immersive

Empower

Data Sheet

Unified Cyber Resilience for Governments

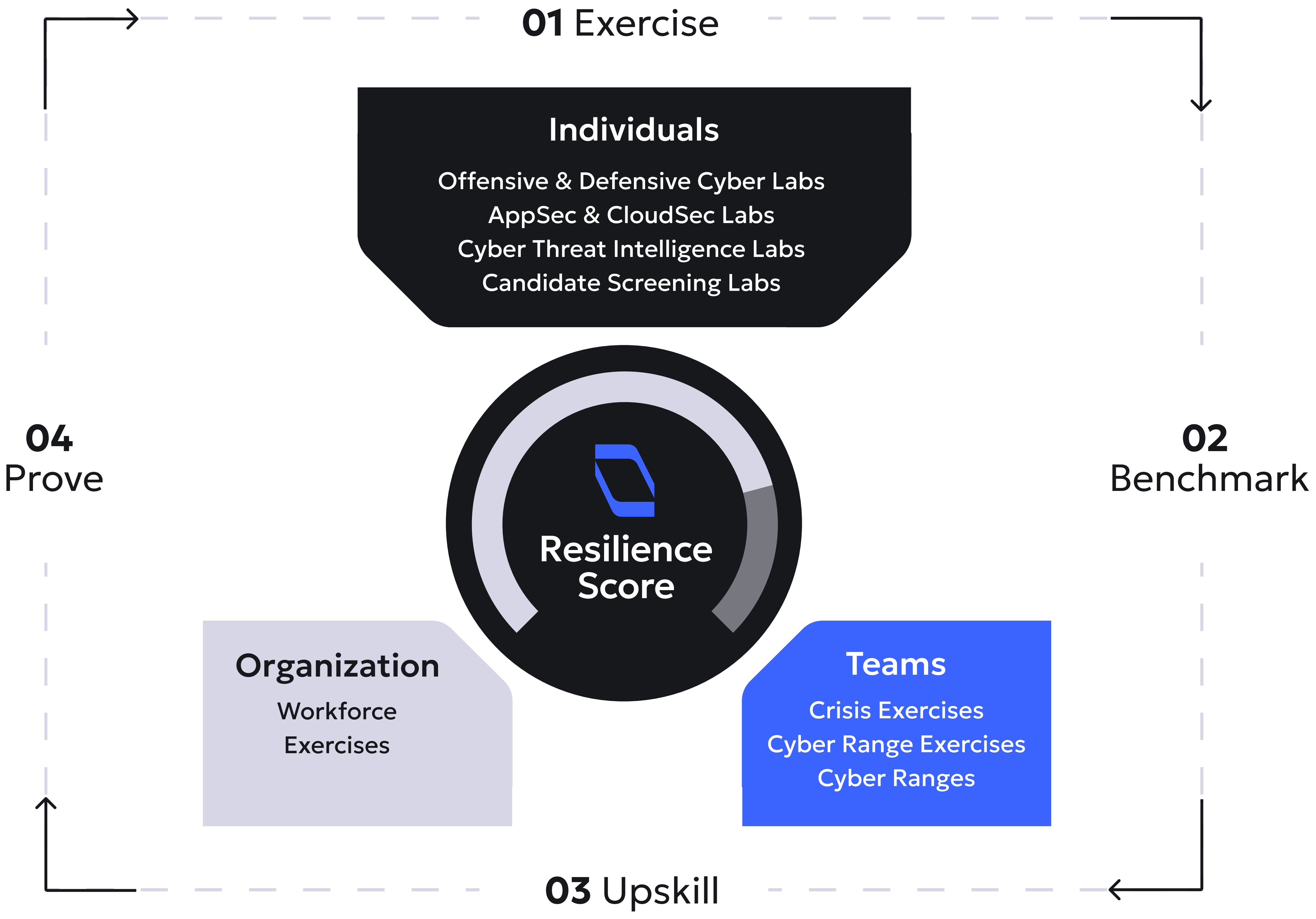
Jan 2025

immersive

Unified Cyber Resilience for Governments

Immersive empowers government agencies globally to effectively prevent and respond to cyber threats.

Our tailored approach continuously assesses, builds, and proves your cyber capabilities, relevant to individual roles, while keeping your organization ahead of an ever-evolving threat landscape. With a single enterprise platform for individuals, teams, and your entire organization, Immersive helps you take a unified approach to cyber resilience.



01 Exercise

Individuals
Offensive & Defensive Cyber Labs
AppSec & CloudSec Labs
Cyber Threat Intelligence Labs
Candidate Screening Labs

02 Benchmark

Resilience Score

Teams
Crisis Exercises
Cyber Range Exercises
Cyber Ranges

03 Upskill

Organization
Workforce Exercises

04 Prove

Challenges

- Address the talent gap by switching to skills-based hiring
- Finding targeted and up-to-date training aligned to job roles
- Protecting Critical Infrastructure
- Regulations with strict accountability

Benefits

- Prove Cyber Resilience: Prove cyber capabilities, aligned to security frameworks, including NIST/NICE, MITRE ATT&CK, and CMMC
- Measure Maturity: Evaluate cyber preparedness according to a rigorous maturity model
- Improve Speed & Quality of Response: Continuously improve cyber capabilities and response to emerging threats with hands-on training and exercising
- Improve Recruitment & Career Development: Identify, hire, build, and retain skilled cybersecurity talent, aligned to specific roles

For Teams

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

- Leadership
- Crisis Management and Incident
- Offensive, Defensive and SOC Teams

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 the Organization

Skills development exercises that drive transformative behavioral change

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

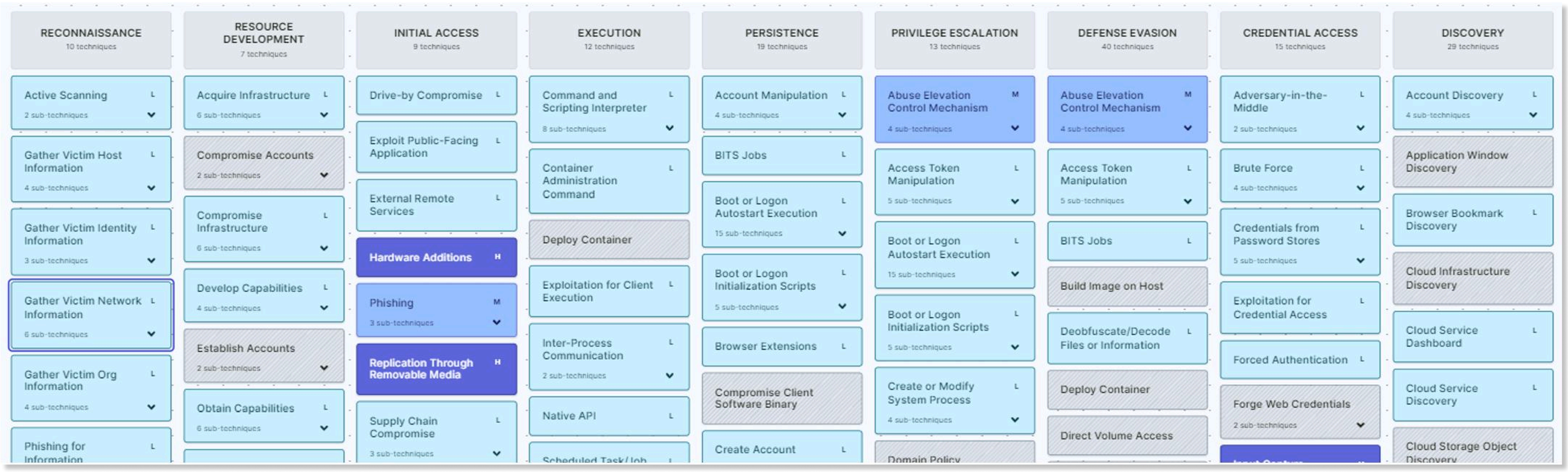
Be Ready.

|

Compliance and Standards

NIST NICE - National Initiative for Cybersecurity Education	The Immersive Labs platform maps all labs to the NIST NICE framework to facilitate the development of cybersecurity skills, curriculum alignment, and skills-based hiring.
MITRE ATT&CK Alignment	Granular performance data can help organizations understand their personnel abilities according to the MITRE ATT&CK framework.
Executive Order 14028 - Executive Order on Improving the Nation's Cybersecurity	Immersive Labs helps agencies build the skills to improve detection of cybersecurity incidents and enhance investigative and remediation capabilities.
NIST 800-84 - Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities	Immersive engages personnel from across your organization to enhance crisis decision making and technical response skills to adaptably and effectively respond to cyber risk.
National Cyber Workforce and Education Strategy 2023 (NCWES)	Immersive launched the Cyber Million program in 2022 with a goal of filling one-million entry-level jobs in the next decade. Learn more: link
NIST Cybersecurity Framework (CSF) 2.0	The Immersive Labs Maturity Model maps to elements of the NIST Cybersecurity Framework to help agencies prove their cyber resilience.
NIST 800-161 rev 1: Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations	Hands-on training and exercises that agencies can require of their systems integrators and other partners. For more information: link
Cybersecurity Maturity Model Certification (CMMC)	Immersive Labs can help organizations improve their maturity in preparation for CMMC Level 2 and Level 3 compliance audits.

Understand MITRE ATT&CK Coverage and Close Gaps



RECONNAISSANCE
10 techniques
Active Scanning L
2 sub-techniques
Gather Victim Host Information L
4 sub-techniques
Gather Victim Identity Information L
3 sub-techniques
Gather Victim Network Information L
6 sub-techniques
Gather Victim Org Information L
4 sub-techniques
Phishing for Information L

RESOURCE DEVELOPMENT
7 techniques
Acquire Infrastructure L
6 sub-techniques
Compromise Accounts
2 sub-techniques
Compromise Infrastructure L
6 sub-techniques
Develop Capabilities L
4 sub-techniques
Establish Accounts
2 sub-techniques
Obtain Capabilities L
6 sub-techniques

INITIAL ACCESS
9 techniques
Drive-by Compromise L
Exploit Public-Facing Application L
External Remote Services L
Hardware Additions H
Phishing M
3 sub-techniques
Replication Through Removable Media H
Supply Chain Compromise L
3 sub-techniques

EXECUTION
12 techniques
Command and Scripting Interpreter L
8 sub-techniques
Container Administration Command L
Deploy Container
Exploitation for Client Execution L
Inter-Process Communication L
2 sub-techniques
Native API L
Scheduled Task/Job L

PERSISTENCE
19 techniques
Account Manipulation L
4 sub-techniques
BITS Jobs L
Boot or Logon Autostart Execution L
15 sub-techniques
Boot or Logon Initialization Scripts L
5 sub-techniques
Browser Extensions L
Compromise Client Software Binary
Create Account L

PRIVILEGE ESCALATION
13 techniques
Abuse Elevation Control Mechanism M
4 sub-techniques
Access Token Manipulation L
5 sub-techniques
Boot or Logon Autostart Execution L
15 sub-techniques
Boot or Logon Initialization Scripts L
5 sub-techniques
Create or Modify System Process L
4 sub-techniques
Domain Policy

DEFENSE EVASION
40 techniques
Abuse Elevation Control Mechanism M
4 sub-techniques
Access Token Manipulation L
5 sub-techniques
BITS Jobs L
Build Image on Host
Deobfuscate/Decode Files or Information L
Deploy Container
Direct Volume Access

CREDENTIAL ACCESS
15 techniques
Adversary-in-the-Middle L
2 sub-techniques
Brute Force L
4 sub-techniques
Credentials from Password Stores L
5 sub-techniques
Exploitation for Credential Access L
Forced Authentication L
Forge Web Credentials
2 sub-techniques
Input Capture

DISCOVERY
29 techniques
Account Discovery L
4 sub-techniques
Application Window Discovery
Browser Bookmark Discovery L
Cloud Infrastructure Discovery
Cloud Service Dashboard L
Cloud Service Discovery L
Cloud Storage Object Discovery

Identify individual and organizational capabilities according to the MITRE ATT&CK Framework and fill gaps with specifically-tailored labs.

Why Immersive?

Immersive Realism

We offer the most realistic, real-world learning environments for all skill levels

Proof of Capability

We equip CISOs with the data to be confident that they have a cyber-resilient workforce

Complete Organizational Coverage

We foster resilience across the organization, with unparalleled content that offers world-class breadth and depth

A Unified Enterprise Platform

We provide a seamless and customized experience for individuals, teams, and the entire workforce

Capability at the Speed of Cyber

We ensure your teams are updated on the latest cyber risks, from zero-day exploits to the evolving AI landscape

immersive

Be Ready

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