immersive

Respond

Data Sheet | Technical Exercises

Build Your Cyber Teams' Technical Capabilities

Jan 2025

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.

Cyber Team Simulations provide 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 production network. You can also choose to bring your own tools.

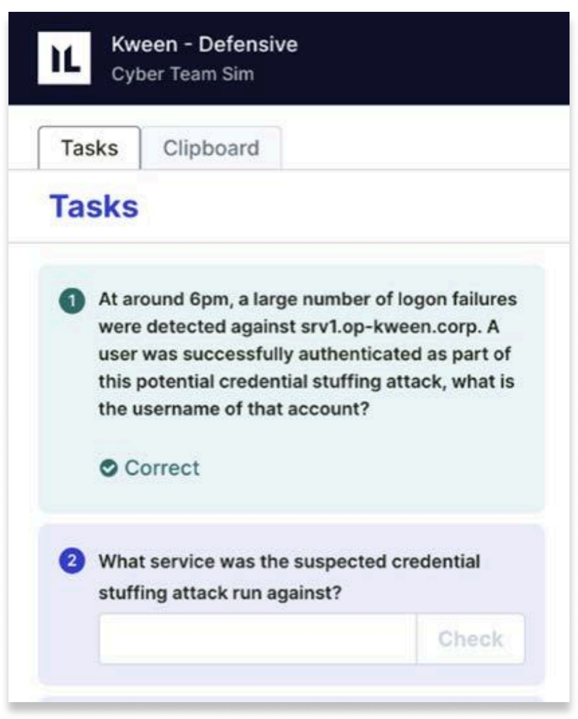
Benefits

- 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 demostrate team improvement over time to prove 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



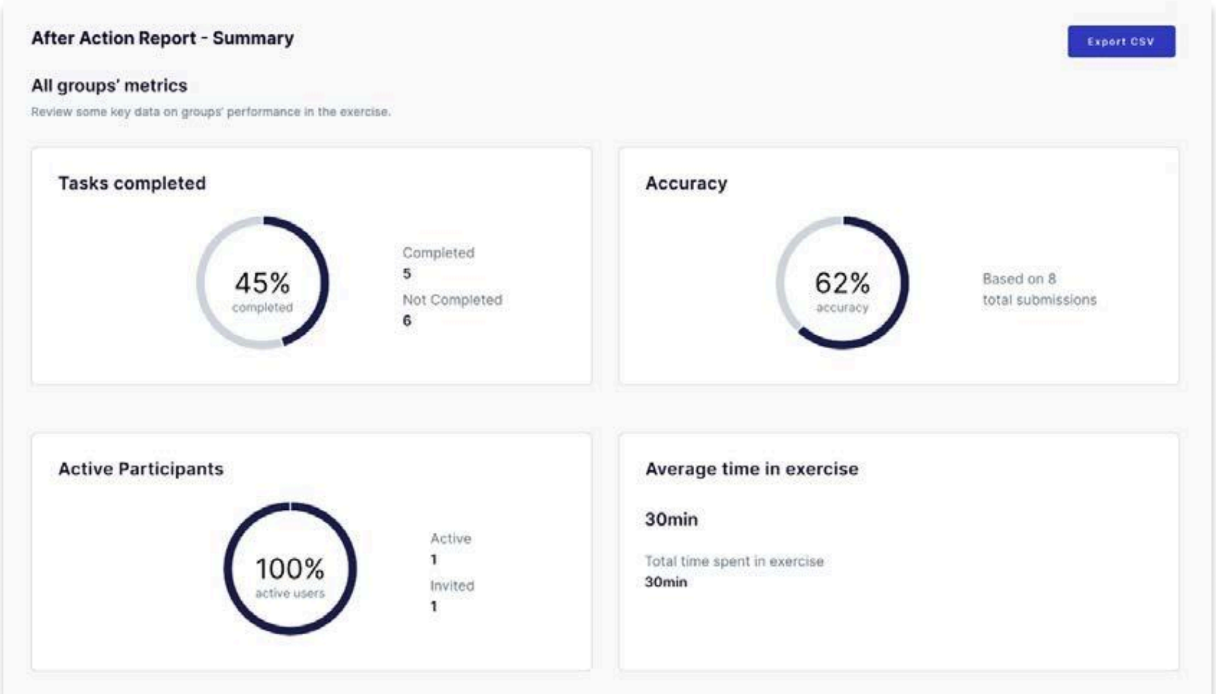
Kween - Defensive
Cyber Team Sim

Tasks

1 At around 6pm, a large number of logon failures were detected against srv1.op-kween.corp. A user was successfully authenticated as part of this potential credential stuffing attack, what is the username of that account?

✓ Correct

2 What service was the suspected credential stuffing attack run against?



After Action Report - Summary

All groups’ metrics
Review some key data on groups’ performance in the exercise.

Tasks completed
45% completed
Completed 5
Not Completed 6

Accuracy
62% accuracy
Based on 8 total submissions

Active Participants
100% active users
Active 1
Invited 1

Average time in exercise
30min
Total time spent in exercise 30min

Scalable

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

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 their environment.

Risk-Free Environments

Use our pre-configured environments or create your own to safely practice all aspects of defensive and offensive cyber security 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).

Trusted by the world’s largest organizations: HSBC Pfizer citi T · · Mobile · airbnb nationalgrid Goldman Sachs

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.

Custom Cyber Ranges

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

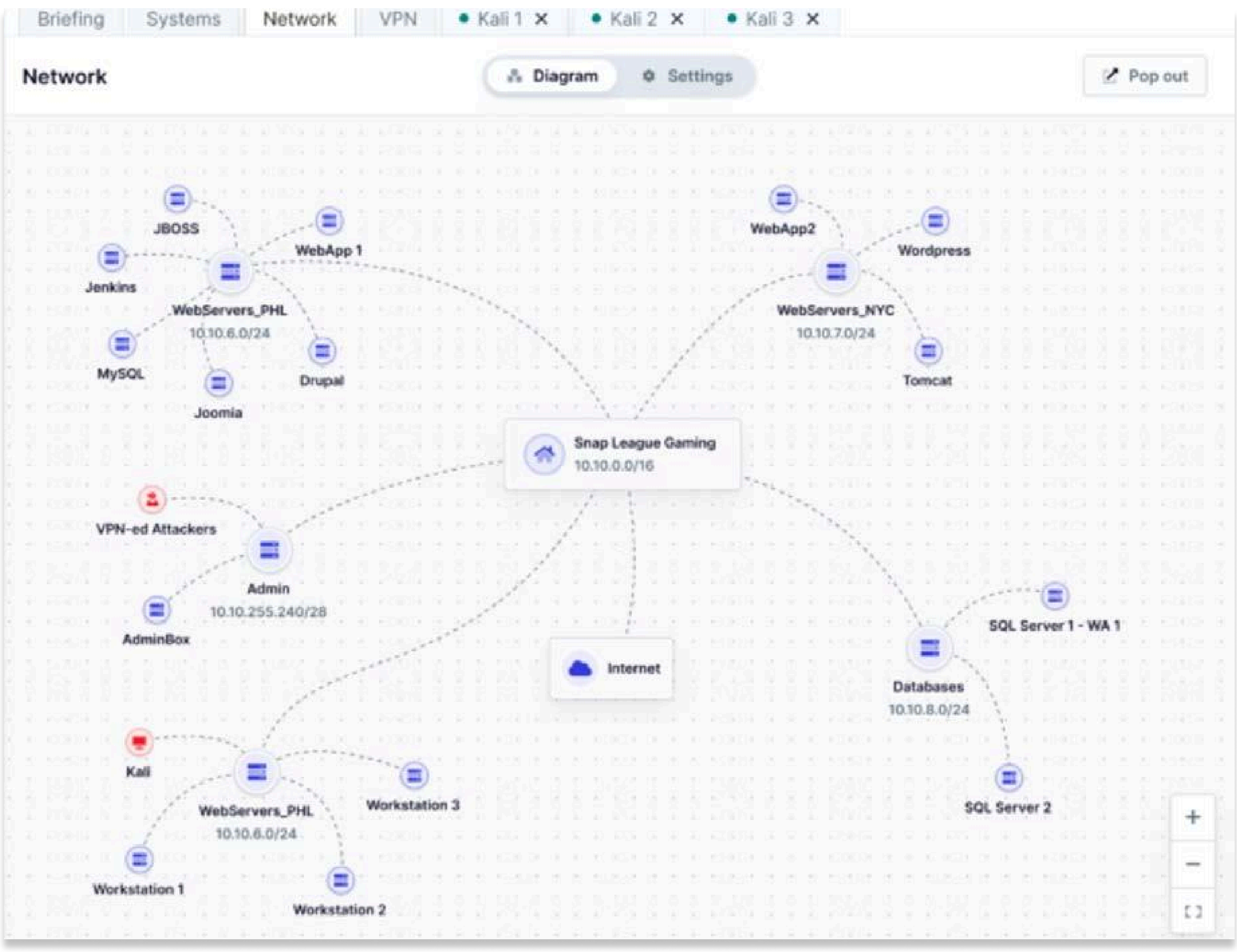
Build in Hours, Launch in Minutes

Immersive Cyber Ranges provides you with on-demand access to your custom ranges in minutes: your environments are available when you need them and automatically power down when you don't.

Bring in Your Own Tools and Vendors

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

… or create your own



Certification & Compliance			Trusted by the World's Largest Organizations			
Information Security Management ISO 27001 Certified	CYBER ESSENTIALS CERTIFIED	GDPR	**400+** Customers	**>3.5M** Total Labs Complete	**>100K** Unique Users	**>2K** Hands-on Challenges

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