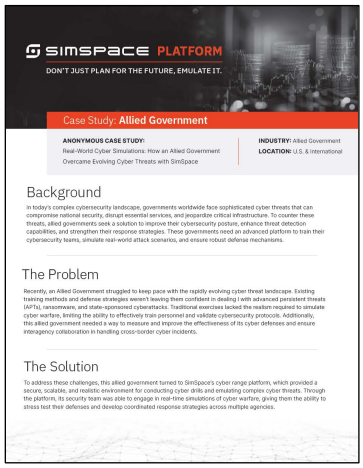

Real-World Cyber Simulations: How an Allied Government Overcame Evolving Cyber Threats with SimSpace

Thank you for downloading this SimSpace case study. Carahsoft is the distributor for SimSpace Cybersecurity solutions available via NASA SEWP V, ITES-SW2, NASPO ValuePoint, and other contract vehicles.

To learn how to take the next step toward acquiring SimSpace's solutions, please check out the following resources and information:

For additional resources:
carah.io/SimSpaceResources

For upcoming events:
carah.io/SimSpaceEvents

For additional Bastille solutions:
carah.io/SimSpaceSolutions

For additional Cybersecurity solutions:
carah.io/Cybersecurity

To set up a meeting:
SimSpace@carahsoft.com
844-445-5688

To purchase, check out the contract vehicles available for procurement:
carah.io/SimSpaceContracts

For more information, contact Carahsoft or our reseller partners:
SimSpace@carahsoft.com | 844-445-5688

SIMSPACE PLATFORM

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

Case Study: **Allied Government**

ANONYMOUS CASE STUDY:

Real-World Cyber Simulations: How an Allied Government Overcame Evolving Cyber Threats with SimSpace

INDUSTRY: Allied Government

LOCATION: U.S. & International

Background

In today's complex cybersecurity landscape, governments worldwide face sophisticated cyber threats that can compromise national security, disrupt essential services, and jeopardize critical infrastructure. To counter these threats, allied governments seek a solution to improve their cybersecurity posture, enhance threat detection capabilities, and strengthen their response strategies. These governments need an advanced platform to train their cybersecurity teams, simulate real-world attack scenarios, and ensure robust defense mechanisms.

The Problem

Recently, an Allied Government struggled to keep pace with the rapidly evolving cyber threat landscape. Existing training methods and defense strategies weren't leaving them confident in dealing l with advanced persistent threats (APTs), ransomware, and state-sponsored cyberattacks. Traditional exercises lacked the realism required to simulate cyber warfare, limiting the ability to effectively train personnel and validate cybersecurity protocols. Additionally, this allied government needed a way to measure and improve the effectiveness of its cyber defenses and ensure interagency collaboration in handling cross-border cyber incidents.

The Solution

To address these challenges, this allied government turned to SimSpace's cyber range platform, which provided a secure, scalable, and realistic environment for conducting cyber drills and emulating complex cyber threats. Through the platform, its security team was able to engage in real-time simulations of cyber warfare, giving them the ability to stress test their defenses and develop coordinated response strategies across multiple agencies.

SimSpace also allowed this entity to conduct in-depth threat intelligence analysis and leverage advanced analytics to improve detection and response times. The platform's tailored environment closely mirrored the government's network and emulated actual cyber threats, enabling the team to train effectively in conditions that reflected the real world. Furthermore, the platform allowed this entity to evaluate the effectiveness of their existing cybersecurity measures, helping them identify vulnerabilities in a controlled setting.

Why SimSpace?

SimSpace is the ideal choice for all allied governments due to its tailored cyber range, scalable solution, and advanced threat emulation capabilities. The platform provided a high-fidelity emulation that allowed this government entity to practice against the same types of cyber threats they would encounter in reality in an environment that models their own. It also offered the flexibility to support the training needs of multiple agencies simultaneously, enabling collaboration on a large scale.

In addition, SimSpace's Platform allowed the security team to test their defenses against a wide array of sophisticated attack scenarios, including those initiated by state-sponsored actors. The platform delivered actionable insights and comprehensive reports, which empowered decision-makers to make informed choices regarding cybersecurity investments and strategies. Most importantly, SimSpace has a proven record of success in helping governments worldwide enhance their cybersecurity posture and improve resilience against advanced threats.

Conclusion

By leveraging SimSpace's cyber range platform, this allied government significantly enhanced its ability to detect, respond to, and mitigate advanced cyber threats. The realistic training and testing capabilities provided by SimSpace improved the skills of the security team, strengthened national security, and ensured that critical infrastructure remained protected against sophisticated cyberattacks. SimSpace continues to play a pivotal role in helping allied governments safeguard their digital ecosystems and build a more resilient cyber defense framework.

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