### 

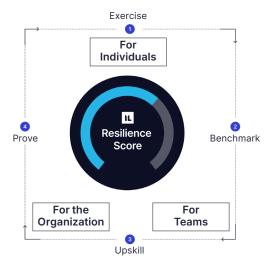
#### SOLUTION BRIEF

# 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 people-centric 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.



#### **For Individuals**

Hands-On Labs offering engaging, gamified learning environments

- Defensive Cybersecurity
   Professionals
- Penetration Testers
- Developers
- Application Security Experts
- Cloud and Infrastructure Security
- Entire Workforce

#### For Teams

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

- Executive Teams
- Crisis Management and Incident Response Teams
- Offensive, Defensive and SOC Teams

#### For the Organization

Skills development exercises that drive transformative behavioral change

- Senior Leaders
- Front-line Employees
- High-risk Targets of Cyber Attacks

Trusted by the world's largest companies, governments, and defense organizations





Нитала мсьэгей

national**grid** 

### Cyber Workforce Resilience Approach

### 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 Principles**



**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.



**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

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



**Exercise**: Use real-world simulations to evaluate and baseline team capabilities and decision-making.

**Benchmark**: Evaluate cyber readiness compared to industry benchmarks and receive actionable recommendations. **Upskill**: Build capabilities across cybersecurity, engineering, application security, cloud security, and the broader workforce.

**Prove**: Demonstrate risk reduction, resilience, and ROI to your board, regulators, and customers.



### **Cyber Workforce Resilience Benefits**

### **Continuously Prove Cyber Capability**

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

- 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

#### **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.

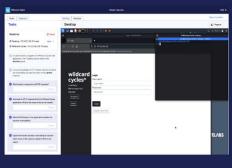
- Reduce vulnerabilities early and across the SDLC
- Reduce cloud security vulnerabilities

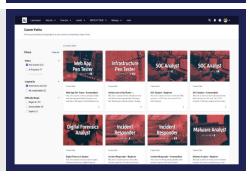
#### **Reduce Cybersecurity Costs**

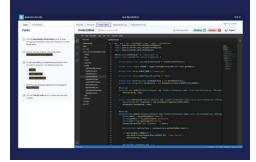
Increase efficacy in recruitment, retention, and career development.

- 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









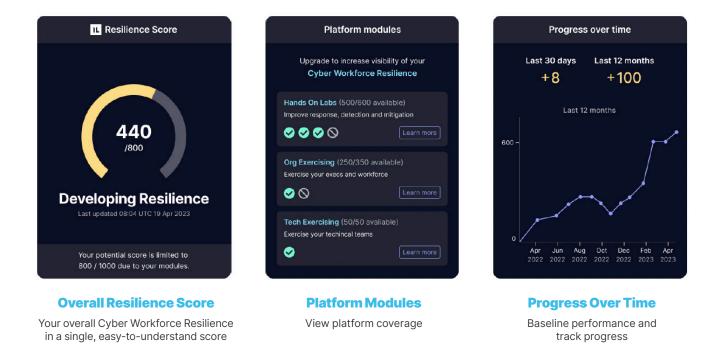


### The Immersive Labs Resilience Score

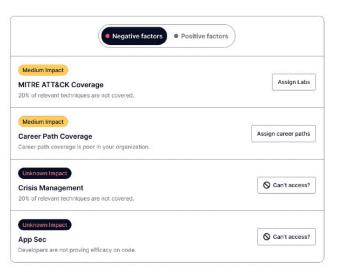
The Immersive Labs Resilience Score is a single value that organizations can use to measure their overall cyber workforce resilience. The algorithm evaluates multiple factors using performance data from across the platform and enables organizations to understand:

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

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



Organizations with the same modules
440 ACME Corp
374 All orgs
389 Financial Services
580 Best in class
Organizations with the whole platform
440 ACME Corp
680 All orgs
710 Financial Services
800 Best in class



#### **Negative/Positive Factors**

Understand the factors impacting your organization-wide resilience. Assign action to improve resilience right from the dashboard.

Compare your organization to benchmarks and "best-in-class" performers

**Benchmark** 



### Immersive Labs Capabilities — For Individuals

### Offensive and Defensive Cyber Labs

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

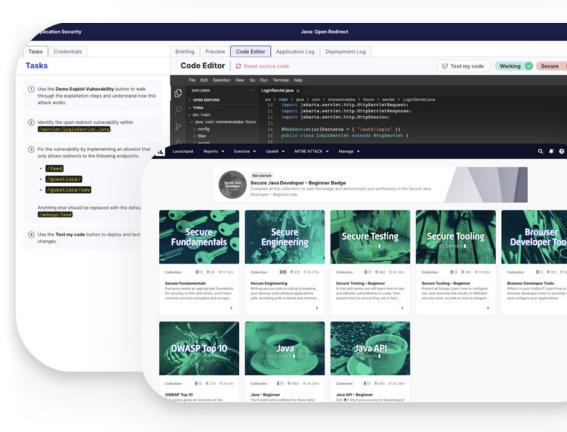
- Get hands on with the latest tools and techniques across bitesize labs
- Map cyber capabilities to industry frameworks such as MITRE ATT&CK
- Address weaknesses with out-of-the-box career paths and role-specific content

rensive Cyber					Header Inject	ion					
Tasks Clipboard		Briefing	Desktop								
asks		Deskto	p								
		S = =	😼 😂 🖿 v	1 2 3 4	• 8						
Machines C	Reset	•						80 10	-	kali@webapp-hacker-	des
Desktop / 10.102.2.99 (Private)	pen >	🔭 Login						(kali@ weba	pp-hacker-des	ktop)-[~]	
Wildcard Cycles / 10.102.58.218 (Private)		← → C		0 🔒 10.102.58	.218						
		For quick acces		narks here on the bool	kmarks toolbar. Mana	ge bookmarks					
<ol> <li>In a web browser, navigate to the Wildcard Cyc application. The IP address can be found in the</li> </ol>											
Machines panel.	-	Launchpad Reports	<ul> <li>Exercise = Up</li> </ul>	USAIL • MITRE ATTACK	<ul> <li>Manage</li> </ul>						¢
2) Use your knowledge of HTTP header injection	10	MITR	E ATT&CK® Frame	swork							
the vulnerability and read the token on the Jup		Personal	of View Organisation View								
endpoint.	KHESS +	EXECUTION	PERSISTENCE	PRIVILEGE ESCALATION	DEFENSE EVASION	CREDENTIAL ACCESS	DISCOVERY	LATERAL MOVEMENT	COLLECTION	11067	
What header is required in all HTTP requests?		ti tarongan	Account Manipulation 1	About Develop	e unagen	in scherper	i coun	Excitation of Bernster 1	- and a	Account Discovery	y
	C	Command and L Scripting Interpreter	Account Manipulation L East-techniques	Advase Devation H Control Mechanism	Abuse Devation M Control Mechanism 4 sale-techniques W	Adversary-in-the-L Middle 2 sit-techniques V	Account Discovery L 4 satractropes V	Exploitation of Remote L Services	Adversary-in-the- Middle 2 sat-techniques	Adversaries may attempt system or within an envir	1 10
	A	Container L Administration	875.086 k	Access Token L Manipulation	Access Token L Manipulation	Brute Force L	Application Window Discovery	Internal Spearphishing	Archive Collected De	adversaries determine with Read more 02	hic
Intercept an HTTP response from the Wildcar	d	Command	Boot or Legon L Autostart Execution	Estimitique 👻	tairanagan 👻	Existencias V Credentials from A	Browser Bookmark L Discovery	Lateral Tool Transfer L	Audio Capture	Progress (19)	
application. What is the value of the server he		Deploy Container	Boot or Legen L	Boot or Logon L Autostart Execution	BITS Jobs 4	Password Stores 5 no-screepen V	Cloud Infrastructure	Remote Service L Bession Hjacking	Automated Collectio		7
		Exploitation for Client 4 Execution	Initialization Scripts East-terimizen V	Boot or Logon L Initialization Scripts	Build Image on Host	Exploitation for L Credential Access	Cloud Service 1	Remote Services L	Browser Session	In programs 10 users	
	C	Inter-Process L Communication	Browser Extensions k	S with the Theory and	Deobfuscate/Decode + Files or information	Forced Authentication L	Choud Service L Deshloard	East-Scriegers W	Hjacking		
Which HTTP header in the application enable: injection vulnerability?	and the second s	Native API L	Compromise Client Software Binary	Create or Modify 4 Bystem Process	Deploy Container	Forge Web-Drodentials	Cloud Service k Discovery	Replication Through * Removable Mode	Cliptored Data	User	
		Scheduled TaskUob 4	Create Account k	Domain Policy	Direct Volume Access	East-Inclusion V	Cloud Storage Object Discovery	Software Deployment L Tools	Data from Cloud Storage Object	Verses Harris	
	nahip	140-1679494 V	Courte or Modify is	Modification 2 sitration	Domain Policy Modification	**************************************	Container and Resource	Taint Shared Content	Data from Configura Repository 2 sal-solvision	Careth Lockwood	
Exploit the header injection vulnerability to re	Nai 1	Shared Modules 4	System Process A site techniques	Except to Host 4	Execution Guardrails	ModPy Authentication L Process	Discovery Domain Trust 4	Use Alternate 4 Authentication Material	Data from informatio	The free	
token found on the /uptime endpoint. What is token?	ti 2	Software Deployment 4 Tools	Event Trippered k Execution	Event Triggered 4 Execution	Taaraataiga 🛛 🐨	Network Sniffing 4	Discovery	Hateral 4 sal-techniques V	Repositories 3 sub-recircipues		
	C Key	Calculation •	arnal Remote	Excludation for 1	Exploitation for Defense Evasion	OS Credential Dumping 1	File and Directory 4 Discovery		Data from Local System	Construction	
		TRADE	Pulces	Privilege Excelution	File and Directory L Permissions Modification	Baal-Inclusion V	Group Policy Discovery 1		Data from Network Shared Drive	Stat Ratings	
	100	Higher H Medium M	ack Execution Flow 1 artectropee	Hijack Execution Filow 5 Haat-technique V	Jakiningan 🖤	Token	Network Service L Scanning		Data from Removabi	etid users	
		Not started N	N plant internal image	Process Injection 4 Trad-formation W	Hide Artifacts N Exit-tectoryan V	Steal or Forge L Kerberon Tickets	Network Share L Discovery		Media		
		No labs mapped	dity Authentication 1	Scheduled Tauklink 4	Hjack Execution Flow 4	Sheet West Security 1			Data Diaged		



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



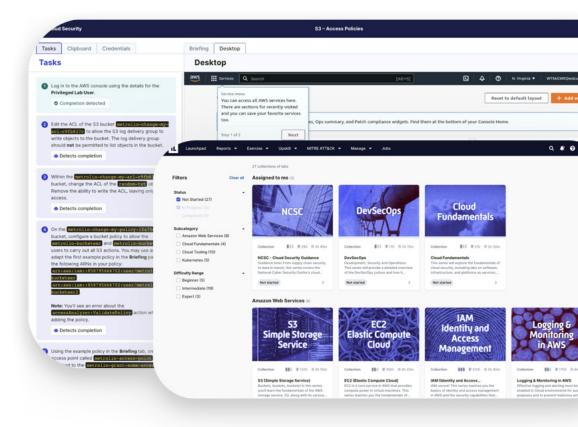
### 

### Immersive Labs Capabilities — For Individuals

#### **Cloud Sec Labs**

Measure and enhance the cloud security capabilities of anyone involved in designing, developing, and/or administering cloud workload.

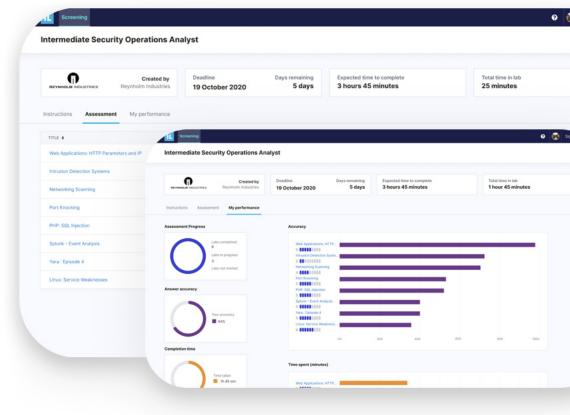
- Assess existing capabilities with demonstrate labs focused on AWS and security aptitude
- Understand skills gaps with reporting at individual, team and organization levels
- Address skill gaps with labs on specific tools and techniques





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



### 

### Immersive Labs Capabilities — For Teams

### **Crisis Sim**

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

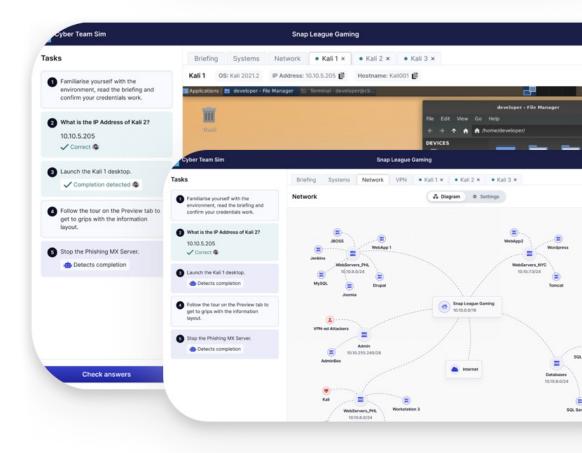
- Exercise teams with real crises that have dynamic storylines and contextual media, delivered through their browser
- Measure and benchmark response to make better informed decisions on crisis strategies
- Build on response skills and muscle memory with a cadence of regular exercising

### Cyber Team Sim

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

CT 05							📄 Case File 10
	<b>05:50_8 MAY</b>	2021		- <		OIL PRICE (PER GALLON)	
	Risk Asses	ssment				2.93 \$	0.0%
	ROLE					2.930	•
	HEAD OF	F RISK MANAGEMENT				2.925	
		a collective decision to comr				2.920	
	decryptors the a is painfully slow	attackers provided are single	-threaded, mea	aning the process		2.915	
	assist in recover				Custom scenario 1		
	-				Create Tree View		
	Processes to				Create Tree View		Last saved 1 minute ago Preview
	ongoing. T take the c				Overview		
	organizati	Navigation			Overview		
	utility in re	Overview	-	Scenario Title		17 / 150 characters	Overview
	The attack	Roles	-	Custom scenario 1			Write an overview of your scenario. Se
	penetrate						the scene, considering what has happened, who is involved, and what
	Providenc	Feedback	-	Industry Sector			potential impact might be.
	systems.	Ranking	-			•	
	Our capac	Analysis		Attack Vector			Scenario details
	suppliers (	Anaryan				•	
		Performance Indicators	-				Ensure you include the industry sector that this scenario affects. What type of
	According obligation	Injects		Threat Actor			'Attack vector' is involved and who the threat actor is.
	To accom						
	been initia	Add Inject	+				
	third-part;	Ending		Briefing		0 / 2000 characters	
	a third of a						
	Legal has	Epilogue	-				
	Agency (C	Summary					
	communic						
	remains ci	View Summary	-				
	accurate a						
						Next: Role	



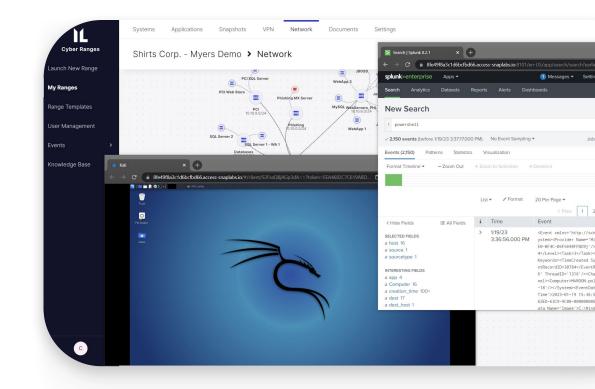
### IL IMMERSIVELABS

### Immersive Labs Capabilities — For Teams

### **Cyber Ranges**

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

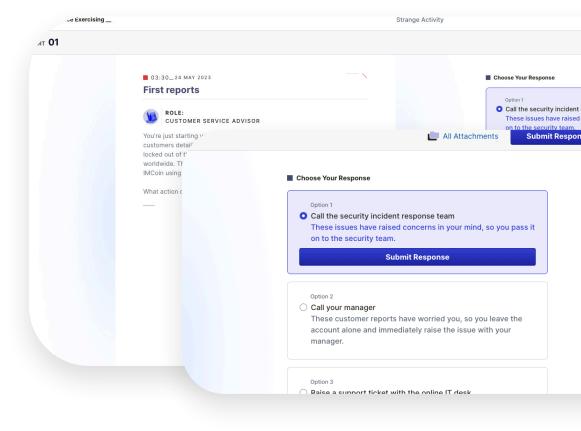


### Immersive Labs Capabilities — For the Organization



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





### 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 Labs – all in a single Enterprise platform.

#### 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...

Immersive Realism	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 world-class breadth and depth	We provide a seamless and customized experience for individuals, teams, and the entire workforce	We ensure your teams are updated on the latest cyber risks, from zero-day exploits to the evolving Al landscape
Hands-On, Active Learning. Live sandbox environments ensure learning covers practical skills, not just theory.	<b>Evidence-Based.</b> Granular, role-based performance data helps organizations understand, baseline, benchmark, and prove their	<b>Breadth &amp; Depth.</b> Cybersecurity exercises and labs tailored to individuals and teams from the store room to the board room.	A Seamless Experience. We ensure a fluid and consistent journey for users and administrators across all labs and exercises.	<b>Cyber Threat</b> <b>Intelligence.</b> Our experts enable teams to understand and defend against attacks in as little as 24 hours.
<b>Gamification.</b> Interactive challenges offer an engaging learning experience.	cyber capabilities. <b>Cyber</b> <b>Resilience Score.</b> Understand, build, and prove your organizational cyber resilience in a single score.	Personalized Learning Paths. Targeted, individualized training ensures each user receives relevant training based on their knowledge gaps.	Built for the world's latest organizations. Leverage our enterprise-class scale, security, reliability, and integrations.	<b>Al Ready.</b> We empower organizations to understand and leverage the cyber impact of Al on their workforce.



### Continuously Assess, Build, and Prove Your Cyber Resilience

Immersive Labs is trusted by the world's largest organisations 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, Summit Partners, Insight Partners, Citi Ventures, and Menlo Ventures.





THE LEADER IN PEOPLE-CENTRIC CYBER RESILIENCE

immersivelabs.com sales@immersivelabs.com

Copyright 2023 Immersive Labs. All rights reserved.