IMMERSIVE LABS
PRODUCT AND SERVICES GUIDE
(INCLUDING SLA)

Version 2022.10

support@immersivelabs.com | www.immersivelabs.com | +44 (0)20 3893 9101 | @immersivelabs

TABLE OF CONTENTS

1. Product and Service Guide

This Product and Product and Services Guide forms part of, and is incorporated by reference, into the Master Services Agreement for Customers and any negotiated agreement between Immersive Labs and its customers or channel partners that covers the purchase of software and professional services provided by Immersive Labs.

The purpose of this Product and Services Guide is to set out details of the products and services we provide to our customers, the overall standard which we aim to achieve inthe provision of our services and to provide a mechanism for resolving any issues.

2. Platform Objectives

The Immersive Labs platform is used for equipping, exercising, and evidencing the cyber skills of entire workforces, preparing businesses to counter the latest cyber threats. Immersive Labs offers a fully interactive, on-demand and gamified cyber skills platform, with a huge range of cyber skills topics mapped against industry frameworks.

3. Purchase Method

Immersive Labs offer three principal purchase routes through which customers can procure access to the platform:

- a module purchase;
- human cyber readiness platform (Enterprise Suite); or
- a combination of Enterprise Suite and additional module(s).

3.1. Modules

A module purchase provides limited access to specific areas of the platform (as further described in Section 4). At the time of publication of this Product and Services Guide, Immersive Labs offers seven modules - the objectives and purchase methods for which are more particularly described below.

	Modules						
	IMMERSIVE CRISIS	IMMERSIVE CYBERPRO	IMMERSIVE APPSEC	IMMERSIVE TALENT	IMMERSIVE CLOUDSEC	IMMERSIVE TEAM SIM	IMMERSIVE RANGES
OBJECTIVE	Stress testing organizational decision making in response to cyber crises	Power up human capability to demonstrate resilience in the face of evolving threats.	Embed security expertise across every individual in the software development lifecycle.	Increase speed and diversity in hiring. De-mystify technical skills and talents.	Embed security best practices in the Cloud for developers, engineers and security professionals.	Immerses technical security practitioners into realistic offensive and defensive security incident scenarios.	Create hyper realistic representations of enterprise networks for high value use cases.
PURCHASE	The level of purchase is specified in the order form/quote.	Each module purchased has an associated "Licence Band". The maximum quantity of Authorised Users or assessments (for Immersive Talent only) shall not exceed the limit set out in the Order. To increase the number of Authorised Users (or assessments) within a module, the Licence Band must be upgraded.					

3.2. *Human Cyber Readiness Platform (Enterprise Suite)*

The Enterprise Suite provides customers with access to the platform for the whole organisation, with content across the four modules listed below as well as access to a fifth bonus module - the Awareness Arcade.

The Enterprise Suite may be purchased in one of four tiers, the table below sets out the tiers available to customers, the nature of access and maximum number of Authorised Users or assessments (as applicable) included with each.

		HUMAN CYBER READINESS PLATFORM			
		Tier 1	**Tier 2**	**Tier 3**	**Tier 4**
MODULE LIMITS BY TIER	**IMMERSIVE CRISIS**	Pre-built scenarios only	Pre-built scenarios as specified in the order form/quote		
	IMMERSIVE CYBERPRO *(number of Authorised Users)*	10	50	100	Unlimited**
	IMMERSIVE APPSEC *(number of Authorised Users)*	250	1,000	2,000	Unlimited**
	IMMERSIVE TALENT *(number of assessments per annum)****	500	1,000	5,000	Unlimited**
	AWARENESS ARCADE *(number of Authorised Users)*	Unlimited**	Unlimited**	Unlimited**	Unlimited**

**** Unlimited access is subject always to a maximum number of 50,000 Authorised Users / assessments per annum.**

***** To the extent that a customer has not utilised its full assessment entitlement within the Immersive Talent module, the number of assessments will refresh at the start of each renewal term and any unutilised assessments from the previous term will not be carried forward.**

4. Platform Content

4.1. *Content Features by Module*

	MODULES							
CONTENT	CRISIS	CYBERPRO	APPSEC	TALENT	AWARENESS ARCADE	CLOUDSEC	TEAM SIM	RANGES
Knowledge	✗	✓	✗	✓ (Limited number)	✗	✗	✗	✗
Tools	✗	✓	✗	✓ (Limited number)	✗	✗	✗	✗
Offensive	✗	✓	✗	✓ (Limited number)	✗	✗	✗	✗
Defensive	✗	✓	✗	✓ (Limited number)	✗	✗	✗	✗
Immersive Originals	✗	✓	✗	✗	✗	✗	✗	✗
Cyber Threat Intelligence	✗	✓	✗	✗	✗	✗	✗	✗
Application Security	✗	✓	✓	✓ (Limited number)	✗	✗	✗	✗
Cyber Crisis Simulations	✓ (Custom content depends on purchase method)	✗	✗	✗	✗	✗	✗	✗
Workforce Security Awareness	✗	✗	✗	✗	✓	✗	✗	✗
Cloud Sec	✗	✗	✗	✗	✗	✓	✗	✗
Team Sim	✗	✗	✗	✗	✗	✗	✓	✗
Ranges	✗	✗	✗	✗	✗	✗	✗	✓

The table above sets out the content features included with each module. For further details on what each content features comprises, please see section 4.2 below for definitions.

4.2. Content Features Defined

CONTENT FEATURE	DESCRIPTIONS
Knowledge Labs	This content covers the basics of cyber security, assisting users to master the fundamentals. It includes a series of introductory labs on compliance, cyber for board members, executives, ethics, and risk.
Tools Labs	Tools labs teach users the tools of the cyber security trade and includes labs covering a variety of network scanning tools, Linux command lines, encoding and encryption methods and techniques for packet analysis.
Offensive	These labs contain cyber skill experiences and content for red teams and penetration testers and include labs such as web application hacking to privilege escalation.
Defensive	These labs contain cyber skill content for security analysts, incident responders and threat hunters and include labs such as log analysis and malware samples.
Immersive Originals Labs	These are gaming labs written by industry leaders and our own elite hackers to put users' knowledge to the test and includes capture the flag style challenges.
Cyber Threat Intel Labs	Labs in this series are based on real-time threat intelligence and give users hands-on experience of real-world attacks and how to defend against them.
Application Security Labs	Application Security Labs are aimed at developers and engineers and teach them how to code securely to mitigate the risk of a cyber breach. The Application Security Labs create a realistic development environment which give users live code to identify, exploit, change, analyse 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.
Cyber Crisis Simulations	Cyber Crisis Simulations throw decision-makers into an emerging attack scenario and are based on traditional table-top scenario exercises. They encourage the key stakeholders in business continuity and crisis management roles to come together and validate or test their personnel and the processes and technology they have in place to react to a real cyber incident. The aim of the Cyber Crisis Simulator is to enable security professionals and senior managers to learn what to do if the worst should happen. For custom Cyber Crisis Simulation scenarios, customer success managers will provide the customer with a template to input their own materials relating to a fictitious scenario, its organization and industry. Our customer success managers will utilise the template to build, configure and deploy a single custom cyber crisis simulation scenario for the customer. For all purchase methods, a facilitator licence is granted. There is an overall maximum limit of 1,000 Authorised Users participating.
Workforce Security Awareness Labs	These labs cover the fundamentals of cybersecurity, such as staying safe online, phishing and password management, aimed at the general working population. These fun practical labs help users develop good cyber security hygiene and keep your business safe.

Cloud Sec Labs	Cloud Security labs are aimed at developers, engineers and security professionals to teach them security best practices in the Cloud to mitigate the risk of a cyber breach in their Cloud domain. The labs allow users to build and configure secure and resilient infrastructure in hyper-realistic hands-on environments using real tools and platforms. Cloud Security labs present a series of tasks which users must work through; automated intelligent logic based on security best practices and external frameworks are used to confirm whether a user has completed these tasks successfully. Once a user has completed all the tasks and answered any necessary questions, they will finish the lab successfully.
Team Sim	Team Sim immerses technical security practitioners into realistic offensive and defensive security incident scenarios played out in complex environments. Teams of security practitioners must work together to complete the tasks at hand: investigating an end-to-end attack chain by a simulated threat actor or carrying out such an attack chain themselves. Team Sim stress tests your teams to more effectively respond to real crisis scenarios and promotes improvements in response processes, techniques, and team composition. Managers within the platform are able to schedule Team Sim exercises from a catalogue of pre-built scenarios after purchase. The number of exercises per annum will be specified in the Order Form. If the number of exercises are not specified in the Order Form, the fall back shall be: • Small – 4 exercises per annum • Medium – 8 exercises per annum • Large – 15 exercises per annum There is a "soft" limit of 10 teams per exercise, 10 participants per team, and a 5 day maximum exercise duration. These can be adjusted on a case-by-case basis.
Ranges	The Immersive Labs Cyber Range provides the fastest way for technical teams to create hyper realistic representations of enterprise networks for high value use cases like detection engineering, malware analysis, tool testing & validation, and research & development activities. Ranges support a wide variety of out of the box systems and software configurations, including the ability to create Custom images. Cyber Ranges customers who also purchase Team Sim may launch the range designs from within the pre-built catalogue of scenarios. The maximum number of range resources (size of the range(s)) is limited by the product tier the customer has purchased.

5. Professional Services

The table below sets out the Professional Services we offer. Professional Services shall only be provided during the term of the contract between Customer and Immersive Labs ("Term") and no Professional Services may be carried forwards, credited or refunded if not used during the Term. For further detail on what each of the professional services entails, please see section 5.2 below (Professional Services Specification). These Professional Services do not currently apply to Team Sim or Ranges products or services.

5.1 Professional Services Specification

PROFESSIONAL SERVICE	SPECIFICATION
Standard Cyber Workforce Advisor	**A designated shared Cyber Workforce Advisor ("CWA") will be assigned to your organization to understand your business objectives and develop your organization's Cyber Workforce Resilience Strategy and help you mature over time. Your CWA will be assigned to you for up to 1 working day per week and will assist in the creation, implementation and tracking of Cyber Workforce Resilience plans.** Activities include: (i) Discovery call, where your CWA will identify and support ongoing cyber initiatives for the duration of the Term (ii) Identify processes and services required for your success, based on best practice and your unique requirements (iii) Your CWA will conduct a Cyber Maturity Assessment (iv) Your CWA will support the build of your communications plan and review it at defined cadences (v) Integrations, automations and Cyber Workforce Resilience projects will be identified and delivered as workstreams (vi) Your CWA will help and enable you to build awareness and launch campaigns within your organization as well as drive adoption initiatives (vii) Metrics will be aligned to activities and reported on during monthly or quarterly business reviews (the frequency of which can be determined by you) (viii) Tracking of objectives & key results (ix) Success criteria defined and reviewed **Approximate Customer Effort: 1 hour per week over 46 weeks** **Approximate Duration: 1 year**
Premium Cyber Workforce	**A designated Cyber Workforce Advisor will be assigned and dedicated to your organization to understand your business objectives and develop your organization's Cyber Workforce Resilience Strategy and help you mature over time. Your CWA will be assigned to you for up to 4 working days per week and**

Advisor	**will assist in the creation, implementation and tracking of Cyber Workforce Resilience plans.** Activities include: (i) Discovery call, where your CWA will identify and support ongoing cyber initiatives for the duration of the term and build your Cyber Workforce Resilience schedule of work (ii) Identify processes and services required for your success, based on best practice and your unique requirements (iii) Your CWA will conduct a Cyber Maturity Assessment (iv) Your CWA will support the build of your communications plan and review it at defined cadences (v) Integrations, automations and Cyber Workforce Resilience projects will be identified and delivered as workstreams (vi) Your CWA will help and enable you to build awareness and launch campaigns within your organization as well as drive adoption initiatives (vii) Metrics will be aligned to activities and reported on during monthly or quarterly business reviews (the frequency of which can be determined by you) (viii) Tracking of objectives & key results against the value achieved toward your organization's benefits (ix) Success criteria defined and reviewed (x) Enable customer ownership of cyber skills development initiatives (xi) Conduct benchmarking analysis **Approximate Customer Effort: 1 day per week over 46 weeks** **Approximate Duration: 1 year**
Standard Cyber Skills Plan	**Partner with a Cyber Security Skills Consultant to create a tailored Cyber Skills Plan for your chosen role, e.g Security Analyst or Penetration Tester. This service tailors out-of-box career paths, including all operational levels within the role. Use this service output to upskill your targeted teams.** Activities include: i) Your consultant will seek to understand your objectives during a discovery call. Following this, they will review key relevant documentation provided by you in support of the project. ii) Your consultant will design your tailored Cyber Skills Plan for your review which includes one iteration of the Plan if required iii) Your chosen custom career path will be deployed on your platform environment for you to assign to your chosen teams or individuals iv) Your consultant will review the progress and evaluate the learning against the Kirkpatrick evaluation model. The output of this will

	be an evaluation sheet v) Following this, collections may be amended, or re-assigned with help from us **Approximate Customer Effort: 4 Hours** **Approximate Duration: 4 weeks + Review in month 3**
Premium Cyber Skills Plan	**Partner with a Cyber Security Skills Consultant to create a fully customized Cyber Skills Plan for your chosen role, e.g Security Analyst or Penetration Tester. This service includes all operational levels within the role. Use this service output to upskill your targeted teams.** Activities include: i) Your consultant will seek to understand your objectives during a discovery call. Following this, they will review key relevant documentation provided by you in support of the project. ii) Your consultant will design your customized Cyber Skills Plan for your review which includes one iteration of the Plan if required. This design will include a skills matrix, content inventory and custom CSP. iii) Your chosen custom career path will be deployed on your platform environment for you to assign to your chosen teams or individuals iv) Your consultant will review the progress and evaluate the learning against the Kirkpatrick evaluation model. The output of this will be an evaluation sheet v) Following this, collections may be amended, or re-assigned with help from us **Approximate Customer Effort: 5 Hours** **Approximate Duration: 8 weeks + Review in month 3**
Cyber Capability Assessment	**Partner with a Cyber Security Skills Consultant to design and execute a Cyber Capability Assessment for 1 Role e.g Security Analyst or Penetration Tester. This service will engage your team in a tailored collection of labs, targeted towards your chosen skill area to assess their capability and will indicate capability against either MITRE TTP's or NICE skill areas.** Activities include: i) Discovery and scoping session, of which the output will be a list of skill indicators and a draft list of assessment labs for the chosen skill area, based on MITRE TTp or NICE. ii) A review and final selection of the labs for the assessment iii) Your consultant will create custom collections for you to assign to your chosen audience iv) The assessment event will take place. IL will provide preparation documentation and support as required, including remote support

	throughout the assessment v) Your consultant will analyze the data post-assessment, provide an insight report and recommendations **Approximate Customer Effort: 3 Hours** **Approximate Duration: 14 weeks. Assessment duration will be between 4 and 8 weeks.**
Standard Crisis Sim Service	**An Immersive Labs Crisis Sim Consultant will partner with you to understand your crisis exercising strategy and aims. They will guide you through a process to create a critical yet plausible crisis scenario, based on specific risks and challenges your organization will likely face during a crisis. Your unique scenario will unfold through a series of injects and will stress-test your organization to make time-bound decisions in the face of jeopardy. Your Consultant will help you to outline and refine your scenario. They will also prepare you for exercise delivery and can facilitate your simulation if required.** Activities include: i) Customer completion of a preliminary questionnaire and selection of attack vector template (vectors include - Ransomware / Phishing / Supply Chain / Insider Threat / DDOS / Zero Day) ii) Ideation workshop, of which the output is a high-level crisis scenario for customer review. At this stage, you must appoint one point of contact responsible for technical content oversight and one point of contact responsible for sign-off. iii) Following customer sign-off, we will design the high-level scenario, of which the output is a signed-off crisis scenario with intricate detail including options, option ranking, rationale and rich media for each inject iv) Iteration of the scenario, concluding with customer sign-off v) We will build and publish the crisis simulation in your platform environment, whilst enabling you to use the platform and support the building process throughout vi) We will prepare you for your crisis sim facilitation via a meeting. This may include full or partial dry-run and pre-exercise communications will be provided by us for your participants vii) We will facilitate or co-facilitate your crisis simulation for your intended audience either remotely or in person (to be agreed between you and us)* viii) We will provide an exercise debrief either as part of your facilitation or thereafter, at the date and time agreed with you **Approximate Customer Effort: 9 Hours** **Approximate Duration: 3.5 weeks dependent on customer availability** *The facilitation date cannot be amended once agreed between us without our prior consent.

Premium Crisis Sim Service	**An IL Crisis Sim Consultant will partner with you and guide you through a process to create a severe yet plausible, fully bespoke crisis scenario within the IL platform. Your crisis scenario will be built from scratch and will be bespoke to your organization.** Activities include: i) Your completion of a preliminary questionnaire ii) Ideation workshop, of which the output is a high-level crisis scenario for your review. At this stage, you must appoint one point of contact responsible for technical content oversight and one point of contact responsible for sign-off. iii) Following customer sign-off, we will design the high-level scenario with significant input from you to achieve a co-authored detailed design of the crisis scenario. The output is a customer signed-off crisis scenario with intricate detail including options, option ranking, rationale and rich media for each inject. iv) Iteration of the scenario (if required and limited to timeline availability), concluding with customer sign-off v) We will build and publish your crisis simulation in your platform environment, whilst enabling you to use the platform and support the building process throughout vi) We will prepare you for your crisis sim facilitation via a meeting. This may include full or partial dry-run and pre-exercise communications will be provided by us for your participants vii) We will facilitate or co-facilitate your crisis simulation for your intended audience either remotely or in person (to be agreed between you and us)* viii) We will provide an exercise de-brief either as part of your facilitation or thereafter, at the date and time agreed with you **Approximate Customer Effort: 13.5 Hours** **Approximate Duration: 4-7 weeks dependent on customer availability** *****The facilitation date cannot be amended once agreed between us without our prior consent.
Advanced Cyber Crisis Sim Consulting	**Partner with a Crisis Sim Consultant to provide expert advisory on the rollout of Cyber Crisis Sim to support your exercising strategy within your organization over the course of 5 non-consecutive hours.** Activities include: i) A scoping call, where an IL consultant will seek to understand your exercising objectives and strategic intent. This session is not included within the 5 hours of consultancy. ii) 5 hours' worth of advisory support for you to execute your exercising plans using the IL Cyber Crisis Sim platform. This may include:

	a. Platform support b. Exercising strategy support c. Execution and delivery support d. Content support **Approximate Customer Effort: 6 Hours** **Approximate Duration: Customer Dependent**
Curated Event	**Partner with a Cyber Security Skills Consultant to construct a custom event. Event support will be provided throughout the event, including event facilitation and end-user support while the event is in progress.** Activities include: i) Event scoping call, where our consultant will seek to understand your event objectives. The output of this call will be an event outline document, provided by us, which you will review and sign off on. ii) We will prepare and configure your event platform, create licenses and an event landing page iii) We will provide pre-event marketing for your distribution to users iv) You will agree custom objectives with your consultant before they configure the objectives within your event platform v) Your consultant will host a kick-off presentation in preparation for your event vi) Your consultant will provide virtual technical support throughout the one-day event as required vii) Your consultant will extract event data and communicate event winners as well as a post-event report. The report will include details on active participants, labs attempted and participant feedback viii) Your consultant will schedule a meeting for a project wash-up, where the report will be formally handed over to you **Approximate Customer Effort 6.5 Hours** **Approximate Duration: 4 weeks**
API Consulting	Our Integrations Consultant will provide the guidance and expertise required to identify and deliver an API integration solution (owned and stored in your environment), enabling a single direction data feed into your environment. Create a custom integration with our API over a course of 5 non-consecutive hours. Activities include: (i) A scoping call between you and your Integrations Consultant, where you will scope the initial solution and agree on approach. This session is not included within the 5 hours of consultancy. (ii) We will generate documentation for the project and to support

	your solution as well as ownership and maintenance responsibilities for the solution. (iii) Your Consultant will provide consulting, advisory and delivery to the agreed method over the course of 5 non-consecutive hours. **Approximate Customer Effort: 6 hours.** Should the customer wish to seek further API consultancy, additional API Consulting services must be purchased. **Approximate Duration: Customer Dependent**

6. Service Availability

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

Immersive Labs operates on a target minimum service availability of 99.5% uptime. We monitor the uptime of our services using a third-party company who generate alerts in the event the site is unavailable. We use a third-party monitoring tool (Uptime Robot) to generate reports, alerts, and dashboards for the uptime of our application.

7. Technical Support

Immersive Labs provides support for both the web application and underlying content served in the platform. We maintain an online support function through the following email address: support@immersivelabs.com.

Immersive Labs monitors the support inbox and aims to respond to queries in accordance with the Response Targets set out in the table below.

Working hours are 09.00 to 17.30 GMT/BST/EST Monday to Friday (excluding UK bank and US public holidays) (as applicable) .

In the event you or your Authorised Users experience a fault with the Platform, please report it as soon as possible to support@immersivelabs.com.

Immersive Labs use four tiers of incident depending on the scale and severity of the issue. A target response time and resolution time is defined for each priority level and will apply during working hours only.

Where development work is required, the target resolution times may be extended. We attempt to achieve the following target response and resolution times across each priority level once we have classified the incident.

	Description	How incident reported	Response target
Priority 1	The production system is unavailable for all users.	Immersive Labs notified via uptime monitor.	Support team working inside and outside of working hours until resolved.
Priority 2	Multiple users cannot access multiple labs.	Notification to support@immersivelabs.com	Investigated inside working hours with a 0.5-day target to resolve.

Priority 3	A single user cannot access multiple labs.	Notification to support@immersivelabs.com	Investigated inside working hours with a 1-day target to resolve.
Priority 4	A single user cannot access a single lab.	Notification to support@immersivelabs.com	Investigated inside working hours with a 5-day target to resolve.

8. 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 on to our Sales and Commercial Manager.

9. Service Credits

For the avoidance of doubt, Immersive Labs does not offer service credits.

10. Changes

The Immersive Labs 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 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'll endeavour to notify you where practical. We shall be entitled to increase the Fees at the start of each Renewal Term upon reasonable notice (for example if we have made changes to packaging and features during the term).

We may modify this Product and Services Guide at any time by posting a revised version on our website 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.

11. Additional Terms

If you purchase the Cyber Crisis Simulator, the terms applicable to Cyber Crisis Simulator and made available from time to time at www.immersivelabs.com/legal shall also apply (CCS Terms). Solely in connection with the access or use of Cyber Crisis Simulator, in the event of any conflict between the terms of the Agreement between us and the CCS Terms, the CCS Terms shall prevail.

If you purchase Team Sim or Ranges, the terms applicable to Team Sim and Ranges and made available from time to time at www.immersivelabs.com/legal shall also apply (Team Sim and Ranges Terms). In connection with the access or use of Team Sim or Ranges only, in the event of any conflict between the terms of this Agreement and the Team Sim and Ranges Terms, the Team Sim and Ranges Terms shall prevail.

Product and Services Guide Version 2022.10