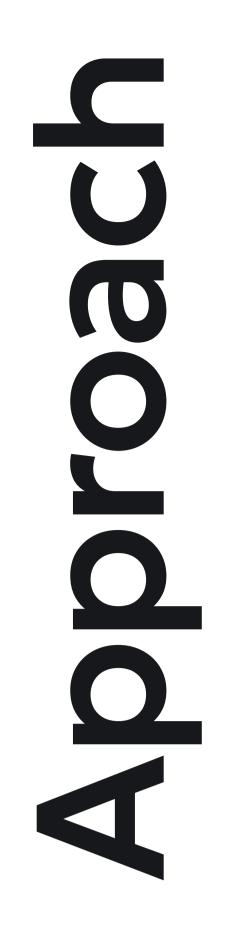


Cyber Workforce Resilience

Even the latest tools and technology are not enough, while legacy cybersecurity training and certifications are failing to ensure resilience.

Organizations need to approach people-centric cybersecurity capabilities and performance with an entirely new level of rigor. They need to know how their teams will respond to an incident or breach - and prove it to their Boards, insurers, and customers.

Realistic exercises that span from executives down to the most technical teams can unlock new levels of real-world performance measurement and evidence.



Cyber Workforce Resilience Methodology



Even a great tech stack isn't enough. People can be your biggest liability or your best



asset. All the latest technology won't help if your people and teams don't have the right capabilities or make the right decisions.



Defense is a team sport.

No single cyber professional can stop an attack, but at the same time, teamwork doesn't happen naturally. It requires deliberate practice.



Learning isn't for spectators.

People and teams improve by doing, not watching videos or reading documents. Only by being pushed to the limit in realistic scenarios are people prepared for real-world crises.

02

Individual and team capabilities are measurable and provable. Measurement and evidence are not only for technical controls. You need the data to be confident that your teams will successfully respond to a cyber incident or crisis. Organizations should prove cyber resilience to their Board, auditors, and other third parties

Cyber Workforce Resilience Methodology

01

In order to help you become resilient, we've developed a simple, four step process.

Exercise

Executive teams Cyber security teams Risk & compliance teams



Capability benchmark Capability gaps (Mitre ATT&CK) Baselining & Progress

Upskill

Defensive, Offensive, Candidate screening Appsec & CloudSec

Prove

03

Board-level reports Compliance reports Capability reports



Workforce Use real-world simulations to evaluate and baseline team capabilities and decision-making.	to industry benchmarks and receive actionable recommendations.	 → Build capabilities across cybersecurity, engineer-ing, application security, cloud security, and the broader workforce. 	 → Demonstrate risk reduction, resilience, and ROI to your board, regulators, and customers.
Data & Intelligence	Team Performance Data	Individual Performance Data	Threat Intelligence API's



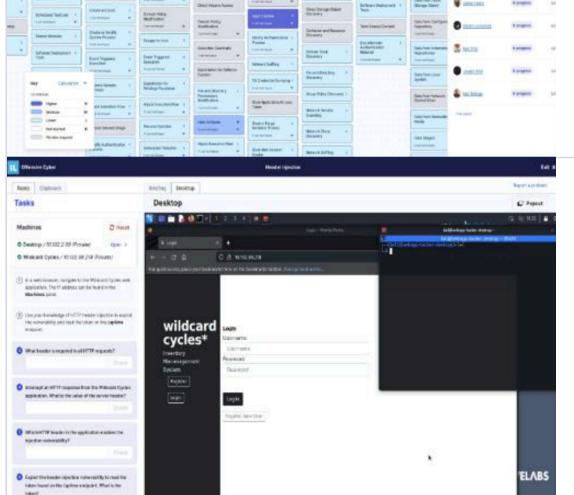


Cyber Workforce Resilience

1	Tennides and a	· · · · · · ·	an • manaras	 sauge + 					1	a * e 🐵	1
		RE ATT&CK® Frame									
-	IBO/CS	MALUTONICS Traditioner	PROBABILITY AVEN	DEBUG Davids	INCOME AND A	Manager Printer	Landau accusació Transmi	Chairton (1), repair	-uet Account Discovery		
-	Environment and the Second	Access Respective - Access Respective -	Transformer *	Harrison A.	Alexandre 1 Gales	Access Sectors 1 Hereiner 9	Equipment Western 1 Sectors	Minister II The	Line in the local second se		
	Sarana I Mineraturia	813.900 F	Avenue Namer 1	francistar 1-	Butters 1	Autopolic Montes Decomo	lancer (prophotos)	New Descale	anterior active as evolve attemption interesting active Bank margin?		
0.	Darke Contactor	Red or regar Associationable Processor &	Benariage a	STLAN A	Internation of Parameters	Renam Stationals () stationals	Lanor Tail Sarahy 1	Nexaple	August 101	Las III	
	Repairies In Carr 1	Best on Logistics	Academic Transmission	torrap or the	Esterates a	September salute Theorem	Securificants	Annual States	h anaresi	Instant	
-	the Property 1	Anna Lorenza -	Net in Logie 1 Network Colors	Destacabilitecele + Nacur Mariadas	Internet in Assess	Sectors 1 Sectors	Recordson -	The Party	9.460	tures.	
		Compression Class Services Reary	Course Weakly *	Trapes Conference	Test American -	-tearthraine +	Approved Transport	Optimize	-		
-	annan i	Qualitation at	Renderation -	Dest Veinte hanni	-	Deschorup-Maint	School Saleson + Sale	Care Inter Chart Distage Tablet	W arazan	*	
	for some .		Multiplan	Decor Artig	Inclusion .		Tax I see Cortan	Taka Tan Taribasa		Variable.	

Continuously Prove Cyber Capability

Leverage granular individual and team performance data to continuously prove capabilities across the organization, aligned to security frameworks.



Laurenged Reports + Eventer + Upsell + MTREATTACK + Manage +

- Understand human cyber capabilities
- Measure progress using credible, well-understood metrics

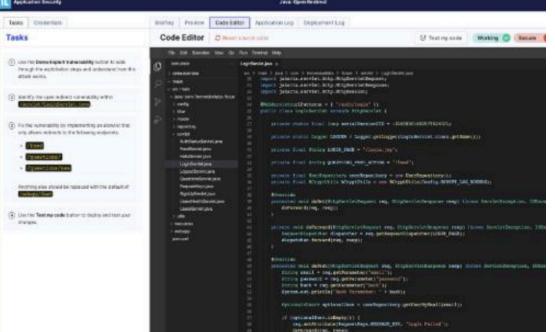
Improve Speed and Quality of Response

Respond faster and more confidently to emerging threats, while improving results.

- Reduce incident response times while improving decision-making
- Reduce time-to-capacity against emerging threats
- Efficiently manage cyber crises

<section-header><complex-block><complex-block><complex-block><complex-block>

Q # 0 6.



Improve Recruitment and Career Development

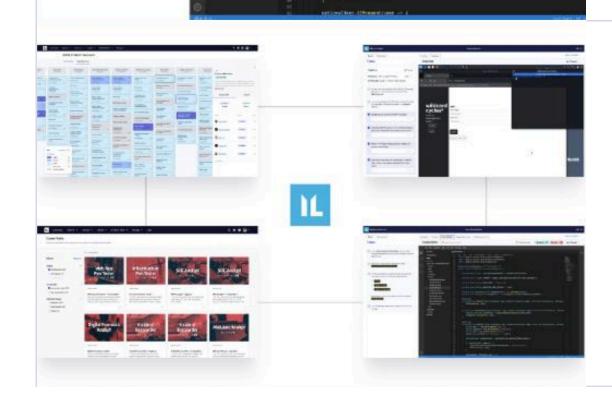
Increase efficacy in recruitment, retention, and career development.

- Identify and hire top-quality cybersecurity talent
- Promote career development and retain existing cybersecurity talent
- Reduce recruiting costs

Reduce Cloud and Application Vulnerabilities

Code securely and identify vulnerabilities in applications and cloud environments.

- Reduce vulnerabilities early and across the SDLC
- Reduce cloud security vulnerabilities



Reduce Cybersecurity Costs

Increase efficacy in recruitment, retention, and career development.

- Consolidate cybersecurity training and capability manaement
- Reduce reliance on third-party staffing and consultants
- Make informed, risk-based cybersecurity investment decisions
- Reduce risk of regulatory fees



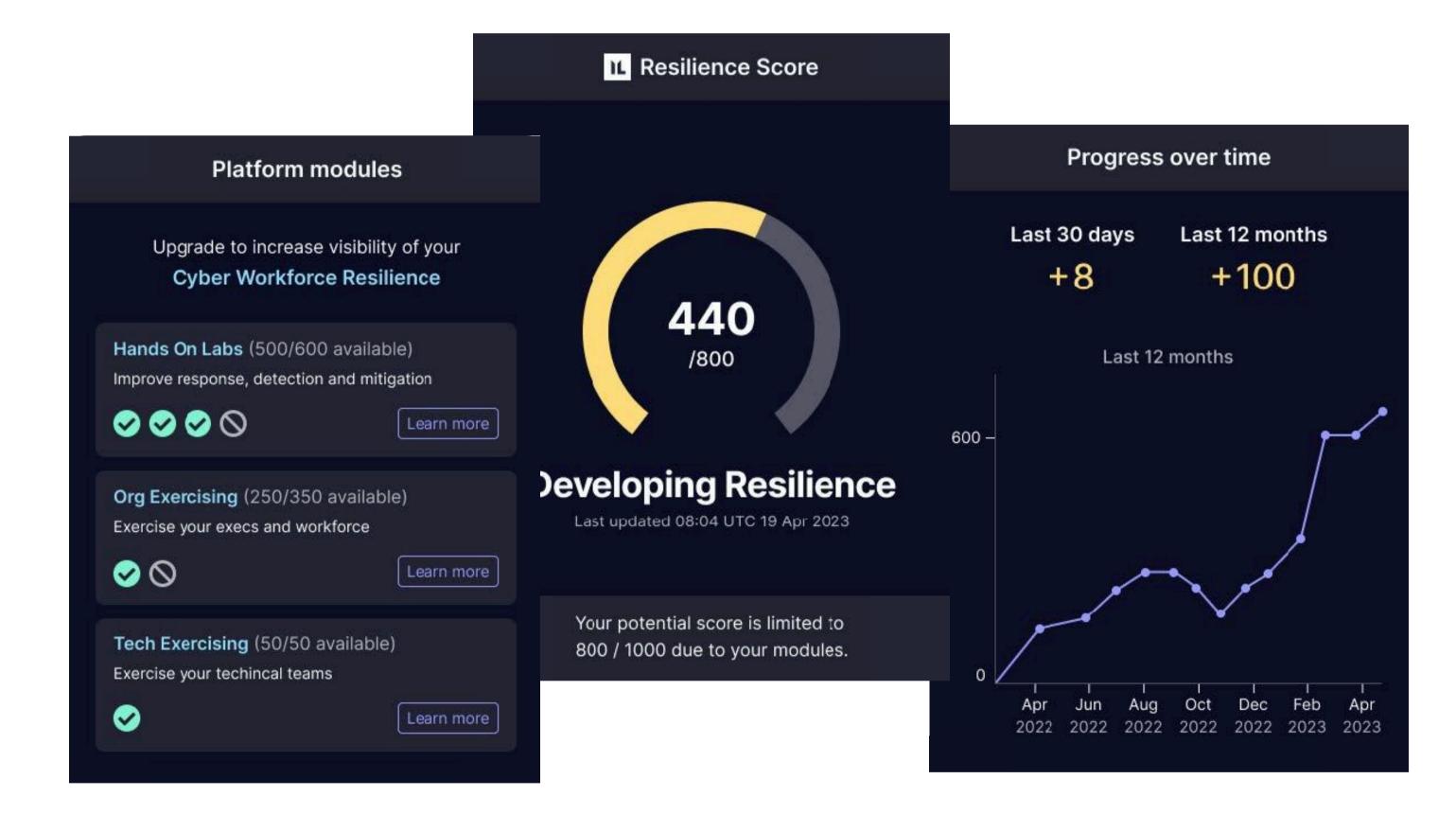


Cyber Workforce Resilience Benefits

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

With the Resilience Score, Immersive provides not only visibility into an organization's current cybersecurity capabilities, but with actionable recommendations to improve resilience.

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



Platform Modules View platform coverage

Overall Cyber Resilience

Your overall Cyber Workforce Resilience in a single, easy-tounderstand score

Progress over time

Baseline performance and track progress

		Benchmark
Negative factors	Positive factors	Organizations with the same modules
Medium Impact MITRE ATT&CK Coverage 20% of relevant techniques are not covered.	Assign Labs	374 All orgs 389 Financial Services
Medium Impact Career Path Coverage Career path coverage is poor in your organization.	Assign career paths	580 Best in class Organizations with the whole platform 440 ACME Corp
Unknown Impact Crisis Management 20% of relevant techniques are not covered.	Q Can't access?	680 All orgs 710 Financial Services
Unknown Impact App Sec Developers are not proving efficacy on code.	O Can't access?	800 Best in class

Benchmark

Compare your organziation to benchmarks and "best-in-class"

performers

Negative / Positive Factors

Understand the factors impacting your organizationwide resilience. Assign action to improve resilience — right from the dashboard!





Immersive Capabilities for Individuals

Offensive and Defensive Cyber Labs

ive Crber				Header Inject	tion				
Tasks Clipboard	Briefing	Desktop							
asks .	Deskt	ор							
		201-	1 2 3 4	ø 8				- 10	Service of the service of the
Machines C Reset					Login — Monila	Cardina -	8		kal (Prostapp-hacker
Desktop / 10.102.2.99 (Private) Open >	A Logi	n (× +				(aligneta	pp-Nacker-des	ali@webapp-hack ktop)-[+]
Wildcard Cycles / 10.102.58.218 (Private)	← → C	; @	O & 10.102.58	.218			- 51		
	For quick acco	ess, place your bookn	narics here on the boo	kmarks toolbar. Mana	age blockmarks				
1) In a web browser, navigate to the Wildcard Cycles web									
application. The IP address can be found in the Machines panel.	Lauretipad Reports	• Evenine • 0	рана – метне котъск	- Managa -					
	MIT	RE ATT&CK® Frame	ework						
Use your knowledge of HTTP header injection to the vulnerability and read the token on the /uptil endpoint.	Perso	of the Organization View							
CINE	EXECUTION	PERSISTENCE	PRVLOC ENCALATION	DEPENSE EVALUON	CHOCHTIAL ACIDESE	DISCOVERY	LATERAL MONTHING	COLLECTION	1001
What header is required in all HTTP requests?	Command and Scripting reseponder	Account Manapulation 1 Link Normali W	Musee Development M Spectral Machinetian	Aloue Deviders In Control Mechanism	Advertary ++ the - + Mode	Account Discovery +	Experietation of Research 1 Services	Adventuary in the Monte	Account Discove Lower overlage
lang 1	Container 1	875.000 1	Access Token	Access Taken	Brute force	Application Window Discovery	Internal Spearphontony	Arctive Collected Dr	spatien or writin as an advertance determine
Intercept an HTTP response from the Wildcard	Administration Commission	Beet or Logon 1 Autoctart Lesson	darigasistina Internet	Manipulation Exercisionae w	**************************************	Roman Restment	Lateral True Truesday - +	i tali internati	Read many 62
application. What is the value of the server heap	Dephy Contained	(1) (1) (1) (1) (1) (1) (1) (1) (1) (1)	Soot on Logoer 4 Autostart Execution	BITS John 9	Destatute from 4 Proceed Divers	Onlovery	Remote Service 1 Descent Hijschorg	Audio Cepture	Program (SB)
C	Equivalent for Over 1 Eventue	Real or Logon i exhalization factors	Californian W	Build Image on Hotel	Capaciton for	Child Infractionary Discovery	1.0000	Automated Collection	In programs
•	anar Process 1	Briefer Lebrason 1	Band or Logico i utilialization Borges internetion	CaroleforceptalDecoder + Pare or Information	Didetta Arceia	Churd Bernice I. Deutlissen	Annuts Devices 4 Transmission 4	Brownie Second History	10 dairs
Which HTTP header in the application enables	Connumitation Literminimum •	Comprision Claret	Costation on Minelity 1	Depley Container	Parasi Jaharrington 1	Claud Bankoe i Discovery	Regeleration Frenege	Ophoant Data	tree
injection valnerability?	Feature #89. 1	Course Account 1		Direct WAlene Access	Forge Web Destendung 3 edertedespein V	Classif Barrage Otamir	Entrane Depayment - 4	Lana trave coolar Bhurepe Object	👹 Jenethen
erte -	Scheduled Taskilob 1 Free Arienee W	Traditional T	Gernald Parksy dardfaadian aa moonato	Discoute Palloy Modification	frank landers	Destroomy	Terret Shared Content	Data from Cardigana Reportery	
Exploit the header injection vulnerability to rear	there would be a	-Create in ModPy + Rystem Process	Takapa School I	1 and 100 million	Modifi Authentication 4 Process	Container and Resource Discovery	Dis Altertary +		
token found on the /uptime endpoint. What is the	Suffrager Deployment 4 Train	Erent Nagarett 4	lasert fraggiered	Consistent Guardialia Los minimatives 19	*	Dumain Trust + Docemeny	Authertigelast Material Visionation W	Data kan shorealin Repositoriya Farminat	Status 🕄
token?	Part Party and	Darighten. Weine der Stater W	Sistinger	Explositation for Onlanse Explosite	Network Seriffing 4	File and Directory •		Daris Nom Local System	O 20100
	Key Cabulation	* arrist Remarks 1	Tapkotation by L Monitege Exclusion	Past and Desertary L.	DS Codecilat Surgery 1 In community (*	Group Policy Discovery 1		Data bara bisturati	a Man Manager
		H ark Environment 1	Rijeck Exception Flow - 4 Training and - 4	Multiuter Les terms	Blood application Advance Topoer	Network Service +		Shared Drive	vid aners
	Lower Net started	L And brinned image	Nacesci Ingelitare 1	High Artificts #	Steat or Forge 4 Karboros Tackets	Scarring		Data tran Ranazaki Minila	
	Air lake mapped	ally Automation 1	Tray Astronaut	Histi Destatos Pare 1	a tak herapata	Network Drang + Drangsvery		Data Majeri	

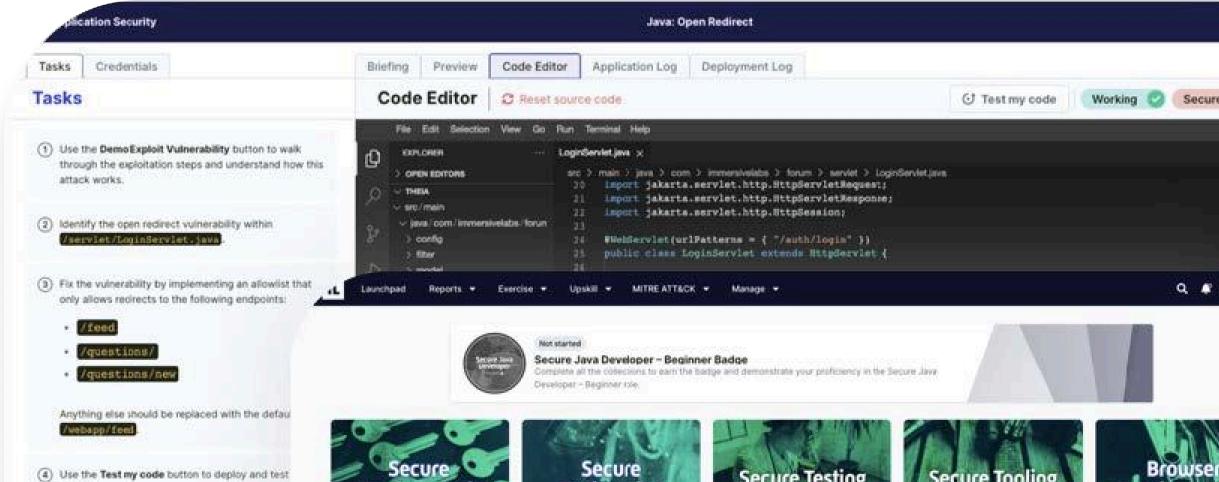
Measure cyber capabilities to make better informed crisis, hiring, and technology decisions and mitigate against emerging threats.

- Get hands on with the latest tools and techniques across bitesize labs
- Map cyber capabilities to industry frameworks such as MITRE ATT&CK
- Address weaknesses with out-of-the-box career paths and role-specific content

AppSec Labs

Part of the Immersive Labs Suite leverage data insights to strengthen the SDLC and reduce vulnerabilities in applications.

 Assess existing capabilities with hands-on lab content across coding,



tooling and testing

- Visualize platform telemetry to understand where vulnerabilities are more likely to occur
- Inject DevSecOps practices where weaknesses are identified

oy and test	Fundamentals	Engineering	Secure Testing	Secure Tooling	Developer
	Collection III II 10 (0.15 10) Secure Fundamentals Everyone needs an appropriate foundation for sometion security principles and recepts.	Coduction III Fant Orin 27m Secure Engineering Writing second code is control to keeping poor designs and code is control to keeping poor designs and code is a control to keeping poor designs and code is a control to be applied to be sufficient and code is a control of the second second code is a code of the second code is a second code of the second code is a code of the second code of the	Collection: IFIT IF 660 - 0 25-104 Secure Testing - Seginner In this shift serves you will lister how to held and elemently - elementations of lister how to held asymptote the ensure they are in fact. 3	Column BIT Wills 0 to 50% Secure Tooling - Deginner Protect all through Learn how to configure, inc, and consistent the results of atfracts constity tools, as well as how to interpret. 2	Collection BIT With Browser Developer Tools What, in your toolbar? Learn tenness developer toolbar? and configure your application
	ORASP TOP 10 Concession Bill Kind Concession OWASPTNE 10	Java Baseler Gall Colocion - Bill Million - Beatman Java - Beatman	Coluction III Table Column		



www.immersivelabs.com | sales@immersivelabs.com | Copyright 2025 Immersive Labs. All rights reserved.

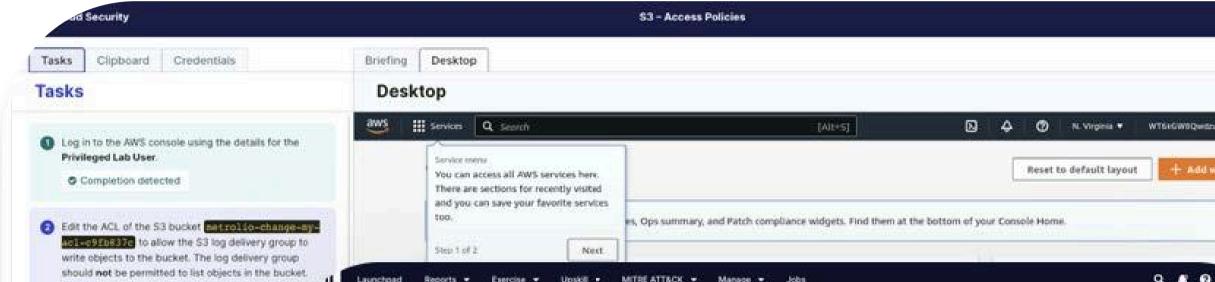
changes.



Immersive Capabilities for Individuals

CloudSec Labs

Part of the Immersive Labs Suite measure and enhance the cloud security capabilities of anyone



involved in designing, developing, and/or administering cloud workload.

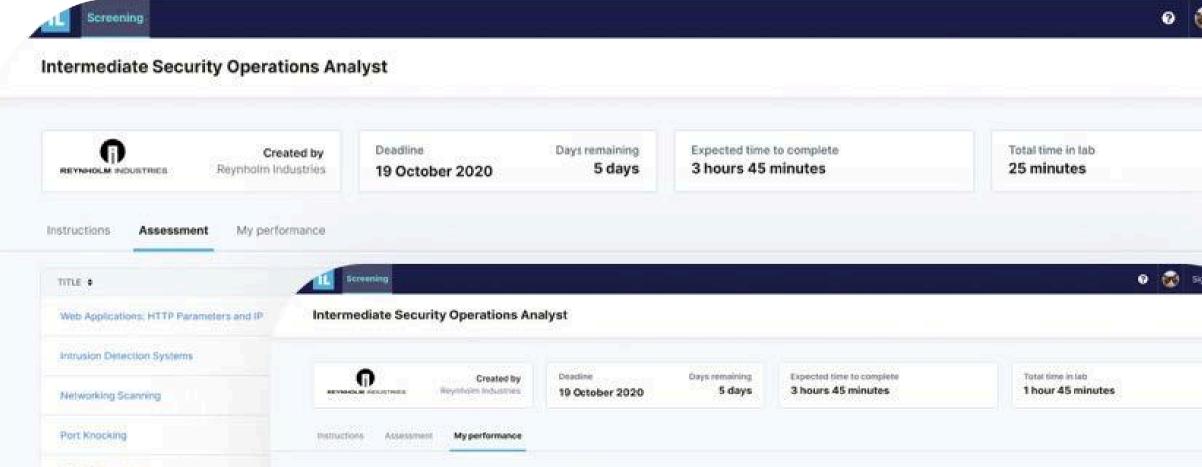
- Assess existing capabilities with demonstrate labs focused on AWS and security aptitude
- Understand skills gaps with reporting at individual, team and organization levels
- Address skill gaps with labs on specific tools and techniques

		27 collections of labs			
Within the netrolic-change-sy-acl-citb81	Filters Clear	rat Assigned to me 🖘			
bucket, change the ACL of the candom top ob Remove the ability to write the ACL, leaving only	20000	A PARD			
access.	Status Not Started (27)	· CHE			
Detects completion	and the Province of the		and and	Cloud	
We when the second s		NCSC	DevSecOps	Fundamentals	
	2010-0020 <u>0000</u> 0	the state	AVYA	rencementer	
On the net collo-change-my-pollog-iten75 bucket, configure a bucket policy to allow the	Subcategory Amagon Web Services (8)	Vistering IN		dial of	
Instruction with the second policy to new the	Cloud Fundamentals (4)	And Manage Character		411 Mar (0.1011)	
users to carry out all \$3 actions. You may use a	Cloud Tooling (10)	Collection III # 290 (0.3) 45m	Collection 100 X 172 0 2h 154	Collection BIG 8120 0 24 304	
adapt the first example policy in the Briefing pa	C Kubernetes (5)	NCSC - Cloud Security Guidance Outdatur time! From supply that security	DevSecOpe Development, Security and Operations.	Cloud Fundamentals Triss series will explore the Sundamentals of	
the following ARNs in your policy:		to data in transit, this prives covers the	This series will provide a detailed conview of the DevileoDpa culture and how it	cloud security, including tabs on software, infrastructure, and platforms as services	
bicketeer	Difficulty Range Beginner (5)	18 A Charles State State Contractory	No. of the other states of the		
APTERMENTAND STORES (STORES)	Intermediate (19)	Not started	Not started >	Nut started	
bucketeer2	🗇 Expert (3)				
Note: You'll see an error about the		Amazon Web Services 🔟	And the second se	lows.	
accounter ly action where the section where the section where the section we section where the section we section where the section section is a section where the section section is a section sectio			XXX XXX	IAM	Lan
adding the policy.		53	EC2		Logging
Detects completion		Simple Storage	Elastic Compute	Identity and	Monitor
		Service	Cloud	Access	in AW
Using the example policy in the Briefing tab, cre				Management	- AN
ress point called embrool inconcern repotent				· 查拉利的指示:"个孩子"。	and the second s
'the metrolio-grant-some-acces		Collector III #1200 (0.26 Mar.	Cuterten #1 # 1000 (0-01/2011	Collection	Collection (1) T
		53 (Simple Storage Service)	EC2 (Elastic Compute Cloud)	IAM (Identity and Access	Logging & Monitoring in
		Ruckets, Isarkets, Isarlets' in this series;	622 in a turn service in AWS that provides	Mold serviced This series teachers you the	Effective logging and alert

Candidate Screening

Reduce reliance on certifications and minimize bias by measuring candidates' capabilities.

 Invite candidates to complete role assessments made up of selected labs



- Measure and compare candidate's practical cyber capabilities
- Understand where new joiners' capabilities will need enhancing

PHP: SQL Injection	Assessment Progress	Accuracy
Splunk - Event Analysis	Lete comparison	Web Applications HTTP
Yara Episode 4	Late in progress 0 Late not instance	Exercision Detection System 2 Exercision Statement Exercision Statement
Linux: Service Weaknesses	Answer accuracy	+ 0000111111 Part Recording + 000001010 Phil-SOL Intertion
	O Hermony	A DECEMBENT AND
	Completion time	
		Time spont (minutes)
	Trectaeri E ti 45 erit	Web Applications HTTH .





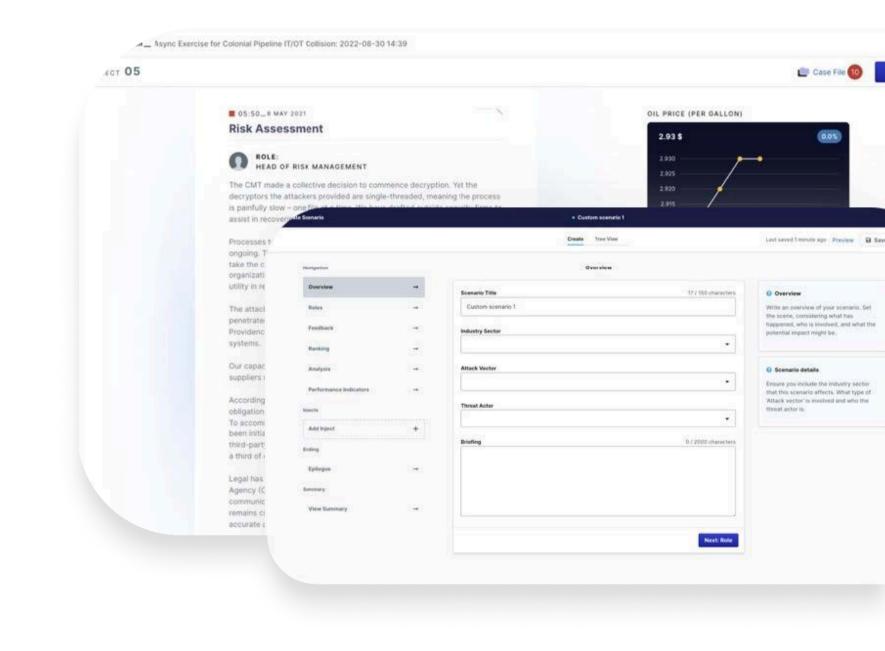
Immersive Capabilities for

Teams

Crisis Sim

Drive measurable improvements in cyber response with crisis scenarios across multiple sectors and attack vectors.

- Exercise teams with real crises that have dynamic storylines and contextual media, delivered through their browser
- Measure and benchmark response to make better informed decisions on crisis strategies



• Build on response skills and muscle memory with a cadence of regular exercising

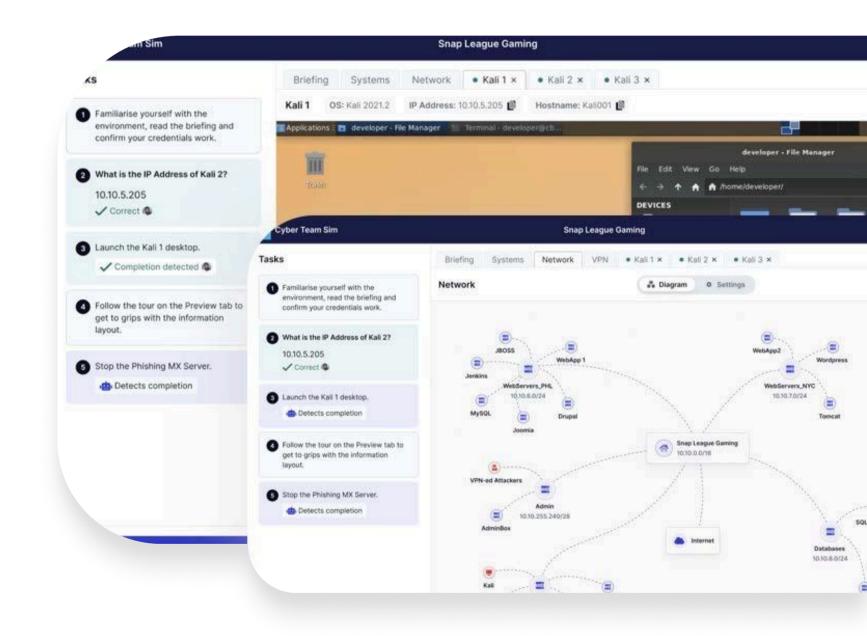
AppSec Labs

Part of the Immersive Labs Suite - prove the effectiveness of red and blue teams as they progress through complex technical scenarios.

- Complex and realistic scenarios engage teams through a series of technical tasks
- Benchmark performance internally or to industry peers
- Scenarios cover the latest threats, ensuring your teams keep pace with attackers

Offensive and Defensive Cyber Labs

Create realistic environments for teams





to upskill, test new tools and techniques.

- Drop teams into simulations that emulate your production network
- Understand how effectively users and processes would work together
- Provide teams with an environment to test and learn with the tools they'll use daily





Immersive Capabilities for Organizations

AppSec Labs

Part of the Immersive Labs Suite target organizational learning gaps left by traditional cybersecurity training with behavioral science,



driving measurable change across individuals, teams, and risk areas.

- Baseline and assess strengths and potential risks across the organization
- Deploy labs covering everything from the basics to more advanced theory and cybersecurity practice
- Educate about best practices to empower with knowledge and judgment
- Build a foundation for behavioral change

Option 1
Call the security incident response team
These issues have raised concerns in your mind, so you pass it
on to the security team.
Submit Response
Option 2
Option 2 Call your manager
○ Call your manager
 Call your manager These customer reports have worried you, so you leave the

We are the Leader in People-Centric Cyber Resilience

All the latest tools and technology are not enough to ensure resilience; people and teams must have the right capabilities and make the right decisions when it counts. Forge a cyber-resilient workforce with Immersive – all in a single Enterprise platform.

world

IMCo

What

A Seamless, Enterprise Platform

True resilience requires people and teams to work together, from store room to board room. With a seamless and tailored experience for individuals, teams, and the entire organization, we provide unmatched cybersecurity exercises and training, along with data-driven insights and guidance to improve resilience. Built for the world's latest organizations, take advantage of enterprise-class scale, security, reliability, and integrations across our Enterprise platform.

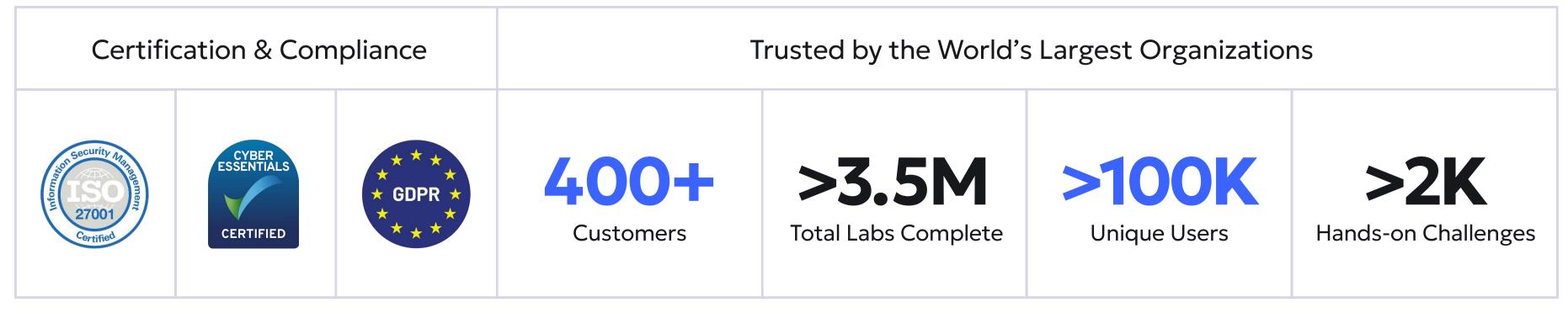


Why We're Different.

Unlike legacy, check-box training and paper certifications, we provide...

<section-header></section-header>	Proof of Capability	Complete Organizational Coverage	A Unified Enterprise Platform	Capability at the Speed of Cyber
We offer the most realistic, real-world learning environments for all skill levels.	We equip CISOs with the data to be confident that they have a cyber- resilient workforce.	We foster resilience across the organization, with unparalleled content that offers	We provide a seamless and customized experience for	We ensure your teams are updated on the latest cyber risks, from zero-day

all skill levels.	resilient worktorce.	content that offers world-class breadth and depth.	individuals, teams, and the entire workforce.	exploits to the evolving Al landscape.
<section-header><section-header></section-header></section-header>	Evidence-Based Granular, role- based performance data helps organizations understand, baseline, benchmark, and prove their cyber capabilities.	Breadth & Depth Cybersecurity exercises and labs tailored to individuals and teams from the store room to the board room. Personalized Learning Paths	A Seamless Experience We ensure a fluid and consistent journey for users and administrators across all labs and exercises.	Cyber Threat Intelligence Our experts enable teams to understand and defend against attacks in as little as 24 hours.
Interactive challenges offer an engaging learning experience.	Cyber Resilience Score Understand, build, and prove your organizational cyber resilience in a single score.	Targeted, individualized training ensures each user receives relevant training based on their knowledge gaps.	World's Latest Organizations Leverage our enterprise-class scale, security, reliability, and integrations.	We empower organizations to understand and leverage the cyber impact of AI on their workforce.



Be Ready.

immersive



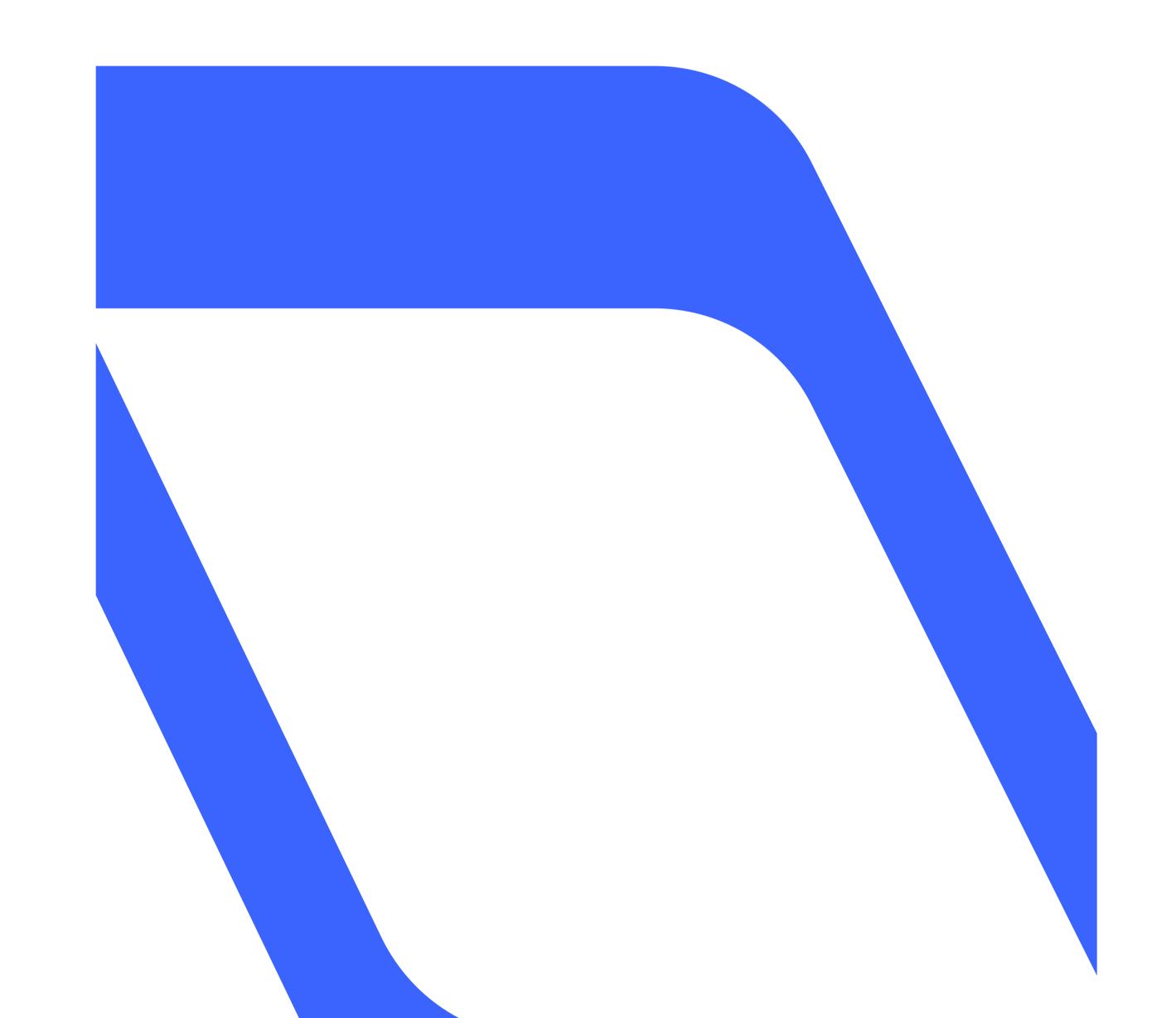


Immersive is trusted by the world's largest organizations and governments, including Citi, Pfizer, Humana, HSBC, the UK Ministry of Defence, and the UK National Health Service. We are backed by Goldman Sachs Asset Management, Ten Eleven Ventures, Menlo Ventures, Summit Partners, Insight Partners and Citi Ventures.













www.**immersivelabs**.com | sales@immersivelabs.com

Copyright 2025 Immersive Labs. All Rights Reserved