

DATA SHEET

Immersive Labs Workforce Exercising



Cybersecurity Awareness Training doesn't drive resilience

Employees across your entire organization need more empowerment and support to change behavior and make effective security decisions.

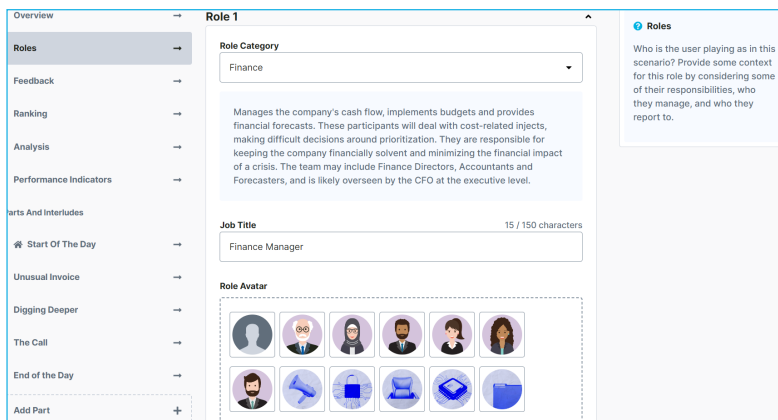
Engagement, metrics, and reporting should go beyond course completion rates to prioritize proving capabilities. A dynamic, data-driven, and continuous approach is necessary to drive or enable cyber resilience.

It's time for a cyber-confident workforce

Filling the gap left by typical security awareness training, Immersive Labs Workforce Exercising embraces behavioral science techniques to drive behavioral change in your workforce.

Engage and captivate your employees with relatable content using scenario-based exercises to baseline, assess, and upskill on crucial security behaviors – then educate with targeted, on-demand labs. Our customizable content covers the most critical risk areas, equipping your entire organization with the knowledge to navigate cyber risks.

Definitively know and understand your cyber readiness using data-driven assessments and readiness scores to help target learning interventions in your most exposed departments. Gain actionable insights and empower your workforce to drive real change. Invest in Immersive Labs Workforce Exercising and transform your organization's cyber resilience.



The screenshot shows a configuration interface for a role. On the left is a navigation menu with items like Overview, Roles, Feedback, Ranking, Analysis, Performance Indicators, and various scenario titles. The main area is titled 'Role 1' and contains a 'Role Category' dropdown set to 'Finance'. Below this is a text box describing the role: 'Manages the company's cash flow, implements budgets and provides financial forecasts. These participants will deal with cost-related injects, making difficult decisions around prioritization. They are responsible for keeping the company financially solvent and minimizing the financial impact of a crisis. The team may include Finance Directors, Accountants and Forecasters, and is likely overseen by the CFO at the executive level.' There is a 'Job Title' field with 'Finance Manager' entered. At the bottom, there is a 'Role Avatar' section with a grid of 12 icons representing different people and roles.

Assign role-based exercises across your organization

Benefits

- **Know using Data:** Gather employee data for tailored training and improved cyber resilience.
- **Change Behavior:** Foster secure practices through engaging labs, prompting change.
- **Assess Risk Areas:** Spot risks and vulnerabilities to fortify security using data-driven insights.
- **Prove with Evidence:** Confirm and demonstrate preparedness and earn stakeholder confidence.
- **Measure Effectiveness:** Gauge change and tweak strategies for robust cyber resilience.
- **Empower:** Instill cybersecurity culture through behavior shaping.

Why Workforce Exercising Matters

Drive Behavioral Change

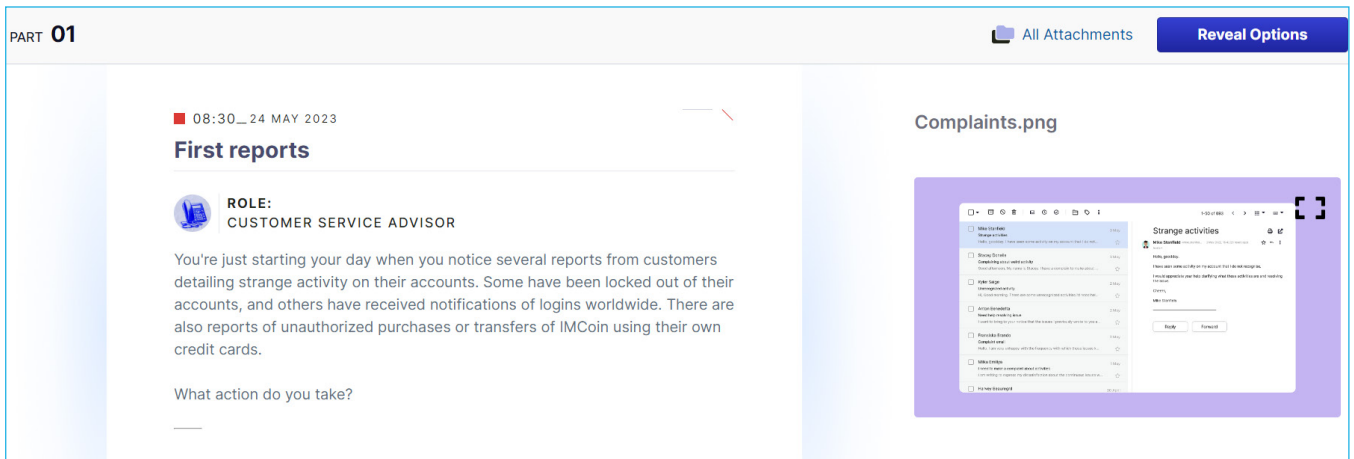
- Go beyond security awareness – it's decisions and actions that count!
- Understand and target risky behaviors to strengthen organizational resilience
- Build a foundation for behavioral change
- Apply relatable content and labs

Baseline, Assess, and Upskill

- Baseline strengths and potential risks across the organization with our Security Hygiene Compass
- Educate on the how and why behind upskilling to empower with knowledge and judgment
- Use outputs to assess and measure education and upskilling impact over time

Target Vulnerable Areas

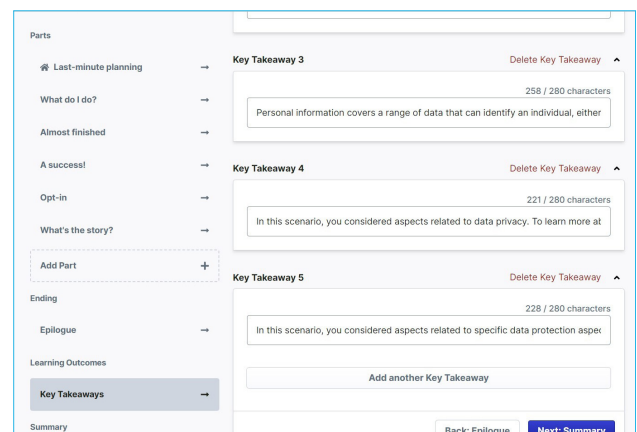
- Pinpoint groups with high risk and exposure to cyber threats, such as finance, supply chain, legal and compliance
- Deploy labs covering everything from the basics to more advanced theory and Cybersecurity practice
- Target on-demand labs and exercises based on Security Hygiene Compass assessments



Use ready-made exercises or tailor them to your exact specifications

84% of cybersecurity leaders want to mitigate risk by managing employee behavior, but only **43%** measure security behavior ¹

¹Gartner (2022). Innovation Insight on Security Behavior and Culture Program Capabilities



Key takeaways can be customized to reinforce behavioral change

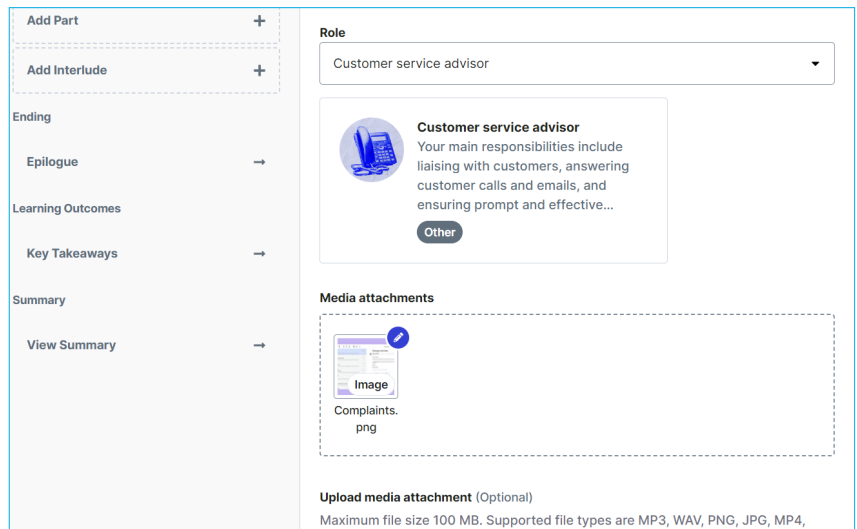
Trusted by the world's largest companies, governments, and defense organizations



WORKFORCE EXERCISING RISK AREA COVERAGE

<p>1 Authentication: Verifying the identity of a user</p>	<p>5 Data handling: Collecting, storing, using, and disposing of data</p>
<p>2 Physical security: Protecting assets and people from physical attacks and unauthorized access</p>	<p>6 Security reporting and responsiveness: Reporting security incidents, data breaches, or suspicious activity and responding proactively to security threats</p>
<p>3 Device security: Securing laptops, smartphones, and other connected devices</p>	<p>7 Digital footprint: Managing an individual's online presence</p>
<p>4 Browsing securely: Responding to browser security alerts and checking for security information on websites (such as HTTPS) before making payments.</p>	<p>8 Social engineering: Detecting and preventing malicious influence and deception attempts</p>

Immersive Labs Workforce Exercising empowers a cyber-confident workforce by leveraging Behavioral Science techniques. Through relatable content and targeted exercises, it addresses key risks and promotes secure behaviors.



Leverage multi-media to increase engagement

Data-driven reports with actionable insights and our exclusive readiness score includes color-coded dashboards displaying risk percentages by security topics – such as social engineering, physical security, and phishing. It also provides a detailed breakdown by risk areas, teams and individuals to help pinpoint where more upskilling is needed.

Certification & Compliance



Trusted by the world's largest organizations

Over **400** customers

>3.5M total labs completed

>100,000 unique users

>1,700 hands-on challenges

Let's get started! Ready to accelerate your Cyber Workforce Resilience journey with stress test exercises? Contact your Immersive Labs Account Manager to learn more.