IMMERSIVELABS

DATA SHEET

FOR BUSINESS LEADERS

Organizations are digitizing faster than ever. This transformation means that a business's core operation and even its worth are reliant on the resilience of core data and technology assets. As a result, having the human capabilities necessary to respond to, and recover from, cyber attacks has become a reputational, financial, and legal issue at board level.

Our progressive platform gives senior management teams the confidence that human assets will respond to cyber incidents more effectively. Informed by the latest psychological theory, it regularly throws a range of decision-makers into emerging attack scenarios to build a more adaptable, agile human response. This achieves three main outcomes:

EQUIPPING

Arming incident responders, from communications, technical and customer teams to legal counsel, with the core skills necessary to address the latest cyber crises. These are mapped to organizational risk for relevance.

EXERCISING

A direct counterpoint to the aging, infrequent tabletop exercise, we enable a progressive form of faster, more frequent, micro-drilling. This uses emerging psychological theory to build cognitively agile teams capable of adapting in intense, information-dense situations.

EVIDENCING

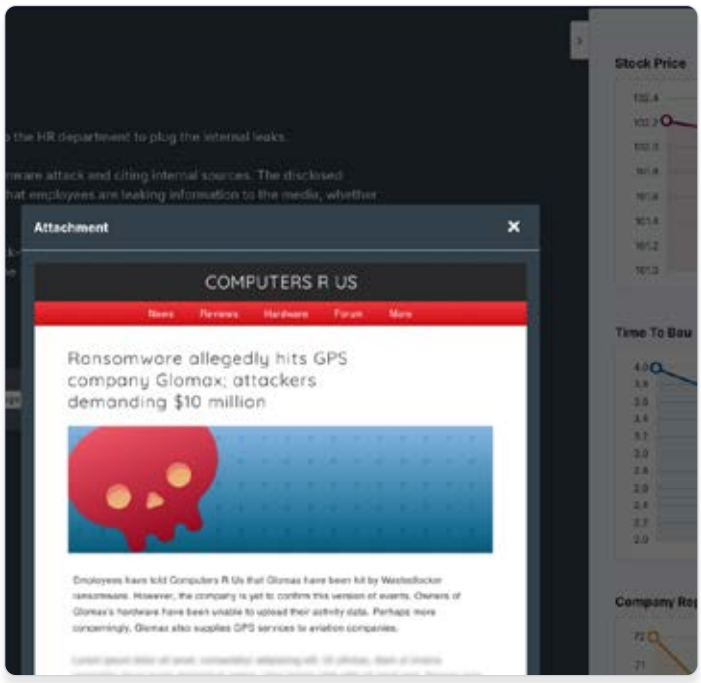
A better understanding of the capabilities of incident response teams using datasets mapped to business outcomes for more informed strategy and investment decisions.

CYBER CRISIS SIMULATOR: A CONTEMPORARY RESPONSE TO EXERCISING IN TODAY'S THREAT ENVIRONMENT

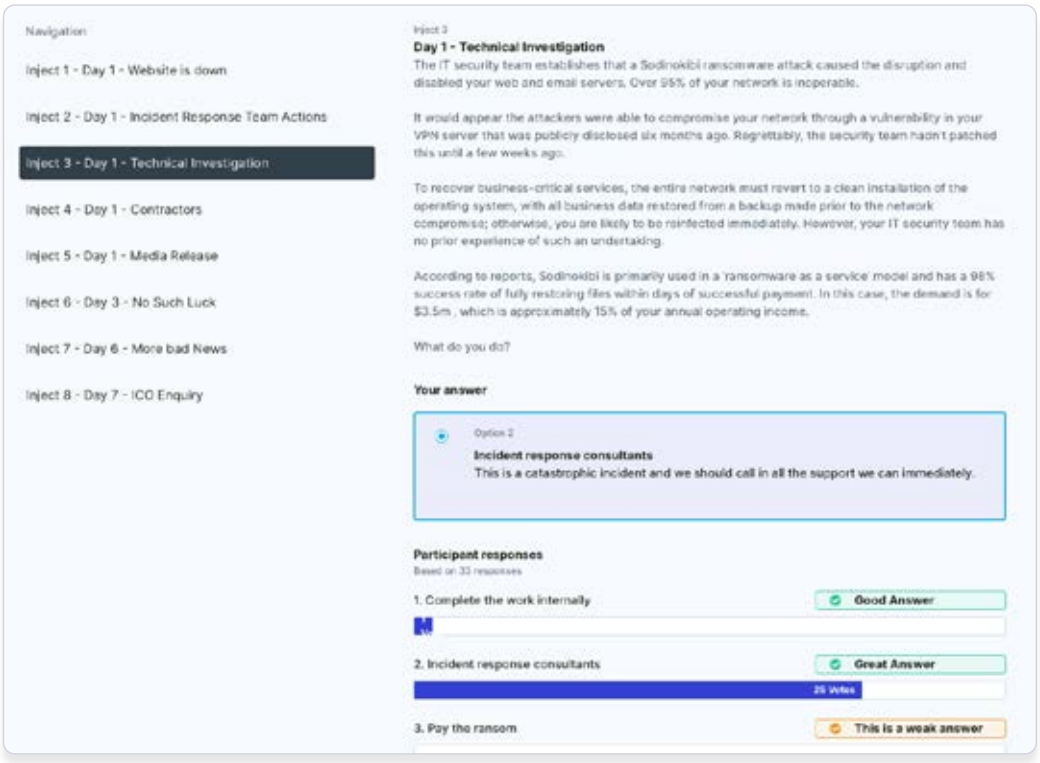
Our Cyber Crisis Simulator is built to encourage resilience by creating human assets more relevant to the modern cyber crisis. By dropping incident management teams into a range of scenarios in the browser we develop skills across silos, create cognitively agile individuals, and measure and map outcomes. It achieves this in a number of ways:

1. **Dynamic storylines:** Incident response teams play through a full simulated cyber crisis featuring rich, realistic narratives in straightforward business language. Decisions have a real-time impact on indicators such as share-price and reputational scores. This makes the orchestration of cyber crisis response across corporate silos more effective, reducing burden on senior management teams.

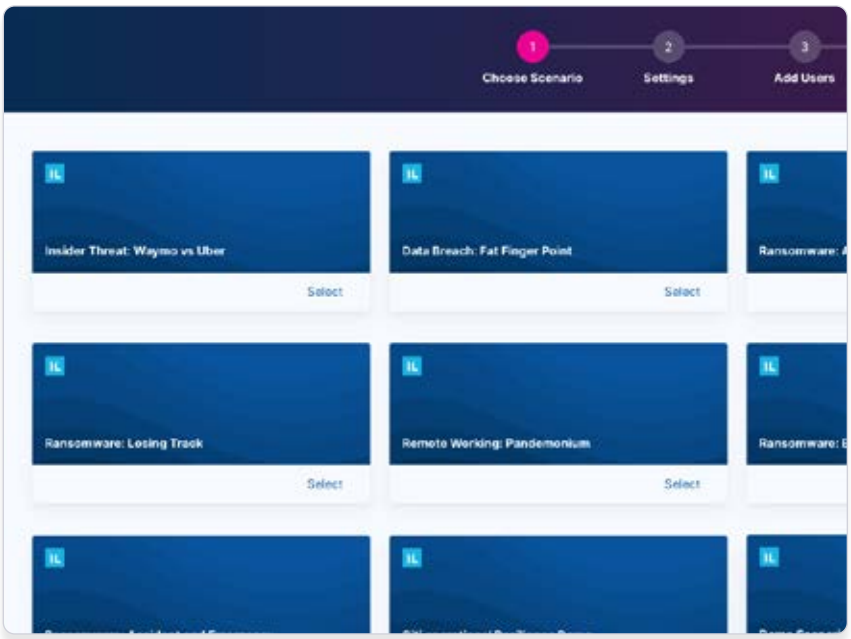
2. **Threat intelligence based:** Simulations are continually updated using the latest attack techniques to ensure the skills learned are kept continuously fresh and relevant. For senior management teams, this means less knowledge gaps in the event of a crisis which slow down response and can amplify impacts such as share price slides and unfocused media response.



3. **Actionable Insights:** Data-based insights update board members on the capabilities of incident response teams, providing confidence and clear evidence of progression. This makes investment decisions easier, as well as providing a more rounded picture of risk and overall resilience.



4. **Low organizational burden:** Being delivered through the browser makes running a crisis simulation as simple as sending a link. This enables an increased frequency of exercise at decreased cost and allows organizations to leverage the benefits of micro-drilling, while simultaneously eliminating the hassle and cost of legacy table-topping. It is also more relevant to a world of dispersed, remote teams.



"Cyber Crisis Simulator allowed us to simultaneously facilitate a realistic ransomware exercise across central banks and financial institutions."

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.