ThreatGrid Cyber War-Gaming Playbook

This playbook provides a structured guide to designing, running and evaluating red team vs. blue team cyber war-gaming exercises. Whether you're training internal security teams or collaborating with external consultants, this guide will ensure impactful and realistic simulations

1. Define Your Objectives

a. Identify key systems or teams to test
b. Define what success looks like (e.g., breach detection time, recovery, reporting accuracy).

2. Assemble Your Teams

a. Red Team: Offensive specialists, ethical hackers, penetration testers.
b. Blue Team: SOC Analysts, network defenders, incident responders.
c. Optional: Purple Team to facilitate collaboration.

3. Design Realistic Scenarios

a. Base simulations on real threat intelligence or recent incidents.
b. Limit scope if needed – e.g., phishing, lateral movement, cloud takeover.

4. Prepare Rules of Engagement

a. Establish clear rules: scope, off-limits systems, acceptable tools.
b. Inform stakeholders and IT teams – without revealing test specifics.

5. Conduct the Simulation

a. Ensure observers or Purple Team are documenting steps.
b. Red Team attempts attack chain; Blue Team monitors and responds in real-time.

6. Debrief & Evaluate

a. Host a structured post-mortem for both teams.
b. Measure detection time, response quality, documentation, and communication.
c. Extract lessons learned and update incident response runbooks.

7. Iterate & Improve

a. Plan the next iteration – adding complexity or changing attack surfaces.
b. Use insights to inform cybersecurity strategy, staffing, and tooling needs.