An exclusive impressive experience in industrial cybersecurity for decision makers

Kaspersky Interactive Protection Simulation Virtual Reality

What is KIPS and how does it help

Kaspersky Interactive Protection Simulation Virtual Reality (KIPS VR) is an information security strategy game with full immersion in virtual reality. For many years, KIPS scenarios have been used to engage top managers from various industries in the realities of cybersecurity. Depending on the company department, KPIs and priorities can be quite different, so it can be difficult for management to understand the specific requirements and roles of other business units. That's why Kaspersky offers a special business simulation to get executives focused on the potential consequences of cyberattacks, help them better understand cybersecurity, and demonstrate that collaboration between departments and well-coordinated teamwork is the key to successful incident response and cybersecurity strategies in general.

KIPS Power Station VR is a new immersive experience in a realistic environment as close as possible to the real operations of a power plant. Virtual reality lets users work through scenarios that power plant staff may experience in real life so they can see the consequences of their IT decisions not just abstractly, but in the highly realistic 3D graphics of a real power plant.

only 25%
of global CISOs say that their board sees eye-to-eye with them on cybersecurity issues.*

KIPS VR: a unique immersive experience no matter the industry

Although only one KIPS scenario out of a possible 12 is currently available in virtual reality, decision makers from other industries will find the game just as absorbing and useful as energy company leaders. KIPS is designed to get company leaders motivated and involved in cybersecurity issues, demonstrate the role of cybersecurity and its business impact visually, and improve mutual understanding and effective interactions between the business units found in any company.

How the game works

Users are divided into teams of 2–4 each representing an information security department at an energy company. The main task of the teams is to maintain stable, uninterrupted operations so that the enterprise performs its economic activities efficiently. The idea is to form a cybersecurity strategy by choosing from the available proactive and reactive resources. Depending on the teams' decisions during the game, their virtual power plants can remain fully operational and withstand attacks by cybercriminals, or experience forced equipment shutdowns, accidents and even explosions.

40%
of companies cited their executives, including the CEOs, as their highest security risk.**

The game has five rounds. After every round, the trainer reviews the results, so teams can see their place in ranking.

The team that finishes with the highest revenue, building the proper defense strategy and responding appropriately to various cyber-incidents, wins.

84%

of C-level executives say they had been targeted by at least one cyberattack in the past year, with phishing attacks again being the most common (54%).*

78%

of IT leaders say the C-Suite is the most likely to be targeted by phishing attacks.*

76%

of CEOs admit to bypassing security protocols to get something done faster, sacrificing security for speed.*
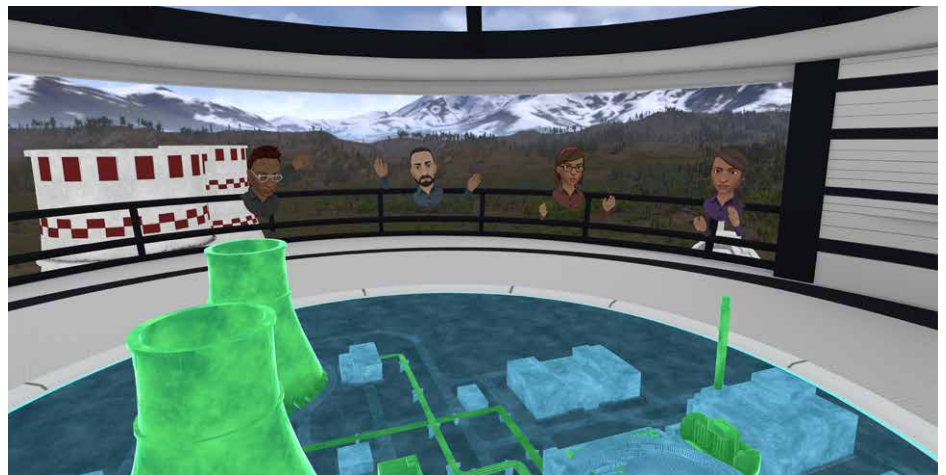
VR training benefits

The transition to VR exposes users to new facets of already familiar and proven strategic simulations:

· The emotional impact of a game in virtual reality is much higher for users than board or online games, which means the main task of KIPS strategic simulators – motivating the users – is solved more effectively. Also, the positive emotions business leaders experience have a positive effect on the perception and absorption of the training material, which in turn contributes to the creation of a corporate environment focused on cybersecurity.
· KIPS is a stimulating event for corporate management, and KIPS VR is a one-of-a-kind experience that's sure to leave a lasting impression.
· New VR technology helps business leaders grow by creating a sense of presence both physically at the power plant they're protecting from cyberattacks, and in terms of interactions between team members. Collaboration in VR is much more tangible than in regular online games, which is especially important today given the transition to remote working in many companies.

Game format:

· 1.5-hour remote session. The game requires the Oculus Quest 2 VR system and a broadband internet connection. Players remain at their workplace.
· Virtual teams get together around their virtual power plant control panels in real time under the guidance of a trainer and embark on an exciting journey into the world of industrial cybersecurity.

Beware, virtual reality can be addictive!

kaspersky.com

2021 AO Kaspersky Lab. Registered trademarks and service marks are the property of their respective owners.

kaspersky

BRING ON
THE FUTURE