

GITAC Joins Forces with Immersive Labs to Disrupt National Cyber Drills

Background

GITAC, founded by David Shavgulidze and Giorgi Gurgenidze, is a non-profit organization dedicated to advancing digital transformation and enhancing cyber resilience across Georgian Critical Information Infrastructure. With extensive experience in public and private sectors, the founders are focused on helping their clients align with EU and U.S. regulations inline with their vision to disrupt current workforce development practices in Georgia. They recognized that traditional cybersecurity training methods, such as paper-based materials and tabletop exercises, are outdated, costly, and inefficient. They wanted to drive a new innovative approach to cyber drills to better prepare the public and private sectors for largescale cyber threats.

Challenge

Transitioning to a modern, digital approach to simulating cyber crises as part of a cross-agency, cross-sector training event presented significant challenges. GITAC's efforts to engage with various cyber training vendors were met with obstacles, as many vendors offered digital solutions, but restricted access to their platforms. The custom scenarios were costly and time consuming. GITAC needed a solution that was not only modern and customizable, but also capable of simulating realistic cyber-attacks and providing hands-on testing labs.

Benefits

Feedback from the event was overwhelmingly positive. Participants praised the drill for its effectiveness and realism (especially compared to traditional training methods), achieving GITAC's goal of fostering a culture of continuous learning in cybersecurity. The National Information and Cybersecurity Center for critical information infrastructure protection (under the LEPL Operational-Technical Agency), the main cyber regulator in the country, rated the first nationwide cyber crisis simulation as highly effective.

“This first cyber public-private partnership project proved to be valuable and tailor-made for Georgia's situation regarding CNI Protection and needs,” said the National Information and Cybersecurity Center. “With the joint forces, GITAC's expertise, and Immersive Labs' cutting edge digital tools, we managed to increase preparedness and resilience of staff from the critical infrastructure. To sustain and improve our results, we plan to work on the regulation on mandatory cyber drills and to **establish annual national cyber crises simulation exercises, as well as develop a renewed national legal and regulatory framework on cybersecurity incident identification and handling.**”

David and Giorgi acknowledged the significant role of Immersive Labs in transforming the cybersecurity culture in Georgia. The training not only improved individual preparedness, but also strengthened overall cross-sector cyber resilience. This case study underscores the effectiveness of innovation driven policy interventions, human-centric workforce development programs, the need for public-private partnership in CIIP and the need for immersive, hands-on training in building a more robust cybersecurity defense framework.

Trusted by the world's largest organizations



Solution

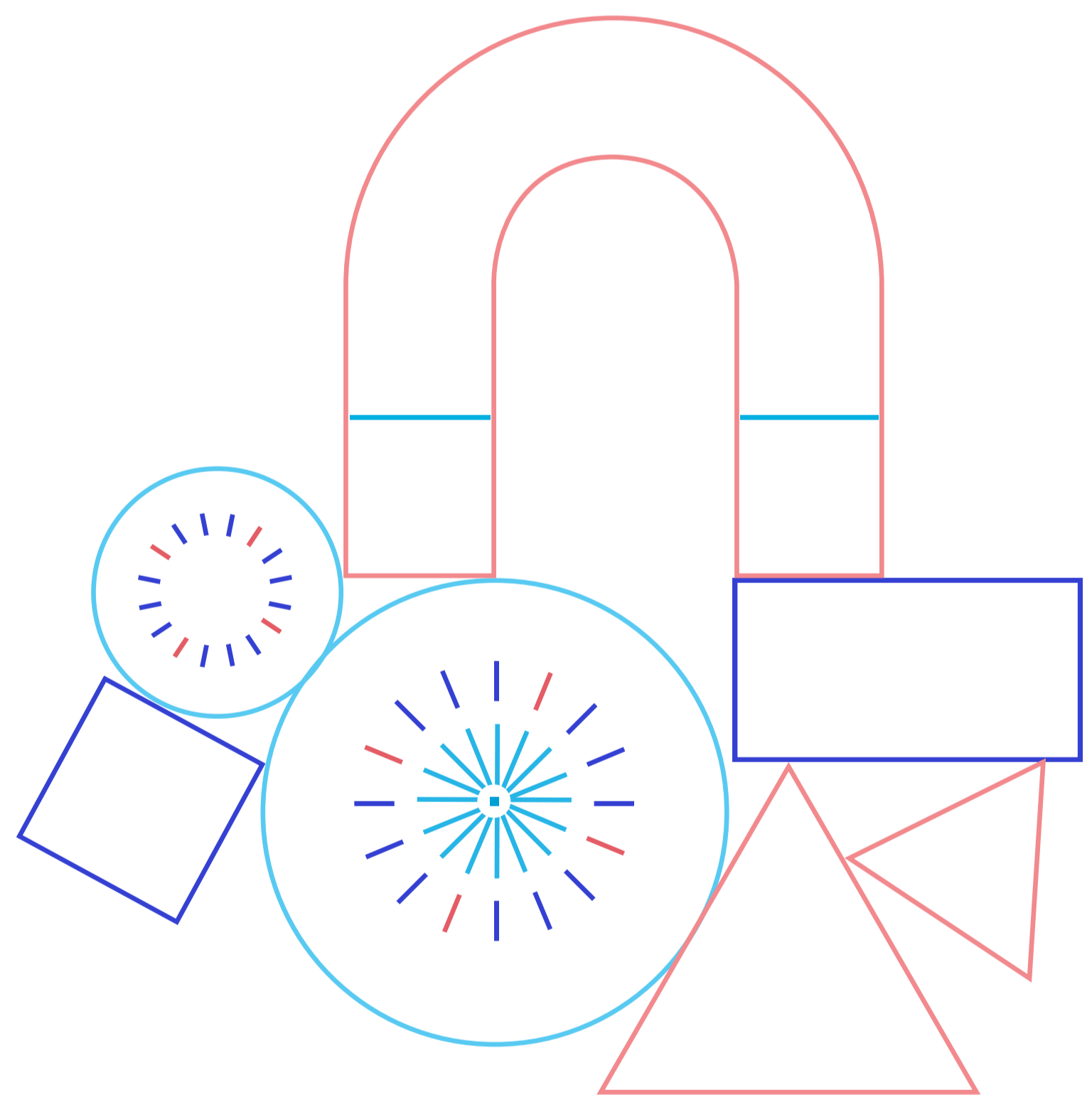
After a thorough evaluation, GITAC chose to forge a new path with Immersive Labs, the global leader in people-centric cyber resilience. Immersive Labs' Cyber Drills and hands-on labs offered GITAC the dynamic, interactive learning experience that they sought, as well as access to the platform. The decision led to the organization arranging the first nationwide interactive cyber drill involving nearly 100 key stakeholders from all of the national and sectoral regulators, including the Center for Critical Information Infrastructure Protection, Central Bank, Ministry of Defense, Communications Regulator, Energy Regulator (GNERC), Digital Governance Agency and representatives from all of the critical sectors, including government, financial, energy, communications, healthcare and insurance.

The cyber drill was designed around a simulated **National Infrastructure Collapse** scenario, which was aimed at creating a realistic doomsday scenario. Participants with the leadership, information security management, and computer emergency response roles

joined forces with the legal and public relations specialists to manage nationwide crisis. The mix of different perspectives (regulatory, investigatory, government, business, technical, managerial, leadership, legal and PR) triggered extensive discussions and debates about the decision making process. At first, teams seemed to be confident and in control of the situation; however, their purely technical approach to crisis management led the teams to a simulated loss-of-life scenario. **The cyber drill was stopped.** No one was ready for this kind of outcome. There was no undo (CTRL +Z) action. While technically sound, their decision had strategically failed. Teams needed time to rethink their strategy and they recognized the need for better collaboration, information sharing, and inclusion in the decision making process. This immersive approach proved effective and memorable. The existing approach to cyber drills was disrupted in favor of this more impactful approach.

Conclusion

By embracing a hands-on, dynamic and digital approach, GITAC significantly enhanced the engagement and effectiveness of their training programs. GITAC plans to further invest in developing Georgian language- and context-aligned cyber crises simulation scenarios powered by the Immersive Labs. This will open new opportunities for the government and private companies in the region to receive unmatched training experience. The successful partnership marks a pivotal advancement in Georgia's cybersecurity culture, setting a precedent for future initiatives aimed at mitigating cyber threats and boosting regional cyber resilience.



Certification & Compliance



Trusted by the world's largest organizations

Over
400
customers

>**3.5M**
total labs
completed

>**100,000**
unique
users

>**2,000**
hands-on
challenges