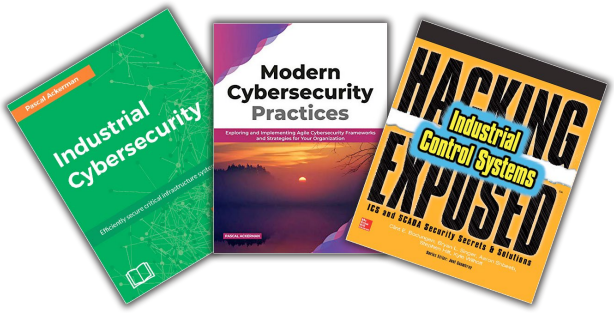
ThreatGEN OT Cybersecurity Training Series

Training Overview

Defending against ICS cyber-attacks requires more than any single solution or even deploying "best practices". A combination of strategies and controls are required, and it requires a tailored approach to be efficient and cost-effective. Whether you need technical skills training, want to build and manage an entire industrial cyber risk management program, or want to learn how to build a cost-effective cybersecurity strategy with limited resources, ThreatGEN has a training program that meets your needs. From beginner to advanced, using practical application and hands-on learning, students will learn the skills necessary to properly assess threats, vulnerabilities, and risks to their ICS, and how to create targeted defensive strategies. And not just learn. Our Red vs. Blue format gives students the unique ability to apply their skills against active "adversaries" working and strategizing against them.

Created by World-Renowned Cybersecurity Experts

We are trusted professionals that *wrote the book* on ICS cybersecurity. Literally. **Clint Bodungen**, lead author of *"Hacking Exposed: Industrial Control Systems"*, **Aaron Shbeeb**, co-author of *"Hacking Exposed: Industrial Control Systems",* and **Pascal Ackerman**, author of *"Industrial Cybersecurity: Efficiently Secure Critical Infrastructure Systems"* and *"Modern Cybersecurity Practices: Exploring & Implementing Agile Cybersecurity Frameworks & Strategies for Your Organization".*



What is Red vs. Blue Training?

Without learning cybersecurity from the "hacker" perspective to gain an understanding of how adversaries attack and compromise ICS networks and assets, you're only getting half of the picture. ***Layered defense is a great concept, but few organizations have the resources to deploy every layer effectively, and in most case, it still ends up being a waste of resources.*** An efficient and cost-effective risk mitigation strategy requires you to understand your vulnerabilities as well as the tactics that attackers will use to exploit these vulnerabilities. Red vs. Blue Training provides the opportunity to learn these adversarial tactics, combined with the defensive methods. Then, students get to apply these skills against an active opponent as they face off against each other, blue team (the defenders) against red team (the attackers).

Cutting-Edge Gamification & Simulation Technology

Traditionally, red team vs. blue team training formats were a significant time commitment, often upwards of five days or more. This can be taxing on constrained schedules and budgets. Additionally, there is a significant technical learning curve associated with being able to play the part of the red team. ThreatGEN® Red vs. Blue training uses cutting-edge computer gaming technology to offer all the most valuable aspects of red vs. blue training, but in a fraction of the time and without a technical learning curve. Students of all levels can even play the part of the red team, regardless of experience or skill level. ThreatGEN industrial process simulation technology allows students to get hands-on experience with technical vulnerability assessments and penetration testing methods on ICS equipment in simulated industrial environments.

+1.833.339.6753 | info@threatgen.com | www.threatgen.com
14090 Southwest Fwy Suite 300, Sugarland, TX 77478