SIMSPACE

whitepaper

OPERATIONAL BENEFITS OF

LIVE-FIRE EXPERIENCES

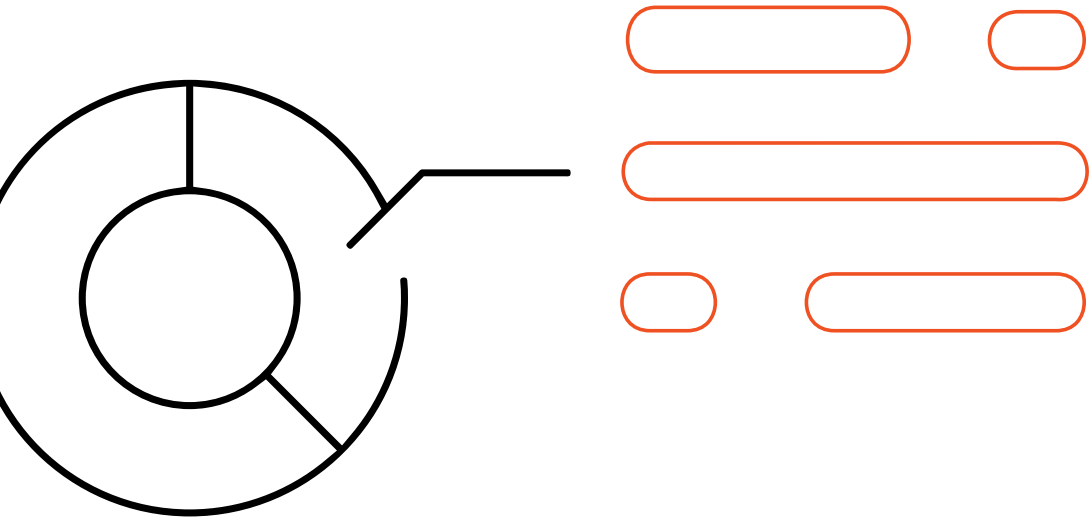
FOR A GLOBAL INSURANCE PROVIDER

SIMSPACE
SECURE WITH CONFIDENCE

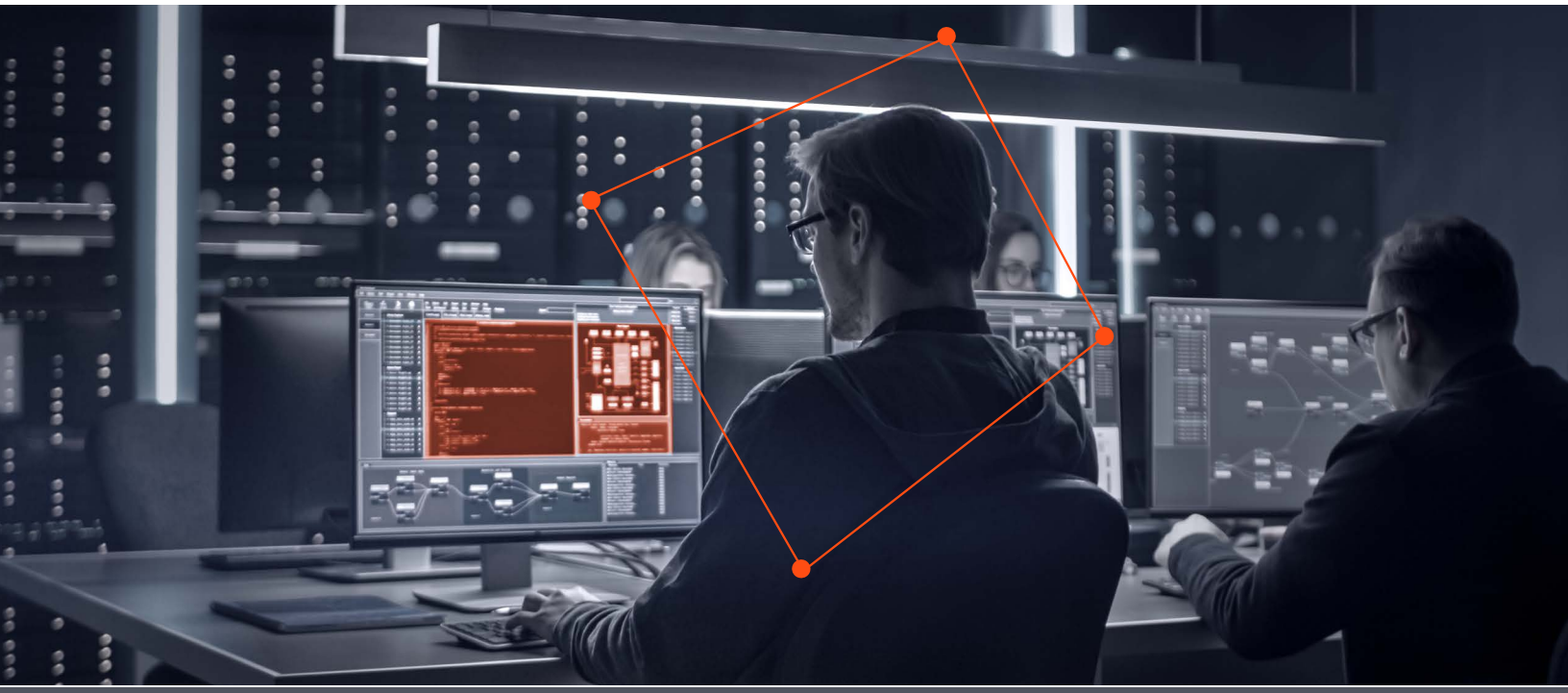
contents

As part of a risk-centric approach to information security, a significant global insurance company turned to SimSpace to help its Security Operations Center (SOC) team optimize its overall cybersecurity posture, reduce risk, and build organizational confidence.

The firm uses the SimSpace Cyber Risk Management Platform to assess and tune its tools and processes. The opportunity for immersive interaction also improves team skills to better defend against evolving cyber threats, including advanced adversaries that too often target the insurance industry. The platform includes a high-fidelity cyber range that replicates environments of any scale and offers expanded coverage through specialized tools and solutions. Best of all, this is achieved without affecting the enterprise's production environment or exposing the organization to service disruption or data loss.



optimize overall cybersecurity posture

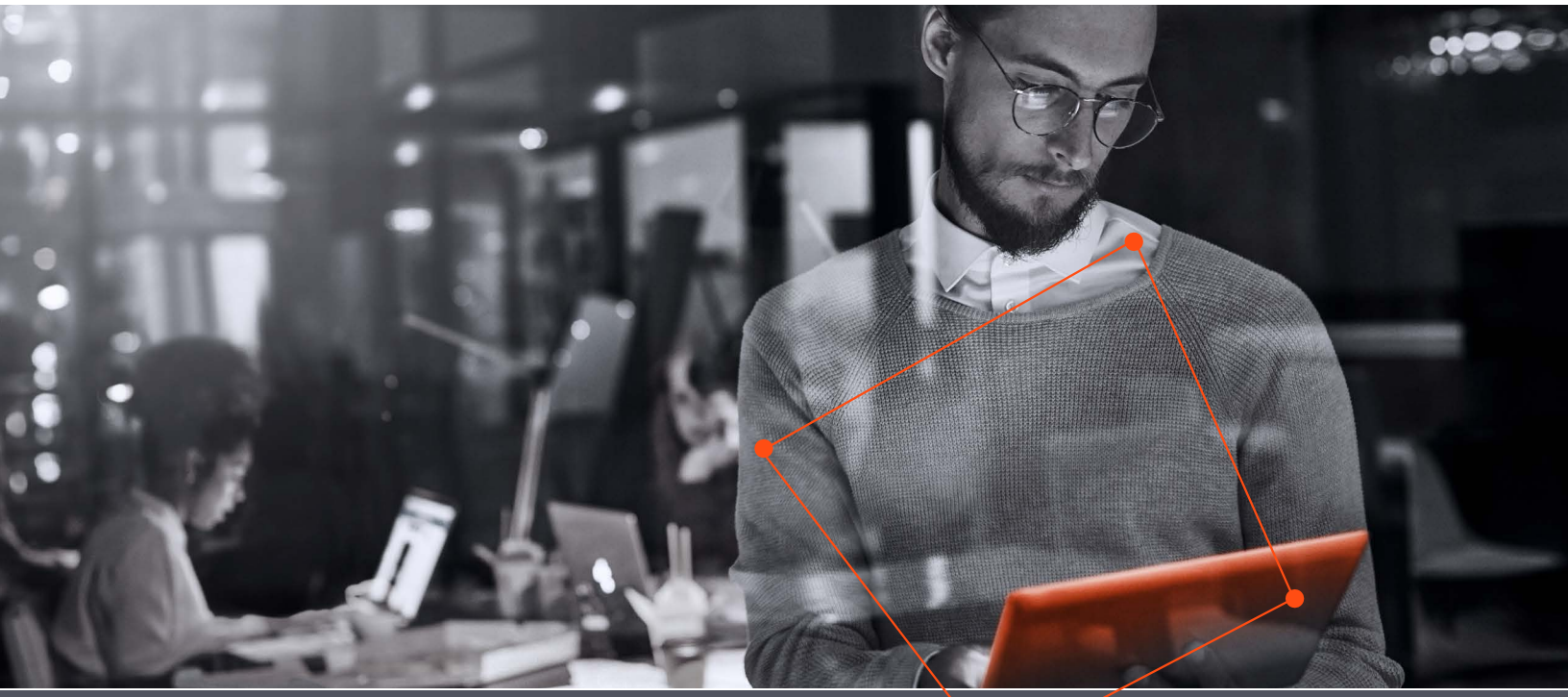


Driving next-level readiness

This insurance giant also works with SimSpace to conduct Live-Fire Experiences (LFXs) — also known as interactive cyber defense exercises — every six months. The company has seen steady improvements by providing its SOC teams with intensive hands-on training defending against cyberattacks using the security products, software, and processes they rely on daily.

Each LFX is a 24-hour "follow the sun" event based on mission performance objectives defined during event planning. SimSpace Professional Services applies its extensive expertise to event design, execution, and after-action reporting, ensuring that the LFX effectively develops individual and team skills while measuring improvements in the organization's responses to cyber threats.

SimSpace Professional Services applies its extensive expertise to event design, execution, and after-action reporting



Planning for a successful LFX

Extensive collaborative planning goes into each LFX prior to execution to optimize training value and return on investment. SimSpace Professional Services works closely with the organization's SOC management and training teams to define the objectives, design, and execution. This sets the stage for a highly impactful learning experience that tests incident response processes and readiness.

Initial planning phase: Define the event scope, including gameplay requirements, learning objectives, and event participants, as well as the event deliverables and schedule. In its most recent LFX, the firm's SOC leaders included a pre-event forensic package analysis and simulated business engagement decisions as part of the event scope.

Mid-planning phase: Design the exercise, including the threat attack plan (objectives, tactics, and techniques), any network conditions or anomalies (hygiene activities), threat density, and the backstory. This is also the time to define cyber range requirements and develop the remote and onsite event support plan.

Final planning phase: Finalize the execution plan, including the timeline, participants (defender players, shoulder surfers, business/management representation, control cell, and observers), and SOC resource requirements for the pre-event challenge and defender team familiarity tasks.

Preparing the cells for battle

As the planning process concludes, the event delivery process begins. This is a critical time in which SimSpace tailors the range topology and prepares the threat and defender teams for a highly realistic simulation exercise that battle-tests the SOC team against actual cyberattacks.

Building phase

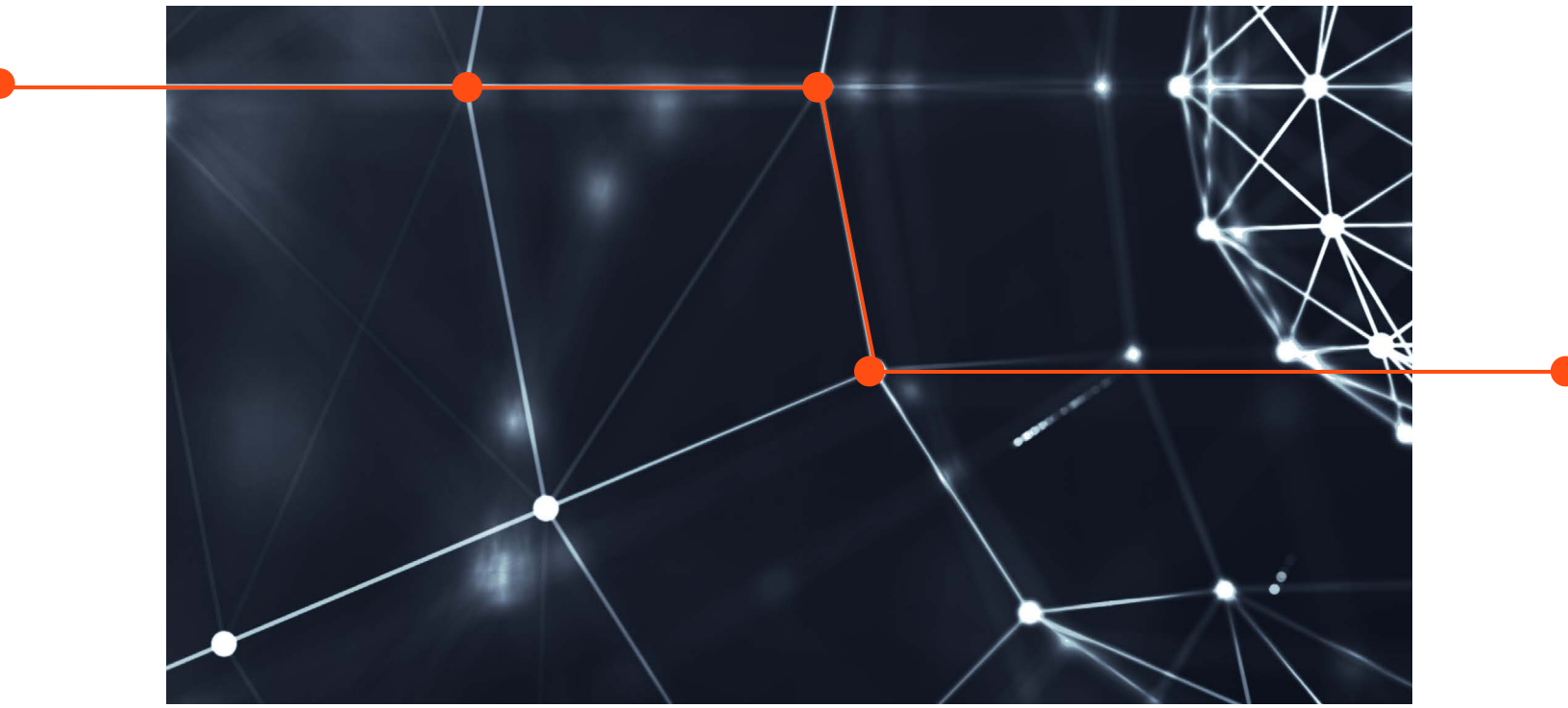
Next, SimSpace builds out the range, making any topology changes based on the planning stage. Because the insurance organization uses a permanent, mature SimSpace range with 1,000 virtual machines and 750 emulated users, fewer adjustments are typically required. For the latest LFX, SimSpace added two new tools to the SOC team's security stack — enhanced user (traffic) emulation with SSH (Secure Shell), FTP (File Transfer Protocol), and chat. SimSpace also incorporated a cloud services segment to represent the company's actual production environment more closely.

Once adjustments are made, SimSpace tests the range, builds and tests the attack logic, and provisions accounts for the SOC team's defender participants. Then SimSpace "freezes" the range in preparation for threat and defender range familiarization periods.

Execution phase

The SOC defender team is given a couple of weeks to get familiar with the range. During this time, they go into the LFX environment to make sure their accounts work, check out the tool configurations, and get a feel for what day-to-day user and network traffic looks like. At the same time, SimSpace holds a couple of range introductions and use sessions to help team members become comfortable with the range portal so they can take full advantage of the familiarization period before the live event.

In addition, the defender forensics analysts work through a forensics package (in this case, a disk image of a workstation at a fictitious newly-acquired company) to identify any issues as they develop their plan to bring this new network segment into their production environment. This backstory forensic analysis adds another layer of challenge to the exercise, as the SOC defender participants must adjust their security settings based on what they find in the forensics report.

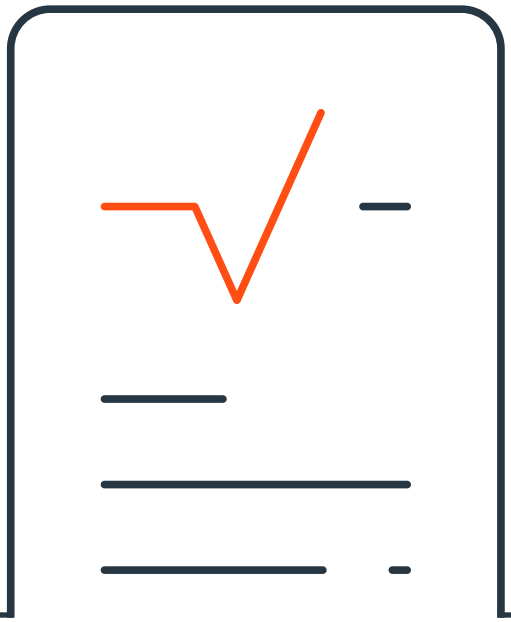


Reporting phase

Approximately two weeks after the LFX, SimSpace delivers a Summary Report presentation and a detailed After-Action Report, complete with actionable performance metrics, to the organization's cybersecurity leaders. These assessments and reports identify strengths and vulnerabilities in the SOC team's personnel, tools, and processes, demonstrate performance trends over time (compared to any previous LFX), and highlight how their scores stack up against other SimSpace customers in the insurance industry. These reports highlight performance against key objectives such as:

- Defending high-value assets from significant compromise
- Reporting indicators of compromise (IOCs) for the most lethal threats
- Detecting hygiene events such as end-user violation of policies
- Correctly reporting IOCs from the forensic package
- Taking appropriate action for reported IOCs

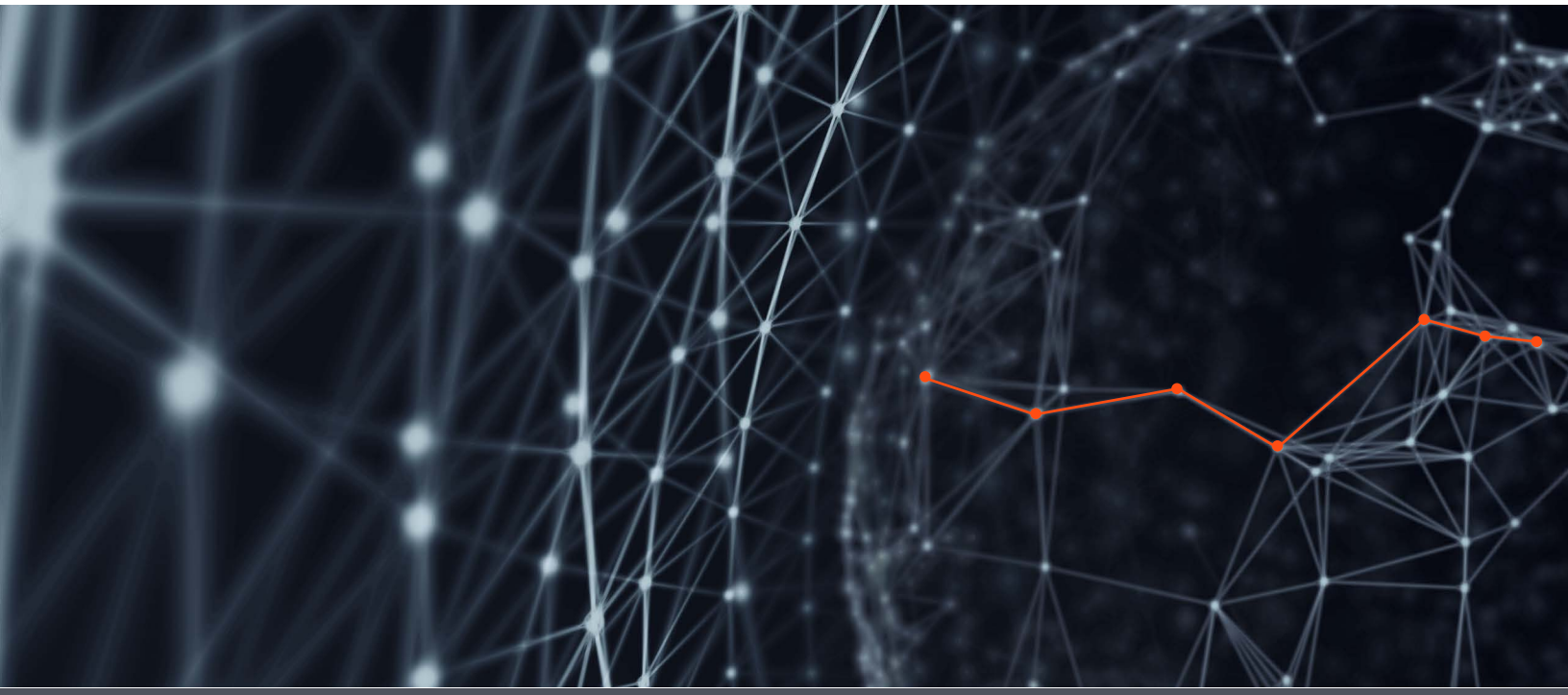
These insights give the SOC team a clearer understanding of where improvements need to be made — whether it's investing in new or improved security tools, refining internal processes such as information sharing or ticketing, training personnel to better defend against specific types of threats, or building better team relationships to enable more coordinated responses. Additionally, the SOC participants, along with the threat cell members, are provided a deep-dive review of selected threat presentations to see how their processes and security product implementation could be improved to provide more effective detection and response results.



Advancing a best-in-class cybersecurity program

As this global insurance organization works to proactively protect its data, networks, and IT systems from growing cyber threats, SimSpace LFXs continue to play an important role in driving continuous security improvements. With comprehensive training and actionable performance metrics, these hands-on events enable the company to quantify and maximize cyber readiness, helping ensure its security team, processes, and technology operate at peak performance.

SimSpace LFXs continue to play an important role in driving continuous security improvements



Take the next step toward cyber readiness

Is your organization ready to take the next step? The team at SimSpace would welcome the chance to meet with you and set up your own personalized demonstration of the SimSpace Cyber Risk Management Platform. Visit simspace.com to schedule some time with one of our experts.

simspace.com info@simspace.com

SIMSPACE