SIMSPACE PLATFORM

DON'T JUST PLAN FOR THE FUTURE, EMULATE IT.

# Case Study: **Critical Infrastructure**

**ANONYMOUS CASE STUDY:**

Strengthening Critical Infrastructure: A Success Story With SimSpace

**INDUSTRY:** Critical Infrastructure

**LOCATION:** U.S.

**Team Size:** 100,000+ employees

## Background

In the realm of critical infrastructure, organizations face unparalleled challenges in securing operational technology (OT) and ensuring the uninterrupted delivery of essential services. As cyber threats become increasingly sophisticated, these organizations must protect sensitive data and ensure the integrity and resilience of systems that support vital societal functions. A leading critical infrastructure organization recognized the need to enhance its cybersecurity posture and ensure compliance with stringent industry regulations. To address these challenges, the organization turned to SimSpace's advanced tailored cyber range platform.

## The Problem

This organization, integral to the nation's infrastructure, was confronted with the daunting task of safeguarding its OT environment against an evolving threat landscape. Traditional security measures, including basic tabletop exercises, were insufficient for addressing the complexities and unique vulnerabilities associated with critical infrastructure. This organization needed a solution to stress test its cyber controls, validate its incident response strategies, and ensure that all operations met regulatory requirements. Additionally, the organization required a platform that could emulate real-world cyber events, enabling them to assess the material impact of incidents in real-time, as required by SEC 8-K filings.

## The Solution

SimSpace's tailored cyber range platform provided the organization with the tools it needed to tackle these challenges head-on. The platform enabled the execution of rigorous regulatory compliance simulations specifically designed to meet the unique requirements of the critical infrastructure sector. Through these simulations, this organization ensured that its operational and cybersecurity practices were fully aligned with regulatory expectations. The SimSpace Platform facilitated realistic cyber drills, allowing this organization to accurately assess the impact of potential cyber incidents. These drills were crucial for ensuring timely and accurate public disclosures, helping the organization maintain compliance with SEC 8-K filing requirements.

The ability to conduct these advanced drills gave this team a clear understanding of the potential consequences of a cybersecurity breach, enabling them to refine their response strategies accordingly. SimSpace also provided the capability to stress test cyber controls within an environment that closely mirrored the organization's OT infrastructure. This testing environment was vital for validating the resilience of their systems against sophisticated and evolving threats, ensuring that their defenses could withstand even the most severe cyber events. The platform's ability to provide advanced risk and impact analysis post-drill, utilizing the FAIR methodology, further allowed the organization to quantitatively assess potential losses from cyber incidents, aligning risk management strategies with actual business impacts.

# Why SimSpace?

This organization chose SimSpace for its unparalleled capability to emulate real-world cyber threats and rigorously test security controls against industry benchmarks. SimSpace's Platform was not just about compliance; it was about building a resilient cybersecurity posture that could stand up to the most severe threats. The platform's ability to validate regulatory compliance through tailored simulations was a key differentiator. These emulations allowed the organization to demonstrate that its cybersecurity practices met the stringent legal and operational requirements for critical infrastructure.

SimSpace also empowered this organization to optimize its incident response strategy through testing and end-to-end cyber drills. By reducing response times and improving accuracy during cybersecurity events, this organization could better protect its OT environment and ensure the continuity of its critical services. The tailored simulations provided by SimSpace ensured that the organization's teams were well-prepared to face and neutralize real-life security challenges effectively.

Finally, SimSpace's focus on resilient OT security was crucial for this organization. The platform enabled rigorous testing and strengthening of security measures around OT, which is vital for maintaining the continuity of services that society relies on. Enhanced reporting capabilities also provided the organization with detailed insights into the efficacy of its current cybersecurity measures, which were invaluable for internal audits, regulatory reviews, and strategic decision-making.

# Conclusion

SimSpace empowered this critical infrastructure organization to transform its cybersecurity strategy from reactive to proactive. By leveraging SimSpace's comprehensive, tailored cyber range platform, the organization could rigorously test its defenses, ensure compliance with stringent regulations, and build resilience against sophisticated cyber threats. As a result, the organization validated that it met its regulatory obligations and strengthened its overall cybersecurity posture, ensuring that it was well-prepared to protect the essential services it provides to society. With SimSpace, this organization now stands resilient in the face of evolving cyber threats, confident in its ability to maintain operational integrity and safeguard critical infrastructure.

## SimSpace customers have seen:

**30%**
**Savings in Operational Costs**

**40%**
**Reduction in Configuration/ Patch Related Breaches**

**45%**
**Improvement in Attack Defense & Breaches**

**48%**
**Improvement in Time to Detect a Breach**

SIMSPACE



simspace.com | info@simspace.com | 617-237-6223