ThreatGen®

Red vs Blue

Game-Based Cybersecurity Simulation Platform

Game Guide

Written By: Clint Bodungen, Grzegorz Piekarski

v1.11

Copyright © 2024 Derezzed Inc. DBA ThreatGEN

All rights reserved.

No part of this book may be reproduced, stored in a retrieval system, or transmitted in any form or by any means without the prior written permission of the publisher, except in the case of brief quotations embedded in critical articles or reviews.

Every effort has been made in the preparation of this book to ensure the accuracy of the information presented. However, the information contained in this book is sold without warranty, either express or implied. Neither the authors, nor the publisher or its dealers and distributors, will be held liable for any damages caused or alleged to have been caused directly or indirectly by this book.

ThreatGEN has endeavored to provide trademark information about all of the companies and products mentioned in this book by the appropriate use of capitals. However, ThreatGEN and the publisher cannot guarantee the accuracy of this information.

To request permission, contact info@threatgen.com

ABOUT THE AUTHORS

Clint Bodungen is a ThreatGEN® co-founder and the ***ThreatGEN® Red vs. Blue*** lead designer, art director, and programmer. He is a is a globally recognized cybersecurity professional and thought leader with 25+ years of experience (focusing primarily on industrial cybersecurity, red teaming, and risk assessment). He is the author of two books, "***Hacking Exposed: Industrial Control Systems***" and "***ChatGPT for Cybersecurity Cookbook***". Clint is a United States Air Force veteran and has worked for notable cybersecurity firms like Symantec, Booz Allen Hamilton, and Kaspersky Lab. Renowned for his creative approach to cybersecurity education and training, he has been at the forefront of integrating gamification and AI applications into cybersecurity training, creating his flagship product, "ThreatGEN® Red vs. Blue", the world's first online multiplayer computer game designed to teach real-world cybersecurity. His latest innovation is ***AutoTableTop™***, which uses the latest generative AI technology to automate, simplify, and revolution IR tabletop exercises.

Clint remains active in the cybersecurity community and hopes to revolutionize the industry approach to cybersecurity education and help usher in the next generation of cybersecurity professionals using gamification and generative AI.

Grzegorz Piekarski is a ThreatGEN® QA analyst and the ThreatGEN® Discord Community manager. He achieved a top high school IT diploma from Technikum Łączności. Primarily interested in computer networking and penetration testing, he has been participating in the ***ThreatGEN® Red vs. Blue*** community for over 5 years and has helped suggest key features to improve the game, resolve issues, and uses Python programming to greatly automate his job as a QA analyst.

Grzegorz remains active in the community with other ThreatGEN® projects like ***ThreatGEN AutoTableTop™***.

CONTENTS

OVERVIEW 1
GAMEPLAY 1
GAME MODES 1
SINGLEPLAYER 1
HOTSEAT MULTIPLAYER 1
INTERNET MULTIPLAYER 1
IR TABLETOP 2
GAME SETTINGS 2
IN-GAME SETTINGS AND GAME MENU 3
SOUND SETTINGS 3
ASSET LABELS 3
NOTIFICATIONS 3
How to Play 4
STARTING THE GAME 4
TURNS 5
PLAYING ACTIONS 5
ACTION QUEUE 7
ACTION LOG 8
ASSETS 8
ENDING YOUR TURN 8
WAITING FOR YOUR TURN 8
NEW TURN 8
NOTIFICATIONS 9
GAME STATUS DISPLAY 9
RESOURCES DISPLAY 9
THREAT INTELLIGENCE SCORE 10
PROFIT & LOSS METER 10
TURN TRACKER 10
TURN TIMER 10
VIEW BUTTONS 10
NETWORK VIEW 11
ACTION TREE VIEW 11
MODE VIEW (BLUE TEAM) 11
LOCATION VIEW (RED TEAM) 11
RESOURCES 11
BLUE TEAM RESOURCES 12
RED TEAM RESOURCES 12
TEMPORARY RESOURCES 13
WINNING 13
ALL CLEAR (BLUE TEAM WIN) 14
DAMAGE ICS PROCESS (RED TEAM WIN) 14
BLUE TEAM DAMAGED THEIR OWN PROCESS (RED TEAM WIN) 14
WEATHERED THE STORM (BLUE TEAM WIN) 14
RED TEAM APPREHENDED – THREAT INTELLIGENCE VICTORY (BLUE TEAM WIN) 14
COMPANY PROFIT/PRODUCTION COMPROMISED (RED TEAM WIN) 14
MILESTONES & ACHIEVEMENTS 14

GAME WIKI 15
BASIC STRATEGY 16
RED TEAM STRATEGY 17
THE BIG PICTURE 17
OPEN-SOURCE INTELLIGENCE (OSINT) 19
HOST SCANNING 19
PORT SCANNING 20
SERVICE ENUMERATION 20
FINDING VULNERABILITIES 21
ATTACKING 22
RESEARCH & UPSKILLING 23
STEALTH AND MAINTAINING PERSISTENCE 24
PILFERING 25
PIVOTING 25
MALWARE 25
RANSOMWARE 25
SOCIAL ENGINEERING 26
PHYSICAL ACCESS 27
BLUE TEAM STRATEGY 27
CYBERSECURITY PROGRAM & GOVERNANCE 28
CYBERSECURITY ARCHITECTURE AND CONTROLS 28
VULNERABILITY MANAGEMENT 29
THREAT MONITORING 31
INCIDENT RESPONSE (IR) 32
APPENDIX 34
APPENDIX A: BLUE TEAM ACTIONS 34
APPENDIX B: RED TEAM ACTIONS 40
APPENDIX C: VULNERABILITIES 47

OVERVIEW

ThreatGEN® Red vs. Blue leverages modern computer gaming technology and methods to create realistic, interactive cybersecurity training simulations. The concept of using computer games for learning is commonly referred to as gamification or game-based learning. A key component of ThreatGEN® Red vs. Blue is Active Adversary Simulation™, which allows you to learn and practice against an actual adversary (computer opponent or another person) working against you, just as it would be in real life. ThreatGEN® Red vs. Blue is also designed so that anyone of any skill level can easily learn and practice cybersecurity (as the Blue Team or the Red Team) *without* a technical learning curve.

GAMEPLAY

ThreatGEN® Red vs. Blue works like a turn-based strategy game. This means that each player takes turns performing actions, much like the way a board game works. In this case, every action in the game represents a real-world cybersecurity counterpart, for both the Blue Team and the Red Team.

GAME MODES

SINGLEPLAYER

Players can play as the Blue Team or the Red Team against a computer A.I. opponent of the opposite team.

HOTSEAT MULTIPLAYER

Hotseat Mode is a multiplayer format where players share the same device. Each player takes their turn and, after ending their turn, they “swap seats” (or pass the device) to their opponent.

INTERNET MULTIPLAYER

In Internet Mode, players connect to the game server via the internet and can play against each other remotely. Games are setup in the game lobby. When setting up a game, players may change their name from the default (your Steam player name, if using Steam), and choose which side they want to play as (only the host may choose). Players may join available games listed in the game list window. Details about each game’s settings are displayed below each game name in the game list.

NOTE: *Players can communicate and find other players to match with on our Discord Server:* https://discord.gg/zxavYD5reC

IR TABLETOP

(Professional Version Only)

Incident response (IR) tabletop scenarios are designed to help organizations test their IR plan and train staff. IR Tabletop Mode allows users to choose from several built-in threat scenarios and which security posture strength they want to start with.

GAME SETTINGS

You can access the settings screen by clicking on the gear icon at the bottom of the start menu.

In the game settings, you can modify each of the following:

- Starting money (Blue Team)
- Starting staff (Blue Team)
- Hacker resource points (Red Team)
- Turn timer
- Maximum number of turns
- Turn notifications on/off
- Music and sound effects volume
- Starting seed number
- Language of the game
- Report format

HINT: *Providing a starting seed number produces the ability for players to experience consistent results. For example, vulnerability distribution among the assets will be the same for everyone using the same seed number. AI decision making and action-based results will also remain consistent, all things being equal. This is useful for scenarios, events, and classroom exercises where players need to be presented with the same conditions.*

NOTE: *Altering the values too far from the default settings can disrupt the overall balance of the game and could give one side a disproportionate advantage over the other.*

The default settings can be restored by clicking on the “restore defaults” button.

IN-GAME SETTINGS AND GAME MENU

While in game, you can access the game menu by clicking on the gear icon in the top right corner of the user interface (UI). This menu will allow you to end, restart, or return to the game. While in singleplayer mode or hotseat mode this will also stop the turn timer and pause the game. For internet multiplayer games, the turn timer will continue to run. The give up button allows players to concede the match with all metrics displayed in the end game screen and recorded in the player stats (professional version).

SOUND SETTINGS

Next to the gear icon, the speaker icon will allow you to toggle the game sound off (mute) and on.

ASSET LABELS

The flag icon will allow you to display asset labels.

NOTIFICATIONS

The notifications icon will display the notifications window, which shows all notifications, achievements, and milestones achieved so far.

How to Play

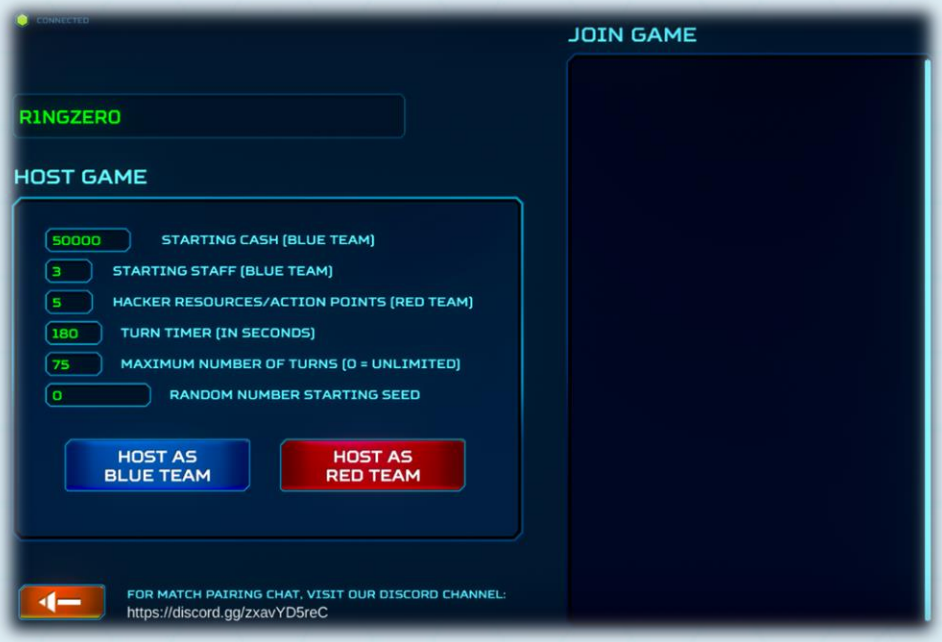
Starting the Game

Selecting singleplayer will allow you to choose to play as the Red Team or the Blue Team, with the computer AI playing as the other team. Choosing the multiplayer hotseat option will start the game beginning with the Blue Team. Choosing the multiplayer internet option, players will enter the lobby first, where they can create/host and join games. Whichever player creates the game will get to choose to play as the Red Team or the Blue Team. When hosting a game, the game settings can also be modified from this screen.

The specific game settings for each game are listed under the game name in the available games list. If a starting seed number is provided, an exclamation point will be displayed to the left of that game, warning the joining player that the host could have an advantage by knowing the seed number.

If the player wants to modify their player name in the professional edition, they should change the Display Name in their ThreatGEN portal account settings.

Only two players are allowed to join each game. One player as the Red Team and one as the Blue Team. Once both players are in the game waiting room, the Blue Team player will be allowed to start the game.



NOTE: *Regardless of what mode you are playing in or which team you choose to play as, the Blue Team always starts first.*

TURNS

Players alternate turns, with a default time limit of 3 minutes per turn. This time limit can be changed in the settings menu, accessible from the main start screen, or when creating a network game.

PLAYING ACTIONS

During your turn, you progress through the game by playing actions. Playing actions represent performing real-world tasks and are the core gameplay mechanic. Such tasks include things like creating and implementing security policies, deploying security controls, attacking assets, responding to incidents, and even requesting budget and hiring new staff. Each action is explained individually under the actions tab in the game wiki. You can also easily access each action's game wiki entry directly by clicking on the question mark icon found on each action.

You can play actions in one of three ways. The first way is to click on an asset. Actions that are directly related to that asset (targeted assets) will show up in the asset's action menu, as long as they are available to play.

The second way is to use the action category buttons found on the bottom left-hand side of the UI. Actions that are not specific to assets can be found here, organized by their associated category.

The last way is by navigating to the action tree using the navigation buttons at the bottom right-hand side of the UI (refer to the V*iew Buttons* section) and clicking the yellow plus "+" button found on the action you want to play. The action tree provides the benefit of displaying all the actions in a hierarchical view, which shows each action's prerequisites, and child actions that are unlocked once completed.

Action view buttons are also color-coded based on the availability of the action:

- **Blue or Red** (based on team color) – The action is not yet available
- **Green** – The action is available to be played
- **Purple** – The action has been played and cannot be played again
- **Yellow** – The action has been played, but can be played again

Targeted Actions

In cases where an action is specific to an asset (targeted actions), a green target icon will appear over the assets that are available to select. Only one asset may be selected at a time. To select another asset, you must choose the targeted action again, and select another asset.

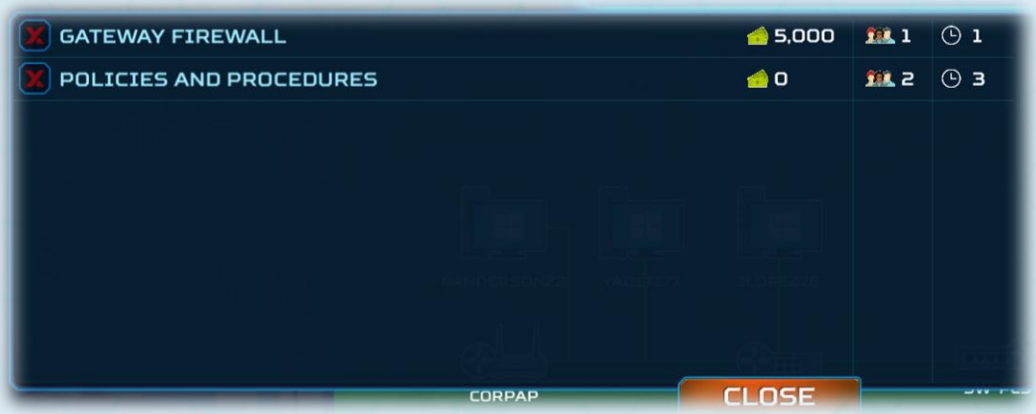
NOTE: *Target selection does not appear when you select a targeted action by clicking directly on an asset.*

Action Options Menus

Some actions will require further input such as attacking, choosing a new location, and research, for example. In such cases, a menu will appear requiring you to select options for that action.

ACTION QUEUE

When you select an action to play, it will appear in the action queue, and the resource cost (money and staff for the Blue Team and "hacker resources" for the Red Team) for that action will immediately be subtracted from your resource pool. Your *staff* or *hacker resources*, however, *are not gone permanently*. They will return once their action has been completed. Actions in the action queue are not committed until you end your turn. If you decided that you do not want to play an action that has already been added to the action queue, you can click on the name of the action (or the red "x") in the action queue to remove it, as long as you have not ended your turn. You may continue to add actions to the action queue, if you have enough resources to play the action you select.



ACTION LOG

The action log is a turn-by-turn record that allows you to see what actions you have already played, what actions are still in the queue, and how many turns are left until their completion.

ASSETS

While actions are *how you play* the game, assets are *what* you are protecting, or attacking. The in-game assets represent the same types of devices that are found in real-world networks. Just like the real world, the in-game assets have distinct characteristics, functions, operating systems… and vulnerabilities. They also have different advantages to attackers in the event they are compromised, as well as varying "production value" to your company's profit & loss. Further details about each asset can be found under the assets tab in the game wiki.

ENDING YOUR TURN

To end your turn, click the green end turn button at the bottom right-hand corner of the UI. At this time, all actions in the action queue will be finalized and submitted.

WAITING FOR YOUR TURN

While you are waiting on your opponent to finish their turn, you may perform some tasks such as looking through your available actions, viewing the Wiki, and you can even get a head start on your next turn by adding actions to the action queue.

NEW TURN

Once it is your turn again, you will be presented with the start turn dialogue. For singleplayer and hotseat modes, the turn timer will not start until you click start turn. For multiplayer internet games, the turn timer will start immediately, regardless of whether you click the start turn button.

NOTIFICATIONS

After clicking the start turn button and if you have any new notifications, you will be presented with the menu window, which can include general notifications, achievements, and milestones. Notifications that haven't been viewed yet will include an exclamation point on the notification.

For more information regarding milestones and achievements, refer to the *Milestones & Achievements* section.

GAME STATUS DISPLAY

The game status display is at the top of the UI. It displays each teams' available resources, current turn (which increments at the end of the Red Team's turn), the total number of turns allocated for that game, the turn timer (which resets at the beginning of each player's turn), and the threat intelligence score (Blue Team only).

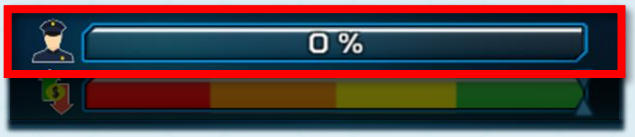
RESOURCES DISPLAY

Each of the resources needed to play actions are displayed at the top right of the UI (staff and money for the Blue Team and hacker resource points for the Red Team). Temporary resources are also displayed here to the right of the standard resources.

For more information regarding resources, refer to the Resources section.

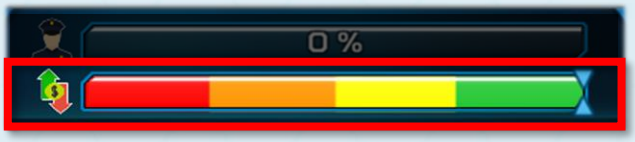
THREAT INTELLIGENCE SCORE

The threat intelligence score (Blue Team only) is at the top center of the UI and reflects your progress toward the threat intelligence victory. When this score reaches 100%, the Blue Team wins with a threat intelligence victory. The threat intelligence score is increased by gathering forensics on compromised assets, detecting attacks and compromises, and when the Red Team is arrested during physical entry attempts.



PROFIT & LOSS METER

The profit & loss meter represents the financial and production status of the company in relation to cyber outages. When assets are out of service, infected with malware, or having data exfiltrated, the meter will trend downward toward red until the issues are remediated. The more important the asset, the faster the meter will move. When the meter remains in the red for too long, the Blue Team loses.



TURN TRACKER

The turn tracker displays the current turn and the total number of turns allowed during the game. For games without the *Weathered the Storm* win condition selected and/or if the number of turns is set to 0 (zero) in the game settings, only the current turn will be displayed.

TURN TIMER

The turn timer displays the time remaining for your current turn. The timer will reset after each turn and will not count down when it is not your turn.

VIEW BUTTONS

The view buttons are found at the bottom right corner of the UI. These buttons control the main view within the interface.

NETWORK VIEW

The network view is the main view that you will be using for most of the game. This view displays the “game board”, which consists of the network environment and assets.

ACTION TREE VIEW

The action tree view displays all the game actions in a “decision tree”. This view allows you to see all the actions, along with their prerequisites, in a hierarchical format. You can select actions from this view by clicking on the yellow plus “+” button. Selected actions will be entered into the action queue.

MODE VIEW (BLUE TEAM)

The mode view lets you see whether you are in regular mode or in incident response (IR) mode.

NOTE: *Some actions are only available while in IR mode or while in normal mode.*

LOCATION VIEW (RED TEAM)

The location view lets you know whether you are remote or on-site. This view is also accompanied by a “radar”, or “minimap”, view showing a representation of the layout map and where you are currently at in the map. Your location is represented by a pulsing yellow beacon. The background image of this view will also change according to your location.

NOTE: *Some actions are only available while being remote or while being on-site.*

RESOURCES

Resources are what you spend to play actions. They are located in the top right corner of the UI for both the Blue Team and the Red Team. As you play actions, the associated resource cost of that action is subtracted from your resource pool.

BLUE TEAM RESOURCES

The Blue Team's resources simulate the same resources affecting network defenders in the real world. These Resources are ***money***, ***staff***, and ***time*** (in the form of turns). Each action has a cost associated with one or more of these resources. The cost of each action is a simulated representation of how much relative money, time, and staff it would take to complete the same action in the real world.

As the Blue Team, you start with limited resources in terms of money and staff. You must find a way to strategically use the resources you have or find a way to increase the number of staff and money available to you. When you "spend" staff on an action, those staff resources will become available again once they complete the action they have been assigned to. However, your money is gone and won't return unless you find a way to get more of it. You can request additional budget, which you may or may not get depending on the mood of the powers that be. This is a pseudorandom calculation that can be affected by other things you do in the game that increase your chances of getting budget. You could compel management to grant you funds, if you can show them that you are at risk and in need of budget for additional controls. But rather than spoiling the challenge, we'll let you experiment for yourself.

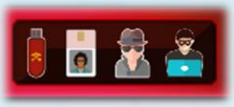
RED TEAM RESOURCES

The Red Team resources are simply represented as "Hacker Points" and time (in the form of turns). The Red Team's hacker points resource is more abstract in concept than the Blue Team's resources, because there are a multitude of factors to consider across many different threat actor types, groups, motivations, and recourse types that real-world adversaries might have.

Just like the Blue Team, each action has a cost associated with one or more of these resources. The amount that each Red Team action costs is largely based on how complex the action is (relevant to its real-world counterpart). Hacker points are returned to your pool once the action they have been assigned to has been completed. Once the game has started, you may find ways to increase your resources (the default is 5) such as upgrading your rig (your computer hardware) and recruiting more hackers. There might also be other hidden ways such as special achievements, which you can discover...

TEMPORARY RESOURCES

The temporary resources window displays each resource when it is available. When these resources are not available, they will not show up in the window.



- **ICS Vendor Certification (Blue Team)**
  For scenarios with ICS, the ICS vendor certification icon will display and be in effect for 10 turns after the ICS vendor certification action is played.

- **Malicious USB (Red Team)**
  When a malicious USB is created, its icon will display and be in effect for 10 turns.

- **Cloned RFID Badge (Red Team)**
  Once an RFID badge is cloned, it will be available, and its icon will be displayed until you are arrested during a physical intrusion attempt.

- **Covert Attack (Red Team)**
  Preparations for a covert attack, and its icon, will be available for the very next attempted attack only. After that, the icon will disappear, and a new covert attack must be prepared.

  NOTE: *As the Red Team, you will not know whether your attack was detected or not.*

- **Network Detection Evasion (Red Team)**
  Just like a covert attack, preparations for evading network attack detection will only be available for the very next attack, and as the Red Team, you won't know whether your experts were successful or not.

WINNING

It's hard to win a game without win conditions. ThreatGEN® Red vs. Blue is an asymmetric game, which means that the objectives of the game and the win conditions are different depending on which side you are playing, the Red Team (the "hackers") or the Blue Team (the defenders).

The following win conditions are available:

ALL CLEAR (BLUE TEAM WIN)

Successfully bring the network to a “vulnerability free” state. This means clearing off all vulnerabilities, public and zero-days, from all assets. (Zero-day vulnerabilities will be explained later.)

DAMAGE ICS PROCESS (RED TEAM WIN)

When ICS scenarios are chosen, the ultimate victory (for the Red Team) would be to damage an industrial control system’s process. In order to do so, you must first find a way to take control of a programmable logic controller (PLC).

BLUE TEAM DAMAGED THEIR OWN PROCESS (RED TEAM WIN)

If the Blue Team doesn't take proper care of their ICS assets, they can end up damaging their own assets for a Red Team win.

WEATHERED THE STORM (BLUE TEAM WIN)

This serves as the default win condition when the maximum turns have expired. If the Red Team hasn’t achieved a victory, Blue Team Wins by virtue of preventing the Red Team from achieving a victory.

RED TEAM APPREHENDED – THREAT INTELLIGENCE VICTORY (BLUE TEAM WIN)

When the Blue Team has gathered enough evidence and the threat intelligence score reaches 100%, the Red Team is apprehended, and the Blue Team wins using this condition.

COMPANY PROFIT/PRODUCTION COMPROMISED (RED TEAM WIN)

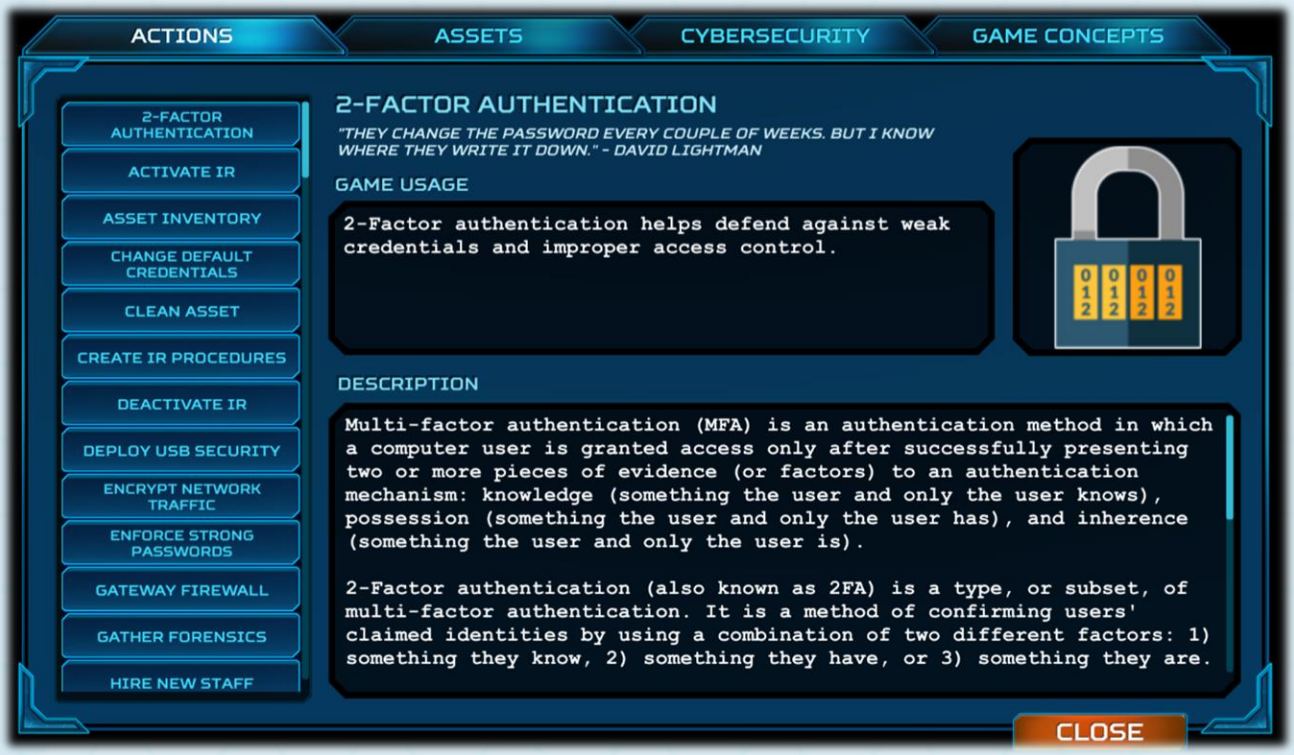
This win condition is awarded when the blue team's profit & loss meter drops into the red for 5 straight turns.

MILESTONES & ACHIEVEMENTS

Milestones represent significant events, tasks, or achievements similar to their comparable real-world counterparts. They are awarded based on several factors including completing specific actions, special sequences and/or a combination of actions, and completing actions under special circumstances or with special conditions. They are essentially the game’s way of letting you know whether you are on the right track or not.

GAME WIKI

The game wiki is not only your in-game guide to all things related to the game, but real-world cybersecurity as well. In addition to detailed information about each action, asset, and game concept, the game wiki also contains information on a multitude of cybersecurity related terms and topics (for both Red Team and Blue Team). It is an in-game cybersecurity glossary. The game wiki can be accessed anywhere you see the question mark "?" icon.



BASIC STRATEGY

ThreatGEN® Red vs. Blue is designed to simulate the way cybersecurity works in real life. Every action you take can have various effects throughout the game that correlate to real-world cybersecurity actions. For example, different security controls are more effective against some attacks versus others. The effects of some security controls can even stack with others, increasing their overall effectiveness. On the Red Team side, hacking certain assets such as an Active Directory server can make it easier to compromise other assets with weak passwords. These are just a few examples of the several combinations that exist within the game, which simulate real-world cybersecurity.

Discovering and understanding the different correlations and related strategies takes time, exploration, and practice, just as it does in real life. It might come easier to some of those with more experience in cybersecurity, but if it doesn't, don't get discouraged. ThreatGEN® Red vs. Blue is designed to be challenging. As your knowledge and understanding of the various cybersecurity concepts, methods, and strategies grow, so will your successes in the simulations.

The Red Team and the Blue Team each have their own unique methods and strategies in real life as well as in the ThreatGEN® Red vs. Blue. Below are the most common methods for each team, regardless of your overall strategy.

HINT: *The strategies covered here aren't just applicable to the game. The information contained in the following section is also sound advice for the real world.*

RED TEAM STRATEGY

As a Red Team operative, your goal is to gain access to the Blue Team's network and take control of systems. Your exact strategy and tactics will depend on your understanding of "hacker" methods (If that's little to none, don't worry. That's where this platform comes in.), the win conditions available to you (discussed in the Win Conditions section), and your own imagination and creativity!

Red Team Process

THE BIG PICTURE

To gain access to the Blue Team's network, the Red Team core strategy mirrors that of real-world hacker methods, often referred to as the "cyber kill chain" or "anatomy of an attack". Regardless of what actions, attack vectors, and exploits you use, this strategy follows the same pattern as shown in the Red Team Process diagram.

Gather Information

Commonly known as reconnaissance ("recon") and intelligence gathering, knowing something about your target is a crucial first step, whether you are looking to gain your first foothold, or you already have one. For cyber-attacks, this involves finding publicly available information (a.k.a. open-source intelligence, or "OSINT") that can be used to identify computer systems and network devices, or even information that aids in social engineering attacks. For physical attacks, this often involves being onsite to entry points such as doors and gates, watching personnel, and even digging through trash for information (a.k.a. "dumpster diving").

Search for Targets

Searching for targets is the process of using the information you've gathered to identify feasible attack vectors. For cyber-attacks, this is usually in the form of host scanning, which we will discuss in more detail later. Much of the potential physical entry points, however, will have already been identified during the physical recon step.

NOTE: *Searching for targets is a process that happens from the very start as you attempt to breach the perimeter (network or physical), but also happens once you have already gained a foothold on the inside as you attempt to move further into and throughout the environment.*

Identify Weaknesses (Attack Vectors)

Before you can successfully compromise any of the targets that you have found, you must identify weaknesses in them that could be exploited. For cyber-attacks, this process starts with port scanning and service enumeration, both discussed in further detail later. These actions will provide further detail about the target and what programs are running on it, which will later be used in formulating the attack. Identifying physical weaknesses isn't as straightforward. There isn't a scanning tool to help automate the process. It's a much more tedious task of observing employee behaviors, procedures, and patterns. It might also require close and personal inspection of doors, locks, windows, etc. and even implementing the use of disguises and fake personas. If this sounds a bit "cloak and dagger," that's because it kind of is. Lucky for you, the in-game complexities of physical recon have been simplified.

Once you have identified software and services running on cyber targets, along with other potential useful information such as what type of assets they might be, you can begin searching for vulnerabilities to exploit. In real life, this involves cross-referencing the information you have found so far with publicly known vulnerabilities or even manually reverse engineering software in the hopes of uncovering zero-day (or non-public) vulnerabilities. In-game, the complexities of vulnerability identification has been simplified into simple actions, which are explained further later.

Formulate the Attack

Now that you have identified targets with exploitable vulnerabilities, it's time to formulate an attack. In real life, this step often involves selecting vulnerabilities, testing exploits in a local lab (for cyber-attacks) and adjusting as needed (which could also involve further research). The in-game process is detailed further, later in this section.

Execute the Attack

You have identified the target, gathered the necessary information, and found vulnerabilities to exploit. Now it's time to execute the attack, detailed further in this section.

Gain a Foothold

Once have a foothold, also known as a pivot, you enter the post-exploitation phase. This is when you attempt to gather further information from the asset you now have control of (if any is available) to assist with further attack. You might also need to "hide your tracks" for stealth. Finally, you'll want to repeat all of the previous steps to identify additional hosts on the network and move throughout the environment (a.k.a., lateral movement).

With an understanding over the overall process, the rest of this section will provide further detail about many of the actions that the Red Team has at its disposal to execute the process. A detailed list of actions and their descriptions can be found in Appendix B.

OPEN-SOURCE INTELLIGENCE (OSINT)

This is also known as, *reconnaissance*. Before you can begin attacking a target (in this case the Blue Team network), you need to gather information about that target such as what internet facing assets the target has (which will function as your entry points, or *attack vectors*).

HOST SCANNING

Once you have performed OSINT, you will have identified Internet Protocol (IP) address ranges that might belong to the Blue Team. IP addresses are unique ID numbers that all network connected devices must have to communicate over the internet or any network. Think of it like a "telephone number" for computers. If two people want to communicate over a telephone network, both parties must have a unique telephone number. A host scan will search a range of IP addresses and see if any devices (called *hosts*) communicate back (almost like looking through a range of numbers in a phone book and calling those numbers and seeing who answers). This can be done many times throughout the game (just as in real life) because new potential hosts can show up at any time. This could be due to new internet facing devices being installed or maybe exposed remote users that are connected to the company network. The host scan action is a prerequisite before being allowed to proceed to the port scan action.

Discovered hosts will show up as unidentified assets (displayed in the game as indeterminate gray computers with a red question mark) labeled with an IP address. Very limited information about the asset will be available in the asset details view, which can be viewed by clicking on the asset.

The host scan action can be played from the action tree, the action buttons at the bottom of the UI, or by clicking on an asset that you have control over (as long as you have access to that asset). This is also the only action that can be played by clicking on the internet icon.

When selecting this action, you will be asked to select a target/pivot from which to scan from. A pivot is essentially a "foothold". It is an asset that you have taken control of on the Blue Team's network, which allows you to launch scans and attacks further inside of the network. Assets that are available to select as pivots will display an animated target icon over the top of them.

When you select a pivot, the action will be entered into the action queue and that action selection is complete. You may select more than one pivot in a single turn as long as you have enough resources. To do so, select the host scan action again. Assets that have already been previously selected, and are already in the action queue, will not display the target animation.

PORT SCANNING

Once you have identified viable target hosts, it's time to learn more about them. A port is a logical connection interface that allows network capable services (running on the host) to communicate and be accessed over the network. Discovering these open ports helps identify potential entry points to exploit on the host, but also helps determine what type of device the asset is. The port scan action is a prerequisite before being allowed to proceed to the service enumeration action.

Assets that have been port scanned will show the device type instead of the IP address and will also display the same port scan icon. Additional information about the asset will also now be available in the asset details view.

The port scan action can be played from the action tree, from the action buttons at the bottom of the UI, or by clicking on an asset that you have discovered. When doing so, you will be asked to select a target to scan. All assets that are available as scan targets will display an animated target icon over the top of them. Assets will only be available as scan targets if they are either internet facing or you have established a pivot with access to them (meaning, you have control of an asset in the same network zone as that asset). When you select a target, the action will be entered into the action queue and that action selection is complete. You may select more than one target in a single turn as long as you have enough resources. To do so, select the port scan action again. Assets that have already been previously selected and are in the action queue, will not turn green.

SERVICE ENUMERATION

Now that you have identified a bit more information about the assets you have discovered (in the real world, this usually means ports and the potential operating system), service enumeration will help further confirm the services running on those assets, along with additional details such as version number and more. These details make it possible to identify public vulnerabilities associated with these services. As a result, the service enumeration action is a prerequisite before having access to the different vulnerability discovery actions.

Assets that have had service enumeration performed on them will now display the actual asset icon, the asset hostname, and service enumeration icon. Complete information about the asset will also now be available in the asset details view.

The service enumeration action can be played from the action tree, the action buttons at the bottom of the UI, or by clicking on an asset that you have previously port scanned.

FINDING VULNERABILITIES

Now that all the previous prerequisite steps have been completed, you can perform vulnerability discovery (often referred to as *vulnerability research* in the real world). Before you can attack an asset, there needs to be one or more vulnerabilities to try to exploit. There are 3 vulnerability discovery options available:

Finding Public Vulnerabilities

The *find public vulnerabilities* action uses information from the service enumeration step to attempt to find publicly known vulnerabilities on that asset. When vulnerabilities are identified, the asset will display the yellow vulnerability shield icon. Keep in mind that this action will not necessarily find every public vulnerability, and it is not guaranteed to find any at all.

Fuzzing

Fuzzing is the process of sending data to an input in a way that could make the service behave in a manner other than how the developer intended. This anomalistic behavior could be a sign of an exploitable bug, or *vulnerability*. The cool thing about such a vulnerability is that these kinds of vulnerabilities are not often public. They are known as ***zero-days*** *(a.k.a. 0days or 0-days)*. Although zero-days are more difficult to obtain, there is also less likely of a chance that they are patched.

Reverse Engineering

Reverse Engineering is one of the most advanced forms of vulnerability research. It is often done in conjunction with fuzzing, as a follow-up to the fuzzing results. Just like the fuzzing action, the reverse engineering action can yield zero-days. Reverse engineering, however, can find much deeper rooted zero-days. This could come in handy when the Blue Team has done a good job of patching everything up and you think there is no longer any way into their network.

You can see what vulnerabilities have been identified for each eligible asset by clicking on the yellow shield icon displayed on the asset.

ATTACKING

Now that you have discovered one or more vulnerabilities, you can attack an asset. When you select the attack action (either from the action menu, the action buttons at the bottom of the UI, or by clicking on an eligible asset), the attack setup screen will appear. You must first select a target (an asset). When you click the select target button, available targets will display the green target animation. Assets will only be eligible attack targets if you have established a pivot with access to them or the target asset is internet facing. Additionally, you must have identified at least one vulnerability on that asset.

Once you have selected a target, you will be returned to the attack setup screen. Next, you will need to choose a vulnerability to exploit. All available vulnerabilities for that asset that you have previously identified so far will show up in the drop-down menu. You will also see a meter indicating your skill level at exploiting each vulnerability listed. The more that the green level indicator has advanced, the better your chances will be for exploiting that vulnerability. This level can be increased by performing research (refer to the *Research* section for more information).

Finally, you must select an attack objective, either *denial* or *manipulation*. A successful denial attack will render that asset inoperable, but you will not have control over it. (Denying an asset still comes in handy for certain strategies.) A successful manipulation attack will give you control over that asset, allowing it to become a pivot or providing any number of other benefits that could be associated with certain assets. Once you have setup the attack, you must commit the attack by clicking on the yellow plus "+" button.

Compromised Asset States

Once you compromise an asset and have control over it, it will be in one of four different states. Each state is represented by a different color:

- **Controlled Asset**
  This asset has been compromised and you currently have control over it. Compromised/controlled assets will appear red with a white skull icon.

- **Denied Asset**
  This asset has been hit by a successful denial of service (DoS) attack and is effectively "offline". Denied Assets will be displayed as gray with a white skull icon.

- **Proxy-Controlled Asset**
  You have control over this asset because you have compromised, and have control over, another asset that is connected to this asset in a way that gives you control over it. (i.e., remote desktop protocol or remote administration application)

- **Disconnected Asset**
  The Blue Team as manually disconnected this asset, which often occurs as the result of Incident Response (IR) or there's no chain of compromised and controlled assets to a root of Red Team control (Internet, a Red Team-owned device, a compromised asset with a reverse shell installed or a compromised device in Red Team's current physical location).

- **Only Physically-Controlled Asset**
  This asset is only physically controlled by the Red Team. As of the current version, this can only happen when they find the HMIs using the Search for HMIs action and are in their physical zone.

RESEARCH & UPSKILLING

At some point, you will notice that exploiting some vulnerabilities is more difficult than others. In fact, some are very difficult. This is where research comes in. Performing research actions on any particular vulnerability will simulate improving your skill at exploiting that vulnerability, essentially increasing your chances of a successful exploit. To perform research, select the research action from the action tree or from the action buttons at the bottom of the UI. Additionally, you can click

on the research icon anywhere vulnerabilities are listed (such as the attack setup screen shown in the image above, for example).

You can research each vulnerability as much as you want throughout the game and your skill level will increase (for the vulnerability researched) each time it is researched. However, over time there will be diminishing returns once your skill level for that vulnerability has reached a certain level.

The shield icon over each asset will also change from a yellow shield to a cracked red shield, and then to a black and blue shield on fire, when any vulnerability on that asset has reached any one of the three skill level milestones, respectively.

STEALTH AND MAINTAINING PERSISTENCE

As you progress through the network, you might want to maintain a persistent presence, or a “foothold”, on the network. Otherwise, it could take a very long time to win, and even significantly reduce your chances of winning, if you must keep finding a way back into the network every time the Blue Team kicks you out. Not to mention, the Blue Team’s threat intelligence score increases each time they detect an attack or a compromise, which could lead to a Blue Team win if they collect enough threat intelligence. Once the Blue Team has deployed security monitoring technology, your attacks and asset compromises will be detected unless you take precautionary measures.

To avoid detection, there are several actions that can be performed. Researching persistence unlocks other stealth related actions and decreases the chances you will be discovered when attempting to cover your tracks. Once you have successfully played the research persistence action, you will gain access to the prepare covert attack action. Using this action before attempting an attack will give you a shot at successfully pulling off a covert attack and hopefully not being

detected by the Blue Team's network intrusion detection sensors. Keep in mind that the Blue Team monitoring does still have a very slight chance of detecting a successful covert attack.

You can also play the *cover your tracks* action once you have taken control of an asset. Doing so will make it very difficult for the Blue Team to detect that you have control over that asset. If you have also previously researched persistence, you won't be left exposed in between the time takes to gain control of the asset and when you cover your tracks.

Finally, installing a reverse shell on an asset will enable you to maintain persistence on that asset, and maintaining that asset as a pivot, even if no other pivots are available to that asset.

PILFERING

Pilfering refers to the act of gathering information from one compromised asset that could help you compromise another asset. Such information often includes user credentials and other valuable information that might pertain to the network. In the game, you can play the *pilfer data* action by clicking on an asset you have control of, as well as from the action menu and the action buttons at the bottom of the UI.

You can also use the *harvest credentials* action to increase your chances or exploiting weak passwords.

PIVOTING

Once you have control of your first asset, what's next? Once adversaries and red teams in real life gain access to an asset, they usually begin exploring the network and start looking for other assets to take control of. This is called lateral movement. You can do the same by performing a host scan from the asset you have control of (refer to the *Host Scanning* section covered earlier.) and then repeating the kill chain process (host scan, port scan, service enumeration, find vulnerabilities, and attack).

MALWARE

Deploying disruptive malware is one way to disrupt the productivity (profit & loss) of the Blue Team. Once the malware is installed, the effects can be amplified by using the malware to exfiltrate data.

RANSOMWARE

Ransomware is another devastating tool in the Red Team's arsenal, which represents one of the most concerning threats in recent times. Unless the Blue Team is lucky enough to have a restore point created prior to the initial compromise, the only recourse they have is to pay the ransom

(which is very expensive), crack the ransomware encryption key (which is very difficult to do), or replace the asset.

NOTE: *This is a two-step process. The ransomware must first be installed and then activated.*

SOCIAL ENGINEERING

Social Engineering in the real world is the process of tricking people into unwittingly giving up their login credentials or clicking on some sort of exploit trap; thereby giving you control of the asset if successful. In the game, the concept is the same and there are several social engineering options that, if successful, can give you control over an asset without actually going through the entire attack setup and process, including the "kill chain" process. The spear phishing action is a one-time action that has a better chance of success than the social engineering campaign options, but it is a bit more costly. The social engineering campaign (labeled attack campaign in the game) offers three different options (email phishing campaign, social media campaign, and watering hole campaign), each with different success rates. Email phishing has the greatest chance of success whereas the watering hole campaign has the least. Campaigns are also sustained efforts. This means that the campaign will continue to try and gain access to assets, by means of the social engineering method selected, even if there have already been successful attempts. The resources required to sustain the campaign will also remain unavailable until you end the campaign.

You will need to research persistence to use these actions, as they will result in opening a reverse shell by default, which'll allow you to control the asset without a direct chain of assets to the internet or RT-owned devices.

You have no control over which user or asset to target when you use social engineering. Whenever it is successful, a random Windows asset will be chosen, and you will then have control over that asset.

Over time, campaigns will yield diminishing returns at least until a new campaign is started. There are also several key security controls the Blue Team can deploy to reduce the chances of your campaign's success. Therefore, social engineering is usually most effective as an early strategy (and could be a powerful one if you land on a key asset), when the Blue Team network security hasn't matured, but it can also be used effectively anytime against a Blue Team that hasn't focused on defending against social engineering attacks. Even if the Blue Team has deployed every security control that protects against social engineering, there is always a slight chance it could succeed. However, you can improve your chances of success again by successfully pilfering data from assets you have control over. Given enough assets, this could add up significantly!

PHYSICAL ACCESS

Physical access is often overlooked as an additional attack vector to computer systems. When it seems like your cyber-attacks are being thwarted and you aren't having much success there, you can always use the *change location* action to move to the physical location of your target. While onsite, you can look for (and potentially exploit) Wi-Fi devices, as well as attempt to navigate deeper into the physical environment. While there, you can attempt to physically access assets, plant trojans and rogue devices, and plant malicious USB sticks.

There are three different means of navigating the physical environment: social engineering (tricking humans to give you access), electronic (subverting electronic locks), and good old fashioned breaking and entering. Each of these methods also have their own varying difficulties and skill advancements in the game.

However, proceed with caution! If you are detected while onsite, you can be escorted off premises or even arrested! If you are arrested, the Blue Team's threat intelligence score will go up. The Blue Team has several controls at their disposal to make traversing through the physical environment more difficult, as well as to make it easier to detect intruders.

BLUE TEAM STRATEGY

As a Blue Team cybersecurity specialist, your goal is obviously to defend your network. However, this is not as straightforward as it sounds. Unlike the Red Team, there aren't any obvious paths to any particular goal like there is with the Red Team's *"kill chain"*. Just as in real life, there are many different tools and strategies at your disposal to defending your network. You must also deal with the fact that you are starting with limited resources (as the default setting) and at some point, you may end up needing to alter your strategy as the Red Team's strategy unfolds. As the Red Team starts to compromise your assets, you will also need activate incident response (IR) mode to gain access to special IR actions. This will also restrict the use of other actions.

With many different attack vectors, strategies, tools, etc., you will find that neither the way the Red Team can attack you nor the way you defend your network is the same every time. Just as in real life, it becomes like a chess match, or even a "cat and mouse" chase. However, building a cybersecurity program and protecting cyber assets generally falls within a standard set of categories:

- **Cybersecurity Program Governance**
- **Cybersecurity Architecture and Controls**
- **Vulnerability Management**
- **Threat Monitoring**
- **Incident Response**

The following sections will examine these categories and how they are implemented in the game.

CYBERSECURITY PROGRAM & GOVERNANCE

Governance is the entire foundation of your cybersecurity program and establishes the baseline for your security controls and deployment strategy. This is where policies and procedures are created, and your overall cybersecurity culture is established.

Creating policies and procedures will unlock other necessary actions, but it also boosts your overall security posture, making it slightly harder for the Red Team to succeed in general. It's also a good idea to implement cybersecurity awareness training early on since that provides the largest increase in defense against social engineering. Humans are usually the weakest link in any cybersecurity posture and are considered "low hanging fruit". Attackers usually exploit this weakness early and often.

Weak passwords and default credentials are also another avenue of "low hanging fruit", which attackers are sure to exploit as soon as they find them. Enforcing strong passwords and changing default credentials as soon as possible is a good idea. Since enforcing strong passwords is tied to your cybersecurity policies and procedures, you can implement that as soon as your policies and procedures are established. However, before you can change default credentials, you'll have to know which assets still have the default credential enabled. Performing a vulnerability assessment will help with that (discussed more in the *Vulnerability Management* section).

CYBERSECURITY ARCHITECTURE AND CONTROLS

While a cybersecurity program and governance form the "blueprints" for your entire security posture, architecture and controls are the actual deployment of technology to carry out and enforce the defenses established by those "blueprints."

Implementing 2-factor authentication (a.k.a. "2FA") is another major defense against "low hanging fruit" attacks such as social engineering and weak passwords and deploying USB security is another layer of defense that can't protect people (the "weakest link") from themselves. Especially if the Red Team decides to show up onsite at your physical location and start dropping tantalizing little gifts for your users to helpfully pick up and insert into their USB ports. It's usually a good idea to install USB security on your most critical assets early on.

An important concept in cybersecurity strategy is that of ***layered defense***, which not only makes it difficult for attackers to gain access, but probably more importantly, it makes it difficult for them to move around freely throughout your network environment if they do gain a foothold. This is accomplished through deploying multiple security controls, but proper network segmentation is the backbone of layered security. Network segmentation is created by deploying firewalls in strategic locations to create logical zones in your network. At the very least, a perimeter firewall

(a.k.a. gateway firewall) should be installed immediately if you do not already have one. A perimeter firewall is the first line of defense for your network. Without it, attackers will have immediate and unabated access to everything. It's essentially the moat and drawbridge to your castle. Segmenting your network is the core to your layered defense strategy. It's probably a good idea to do this right after your shored up your "low hanging fruit" defenses.

Unsecured Wi-Fi access points are a convenient solution for most organizations as well as a convenient attack vector for attackers. It's an easy entry point that can allow attackers access to your network while sitting at a comfortable distance away such as the parking lot or an adjacent building with the right equipment. Leaving your Wi-Fi router or access points unsecured for too long will most likely be an issue.
Physical security is often overlooked when it comes to protecting computer systems. However, it remains an easy attack vector if not given proper attention. The downside is that many physical security measures, such as electronic locks and CCTV, can be quite expensive. At a minimum, you should install video surveillance as soon as you can afford it so at least you aren't completely "blind". Video surveillance will also increase the chances of an onsite attacker getting caught and possibly even arrested.

VULNERABILITY MANAGEMENT

Vulnerability management is the practice of mitigating risk by identifying and remediating vulnerabilities.

Vulnerability Identification

Before you can fix vulnerabilities, you must know about them. Identifying and removing vulnerabilities in your own network is one of the core Blue Team objectives. You can identify vulnerabilities by performing vulnerability mapping, vulnerability assessments, and penetration testing. Penetration testing, while more costly, will most likely identify zero-day vulnerabilities (discussed in the Red Team strategy section), which are more deeply rooted.

When vulnerabilities are identified, assets with vulnerabilities will display the yellow shield icon. Clicking on the yellow shield will display more details about which vulnerabilities an asset has. Keep in mind that performing vulnerability discovery actions will not necessarily find all potential vulnerabilities. You will most likely have to perform vulnerability discovery actions more than once.

Risk Analysis

In the real world, organizations with limited resources must decide, based on cost to benefit ratio, where to spend those limited resources. For example, the impact of a compromised Active Directory server is much higher than that of a user workstation. So, it would make much more sense to secure the Active Directory server rather than the user workstation if you could only

secure one of them. It would make even less sense to spend resources on the user workstation if attackers don't even have access to it. This is a very simplified example from the perspective of the real world, but in terms of game strategy it is proportionately correct and something you should consider.

The most recommended strategy is to identify what your most critical assets are first *(**HINT:** you can click on each asset to see more details)*. Start with building your security baseline (protect the perimeter and "low hanging fruit") and then deploy defenses and remediate vulnerabilities on your most critical systems before moving on to the others.

Vulnerability Remediation

Most asset remediation will involve patching, hardening systems (which includes fixing insecure configurations), changing default credentials, and tending to antivirus software. The easiest way to do this is by clicking on the asset that needs attention. For learning purposes, it's also a good idea to refer to the in-game wiki if you are unsure what a particular vulnerability is and what the associated remediation is, rather than just randomly clicking on everything for a particular asset because an action is available. Remember, with limited resources, a well thought out and cost-effective approach is a more effective strategy.

NOTE: *Since software is maintained by third party vendors, the Blue Team is not in control of when patches for vulnerabilities will be made available. Hence, the Blue Team must wait until a patch becomes available before removing the vulnerability from an asset.*

Industrial Control Systems (ICS) Considerations

If you are playing a scenario that includes ICS, performing vulnerability assessments and patching assets in the same way you would on an enterprise IT network might cause issues. Therefore, it is highly recommended to obtain vendor certification before patching and establish proper testing methods before doing a vulnerability assessment.

Access Control

Another way to manage vulnerabilities, especially if you are unable to patch them, is to deny or limit access to the vulnerable asset. Many of the other strategies that were previously discussed contribute to this such as network segmentation, authentication (strong passwords and 2FA), permissions management (system hardening), removable media security (USB security), and human-based risk management (social engineering defenses). Each of these controls address various attack vectors (avenues or pathways to access and attack an asset) that the Red Team has at its disposal such as direct cyber-attacks over the network, spear phishing, social engineering campaigns, malicious USBs, and physical access.

It is important to consider each of the attack vectors and controls in mind when creating (or changing) your cybersecurity program and strategy, especially with limited resources. Threat monitoring and threat intelligence will play a big part in understanding where the attackers are trying to gain access and, therefore, where you need to focus your efforts and resources.

THREAT MONITORING

In order to know whether or not you have been compromised, you will need to deploy security monitoring (also referred to as an intrusion detection system or IDS), which consists of a security information and event system (SIEM) and sensors (or agents). A SIEM is the first required component for your threat monitoring solution. IDS sensors are required to detect active attacks over the network. If an attack is detected, a red target animation will display over the asset being attacked. This does not necessarily mean the asset is compromised, however. To determine that, you'll need to perform *threat hunting* on the asset or install *endpoint protection*, which includes a host-based intrusion detection system (HIDS). Additionally, IDS devices might also detect reverse shell callback from compromised devices that have reverse shells installed, marking them as compromised. When you detect a compromised asset, it will turn red and display a skull icon.

HINT: *Just as there are special ICS considerations for vulnerability management, there are also special ICS considerations for threat monitoring. To detect ICS specific threats, you will need to deploy ICS threat monitoring in addition to standard threat monitoring.*

The visual characteristics for the different asset threat detections are as follows:

- **Controlled Asset**
  Your asset has been compromised and is currently controlled by the Red Team. Compromised/controlled assets will appear red with a white skull icon.

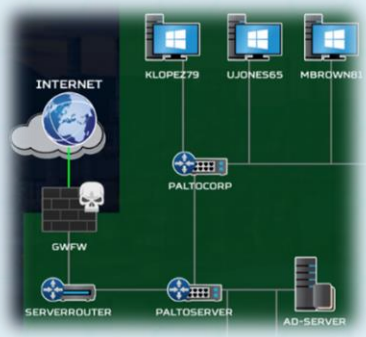
- **Denied Asset**
  Your asset has been hit by a successful denial of service (DoS) attack and is effectively "offline". Denied Assets will be displayed as gray with a white skull icon.

- **Asset Locked by Ransomware**
  Your asset has been compromised and is currently locked (denied) with ransomware. Ransomware locked assets will be displayed as gray with a red lock icon.

- **Targeted Asset**
  Your Asset has been targeted, but not necessarily compromised yet. Assets that have been targeted by the Red Team will have a red animated target placed over the targeted asset.

  You must have an IDS sensor deployed in the same zone as the targeted asset to detect targeting.

- **Asset Disconnected from the Network**
  If assets such as routers, firewalls, and switches are upstream to other assets, all its downstream assets will also be denied, and the connection lines (usually green) will turn gray as well~~.~~, unless the part of the network's fully air gapped.



Threat Intelligence

Threat intelligence refers to the information you have or know about a particular threat. The more you know, the better you are able to defend against such threats. In-game, the Blue Team can win by collecting enough threat intelligence to have the Red Team identified and apprehended. This happens when your threat intelligence score reaches 100%.

There are several ways to increase your threat intelligence score. The most impactful way is to *gather forensics* evidence when you have detected a compromise, and before you fix the asset. The other methods happen automatically and include detecting attacks with IDS, detecting compromises with endpoint protection or threat hunting, and when the Red Team is arrested onsite.

INCIDENT RESPONSE (IR)

At some point, your assets will be compromised or denied. When this happens, you will need to deal with those incidents, or you will most assuredly lose the game. Most IR actions are only available while in IR mode. Therefore, you'll need to activate IR mode by selecting the action (in the action menu or the action buttons at the bottom of the UI) or by clicking the activate IR button in the lower center UI.

NOTE: *While in IR mode, several standard actions will not be available. Additionally, you cannot deactivate IR mode while assets are disconnected from the network.*

Once in IR mode, there are several options become available. If the asset is offline (denied), sometimes simply rebooting the asset will fix the problem. For a complete compromise where the Red Team has taken control of the asset, rebooting won't work. Therefore, cleaning or replacing the asset are your only options. Cleaning the asset is more cost effective but is not always guaranteed. Replacing the asset is more expensive but is guaranteed to remove the threat. Restoring from backup could also work, ***as long as you have created restore points*** and you did so prior to the initial compromise. In some cases, cutting the asset's network connection might be the most immediate response.

HINT: *Establishing IR procedures first will help improve your odds of a successful incident response, such as cleaning an asset.*

Ransomware infections present two additional and unique options. If you have the resources, you can pay the ransom to recover your infected systems but doing so will cause a significant (temporary) drop to your profit & loss meter and award the Red Team one additional permanent resource. Otherwise, if you have enough time and security skills training, you can attempt to crack the ransomware encryption key.

BLUE TEAM STRATEGY HINT*: Keep in mind that you have to manage your budget effectively and make note of passive staff costs. Each staff member costs $750 per turn to keep on board, so make sure to keep that in mind when spending money on various BT actions. If you have insufficient budget at the end of your turn to keep all your staff, staff will be laid off to a minimum of one.*

APPENDIX

APPENDIX A: BLUE TEAM ACTIONS

2-Factor Authentication	2-Factor authentication (2FA) and multi-factor authentication (MFA) increases defense against password attacks, improper access control, and social engineering attacks. This action can only be played once.
Activate IR	Activate Incident Response (IR) Mode, which enables IR related actions that aren't otherwise available in normal mode. While in IR Mode, some standard actions are not available. NOTE: If IR mode is activated with actions in the queue that are not related to IR, those actions will be abandoned and fail.
Asset Inventory	Provides a bonus for discovering vulnerabilities during vulnerability mapping and vulnerability assessments. It also has a chance to discover rogue devices. This action can be played multiple times to attempt to discover rogue devices, but the vulnerability discovery bonus is only given the first time you play this action (and that bonus remains persistent).
Change Default Credentials	Change the default credentials on network and ICS devices to prevent easy exploitation by simply entering the default credentials. This action can be played once per device.
Clean Asset	Try to get a denied or compromised asset back in working order again. Only available in IR mode.
Crack Ransomware Key	Attempt to crack the ransomware key to recover infected systems. This is an extremely difficult task and the chances for success are rare. Security skills training is also needed. NOTE: Cracking the ransomware key will only remove the ransomware and WILL NOT REMOVE the initial compromised state. Replacing the asset or restoring from backup are alternative ways to remove ransomware that also remove the initial compromise. Paying the ransom is another alternative, but your PnL will take a hit it will not remove the compromise (it's a good option when your resources are low). This action can be played as many times as needed, but you need to be in IR mode to do so.
Create IR Procedures	Establish an incident response plan as the foundation for an incident response. This will increase the chance of recovering a system after a compromise, denial of service (DoS), or outage. This action can only be played once.
Create Backup Process	Enables system backups and allows creating restore points on assets. This action can only be played once.
Create Restore Point	Once a backup process is created, this action creates a backup/restore point, which the asset can be reverted back to in the event of a compromise or infection. The asset will revert back to the EXACT state it was in at the time of creating the restore point. (NOTE: This means that

	you will need to redeploy asset specific actions to that asset.) This action is free to play and can be played on each Windows and Linux computer once per turn.
Deactivate IR	Go back to normal operations. IR mode actions will no longer be available and standard mode actions will be available again. NOTE: To play this action, the network must have no disconnected assets.
Deploy USB Security	Prevent compromises due to malicious USB drops. Can be played on each asset, once per asset (unless the device is restored to a point before the action was played.
Disconnect from Network	Disconnects the asset from the network without bringing the asset down. This prevents unauthorized data exfiltration and prevents adversaries from pivoting or remotely controlling the asset. Can only be played in IR mode.
Encrypt Network Traffic	Prevent leaking password information to network sniffing by encrypting traffic and using encrypted protocols. This improves your overall defense against password attacks. Can only be played once.
Endpoint Detection	Add endpoint detection, historically referred to as a Host-Based Intrusion Detection System (HIDS) to an asset. Alerts when an asset is compromised. Can be played on each asset (AFTER the SIEM is installed), once per asset (unless the device is restored to a point before the action was played. Cannot be played on ICS devices and computers.
Enforce Strong Passwords	Removes weak password vulnerabilities. Can only be played once new weak passwords are discovered and remain on an asset.
Gateway Firewall	Installs the Gateway Firewall for network perimeter defense. Assets are no longer exposed to the internet (except for the Gateway Firewall, VPN, and Remote Users) and prevents the Red Team from being able to scan and attack every one of your assets directly from the internet.
Gather Forensics	Gathering forensics contributes to your threat intelligence score. When your threat intelligence score reaches 100%, the red team operations are shut down and you win a threat intelligence victory. Security Skills Training increases the chance of success. This action can be played on each compromised asset, but with diminishing returns after each successive time it is played.
Harden RDP	Hardening RDP removes insecure remote desktop connections to other assets. This is especially important for workstations that have remote desktop connections to critical assets. This action can only be played on assets with RDP enabled, and only once on each of those assets (unless the device is restored to a point before the action was played.
Hire New Staff	You need staff to perform almost every action in the game. This action adds 1 staff resource. You can hire as many staff in a game, even per turn, as you can afford. Each staff member will also have the cost of 750$ per turn. If you can't afford to pay this cost at the beginning of your turn, BT staff will be laid off (down to 1 staff resource).
ICS Safe Testing Methods	Establish vulnerability and penetration testing methods safe for ICS environments. Prevents damaging ICS devices from vulnerability

	assessments and penetration testing. This action can only be performed once.
ICS Security Monitoring	Provides visibility into compromised ICS assets, which standard security monitoring can't do. This action is required to see compromises on ICS devices such as PLCs and field radios. This action can only be played once.
ICS Vendor Certification	Get vendor approval before applying patches to ICS hosts and servers. Prevents damaging ICS specific devices and computers when patching. This action expires every 10 turns from the time it was first played, and then can be played again upon expiration. When ICS Vendor Certification is active, a certificate icon will appear in the certification window at the upper left-hand side of the UI near the resources display.
Implement SDLC (Code Review)	Helps protect against application vulnerabilities by implementing secure coding practices and code review process (NOTE: This also implies enforcing such contractual standards upon your vendors). Improves defenses against: Command Injection, CSRF, Directory Traversal, Format String Error, Heap Overflow, Incorrect Access Control, Integer Overflow, Local File Inclusion, Outdated Software, SQL Injection, Stack Overflow, XSS. This action can only be performed once.
Implement Strong Wi-Fi	Use stronger WiFi security technology to help secure the WiFi router against unauthorized access and WiFi "cracking". (NOTE: Due to the granularity and numerous complexities involved in real-world WiFi security, this action is a high-level abstraction representing the actual process). This action can only be played once per WiFi device (unless the device is restored to a point before the action was played.
Install Anti-Virus	Installs the missing anti-virus and protects against malware (including ransomware) as well as social media threats such as email phishing, spear phishing, social media exploits, and malicious website code such as with watering hole exploits. This gives you an overall improved defense against these types of attacks. Can only be played on assets with missing anti-virus discovered.
Install Electronic Locks	Put electronic locks on all of the doors to make physical break-ins more difficult. This action can only be played once.
Install Network Security Sensor	Install a network sensor that can detect malicious activity transmitted over the network, in the zone the sensor is installed. Network attack attempts will show as a red pulsing target animation on the asset. This action can be played once for each network zone where network sensors are allowed (indicated by the green targeting icons when selected.)
Install Physical 2FA	Use physical two-factor authentication (2FA) for access to your facilities. It makes electronic break-ins more difficult by increasing the effectiveness of electronic locks. It also makes physical entry attempts using social engineering a bit more difficult. This action requires electronic locks and can only be played once.
Install SIEM	Installs a Security Information and Event Management (SIEM) to monitor information and events from endpoint detection, network sensor

	agents, and network device log collection. Enables each of these detection agents to alert on network-based attacks and system compromises respectively. NOTE: If the SIEM is offline or compromised, none of the detection agents will alert.
Install Video Surveillance	Installs security cameras (CCTV), which makes it easier to detect physical intruders onsite. Video surveillance makes it more difficult for the Red Team to remain onsite for long and/or progress further into your physical location. The Red Team can, however, lessen the effects of video surveillance with a high skill rating in human social engineering. This action can only be played once.
Install VPN	Installs a VPN for protecting remote access and isolates remote users to a single zone (usually the DMZ) once the network is segmented. Otherwise, when the network is segmented without a VPN, users can randomly associate with any zone. If they were compromised and used as a pivot, the Red Team would have visibility into whatever zone they are associated with.
Log Collection and Analysis	Log Collection and Analysis alerts when a network device asset is compromised. Playing this action enables log collection on network devices and only needs to be played once on each asset you want log collection enabled on. A SIEM is required to enable log collection.
Pay Ransom	Pay the ransom to recover systems infected with ransomware. Doing so will cause a significant, but temporary, drop to your PnL meter, which will begin recovering at the normal recovery rate the next turn. NOTE: Paying the ransom will only remove the ransomware and WILL NOT REMOVE the initial compromised state. Replacing the asset or restoring from backup are alternative ways to remove ransomware that also remove the initial compromise. Cracking the ransomware key is also another option, but it is extremely difficult, and success is rare. This action can be played as many times as needed, but you need to be in IR mode to do so.
Penetration Test / Internal Penetration Test	Penetration testing identifies vulnerabilities, including ZERO-DAYS, and increases the chance of a successful budget request. Careful! Some environments such as ICS can suffer adverse effects (such as disabling PLCs) from traditional penetration testing methods without the proper precautions in place (ICS Safe Testing Methods)! A vulnerability assessment is required prior to penetration testing being available. This action can be played many times. The internal penetration test differs from a standard penetration test in that you have skills staff that can perform the test rather than paying an external firm to do it. Therefore, it requires less cash resources, but it does require security skills training before being available.
Policies and Procedures	Creates a written set of rules and guidelines for establishing baseline security. This action unlocks several additional Blue Team actions (refer to the Blue Team action tree for additional details on what this action unlocks). This action can only be played once.

Reboot Asset	Attempts to fix an out of service asset, including a denial of service (DoS) attack. It might not always succeed (and sometimes it might even take more than one try), but in many cases it's worth a shot. This action can be played as many times as needed, but you must be in IR mode to do so.
Reconnect to Network	Reconnect the asset to the network. It might be a good idea to be sure the asset is clean before doing so, however. This action can be played as many times as needed, but you must be in IR mode to do so. NOTE: All assets must also be reconnected before you can exit IR mode.
Replace Asset	Buy a completely new asset to remove a compromise. NOTE: In doing so, you will not need to reapply fixes. It is assumed that all the most recent patches and fixes are applied during the recommissioning process (this includes USB security). Endpoint detection, however, will need to be reinstalled. This action can be played as many times as needed, but you must be in IR mode to do so.
Request Budget	If successful, the player gains additional funds. Success is dependent on many factors including when in the game you request it, frequency of requests, and other supporting actions that might justify your need for budget. ***HINT:*** *Find a way to show management your network is at risk by identifying vulnerabilities.* Having compromised assets is another way to compel management to give you money, though not recommended.
Restore From Backup	Revert the asset to its last known restore point from backup. WARNING: This does not guarantee a clean asset if the last backup was performed after the asset has already been compromised! This action can be performed as many times as needed once a restore point has been created for that asset.
Security Awareness Training	Security awareness training strengthens your overall security posture and helps protect against social engineering campaigns, spear phishing, physical intrusion, and other onsite physical threat activities. This action can only be played once, and it requires policies & procedures to be in place.
Security Skills Training	This is the next level of security training that further strengthens the overall security posture and is also required for more advanced actions such as cracking ransomware encryption, internal threat hunting, internal vulnerability assessment, and internal penetration testing. This action can only be played once and requires security awareness training first.
Segment Network	Properly segmenting your network prevents a threat from moving freely through your entire network, by restricting them to zones (i.e., subnets) divided by firewalls. NOTE: If your network has already been compromised, segmenting your network will also remove Red Team's access to any compromised assets they have control of. This action can only be played once, after the gateway firewall has been installed.

System Hardening	Fixes configuration-based vulnerabilities such as: directory traversal and incorrect access control. This action requires applicable vulnerabilities to be discovered and can be played on each asset as needed.
System Patches	Helps protect assets against known exploits by patching application vulnerabilities such as: command injection, CSRF, directory traversal, format string error, heap overflow, incorrect access control, integer overflow, local file inclusion, SQL injection, stack overflow, and XSS. WARNING! Some environments such as ICS can suffer adverse effects from traditional patching methods without the proper precautions in place (ICS Vendor Certification! NOTE: Some vulnerabilities may not have patches available yet and won't be available until one or more turns later. This action requires applicable vulnerabilities to be discovered and can be played on each asset as needed.
Threat Hunting	Send personnel to directly inspect an asset for evidence of a compromise. NOTE: If evidence is not found, it doesn't mean there is absolutely no compromise. The attacker might just be well hidden. This action requires security skills training and can be played on any asset as many times as you want.
Update Anti-Virus	Updates outdated malware signatures (including ransomware. Anti-virus protects against malware as well as social media threats such as email phishing, spear phishing, and malicious website code such as with watering hole exploits. This gives you an overall improved defense against these types of attacks. Can only be played on assets with outdated anti-virus discovered.
Update Firmware	Patch any known firmware vulnerabilities in embedded devices (including network devices). This action can only be played on assets where outdated firmware has been discovered.
Vulnerability Assessment / Internal Vulnerability Assessment	A vulnerability assessment (which usually includes active vulnerability scanning) is more comprehensive than a penetration test. Therefore, it identifies more known vulnerabilities on assets, but it WILL NOT find ZERO-DAYS. It also increases the chance of a successful budget request. Careful! Some environments such as ICS can suffer adverse effects (such as disabling PLCs) from traditional vulnerability assessment methods without the proper precautions in place (ICS Safe Testing Methods)! These actions requires that an asset inventory be performed first, and then can be played many times. The internal vulnerability assessment differs from a standard vulnerability assessment in that you have skills staff that can perform the assessment rather than paying an external firm to do it. Therefore, it requires less cash resources, but it does require security skills training before being available.
Vulnerability Mapping	Maps system and application versions to known vulnerabilities. Less of a chance to find vulnerabilities compared to a vulnerability assessment or penetration test but less resource intensive. It also does not risk damaging ICS. This action requires that an asset inventory be performed first, and then can be played many times.

APPENDIX B: RED TEAM ACTIONS

Activate Ransomware	Lock the asset (put it in a denied state) by activating the ransomware. Doing so will increase the rate at which the company's profit/loss meter declines. Ransomware infected assets will be displayed as gray with a red lock icon. This action can be played once per asset that already has ransomware installed.
Attack Campaign	Begin a series of online social engineering attacks that include social media, "watering hole" websites, and email phishing. Once activated, these attacks will remain ongoing until you end the campaign, and there is a chance each turn that a Windows asset could be compromised. (The campaign will show as "succeeded" in your action log, but that means the campaign is setup and active at that point.) NOTE: Your resources will REMAIN COMMITTED to the campaign until you end the campaign. The chances of a successful compromise decrease each turn that the campaign is active. (HINT: Overall chances of success can be increased by researching Electronic SE.) The Blue Team also has several defensive options that could make successes more difficult. This action can be performed many times once OSINT has been completed and Persistence has been researched.
Attack	Once the entire "kill chain" has been completed (OSINT, Host Scan, Port Scan, Service Enumeration, identify vulnerabilities) for an asset, you will be able to attack it. (See "Cyber Kill Chain" under the Cybersecurity Concepts tab.) Playing the Attack action displays the attack dialogue, where you will be able to craft your attack. Crafting attack allows you to select the vulnerability to exploit (based on the vulnerabilities you have identified for that asset) and the objective (denial of service or manipulation/take control of the asset). This action can be played many times on assets which you have completed the kill chain and identified vulnerabilities for. You cannot attack an asset that is currently offline or already compromised. HINT: If you are seeing attacks fail frequently, try researching an associated vulnerability a bit further.
Change Location	This action allows you to move to a new physical location. You begin the game at your remote location. The first location you are allowed to travel to is the perimeter of your target (requires physical recon). After that, there are a range of options where you can move to using one of three different methods: Physical Entry (picking locks, etc.), Electronic Entry (subverting/defeating electronic locks), or Social Engineering (using disguises and trickery to full people). Each method has associated skills you can increase that will improve your chances of success (see the research actions for more details). However, the Blue Team also has specific defenses for each method as well as overall physical security defenses that can "move the needle" further toward their favor.
Clone RFID Badge	Clone the RFID badge (proximity card) of an employee to improve your chances of electronic entry. You must be onsite and the Blue Team must have electronic locks installed. Due to the complexity involved with cloning

	RFID badges, this action has a moderate chance failure. However, this action can be played until a badge is successfully cloned, and then no longer needs to be played.
Cover Tracks	Hide the evidence that you have compromised an asset, making it more difficult for the Blue Team to detect. NOTE: Covering your tracks is never 100% perfect, and there is always still a chance that the Blue Team might still detect your presence (and you won't know for sure whether or not your efforts have kept you concealed). This action can be played on each asset once you have gained control of that asset. To play this action, you must have researched persistence.
Crack Wi-Fi	Try to gain access to the WiFi network using a variety of Wi-Fi hacking techniques (abstracted in game for ease of use). This action is available once a WiFi router or access point has been discovered using the WiFi Scan action. It can be played on each discovered WiFi device until it succeeds for that device or until strong WiFi security has been implemented on that device. This action will not be available if strong WiFi security has been implemented by the Blue Team.
Create Malicious USB	Create a malicious USB that can be dropped onsite. Successful USB drops will provide compromise access to a Windows asset. This action is available as long as you don't already have a malicious USB in your inventory (displayed in the temporary resources window at the top left-hand side of the UI next to the resources display). Once created, the malicious USB will be available to use for 10 turns. This action requires Persistence research.
Create Reverse Shell	Establishes a direct connection to the asset that will persist even if the pivot is lost (i.e., a direct chain of controlled assets is no longer required to access this asset). This also allows the asset to remain as a pivot. Assets with a reverse shell installed have a low chance to be detected as compromised every turn if there is an IDS sensor installed (and active) in their zone. This action can be played once Persistence has been researched.
Damage ICS Process	Attempt to damage to the industrial control system (ICS) process, which is a win condition in maps/environments with ICS. This action can only be used on environments that have ICS, once you have gained control of a programmable logic controller (PLC) asset.
Email Phishing Campaign	Deceive targets with malicious emails masquerading as a legitimate email. Once activated, the campaign will remain ongoing until you end the campaign, and there is a chance each turn that a Windows asset could be compromised. (The campaign will show as "succeeded" in your action log, but that means the campaign is setup and active at that point.) NOTE: Your resources will REMAIN COMMITTED to the campaign until you end the campaign. The chances of a successful compromise decrease each turn that the campaign is active. (HINT: Overall chances of success can be increased by researching Electronic SE.) The Blue Team also has several defensive options that could make successes more difficult. This action can be performed many times once OSINT has been completed.

End Campaign	Bring an attack campaign to a close. The resources being used to sustain the campaign will be returned to your resource pool.
Evade Network Detection	This action will prepare evasion techniques for the next attack attempt to avoid detection by IDS sensors. If setup is successfully prepared, you will receive the Evade Network Detection icon in the temporary resources window at the top left-hand side of the UI. HINT: Failure could indicate that your IDS Evasion skill isn't high enough. Once this action is used by an attack, it will need to be played again for another attack.
Exfiltrate Data	Cause harm to the target company by exfiltrating data (assumed to be sold on the black market, extorted, or publicly exposed). This supports the "Company Production Compromised" win condition by increasing the profit/loss (PnL) meter's decline rate. Playing this action on multiple assets has cumulative effects to the PnL meter. You can play this action on workstations and servers that you have gained control of.
Find Public Vulnerabilities	Search public databases, alerts, and other sources for known vulnerabilities using data you have discovered from port scanning and enumerating services. NOTE: Discovering vulnerabilities on an asset is required before you can attack that asset. Once you have completed service enumeration on at least one asset, this action can be played many times but only assets with service enumeration have a chance for vulnerabilities to be discovered. This action can fail if no vulnerabilities are found at that time, but this does not mean all vulnerabilities have been discovered. HINT: Try again or try using more advanced vulnerability discovery methods such as the Fuzzing or Reverse Engineering actions.
Fuzzing	Run a data fuzzing engine against an asset to discover new vulnerabilities. Unlike public vulnerabilities, fuzzing has a chance to discover zero-day vulnerabilities. HINT: Zero-day vulnerabilities are less likely to be discovered/patched by the Blue Team until later on in the game. NOTE: Discovering vulnerabilities on an asset is required before you can attack that asset. Once you have completed service enumeration on at least one asset, this action can be played many times but only assets with service enumeration have a chance for vulnerabilities to be discovered. This action can fail if no vulnerabilities are found at that time, but this does not mean all vulnerabilities have been discovered.
Harvest Credentials	Collect user account and password information stored on the asset to aid with weak password attacks. This action can be played on each controlled assets for a cumulative bonus to password attacks, but the gains diminish slightly each time the action is played.
Host Scan	This action is available once you have done open-source intelligence (OSINT), or reconnaissance. Host scanning searches for undiscovered assets connected to the network. Only internet facing assets are discoverable from the internet. To discover assets protected behind a firewall, you must have control of an asset (host) on the same network segment as the asset to be discovered (this concept is known as a "pivot"). A host scan can fail if there are no hosts are discovered, but new hosts could show up over time

	as the Blue Team manages their network or as host come online (this happens often with remote users especially). HINT: Remote users disappear and reappear from your view often. Attacking them and using them as a pivot can be challenging, but also rewarding sometimes.
Insider Physical Recon	Once you are onsite and past the perimeter, you can search the area for assets. Unlike host scanning, when you find assets, you have a bit more information about them since you can physically see them and possibly access them. However, having physical access does not grant you remote access unless you plant a trojan.
Install Disruptive Malware	Install malicious software (malware) on a compromised asset. Doing so increases the company's profit/loss meter decline (supporting the "Company Profit/Loss Compromised" win condition). This task can be difficult if the asset has anti-virus installed, and even more difficult, sometimes impossible, if the anti-virus is up to date.
Install Ransomware	Install ransomware on a compromised asset. The ransomware still needs to be activated to lock the asset and increase the rate at which the company's profit/loss meter declines. This task can be difficult if the asset has anti-virus installed, and even more difficult, sometimes impossible, if the anti-virus is up to date.
Malicious USB Drop	Leave a malware infected USB stick for someone to find. Successful USB drops will provide compromise access to a Windows asset. This action is available (for 10 turns) once you have created a malicious USB and have it in your inventory (displayed in the temporary resources window at the top left-hand side of the UI next to the resources display). The Blue Team has several malicious USB defenses including USB security and security awareness training. Failed drops simulate a USB never picked up or not getting plugged into a computer.
OSINT (Recon)	Open-Source Intelligence (OSINT) searches for publicly available information about your target. OSINT is the first step in the "cyber kill chain" (see Cyber Kill Chain in the Cybersecurity Concepts section) and is required before being able to conduct any cyber activity on the Blue Team, to include social engineering campaigns and spear phishing. This action can only be played once.
Password Attack	Attempts a remote password attack on the selected asset (this is an abstraction of many different types of remote password attack techniques). If the Blue Team is not enforcing strong passwords and weak passwords are used on the asset, there is a very high probability of success. You can further increase your chances by increasing your weak password skill. If 2-factor authentication (2FA) is deployed, it would significantly reduce the chances of success. Once you have enumerated services on an asset, you can attempt password attacks on that asset (except for embedded ICS devices). Consistent failures might be an indicator that the Blue Team has strong passwords enforced and/or has 2FA deployed.

Physical Recon	Gathers intel about the Blue Team's physical location, buildings, facility, etc. This action is required for further physical onsite actions. This action can only be played once.
Pilfer Data	Collect data from the asset to help improve the chances of success for social engineering attacks. This action can be played multiple times on all assets you have control of for a cumulative bonus to all social engineering type attacks (including phishing and campaigns). NOTE: The gains diminish slightly each time the action is played. HINT: Finding useful information can fail for several reasons (each system might have a plethora of data stored throughout many locations), but one failure does not mean this action is exhausted.
Plant Rogue Device	Install a rogue device while onsite (similar to a small "jump box" such as a Pwnie Express or LAN Turtle), which gives you remote access (pivot) to the network zone where it is installed. This action can only be played onsite once you have progressed past the perimeter. The Blue Team does have a chance to discover the device through the use of asset inventory, vulnerability assessments, and IDS.
Plant Trojan	Install malicious software on an asset while onsite, which gives you remote access (pivot) in the same zone as the asset with the installed trojan. This action can only be played onsite once you have progressed past the perimeter and have discovered devices by playing the Insider Physical Recon action. The Blue Team can only detect your presence on that asset with endpoint detection or by performing threat hunting. You can decrease your odds of detection by playing the Cover Tracks action once the trojan is successfully installed. NOTE: This action can fail simply due to installation difficulties and configuration. HINT: Failures are not an indication that the action will not work. Keep trying.
Port Scan	A port scan discovers additional information on newly discovered assets after you have performed a host scan. The asset must be internet accessible, or you must have control of another asset (a pivot) on the same network segment. This action can only be played once per asset. Once an asset has been port scanned, the "port scanned" icon will appear on that asset.
Prepare Covert Attack	Preparing a covert attack makes it difficult for the Blue Team to detect that an attack has compromised the asset. Play this action before you attack (It will remain active until you have a successful attack.) This action takes effect on the very next successful manipulation attack. Once successfully used, it will need to be played again to reactivate for the next attack. This action can be played many times once you have researched persistence. NOTE: This action can fail due to the technical complexity, and a success does not guarantee your attack is 100% undetected (although it is extremely difficult for the Blue Team to do so). HINT: You still need to cover your tracks to remain undetected on the asset.
Recruit Hackers	Find people to help share the workload. Adds 2 resources to your resource pool once successful. Can only be achieved once. HINT: Your chances are

	slim at the beginning of the game as you start with little to no "street cred". You can increase your chances throughout the game as you do things to improve your reputation (usually publicly visible things).
Research	Research a skill to improve the chance of success for future actions based on that skill. These skills are mostly based on vulnerability exploitation, but also have other technical relevance such as persistence.
Reverse Engineering	Find vulnerabilities by directly analyzing a copy of the asset/software for vulnerabilities. Unlike public vulnerabilities, reverse engineering has a chance to discover zero-day vulnerabilities and has a greater chance than fuzzing. NOTE: Discovering vulnerabilities on an asset is required before you can attack that asset. Once you have completed service enumeration on at least one asset, this action can be played many times but only assets with service enumeration have a chance for vulnerabilities to be discovered. This action can fail if no vulnerabilities are found at that time, but this does not mean all vulnerabilities have been discovered.
Search for HMIs	For ICS environments only. Once you are in the plant, this action looks for any accessible human machine interface (HMI) devices while onsite. If successful, there is a chance you will have direct access and control. If not (simulating there might be a person at or near the HMI), you can play this action many times in an effort to gain control of an unoccupied HMI.
Service Enumeration	Service enumeration gains more information about a discovered host by identifying which service(s) is/are running. Port scanning the asset must be completed first, and this is a necessary step before being able to attack the asset. The asset must be internet accessible, or you must have control of another asset (a pivot) on the same network segment. This action can only be played once per asset. Once an asset has been service enumerated, the “service enumeration” icon will appear on that asset.
Sniff Network Traffic	Search network traffic for clear text password information, which gives you a permanent bonus to password attacks. This action is available only after you have gained control of an asset and can only be played once. The benefits of this action can be countered by the Blue Team by encrypting network traffic.
Social Media Campaign	Deceive targets by exploiting people’s trust on a social media site. Once activated, the campaign will remain ongoing until you end the campaign, and there is a chance each turn that a Windows asset could be compromised. (The campaign will show as "succeeded" in your action log, but that means the campaign is setup and active at that point.) NOTE: Your resources will REMAIN COMMITTED to the campaign until you end the campaign. The chances of a successful compromise decrease each turn that the campaign is active. (HINT: Overall chances of success can be increased by researching Electronic SE.) The Blue Team also has several defensive options that could make successes more difficult. This action can be performed many times once OSINT has been completed.

Spear Phishing Attack	This is a one-time action and not a campaign. Deceive targets with specially crafted, malicious emails masquerading as a legitimate email. If successful, a Windows asset will be compromised. HINT: This has a slightly better chance of success than an email attack campaign and the overall chances of success can be increased by researching Electronic SE. The Blue Team also has several defensive options that could make successes more difficult. This action can be performed many times once OSINT has been completed and Persistence has been researched.
Upgrade Rig	Upgrade equipment to increase working capacity. Increases total available resource points by 1.
Watering Hole Campaign	Deceive targets by exploiting people's trust on a web site (typically a commonly visited site by your target, which you have taken over and inserted malicious code into). Once activated, the campaign will remain ongoing until you end the campaign, and there is a chance each turn that a Windows asset could be compromised. (The campaign will show as "succeeded" in your action log, but that means the campaign is setup and active at that point.) NOTE: Your resources will REMAIN COMMITTED to the campaign until you end the campaign. The chances of a successful compromise decrease each turn that the campaign is active. (HINT: Overall chances of success can be increased by researching Electronic SE.) The Blue Team also has several defensive options that could make successes more difficult. This action can be performed many times once OSINT has been completed.
Wi-Fi Scan	Scan for Wi-Fi access points that could potentially be used as an onsite pivot. Once discovered, Wi-Fi security must still be "cracked" for this access point to be used as a pivot.

APPENDIX C: VULNERABILITIES

Vulnerability	Description	Remediation
Command Injection	Command Injection vulnerabilities allow an attacker to execute commands through an operating system's command line application, such as Windows' cmd.exe and PowerShell as well as the MacOS and Linux terminals. The attack vectors include specially crafted web URLs and leveraging other application vulnerabilities that allow arbitrary code execution.	**System Patches**
CSRF	Cross-site request forgery (CSRF) happens on a website or web-based application where unauthorized commands are submitted from a user that the web application trusts. In a CSRF attack, an innocent end user is tricked by an attacker into submitting a web request that they did not intend. This may cause actions to be performed on the website that can include inadvertent client or server data leakage, change of session state, or manipulation of an end user's account. This can happen without the user's interaction or even knowledge. Unlike cross-site scripting (XSS), which exploits the trust a user has for a particular site, CSRF exploits the trust that a site has in a user's browser.	**System Patches**
Default Credentials Enabled	Many network devices, as well as a whole range of other embedded devices, often have default authorization credentials enabled in the factory settings by the manufacturer. Administrators sometimes neglect to change these default credentials to something more secure. This can allow an attacker to lookup the default credentials for a specific device and allow them easy access.	**Change Default Credentials**
Directory Traversal	Directory traversal (or path traversal) vulnerabilities allow attackers to exploit insufficient security validation or sanitization of user-supplied file names, such that characters representing "traverse to parent directory" are passed through to the operating system's file system. An affected application can be exploited to gain unauthorized access to the file system. Directory traversal is also known as the ../ (dot dot slash) attack, directory climbing, and backtracking. Some forms of this attack are also canonicalization attacks.	**System Hardening**
Format String Error	Format string vulnerabilities are a class of bugs that take advantage of an easily avoidable programmer error. If the programmer passes an attacker-controlled buffer as an argument to a printf (or any of the related functions,	**System Patches**

	including sprintf, fprintf, etc), the attacker can perform writes to arbitrary memory addresses.	
Heap Overflow	A heap overflow is a type of buffer overflow. In information security and programming, a buffer overflow, or buffer overrun, is an anomaly where a program, while writing data to a buffer, overruns the buffer's boundary and overwrites adjacent memory locations. Buffers are areas of memory set aside to hold data, often while moving it from one section of a program to another, or between programs. Buffer overflows can often be triggered by malformed inputs; if one assumes all inputs will be smaller than a certain size and the buffer is created to be that size, then an anomalous transaction that produces more data could cause it to write past the end of the buffer. If this overwrites adjacent data or executable code, this may result in erratic program behavior, including memory access errors, incorrect results, and crashes. Exploiting the behavior of a buffer overflow is a well-known security exploit. On many systems, the memory layout of a program, or the system as a whole, is well defined. By sending in data designed to cause a buffer overflow, it is possible to write into areas known to hold executable code and replace it with malicious code, or to selectively overwrite data pertaining to the program's state, therefore causing behavior that was not intended by the original programmer. Buffers are widespread in operating system (OS) code, so it is possible to make attacks that perform privilege escalation and gain unlimited access to the computer's resources. The famed Morris worm in 1988 used this as one of its attack techniques. A heap overflow, heap overrun, or heap smashing is a type of buffer overflow that occurs in the heap data area. Heap overflows are exploitable in a different manner to that of stack-based overflows. Memory on the heap is dynamically allocated at runtime and typically contains program data. Exploitation is performed by corrupting this data in specific ways to cause the application to overwrite internal structures such as linked list pointers. The canonical heap overflow technique overwrites dynamic memory allocation linkage (such as malloc	**System Patches**

	metadata) and uses the resulting pointer exchange to overwrite a program function pointer.	
Incorrect Access Control	In this context, access control refers to access permissions, or authorization to access information and data on a computer or device. Incorrect access permission settings can allow an attacker easier access by using credentials with lower permissions than what should be allowed.	**System Hardening**
Integer Overflow	An integer overflow occurs when an arithmetic operation attempts to create a numeric value that is outside of the range that can be represented with a given number of digits, either higher than the maximum or lower than the minimum representable value. This can result in a value that wraps around to the minimum or maximum value, which can lead to unintended behavior and potentially compromise security. Anticipated, overflow can compromise a program's reliability and security.	**System Patches**
Local File Inclusion	A file inclusion vulnerability is a type of web vulnerability that is most commonly found to affect web applications that rely on a scripting run time. This issue is caused when an application builds a path to executable code using an attacker-controlled variable in a way that allows the attacker to control which file is executed at run time. A file inclusion vulnerability is distinct from a generic directory traversal attack, in that directory traversal is a way of gaining unauthorized file system access, and a file inclusion vulnerability subverts how an application loads code for execution. Successful exploitation of a file inclusion vulnerability will result in remote code execution on the web server that runs the affected web application. An attacker can use remote code execution to create a web shell on the web server, which can be used for website defacement. Local file inclusion (LFI) is similar to a remote file inclusion vulnerability except instead of including remote files, only local files i.e. files on the current server can be included for execution. This issue can still lead to remote code execution by including a file that contains attacker-controlled data such as the web server's access logs.	**System Patches**
Missing Antivirus	Antivirus software, also called anti-malware, can help protect end-users from a range of malicious software by detecting it and preventing its execution.	**Install Anti-Virus**

Outdated Antivirus	Outdated antivirus software can expose end-users to more recent malicious software (malware), due to an outdated malware signature database.	**Update Anti-Virus**
Outdated Firmware	Firmware is software that resides at the chip level (as opposed to a hard drive). It is used by computer systems to help operating systems interface with other hardware components and for simpler systems and embedded devices, it can be used as the actual operating system. Firmware can contain a range of vulnerabilities, which cannot be fixed through normal system and application patching. Updating outdated firmware is required in such cases.	**Update Firmware**
Remote File Inclusion	A file inclusion vulnerability is a type of web vulnerability that is most commonly found to affect web applications that rely on a scripting run time. This issue is caused when an application builds a path to executable code using an attacker-controlled variable in a way that allows the attacker to control which file is executed at run time. A file inclusion vulnerability is distinct from a generic directory traversal attack, in that directory traversal is a way of gaining unauthorized file system access, and a file inclusion vulnerability subverts how an application loads code for execution. Successful exploitation of a file inclusion vulnerability will result in remote code execution on the web server that runs the affected web application. An attacker can use remote code execution to create a web shell on the web server, which can be used for website defacement. Remote file inclusion (RFI) occurs when the web application downloads and executes a remote file. These remote files are usually obtained in the form of an HTTP or FTP URI as a user-supplied parameter to the web application.	**System Patches**
SQL Injection	SQL injection is a code injection technique used to attack data-driven applications, in which malicious SQL statements are inserted into an entry field for execution (e.g. to dump the database contents to the attacker). SQL injection relies on security vulnerabilities in an software, where user input is either incorrectly filtered for string literal escape characters embedded in SQL statements or user input is not strongly typed and unexpectedly executed. SQL injection is mostly known as an attack vector for websites but can be used to attack any type of SQL database.	**System Patches**

	SQL injection attacks allow attackers to spoof identity, tamper with existing data, cause repudiation issues such as voiding transactions or changing balances, allow the complete disclosure of all data on the system, destroy the data or make it otherwise unavailable, and become administrators of the database server.	
Stack Overflow	A stack overflow is a type of buffer overflow. In information security and programming, a buffer overflow, or buffer overrun, is an anomaly where a program, while writing data to a buffer, overruns the buffer's boundary and overwrites adjacent memory locations. Buffers are areas of memory set aside to hold data, often while moving it from one section of a program to another, or between programs. Buffer overflows can often be triggered by malformed inputs; if one assumes all inputs will be smaller than a certain size and the buffer is created to be that size, then an anomalous transaction that produces more data could cause it to write past the end of the buffer. If this overwrites adjacent data or executable code, this may result in erratic program behavior, including memory access errors, incorrect results, and crashes. Exploiting the behavior of a buffer overflow is a well-known security exploit. On many systems, the memory layout of a program, or the system as a whole, is well defined. By sending in data designed to cause a buffer overflow, it is possible to write into areas known to hold executable code and replace it with malicious code, or to selectively overwrite data pertaining to the program's state, therefore causing behavior that was not intended by the original programmer. Buffers are widespread in operating system (OS) code, so it is possible to make attacks that perform privilege escalation and gain unlimited access to the computer's resources. The famed Morris worm in 1988 used this as one of its attack techniques. A stack overflow occurs if the call stack pointer exceeds the stack bound. The call stack may consist of a limited amount of address space, often determined at the start of the program. The size of the call stack depends on many factors, including the programming language,	**System Patches**

	machine architecture, multi-threading, and amount of available memory. When a program attempts to use more space than is available on the call stack (that is, when it attempts to access memory beyond the call stack's bounds, which is essentially a buffer overflow), the stack is said to overflow, typically resulting in a program crash, which could be exploited by an attacker to write arbitrary code to the system.	
Weak Password	Weak passwords allow attackers to easily bypass authentication controls by cracking the password. Password cracking is the process of recovering passwords from data that has been stored in or transmitted by a computer system in scrambled form. A common approach (brute-force attack) is to repeatedly try guesses for the password and to check them against an available cryptographic hash of the password. Another type of approach is password spraying, which sequentially tries a list of common passwords. Both methods are usually automated.	**Enforce Strong Passwords, 2-Factor Authentication**
Weak Wi-Fi Security	The most common types of Wi-Fi security are Wired Equivalent Privacy (WEP) and Wi-Fi Protected Access (WPA). WEP is an old IEEE 802.11 standard from 1997. It is a notoriously weak security standard and the password it uses can often be cracked in a few minutes with a basic laptop computer and widely available software tools. WEP was superseded in 2003 by WPA, or Wi-Fi Protected Access. The current standard is WPA2, even though some hardware cannot support WPA2 without firmware upgrade or replacement. WPA2 uses an encryption device that encrypts the network with a 256-bit key; the longer key length improves security over WEP. Enterprises often enforce security using a certificate-based system to authenticate the connecting device, following the standard 802.11X. Using weaker Wi-Fi security can allow attackers access to the network that the wireless router or access point is connected to. Attackers can gain this access from anywhere that is in range of the Wi-Fi signal such as a parking lot or nearby building. This range can be extended by the attacker using special equipment. This vulnerability doesn’t need to be discovered before remediating it using the Implement Strong Wi-Fi action.	**Implement Strong Wi-Fi**

XSS	Cross-site scripting (XSS) is a type of security vulnerability that can be found in some web applications. XSS attacks enable attackers to inject client-side scripts into web pages viewed by other users. A cross-site scripting vulnerability may be used by attackers to bypass access controls such as the same-origin policy. Cross-site scripting carried out on websites accounted for roughly 84% of all security vulnerabilities documented by Symantec up until 2007. XSS effects vary in range from petty nuisance to significant security risk, depending on the sensitivity of the data handled by the vulnerable site and the nature of any security mitigation implemented by the site's owner network.	**System Patches**

It's Cyber Warfare... Turn-Based Strategy Style

ThreatGEN: Red vs. Blue is a challenging cybersecurity simulation (turn-based) strategy game, based on real-world cybersecurity! Play as the hackers (red team) or the cyber defenders (blue team) against the computer A.I. or go head-to-head against a friend over the internet. ***HINT: This is a challenging game. So, if you are a beginner, be sure to read this game guide and reference the in-game wiki!***

Learn Real-World Cybersecurity!

ThreatGEN: Red vs. Blue was created by experienced, professional (ethical) "hackers" and penetration testers and is designed to help you learn real-world cybersecurity! Learn how hackers think, operate, and attack systems by playing the part of the red team (no prior skills necessary)! Play the part of the blue team and learn about real cybersecurity controls, technology, methods, and strategies!

Gameplay

ThreatGEN: Red vs. Blue is a turn-based strategy game played much like popular global domination board games. Rather than a world map, the "game board" consists of a computer network, which players compete for control over. No technical skill is required to play. Instead of simulated computer terminals and computer code, players choose and commit actions using the action menu, similar to a skill tree used in many other computer and console games.

By the Community... For the Community

Every single member of the development team for this game actually comes from the cybersecurity (or INFOSEC) community. Most of us work, or have worked, for years as cybersecurity professionals, and we all remain active members of the community. Developers Clint Bodungen and Aaron Shbeeb are authors of the book, Hacking Exposed: Industrial Control Systems. ThreatGEN: Red vs. Blue was developed and tested as a result of the feedback from more than 300 beta testers in the cybersecurity community. Our goal is to continue to make regular updates based on continued feedback, making this truly a game by the community, for the community.

Features

- Based on real-world cybersecurity
- 1-on-1 internet and local hotseat (shared screen) multiplayer
- Singleplayer versus the computer AI
- Cross-platform multiplayer enabled
- Touch screen optimized
- In-game real-world cybersecurity advice and hints
- Configurable settings
- In-game "Wiki" with gameplay concepts and instructions, as well as real-world cybersecurity definitions and concepts
- Comprehensive game guide (pdf)
- Active Discord community with gamers as well as cybersecurity professionals and enthusiasts

For information about our professional, education, and event versions, visit our website: https://threatgen.com