SIMSPACE PLATFORM

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

Case Study: **Federal and Military**

ANONYMOUS CASE STUDY:

Strengthening National Security: Enhancing Federal Cyber Defense with SimSpace's Realistic Simulations

INDUSTRY: Federal and Military

LOCATION: U.S.

Team Size: 100,000+ employees

Background

The federal government and military face unique challenges in preparing for cyber warfare, a realm where threats evolve faster than traditional defense mechanisms can respond. These institutions safeguard national security and critical infrastructure, making them prime targets for sophisticated cyberattacks. With higher stakes than ever, they require robust, real-world training environments to enhance cyber resilience and maintain operational readiness.

The Problem

Federal and military agencies face several critical challenges in their cybersecurity efforts. The threat landscape is rapidly evolving, with adversaries growing increasingly advanced in their tactics. Recently, an agency in this sector struggled to keep its cybersecurity team ahead of these threats, with limited opportunities to practice responding to live attacks without risking disruption to essential operations. This lack of hands-on experience disadvantaged its team when confronted with real threats.

Moreover, the agency lacked the ability to rigorously test new defenses and strategies in a controlled yet realistic environment, which is crucial. So far, the conventional training tools they tried lacked the depth and flexibility to simulate real-world cyber attacks effectively. As a result, this agency struggled to keep its security team fully prepared for the dynamic nature of cyber warfare.

The Solution

SimSpace's tailored cyber range platform offered a transformative solution to these challenges by providing a highly immersive and dynamic environment. The platform allowed this agency's security team to engage in realistic, high-fidelity simulations, enabling them to replicate sophisticated cyber threats they encounter in the field. These live-fire cyber drills prepared them to better manage actual threats by giving them invaluable experience in real-world scenarios.

Additionally, SimSpace's platform enabled this agency to stress-test new tools and strategies before deploying them in live networks. This team ensured readiness and minimized operational risk by evaluating the effectiveness of their cybersecurity measures in a controlled environment. SimSpace also provided continuous training opportunities, allowing the team to develop and enhance their skills through advanced, multi-layered cyber drills. This capability ensured they were well-equipped to coordinate responses to complex, multi-faceted attacks. Ultimately, SimSpace's tailored training scenarios helped this agency refine its skills in incident response, threat mitigation, and long-term operational continuity.

Why SimSpace?

SimSpace emerged as the ideal solution for this agency for several reasons. The platform offered unparalleled realism, emulating large-scale network environments that mirrored the complexity of real-world federal systems. This realistic training, combined with the platform's scalability, prepared the agency for both small and large-scale cyber operations with precision.

The platform also demonstrated proven impact. This agency used it to stress-test its defenses against nation-state-level adversaries, which allowed it to adapt its strategies based on data-driven insights from these simulations. Additionally, SimSpace's comprehensive assessment capabilities provided this security team with critical insights into their cyber readiness. These detailed after-action reports helped prioritize necessary improvements and ensured that this team stayed one step ahead of emerging threats post-cyber drill.

Conclusion

Federal and military organizations in the US require top-tier cybersecurity solutions to safeguard national interests. SimSpace's Cyber Range Platform has proven to be a critical asset, offering realistic training environments, measurable outcomes, and the ability to continuously evolve defense strategies. With SimSpace, these agencies have strengthened their defenses, ensuring their readiness to combat the most sophisticated cyber threats.

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