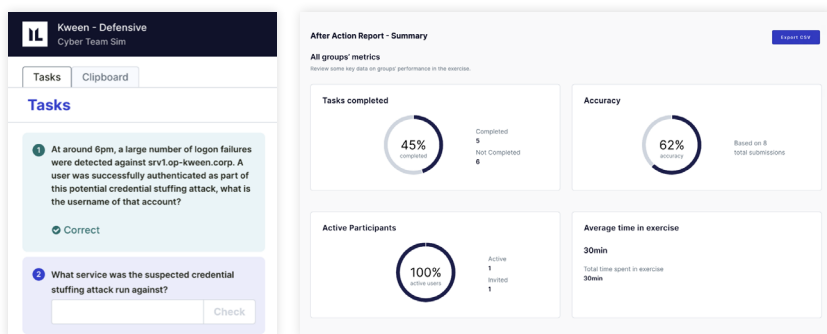# IMMERSIVELABS

Technical Exercises

Build your cyber teams' technical capabilities

Responding to a security incident on your network and preparing for an inevitable attack is the job of a team rather than an individual. In addition, certifications and point-in-time solutions can't keep pace with attackers – organizations need data that proves their offensive and defensive teams are prepared for the latest threats.

Immersive Labs provides the ability to exercise your teams' capabilities in complex environments that are representative of what they experience in their day-to-day operations. These provide security teams with preconfigured, task-based, technical simulations that enable teams to collaborate through real-world scenarios.

With our custom cyber range capability, you can even replicate your own environment so you can work within it safely, without compromising the security and robustness of your network. You can even bring your own tools.

Benefits

- Regular practice in realistic scenarios helps your teams perform optimally when real incidents occur
- Practice more frequently using always-available scenarios that you can use in minutes
- Rapidly build complex, customized environments, enabling teams to practice with enterprise tools in environments similar to their day-to-day work environment
- Prove team performance and build confidence that your people are prepared to respond to the latest threats
- Identify gaps in current knowledge and show team improvement over time, confirming ROI on upskilling

Audiences

- Defensive Teams
- Penetration Testing Teams
- SOC Team

An overview of tasks to complete in Cyber Team Sim and associated after-action reporting

Based on the Latest Cyber Threats
Pre-built scenarios are designed to simulate the real-world attacks your organization is likely to face and situations in which your team must deal with to strengthen weaknesses in the environment.

Risk-free Environments
Use our pre-configured environments or create your own to safely practice all aspects of defensive and offensive cybersecurity and build team resilience. Develop and measure team dynamics through a safe experience that sits outside of your own infrastructure.

Data-Driven
Results of cyber team simulations are scored for individuals and the entire team. This provides the proof required that the organization will be ready for a real-life cyber attack (or that more exercising is required).

Scalable
Exercises can be undertaken by a dispersed team, no matter where they are in the world.

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

HSBC · Pfizer · Citi · DAIMLER · McLaren · nationalgrid

THE LEADER IN PEOPLE-CENTRIC CYBER RESILIENCE   immersivelabs.com | sales@immersivelabs.com

Work through exercises in pre-built environments...

A sample of technical scenarios

| TITLE	DESCRIPTION
Artica - Defensive	You must detect a live attack against the Artica Shipping Company and work to identify the extent of the breach. Nothing is known about the compromise ahead of time, you will have to utilize the tools available to you to gain insight into the attackers' actions.
Artica - Offensive	Artica Shipping Company comprises a small IT estate and have requested a security audit before expanding their current network further. Your goal is to compromise the domain controller with a domain admin account. Flags have been placed around the machines in the range for you to collect as you progress.
Kween - Defensive	Kween Industries suspect that their network has been compromised by an unknown attacker. You've been called in to investigate! The client has given you access to their Splunk and Velociraptor setups and have provided information regarding their network.
Kween - Offensive	Kween Industries have hired you to perform a penetration test of their network as part of a security audit.
Qing - Defensive	The Qing corporation recently experienced disruption to its OT equipment. They are concerned that it may be the result of malicious action by an unknown attacker and have demanded a full investigation before resuming operations. However, the company notes that their coverage of the OT network is limited so proof of unauthorized access to the OT network will suffice.
Qing - Defensive	The Qing corporation has requested a test of their infrastructure security. Their environment consists of mostly Windows machines controlled by a single Active Directory domain. The customer is particularly interested in identifying any vulnerabilities that lead to unauthorised access to their OT network, and any subsequent vulnerabilities that would allow an attacker to interfere with or damage their operational equipment.

... or create your own

Custom Cyber Ranges

Emulating your production environment provides security teams with a safe area to test tools, develop, and learn whilst facilitating these types of environments in-house can be a drain on resources.

Immersive Labs Cyber Ranges enables you to build customizable environments, available on demand when you need them. Create complex ranges in hours, not weeks – with minimal maintenance.
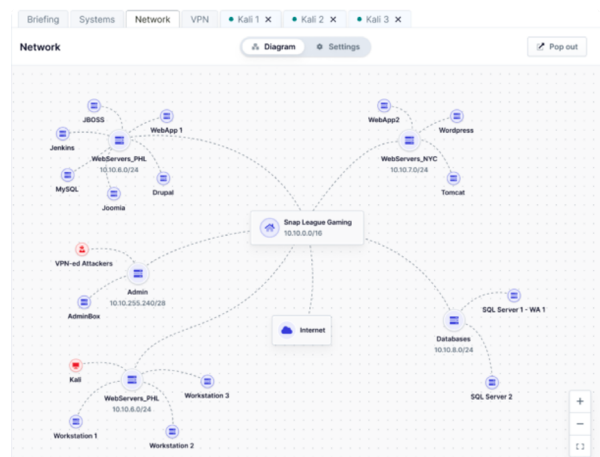
Build in hours, launch in minutes

Immersive Labs Cyber Ranges provides you with on-demand access to your custom ranges in minutes: your enviroments are available when you need them and automatically power down when you dont.

Bring in your own tools and vendors

Cloud-based networks can be customized to meet your team's needs and emulate virtually any target enviroment. Whatever your use case, ensure the highest relevance by bringing existing tools and vendors into a range.