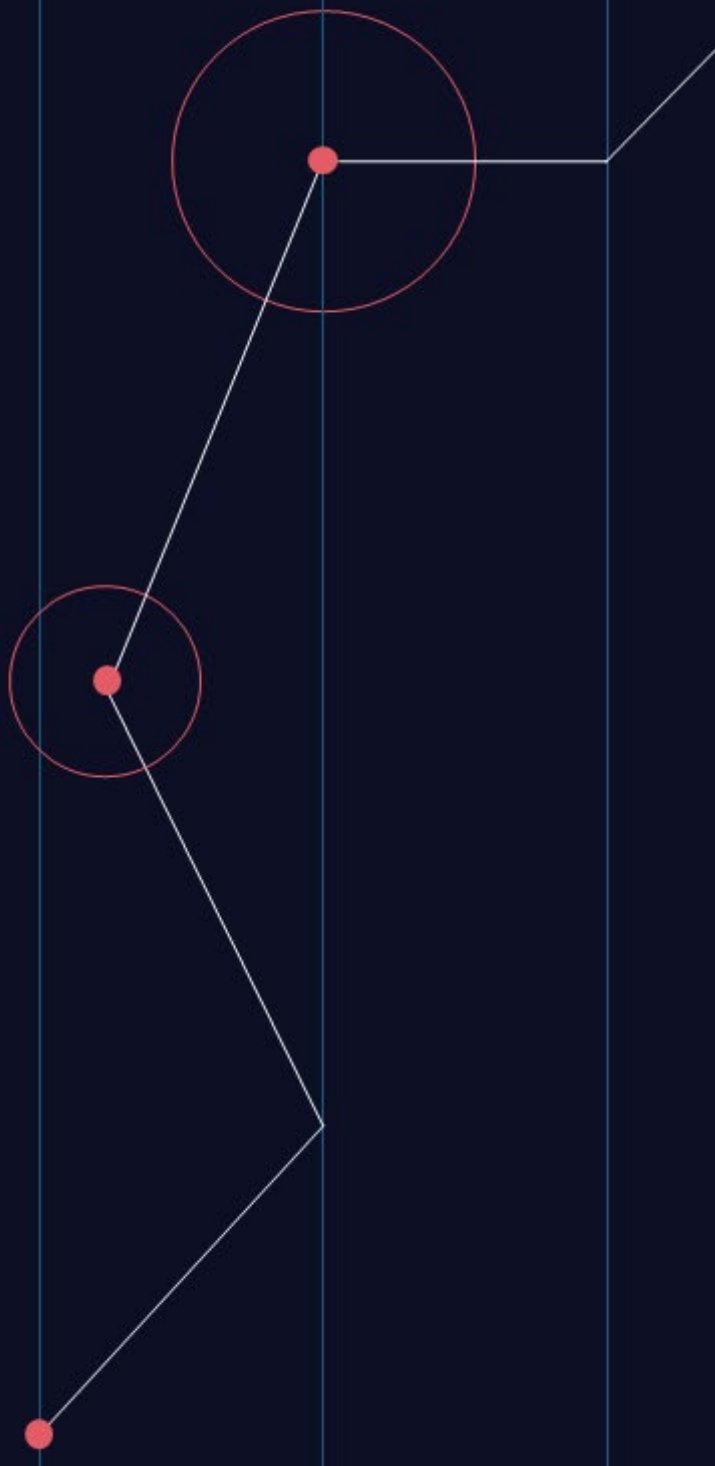
IMMERSIVELABS

The Leader in People-Centric Cyber Resilience

PRODUCT AND SERVICES GUIDE

Version 2024.06



1. Product and Services Guide

This Product and Services Guide forms part of and is incorporated by reference into the Immersive Labs Master Services Agreement (**MSA**), which covers the licensing of access to the Immersive Labs Platform and services provided by Immersive Labs to you, the Customer.

The purpose of this Product and Services Guide is to set out details of the products and services we provide to you, the overall standard that we aim to achieve, and your remedy for resolving any technical issues.

The specific products and services to be provided to each customer and the relevant purchase method shall be as specified in the applicable Order Form.

2. Platform Objectives

Immersive Labs helps organizations continuously assess, build, and prove their cyber capabilities and team readiness, from front-line cybersecurity and development teams to Board-level executives. We accomplish this using a Cyber Workforce Resilience Platform.

Unlike legacy training that focuses on individuals and learning in isolation, Immersive Labs prepares both individuals and teams with exercises, labs, and simulations that test performance in realistic scenarios.

We upskill teams with advanced cyber capabilities, including reverse engineering, exploit development, cyber range technology, and malware analysis – and provide the data needed to prove customer cyber resilience.

3. Purchase Methods

3.1 Module Purchases

A module purchase provides limited access to specific areas of the Platform, subject to the licensing restrictions in the MSA. At the time of publication of this Product and Services Guide, Immersive Labs offers seven modules – for which the objectives, purchase methods, and licensing models are more particularly described in Section 4.

3.2 Enterprise Suite Purchases

The Enterprise Suite provides customers with access to all platform modules, except for Cyber Ranges. This comes in two forms:

a) Cyber Workforce Resilience Package: Flexible adoption of key modules to reflect the size of the organization, subject to minimum requirements within each solution area.

b) Ultimate Cyber Workforce Resilience Package: Unrestricted (subject to fair use - e.g., a maximum number of 50,000 Authorized Users/assessments per annum) of Hands-on Labs and Organizational Exercising solution areas, and access to a Large Team Sim credit package.

4. Platform Solution Areas

The Immersive Labs platform comprises three main solution areas, with a selection of underlying modules within each of these. Each solution area plays a key role in helping drive the resilience of your entire organization, building upon one another in a complementary manner.

Solutions	Description	Module
Hands-On Labs - Cyber Training for Individuals	Highly technical labs that cover a huge range of cybersecurity topics, including offensive, defensive, cloud, and application security	CyberPro
		Application Security
		Candidate Screening
Immersive Crisis Exercises	Engaging team-based simulations that	Cyber Team Sim

	respond to security threats	Cyber Ranges
		Cyber Crisis Simulator
Cyber Exercises for Organizations	Skills development exercises to drive behavioral change	Workforce

4.1 Hands-On Labs

Learn from highly technical labs that cover all aspects of cybersecurity, including offensive, defensive, cloud, and application security, along with governance, risk, and compliance. Use gamified techniques and master topics from security fundamentals to malware reverse engineering and advanced threat hunting. Granular reporting on performance data for both individuals and teams helps benchmark and prove cyber capabilities.

Access to hands-on lab products such as CyberPro and AppSec is provided on a per-user basis. A single license provides a specified user with access to the relevant labs for the term specified in the Order Form. These licenses may not be transferred or shared between users during the term.

The candidate screening product is also labs-based and is licensed on a per-assessment basis, where a package of assessments is allocated to be used over the term specified in the Order Form. One assessment is consumed for every lab that is assigned to a user.

CyberPro

CyberPro is our comprehensive license for Hands-on Labs, covering a huge range of topics - from the fundamentals of cybersecurity to the most advanced areas. Equip your security team with the skills that they need, highlighting areas of comparative strength and weakness against industry standard frameworks such as MITRE ATT&CK.

Key cybersecurity lab areas include (but are not limited to):

- Fundamentals
- Defensive Cyber
- Application Security
- Malware & Reverse Engineering
- Cyber Threat Intelligence
- Cloud Security
- Challenges & Scenarios
- Offensive Cyber
- Tools

Labs are written by industry leaders and our elite hackers to put users' knowledge to the test using hands-on challenges.

Labs may be based on real-time threat intelligence and give users hands-on experience with real-world attacks and how to defend against them.

AppSec

Application Security Labs are aimed at developers and application security engineers with the objective of teaching them how to code securely to mitigate the risk of a cyber breach. Cloud Security labs are included in the Application Security package, helping to equip developers with the skills they need to deploy securely to the cloud.

The Application Security Labs create a realistic development environment that gives users live code to identify, exploit, change, analyze, and validate security vulnerabilities. Once the user submits their revised code, the labs scan for vulnerabilities and detect bugs. The user must fix all detected bugs and redeploy the code to pass all functional checks before they can complete a lab.

Candidate Screening

Candidate Screening helps organizations test applicants against the specific skills required for an open cybersecurity position. Immersive Labs' hands-on challenges enable remote testing of relevant technical abilities before advancing a candidate to the interview stage. Our labs simulate real-world scenarios, allowing organizations to test how well a candidate might perform on the job and under pressure.

Choose from a predefined selection of screening labs covering a wide range of topics or create a custom assessment from any lab to which the hiring manager has access. These assessments may then be assigned to prospective candidates for completion.

Unlike other hands-on labs modules, candidate screening is purchased on a “per assessment” basis, with a single assessment allowing the playthrough of an assigned collection of labs by a potential candidate.

4.2 Immersive Crisis Exercises

Cyber Team Sim

Highly technical response exercises that stress test SOC and incident response teams. Provides reporting with evidence of team capabilities against specific threat scenarios run on a pre-configured cyber range. Advanced users can also replicate their environment and tools using custom cyber ranges.

Managers within the platform can schedule Team Sim exercises from a catalog of pre-built scenarios after purchase.

Customers access Team Sim through a credit system. Groups of up to 10 users may work together to complete a specified scenario. Multiple groups may take part in the same exercise, with separate virtual environments created for each of these. One Team Sim credit is consumed for each group (of up to 10 users) playing through a single scenario.

There is no carry-over of unused credits to subsequent years, and credits are always consumed in whole numbers (e.g. a group of 5 users would still consume 1 credit). Exercises may be run for a maximum of 5 days.

The number of credits within the applicable License Band (Small, Medium, Large, or Custom) will be specified in the Order Form, clearly showing the number of credits assigned per year and the total for the whole term.

Team Sim customers who also purchase Cyber Ranges may customize scenarios from the pre-existing catalog or create these from scratch to more closely meet their requirements.

Cyber Ranges

Immersive Labs Cyber Ranges with pre-configured range templates provide the fastest way for technical teams to create hyper-realistic representations of enterprise networks. Ranges enable high-value use cases like detection engineering, malware analysis, tool testing & validation, and research & development activities. Immersive Labs Cyber Ranges support a wide variety of out-of-the-box systems and software configurations and also enable the creation and deployment of custom Ranges.

Cyber Range customers who also purchase Team Sim may create custom exercises by modifying pre-existing scenarios or creating these from scratch.

Note that where you have been approved to bring your own third-party tools to use in a custom scenario, you are responsible for purchasing and paying fees for such tooling.

When creating custom scenarios in the Ranges Platform, customers shall not modify the baseline provisioned IOPS volume (being 3,000 IOPS) for the relevant application. For use cases where the application needs more performance than the baseline, we will discuss and agree any volume increased, in which case we reserve the right to adjust the charges to reflect any increased cost.

The maximum number of range resources (size of the range(s) based on the CPU/GB RAM (as maximum resources that may be allocated to a range at one time)) is limited by the selected package (Small, Medium, Large, or Custom) you have purchased, details of which will be specified on the Order Form.

Cyber Crisis Sim

Stress test crisis decision-making with scenarios that deliver severe but plausible exercises from the C-suite to employees at all levels of the organization. Leverage simulations that reflect how real-life crises unfold. Browser-based to remove the logistical burdens of in-person exercises ideal for globally-dispersed teams. Reports track individual and team performance to prove readiness and enhance cyber crisis decision-making.

Customers have the ability to use catalog scenarios, modify catalog scenarios, or create new ones from scratch using the Cyber Crisis Sim content builder. This allows teams to run exercises that are fully tailored to their needs, offering an immersive and highly realistic experience.

Crisis Sim can be purchased in small, medium, or large (unlimited) packages which outline how many exercises can run per annum, details of which will be specified on the Order Form.

There is an overall maximum limit of 1,000 Authorized Users participating in any given exercise.

4.3 Cyber Exercises for Organizations

Workforce Exercising

Workforce Exercising is our license package which provides on demand Labs to drive behavioral change in the whole of an organization's workforce. Employees will be provided with relatable content, using scenario-based exercises, to baseline, assess, and upskill on crucial security behaviors. The customizable content covers the most critical risk areas, equipping your entire organization with the knowledge to navigate cyber risks.

Access to Workforce Exercising is provided on a per-user basis. A single license provides a specified user with access to the relevant labs for the term specified in the Order Form. These may not be transferred or shared between users during the term.

5. Service Availability

The Immersive Labs Platform is designed to be available 24 hours a day, 7 days a week, 365 days a year.

We use reasonable commercial endeavors to operate a target minimum platform availability of 99.5% uptime excluding any excusable downtime (being any downtime due to circumstances beyond our reasonable control (e.g., caused by: (i) the customer using the Platform in a manner not authorized, (ii) a force majeure event, (iii) third-party services, vendors, equipment, apps, software, connections or utilities, and (iv) routine schedule maintenance)). We monitor the uptime of our services using a third-party company that generates alerts in the event the site is unavailable and can generate reports, alerts, and dashboards for the uptime of the Platform.

For the avoidance of doubt, we do not offer service credits.

You are required to provide any software or hardware that is necessary for you or your users to gain access to the Immersive Labs Platform (including enabling any whitelists that may be required) and your network and systems must comply with the Minimum System Specification.

6. Customer Support

We provide support for both the web application and underlying content served in the Platform. Our Customer Support can be contacted 24/7 via our online support portal, telephone and email.

Contact Options	Details
Support Portal	Accessed on the Platform or via https://immersivelabs.zendesk.com/hc/en-us
Telephone	UK: +44(0) 345-646-1544 US: +1 855-202-2423

Email	support@immersivelabs.com

We monitor the support tickets and the support inbox and aim to respond to queries in accordance with the Response Targets set out in the table below.

Working hours are 09.00 to 17.00 GMT/BST/EST Monday to Friday (excluding UK bank and US public holidays) (as applicable).

In the event you or your Authorized Users experience a fault with the Platform, please report it as soon as possible using one of the methods above.

We use four tiers of incident depending on the scale and severity of the issue and have target response and resolution times for each priority level (which will apply during working hours only).

Where development work is required or where the incident is due to excusable downtime, the target resolution times may be extended. We will attempt to achieve the target response and resolution times across each priority level once we have classified the incident. To the extent this cannot be achieved, we shall use our reasonable commercial endeavors to resolve the incident promptly or provide you with an alternative means of accomplishing the desired performance.

	Description	Reporting Method	Response Target
Priority 1	All users in a region cannot access any content or reports. OR A significant percentage of users cannot access a material proportion of content or reporting.	Immersive Labs notified via uptime monitor. Support Ticket CSM Communication	Support team working inside working hours and on-call hours until resolved, with a 2-hour initial target to resolve.
Priority 2	Multiple users cannot access multiple items of content or multiple reports.	Support Ticket CSM Communication	Investigated inside working hours with a 0.5-day target to resolve.
Priority 3	Multiple users cannot access a single item of content or report. OR A single user cannot access multiple items of content or reports.	Support Ticket CSM Communication	Investigated inside working hours with a 1-day target to resolve.
Priority 4	A single user cannot access a single item of content or report.	Support Ticket CSM Communication	Investigated inside working hours with a 5-day target to resolve.

We offer **Premium Support** as additional option for customers to purchase, which includes access to support services provided by our Cyber Resilience Team, and details of this can be found in the Premium Support Statement of Work.

7. Complaints

Complaints with Immersive Labs' support services should be addressed to the Immersive Labs account manager or to support@immersivelabs.com who will then forward the complaint to your account manager or a member of our Senior Leadership Team (as appropriate).

8. Changes

The Platform is provided as a software-as-a-service solution. Therefore, we may make changes (including procedural and functionality changes) without prior notice. If these changes result in a

material degradation to the performance, accessibility, or available functionality, you may write to us and raise a query with your account manager or by emailing support@ immersivelabs.com.

We reserve the right to add, amend and discontinue features and modules from time to time. Where this occurs, we will endeavor to notify you where practical.

We may modify this Product and Services Guide at any time by posting a revised version on our website at www.immersivelabs.com/legal/ or by otherwise notifying you. All modified terms will become effective upon posting or as otherwise stated in the notice. By continuing to use the Platform after that date, you agree to be bound by the modified terms and conditions.

9. Disclaimers

We are not responsible for any delays, delivery failures, or other loss or damage resulting from the transfer of data over communications networks and facilities, including the internet and Immersive Labs does not warrant that your use of the Platform will be uninterrupted or error-free.

Immersive Labs does not warrant that the services, this guide, and/or information obtained by you through the services will meet any outcomes or results or your requirements and any reliance on any opinion, statement or other information is at your sole risk.

The products and services (including the Platform and any professional services) are provided by us to you for internal training and educational purposes only and shall not be taken to be advice; we do not accept any responsibility to any party for the use of the products and services for any purpose other than such training or educational purposes.

Version 06.2024

This Agreement was last updated on 9 September 2024