# 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

DATA SHEET

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**

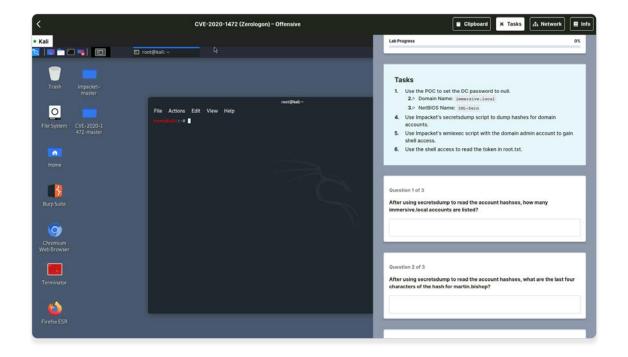
Our platform embeds skills by immersing individuals in challenges, scenarios and simulations in the browser to teach everything from threat hunting and reverse engineering, to SecDevOps. We build more relevant skills in a number of ways:

#### 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.

SUNBURST Supply Chain Compromise Badge Complete all the labs to earn the badge and prove you have beaten the SUNBURST Supply Chain Compromise challenge.						
Series					۹	
ITLE •	POINTS .	DIFFICULTY .	LAB TYPE .	TIME REQUIRED *	STATUS *	
Compromising SolarWinds: Orion	40	3 00010000	Practical Lab	25 Minutes	Completed	Restart
Who are UNC2452?	20	= 00000000	Practical Lab	20 Minutes	In Progress	Continue
Build Server Investigation	400	7 888888811	Practical Lab	40 Minutes	Not started	Start
dentifying IoCs	100	4 8888 588 58	Practical Lab	60 Minutes	In Progress	Continue
BusinessLayer.dll Analysis	400	7 888888888	Practical Lab	60 Minutes	Not started	Start

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.



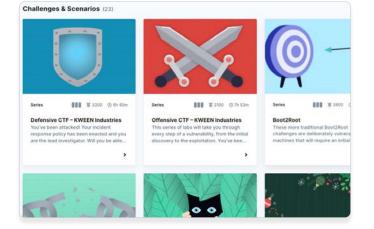


#### 3. Actionable insights:

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.

MITRE	TROV					MIT	RE ATT&CK® Fra	mework Mappin	9				
	d our labs to tech	niques within V6	of the MITRE AT	таске	framewo	rk. O	S+ Users	2 - 4 Users	1User	0 Users	No Labs Mapped		
The framework	below shows you	progress through	gh the mapped la	bs.									
Ormaniaatia	- Mieur												
Organisatio	n view												
Initial Access	Execution	Persistence					redential Discovery	Lateral	Collection	Command and	Exfiltration		
		00000000000	Escalation	Ev.	asion	Access		Movement	Concention	Control			
Drive-by Compromise	AppleScript	.bash_profile and .bashrc	Access Token Manipulation		as Token Account Manipulation		Account Discovery	AppleScript	Audio Capture	Commonly Used Port	Automated Exfiltration		
Exploit Public- Facing Application	CMSTP	Acc Techniqu Fe DLL Sea	e arch Order Hijack	ing 🗹	Padding	Bash History	Application Window Discovery	Application Deployment Software	Automated Collection	Communication Through Removable	Data Compressed		
External Remote Services	Command-Line Interface	Man Paul Th	illings ffries-Harris Mowat Apostol		Jobs	Brute Force	Browser Bookmark Discovery	Distributed Component Object Model	Clipboard Data	Connection Proxy	Data Encrypted		
Hardware Additions	Compiled HTML File	App Rae Jef Taylor M			ries-Harris			Credential Dumping	Domain Trust Discovery	Exploitation of Remote Services	Data from Information Repositories	Custom Command and Control Prot	Data Transfer Size Limits
Replication Through Removable M	Control Panel Items	App			nar mand lory	Credentials in Files	File and Directory Discovery	Logon Scripts	Data from Local System	Custom Cryptographic Protocol	Exfiltration Over Alternative P_		
Spearphishing Attachment	Dynamic Data Exchange		File Delete Zero-I vs: DLL Hijacking	Day	STP	Credentials in Registry	Network Service Scanning	Pass the Hash	Data from Network Shared Drive	Data Encoding	Exfiltration Over Command and C		
Spearphishing Link	Execution through API	Authentication Package	DLL Search Order Hijacking	Code	Signing	Exploitation for Credential Access	Network Share Discovery	Pass the Ticket	Data from Removable Media	Data Obfuscation	Exfiltration Over Other Network		
	Execution through Module Load	BITS Jobs	Dytib Hijacking		ille After livery	Forced Authentication	Network Sniffing	Remote Desktop Protocol	Data Staged	Domain Fronting	Exfiltration Over Physical Medium		
Spearphishing via Service	Long			Compiled HTML File					100000	Domain			

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.