

Empower

Data Sheet

Unified Cyber Resilience for Governments

Jan 2025



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.



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

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	RESOURCE DEVELOPMENT 7 techniques	INITIAL ACCESS 9 techniques	EXECUTION 12 techniques	PERSISTENCE 19 techniques	PRIVILEGE ESCALATION 13 techniques	DEFENSE EVASION 40 techniques	CREDENTIAL ACCESS 15 techniques	DISCOVERY 29 techniques
Active Scanning 2 sub-techniques	Acquire Infrastructure 6 sub-techniques	Drive-by Compromise 1 sub-technique	Command and Scripting Interpreter 8 sub-techniques	Account Manipulation 4 sub-techniques	Abuse Elevation Control Mechanism 4 sub-techniques	Abuse Elevation Control Mechanism 4 sub-techniques	Adversary-in-the-Middle 2 sub-techniques	Account Discovery 4 sub-techniques
Gather Victim Host Information 4 sub-techniques	Compromise Accounts 2 sub-techniques	Exploit Public-Facing Application 1 sub-technique	Container Administration Command 1 sub-technique	BITS Jobs 1 sub-technique	Access Token Manipulation 3 sub-techniques	Access Token Manipulation 5 sub-techniques	Brute Force 4 sub-techniques	Application Window Discovery 1 sub-technique
Gather Victim Identity Information 3 sub-techniques	Compromise Infrastructure 8 sub-techniques	External Remote Services 1 sub-technique	Deploy Container 1 sub-technique	Boot or Logon Autostart Execution 15 sub-techniques	Boot or Logon Autostart Execution 19 sub-techniques	BITS Jobs 1 sub-technique	Credentials from Password Stores 5 sub-techniques	Browser Bookmark Discovery 1 sub-technique
Gather Victim Network Information 6 sub-techniques	Develop Capabilities 4 sub-techniques	Hardware Additions 1 sub-technique	Exploitation for Client Execution 1 sub-technique	Boot or Logon Initialization Scripts 5 sub-techniques	Boot or Logon Initialization Scripts 5 sub-techniques	Build Image on Host 1 sub-technique	Exploitation for Credential Access 1 sub-technique	Cloud Infrastructure Discovery 1 sub-technique
Gather Victim Org Information 4 sub-techniques	Establish Accounts 2 sub-techniques	Phishing 3 sub-techniques	Inter-Process Communication 2 sub-techniques	Browser Extensions 1 sub-technique	Boot or Logon Initialization Scripts 5 sub-techniques	Deobfuscate/Decode Files or Information 1 sub-technique	Forced Authentication 1 sub-technique	Cloud Service Dashboard 1 sub-technique
Phishing for Information 1 sub-technique	Obtain Capabilities 6 sub-techniques	Replication Through Removable Media 1 sub-technique	Native API 1 sub-technique	Compromise Client Software Binary 1 sub-technique	Create or Modify System Process 4 sub-techniques	Deploy Container 1 sub-technique	Forge Web Credentials 2 sub-techniques	Cloud Service Discovery 1 sub-technique
		Supply Chain Compromise 3 sub-techniques	Scheduled Task/Job 1 sub-technique	Create Account 1 sub-technique	Domain Policy 1 sub-technique	Direct Volume Access 1 sub-technique		Cloud Storage Object Discovery 1 sub-technique

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
--	---	--	--	--

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.

