

Revolutionizing Cyber Incident Response Preparedness with ThreatGEN Red vs. Blue

A Case Study with an international energy company – August 2023



An international energy company operating complex networks vulnerable to cyber threats partnered with ThreatGEN to employ the ThreatGEN® Red vs. Blue simulation platform for immersive cybersecurity training and IR tabletops. The simulations helped evaluate and enhance the energy company's ability to detect, respond to, and recover from cyberattacks that could disrupt operations and safety.

The Value of Tabletop Exercises

Tabletop exercises (TTXs) simulate emergency scenarios to train response teams. For cybersecurity, TTXs present mock attacks to test and improve incident response plans in a controlled environment. Well-designed TTXs drive better preparedness by:

- Identifying gaps in response plans through realistic practice scenarios.
- Engaging participants and promoting retention of response processes.
- Providing safe failure experiences to learn from mistakes.
- Testing communication and coordination capabilities.
- Delivering measurable insights to enhance response efficiency.



Figure 1 - ThreatGEN network environment for Blue Team

However, traditional tabletop exercises have limitations:

- Significant time and manual effort required for scenario development.
- Static scenarios lack adaptability seen in real attacks.
- Limited metrics to demonstrate improvements over time.
- Difficulty sustaining engagement with outdated delivery methods.

ThreatGEN's Game-Based TTX Platform

ThreatGEN® Red vs. Blue revolutionizes TTXs using an interactive game platform developed by cybersecurity experts. Key capabilities include:



- Automated scenarios based on the latest threat intelligence.
- Adaptive adversary A.I. that responds to participants' actions.
- Detailed analytics measuring performance over time.
- Multiplayer simulations driving competition and engagement.
- Expert facilitation providing targeted recommendations.



Figure 2 - ThreatGEN end game screen

For this international energy company, ThreatGEN's platform enabled a new level of preparedness through consistent, measurable practice against dynamic threats.

The Power of Iterations and Ongoing Metrics



Rather than an annual exercise, the international energy company now conducts monthly facilitated TTX sessions using ThreatGEN's platform. This regular cadence provides two key benefits:

- 1) Repeated practice responding to a variety of the latest threats, ingraining effective muscle memory.
- 2) Ongoing metrics showing the measurable improvement of response capabilities over time.

Expert facilitation from ThreatGEN ensures targeted feedback tailored to their environment after each exercise. Detailed analytics track performance trends to guide training priorities.

Through revolutionary TTX simulations, this company continuously raises the proficiency of their cyber incident response team. ThreatGEN's modern platform equips the company to effectively counter emerging threats and minimize business disruption.

Conclusion

ThreatGEN's solution finally brings value to the incident response tabletop exercises that used to be a perfunctory check box item. ThreatGEN solution is priced as follows:

- \$6,500 – ThreatGEN® Red vs. Blue TTX module with 10 user licenses
- \$150 – additional user licenses, sold in 10 packs, with volume discounts after 20 licenses
- \$1,500 – 4-hour virtual TTX facilitation (include preparation meeting)
- \$3,500 – 6-hour onsite TTX facilitation (plus expenses)

