# FOR CYBERSECURITY TEAMS

*An effective cybersecurity team is one where human assets align directly to risk, ensuring the skills are in place to identify weaknesses, apply security controls, and respond to incidents. In a fast-paced and highly fluid threat landscape, however, passive training courses and certifications struggle to achieve this.*

Our progressive Human Cyber Readiness platform is specifically designed to address this problem, providing three core outcomes:

## EQUIPPING

Continually introducing new capabilities which map to the demands of the breaking threat environment and the ever-changing nature of organizational risk.

## EXERCISING

Simulate both full-scale organizational crises and smaller, highly technical, incidents to build cognitively agile human assets who can adapt in a crisis.

## EVIDENCING

Understand your skills capabilities with real-time data on human assets for better strategies, resource planning and board reporting.

## BUILDING HUMAN CYBER READINESS IN CYBERSECURITY TEAMS

Our platform embeds skills by immersing individuals in challenges, scenarios and simulations in the browser to teach everything from threat hunting and reverse engineering, to SecDevOps. We build more relevant skills in a number of ways:

1. **Threat intelligence based:** Skills development is based on emerging tactics, techniques and procedures from some of the industry's most well-regarded threat intelligence feeds. Human assets can be fully versed on attacks just hours after they emerge in the wild. For security teams, this means a process of continuous skills evolution, stopping defenders being outpaced by attackers.
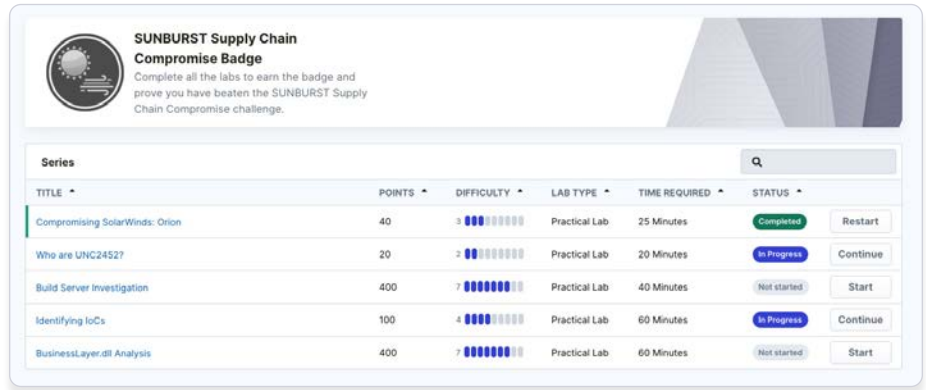


2. **Dynamic storylines:** Realistic cyber narratives are played out on a rich media platform capable of simulating everything from social engineering in a bank to a company-wide crisis in a power station. Replacing the static slide-based approach leads to greater engagement which, in turn, means cyber teams take ownership of their personal skills development. In this way, the platform also becomes a talent retention tool.
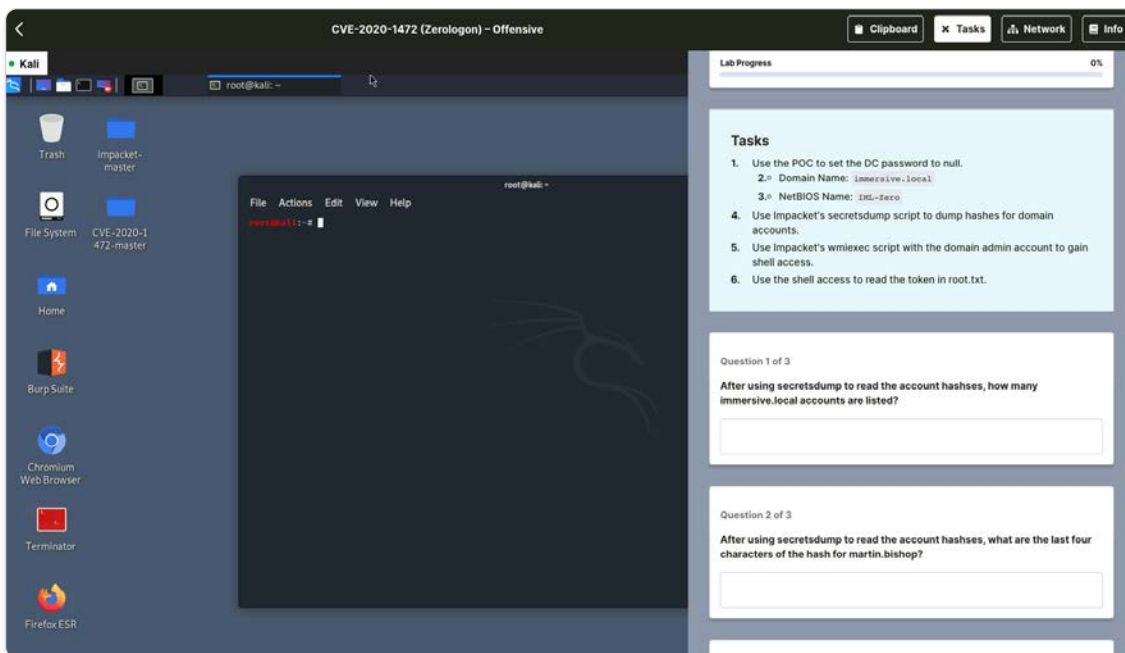
**3. Actionable insights:**
Use real-time data to measure and visualize the skill levels of your organization's human assets and map this against frameworks such as NIST NICE and MITRE ATT&CK for context. This helps security teams understand capability blackspots relevant to the threat environment, make better strategic decisions, invest with confidence and report to the board.
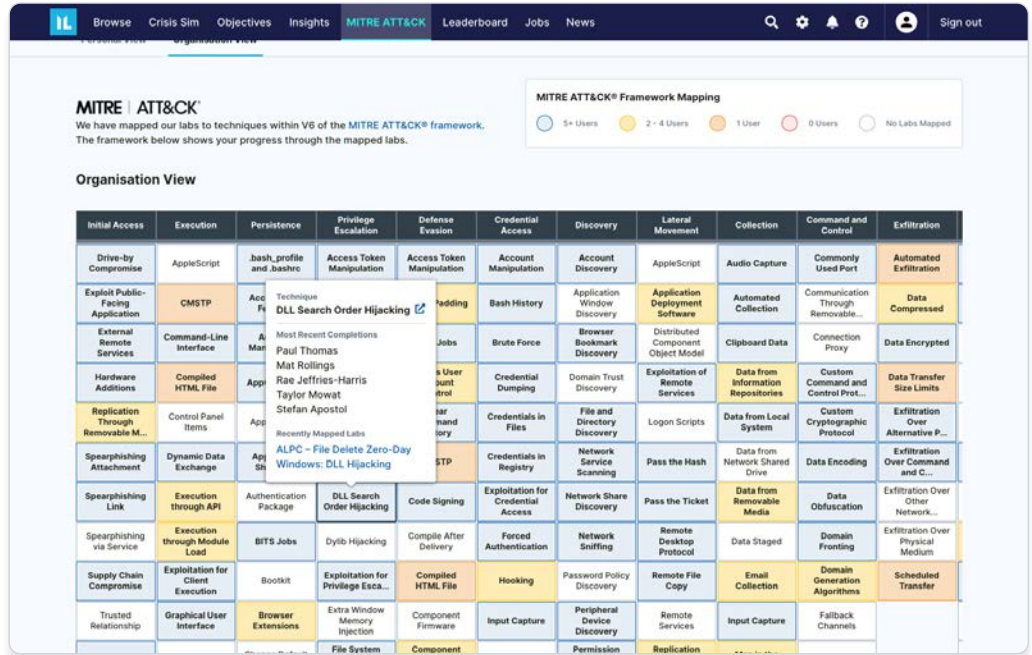


**4. Browser-based:** With skills development and crisis simulations no longer time-intensive meetings requiring lots of attendees, our platform is perfect for large dispersed cybersecurity teams. It also enables a culture of micro-drilling, letting cybersecurity teams run faster, shorter, more relevant incident response simulations. Such an approach is used by progressive cybersecurity leaders to deal with the problem of skills decay and create more adaptable IR teams capable of thinking on their feet in highly pressurized situations.
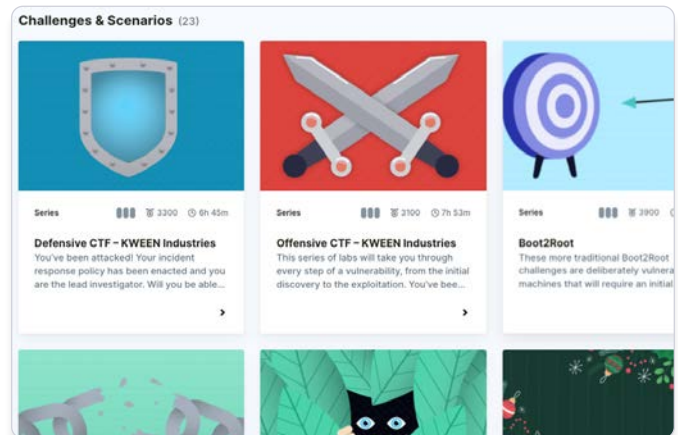
## DON'T JUST TAKE OUR WORD FOR IT.

We have a network of customers, including some of the world's biggest names cross finance, defense, military, government, and more.

**Immersive Labs is the world's first human cyber readiness platform.**

Our technology delivers challenge-based cybersecurity content developed by experts and powered by the latest threat intelligence. Our unique approach enables businesses to battle-test and evidence their workforce's preparedness to face emerging cyber threats.