RED VS BLUE

PLAYER'S GUIDE

THREATGEN®

Table of Contents

Overview

ThreatGEN: Red vs. Blue is a turn-based strategy game set in a corporate computer network. However, unlike traditional games, this one is designed to teach actual real-world information security (INFOSEC), cybersecurity, and risk management concepts, theory, and strategy. Beginners in this field are introduced to, and learn, cyber-defense concepts, security controls, techniques, and risk mitigation strategy. They are also introduced to adversarial, "hacker" concepts, methods, and strategies. Understanding both sides is crucial to effective cybersecurity and risk management. More advanced practitioners can also benefit from the lessons learned in the game by seeing the overall "bigger picture" of how the cybersecurity concepts (on both sides) relate to one another, in addition to learning and practicing various risk mitigation and "red teaming" tactics and strategies.

The game also introduces and exercises many complexities and situations that professionals deal with in the real-world such as remote users causing issues, incident/breach response, and limited Resources such as Money and Staff (along with the difficulties of increasing those Resources such as "fighting" for budget).

Every Action you take can have various effects throughout the game. For example, security controls are more effective against some attacks versus others. The effects of some security controls can even stack with others. On the Red Team side, hacking certain Assets such as the 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.

The objectives of the game are different depending on which side you are playing, the Red Team (the "hackers") or the Blue Team (the defenders). The objectives, or win conditions, can also be customized in the settings.

Game Modes

Single Player Mode *(Coming Soon)*

ThreatGEN: Red vs. Blue is currently multiplayer only. Single player is not yet supported. However, single player will be coming very soon in an update. Players will be able to play as the Blue Team or the Red Team against a computer ("A.I.") opponent.

Hot Seat Mode

Hot Seat 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 MODE

In Internet Mode, players connect to the game server via internet connection and can play against each other remotely. Games are setup in the game lobby. Players may choose to change their name from the default (your Steam player name) and create a game. Keep in mind that the player that creates the game will start as the Blue Team. A chat screen is available in lobby and in game staging rooms to allow players to coordinate.

LOCAL NETWORK MODE *(COMING SOON)*

The Local Network Mode is not yet available but will be available very soon in an update. Much like the Internet Mode, this mode allows players to play against a live opponent using separate devices, but over a local area network (LAN) rather than over the internet.

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)
- Start Staff (Blue Team)
- Hacker Resource Points (Red Team)
- Turn Timer
- Turn Milestone Notifications on/off
- Maximum Number of Turns
- Win Conditions

There are some settings that will override others. For example, you can't have "0" for the maximum number of turns if you have the Play for Score win condition checked. So, altering either of those will enforce defaults upon the other.

Keep in mind that altering the values 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 game screen. This menu will allow you to end the game, restart the game, or return to the game. While in Single Player (coming soon) Mode or Hot Seat Mode this will also stop the Turn Timer and pause the game. For all other game modes, the Turn Timer will continue to run.

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

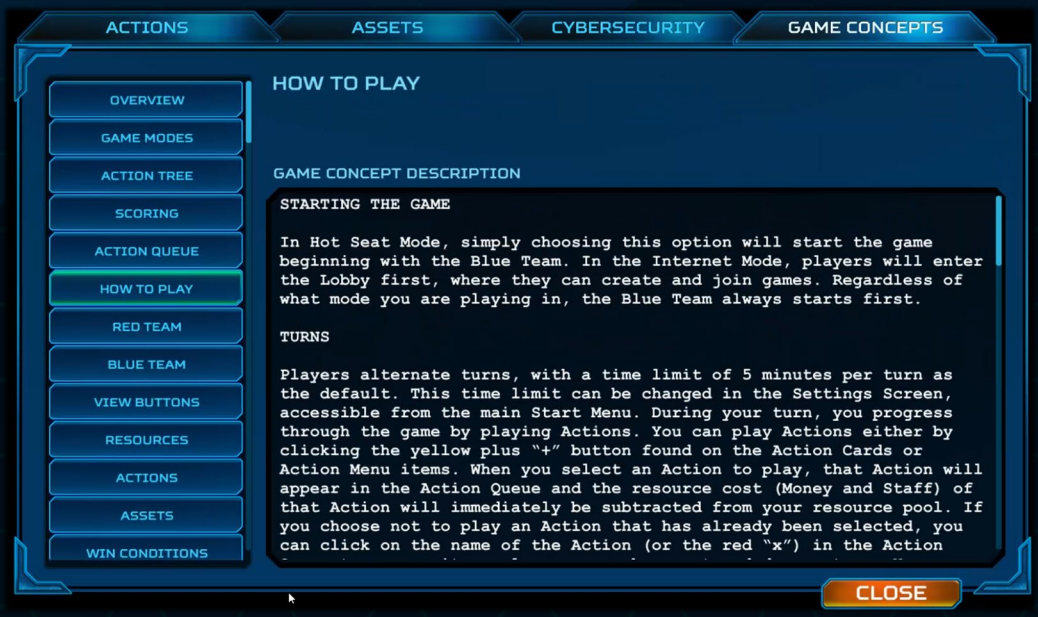
Asset Labels –
The flag icon will allow you to display Asset labels (Blue Team only).

Scoreboard

The Scoreboard is at the top center of the Network View. It displays the current turn (which increments at the end of the Red Team's turn), the Turn Timer (which resets at the beginning of each player's turn), and your current score.

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's literally an in-game cybersecurity glossary. The Game Wiki can be accessed anywhere you see the question mark "?" icon.



How to Play

Starting the Game

In Hot Seat Mode, simply choosing this option will start the game beginning with the Blue Team. In the Internet Mode, players will enter the Lobby first, where they can create and join games. Regardless of what mode you are playing in, the Blue Team always starts first.

Turns

Players alternate turns, with a time limit of 5 minutes per turn as the default. This time limit can be changed in the Settings Screen, accessible from the main Start Menu. During your turn, you progress through the game by playing Actions. You can play Actions either by clicking the yellow plus "+" button found on the Action Cards or Action Menu items. When you select an Action to play, that Action will appear in the Action Queue and the resource cost (Money and Staff) of that Action will immediately be subtracted from your resource pool. If you choose not to play an Action that has already been selected, 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 as long as you have the Resources to pay for the Action you wish to select.

SPECIAL ACTIONS

Some Actions require further player input before it can be selected and entered into the Action Queue:

Host Scan (Red Team) –
You will be asked to select a *Pivot* from which to scan from. A Pivot is essentially a "foothold". It's an Asset that you have taken control of on the Blue Team's network, allows you to launch scans and attacks further inside of the network. Assets that are available to select as Pivots will turn green. Pivots will always include the Internet and will also include Assets that you have control over. 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 pay for it. 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 turn green.

Port Scan (Red Team) –
You will be asked to select a target (an Asset), which to scan. All Assets that are available as scan targets will turn green. Assets will only be available as scan targets if you have established a Pivot with access to them (i.e. Assets are internet facing or 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 pay for it. To do so, select the Port Scan Action again. Assets that have already been previously selected, and are already in the Action Queue, will not turn green.

Service Enumeration (Red Team) –
Same as the Port Scan Action.

Attack (Red Team) –
When you select the Attack Action, the Attack Setup Screen will appear. You must first select a target (an Asset). When you click the Select Target button, available targets will turn green.

Assets will only be available as attack targets if you have established a Pivot with access to them (i.e. Assets are internet facing or you have control of an Asset in the same network zone as that Asset). 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 Vulnerabilities that you have previously identified for that Asset so far will show up in the Vulnerabilities drop-down menu. (Vulnerabilities that have an asterisk "*" next to them are Vulnerabilities that you have performed Research for; meaning, you have a better chance of exploiting that Vulnerability. Vulnerabilities with two asterisks "**" indicates that you have performed Advanced Research for that Vulnerability.) Finally, you must select an Attack objective, either Denial or Control. A successful Denial attack will render that Asset inoperable, but you will not have control over it. A successful Control 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.

ENDING YOUR TURN

You end your turn by clicking the green End Turn button at the bottom right corner of the game screen. At this time, all Actions in the Action Queue will be finalized and submitted.

BETWEEN TURNS

While you are waiting on your opponent to finish their turn, you may perform some tasks such as looking through your available Actions (either in the Action Cards or in the Action Menu) and viewing the Wiki. However, you are unable to play any Actions.

NEW TURN

Once it is your turn again, you will be presented with the Start Turn dialogue. For Single Player and Hot Seat modes, the Turn Timer will not start until you click Start Turn. For Internet and Local Network modes, the Turn Timer will start immediately, regardless of whether or not you click the Start Turn button. After clicking the Start Turn button you will be presented with Milestone notifications that you may have achieved.

WINNING

Winning the game depends on the Win Conditions that are selected, discussed in the Win Conditions section.

Red Team

The Red Team is led by the hacker, and your guide, Breach. 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 the Win Conditions available to you (discussed below in the Win Conditions section).

RED TEAM METHODOLOGY

In order to gain access to the Blue Team's network, the Red Team methodology mirrors that of real-world hacker methods. This methodology is outlined in the Red Team Action Menu and enforced through the prerequisite tree. In short, the basic concept is as follows:

Open Source Intelligence (OSINT) –
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 act as your entry points, or *attack vectors*).

Host Scan –
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 in order 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 a 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.

Port Scan –
Once you have identified viable target hosts (Assets displayed in the game as indeterminate gray computers with a red question mark), it's time to learn more about them. A *port* is a logical/virtual "window" 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. Port Scanned Assets will show the device type icon rather than a gray computer with a question mark, and will also display the same Port Scan icon found on the Port Scan Action Card. The Port Scan Action is a prerequisite before being allowed to proceed to the Service Enumeration Action.

Service Enumeration –
Now that you have identified a bit more information about the Assets you have discovered (this usually means ports and potential operating system, in the real-world), 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 display the same blue Service Enumeration icon found on the Service Enumeration Action Card.

FINDING VULNERABILITIES

Now that all of the previous prerequisite steps have been completed, you can begin your 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, which to attempt to exploit. There are 3 Vulnerability discovery options available:

Finding Public Vulnerabilities –
As mentioned previously in the Service Enumeration section, the Find Public Vulnerabilities Action is as it sounds. It uses information from the Service Enumeration step to attempt to find associated public Vulnerabilities. When Vulnerabilities are identified, the Asset will display the yellow Vulnerability shield icon.

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*. 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-on to the fuzzing results. Just like the Fuzz Action, the Reverse Engineer 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'll be able to see what Vulnerabilities have been identified for each eligible Asset by going into the Attack Setup Screen (by selecting the Attack Action) and selecting the desired Asset.

ATTACKING

Now that you have discovered a Vulnerability or two (as indicated by the yellow or red Vulnerability shield icon), you can attack. When you select the Attack Action, the Attack Setup Screen will appear. You must first select a target (an Asset). When you click the Select Target button, available targets will turn green. Assets will only be available as attack targets if you have established a Pivot with access to them (i.e. Assets are internet facing or you have control of an Asset in the same network zone as the target Asset). 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 Vulnerabilities for that Asset that you have previously identified so far will show up on the drop-down menu. (Vulnerabilities that have an asterisk "*" next to them are Vulnerabilities that you have performed research for; meaning, you have a better chance of exploiting that Vulnerability. Vulnerabilities with two asterisks "**" indicates that you have performed advanced research for that Vulnerability.) Finally, you must select an attack objective, either Denial or Control. A successful Denial attack will render that Asset inoperable, but you will not have control over it. A successful Control 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.

RESEARCH

At some point, you will notice that exploiting some Vulnerabilities is more difficult than others. In fact, some are very difficult. This is where the Research Actions come in. Performing research on any particular Vulnerability will "improve your skill" at exploiting that Vulnerability, essentially improving your chances of a successful exploit. The Advanced Research Actions will improve your skill and your chances even further.

MAINTAINING PERSISISTENCE

As you progress through the network, you might want to maintain a persistent presence, or "foothold", on the network. Otherwise, it could take a very long time to win, and even significantly reduce your chances of winning, if you have to keep finding a way back into the network every time the Blue Team kicks you out. Once the Blue Team has deployed Security Monitoring, your attacks will be detected, and they will be able to remove you from the network by activating Incident Response. To attempt to avoid this detection, you will need to Research Persistence. 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 maintain a persistent presence. Keep in mind, the Blue Team monitoring does still have a very slight chance of detecting a successful covert attack (and your covert presence each turn after a successful covert attack).

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, Social Engineering is an alternative attack method requiring a lot less "setup". The chance of success can be diminished significantly by several

key security controls, however. Therefore, this is pretty much an early game strategy (but could be a powerful one if you land on a key Asset). You have no control over which user or Asset to target when you play the Deploy Social Engineering Action. If successful, a random Windows Asset will be chosen. 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 temporarily improve your chances of success again by successfully "pilfering" key Assets.

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. In the game, Pilfering happens automatically once you take control of an Asset. However, the quality of information that can be obtained is determined by the Asset type. For example, if you take control of the Active Directory Server, the information obtained would improve your chances of compromising other Assets significantly more than information obtained from a standard User Workstation. The information obtained is also only relevant to specific Vulnerabilities. For example, finding user credentials will only improve your ability to exploit the Weak Password Vulnerability.

Blue Team

The Blue Team leader, and your guide, is Cipher. As a Blue Team Cybersecurity Specialist, your goal is obviously to defend your network. This is not as straightforward as it sounds, however.

STRATEGY

Unlike the Red Team, there aren't any linear paths to any particular goal like there is with the Red Team's path to being able to attack. Just as in real-life, there are many different tools and strategies at your disposal to defending your network. You also must deal with the fact that you are starting with limited Resources (as the default setting) and at some point, you may end of having to alter your strategy as the Red Team's strategy unfolds. As the Red Team starts to compromise your Assets, you might also have to switch to Incident Response mode. With many different attack vectors, strategies, tools, etc., you'll find that neither the way the Red Team can attack you nor the way you defend your network is a linear process. Just as in real-life, it becomes like a chess match, or even a "cat and mouse" chase.

Threat Intelligence –
The "chess match-like" nature of the game is where concepts like "threat intelligence" and "risk analysis" are simulated. Over the course of playing, you will notice player tendencies such as regular opponents over time or even with immediate opponents over the course of a single game. Just like real-world threat intelligence uses threat actor and campaign tendencies to enhance defense capabilities, learning your opponent's tendencies can give you similar benefits in the same way. Considering the broad array of strategies available to you and your limited Resources, this concept should play a major part in your overall strategy.

Risk Analysis –
The aspect of "risk analysis" in the game is similar "threat intelligence". In the real-world, organizations with limited Resources must decide, based on cost-benefit ratio, where to spend those limited Resources. For example, the impact of a compromised Active Directory Server is much higher than 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 since 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.

VULNERABILITY IDENTIFICATION

Identifying and removing Vulnerabilities in your own network is one of the core Blue Team objectives. You can identify vulnerabilities by performing Code Review, Vulnerability Mapping, Vulnerability Assessments, and Penetration Testing. 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.

SECURITY (THREAT) MONITORING

In order to know whether or not you have been compromised, you'll 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).

If you are compromised when Security Monitoring deployed, your assets will change appearance:

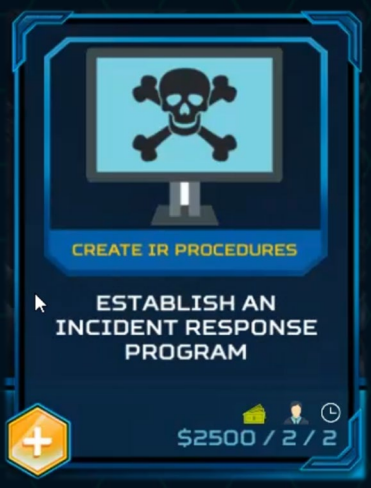
Asset Controlled –
Your Asset has been compromised and is currently controlled by the Red Team. Compromised/Controlled Assets will appear red with a white skull icon.

Asset Denied –
You Asset has been hit by a success Denial of Service (DoS) attack and is effectively "offline". Denied Assets will be displayed as orange with a white skull icon. There is a possibility this Asset could "self-recover".

Asset Damaged –
Your Assets has been damaged for one reason or another (possibly due to a DoS attack or other exploit gone wrong) and is permanently "offline" until it is repaired or replaced. Just like a denied Asset, Damaged Assets will be displayed as orange with a white skull icon. A damaged ICS process is a win condition for the Red Team.

INCIDENT RESPONSE

At some point, your Assets will be compromised, denied, or damaged. When this happens, you'll need to deploy incident response. In order to do so, you'll need to, of course, establish an Incident Response Plan first (Create IR Procedures), and then Active IR. There are preparation actions, such as performing Backups, that can help improve your odd of a successful Incident Response. Also, note that to Activate IR, it requires more than the 3 staff that you start with (as the default). So, you will need to be aware of this and plan for it.



View Buttons

The View buttons are found at the bottom right corner of the game interface. 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, Action Card Stage ("deck"), and most all other interactions.

actions view

The Actions View displays all of the game Actions and "dependency tree". This view allows you to see all of the prerequisites for each Action in a hierarchical format. You can also select Actions directly from this view by clicking on the yellow plus "+" button. Selected Actions will be entered into the Action Queue just as they are when you select them from the Action Cards.

world view

The World View is currently used to mask the "game board". The default scenario takes place in a refinery network environment (more scenarios are being developed as DLC). Therefore, the default World View features a picture of a refinery/plant. Future scenarios will feature pictures related to their specific environment and theme.

Resources

Resources are what you expend to play Actions. They are located in the top right corner of the game interface for both the Blue Team and the Read 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 closely the same Resources effecting 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. How much each Action costs 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 strategize with the Resources you have and/or find a way to increase your Resources. Time (turns) is what it is. You can't get time back just like in real-life. Your Staff will become available again once they complete the Action they have been assigned to. But 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. There are things you can do in the game that increase your chances of getting budget. You could compel management to grant you funds if you can show them 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 uses the more abstract Hacker Points resource because there are a multitude of factors to consider across many different threat actor types, groups, and motivations. Just like the Blue Team, each Action has a cost associated with one or more of these Resources. How much 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 cannot increase your Hacker Points above the total number that you begin the game with (the default is 5).

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 or in the Actions List in the Appendixes of the *ThreatGEN Game Guide*.

Playing Actions

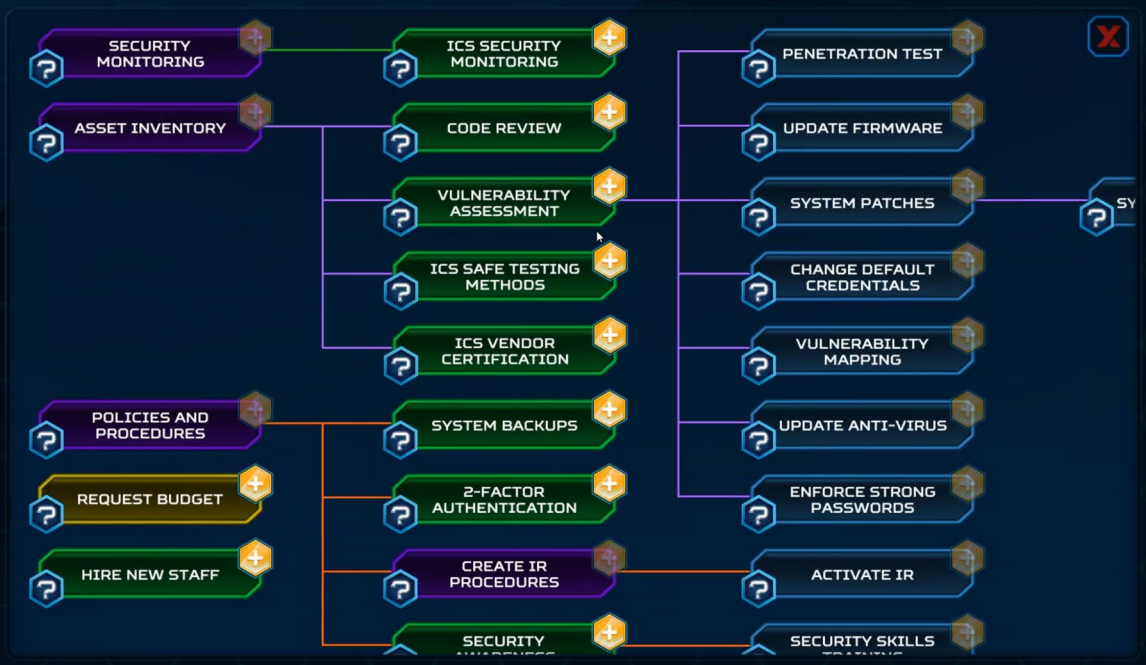
To play Actions, you click on the yellow plus "+" button found on the Action cards or Action menu items.

Action Cards –
The Action Cards are found in the Network View (you can't miss them). Action Cards are the quick way to play Actions. You can scroll through them (left and right) by clicking on the arrows to the left and right of the Action Cards. The Action Cards contain the name of the Action, a brief description, the Action icon, the Resources cost, and the "submit Action" button.

Action Menu –
The Action Menu is accessed by clicking the Action view button. Rather than the ability to quickly scroll through and play Actions directly from the Network View, the Action Menu allows you to see all Actions along with their associated requirements and dependencies. You can also access each Action's associated Game Wiki entry by clicking on the question mark "?" button. You can play each Action directly from the Action Menu by clicking on the Action's submit button (the yellow plus "+" sign).

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

- Blue – 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

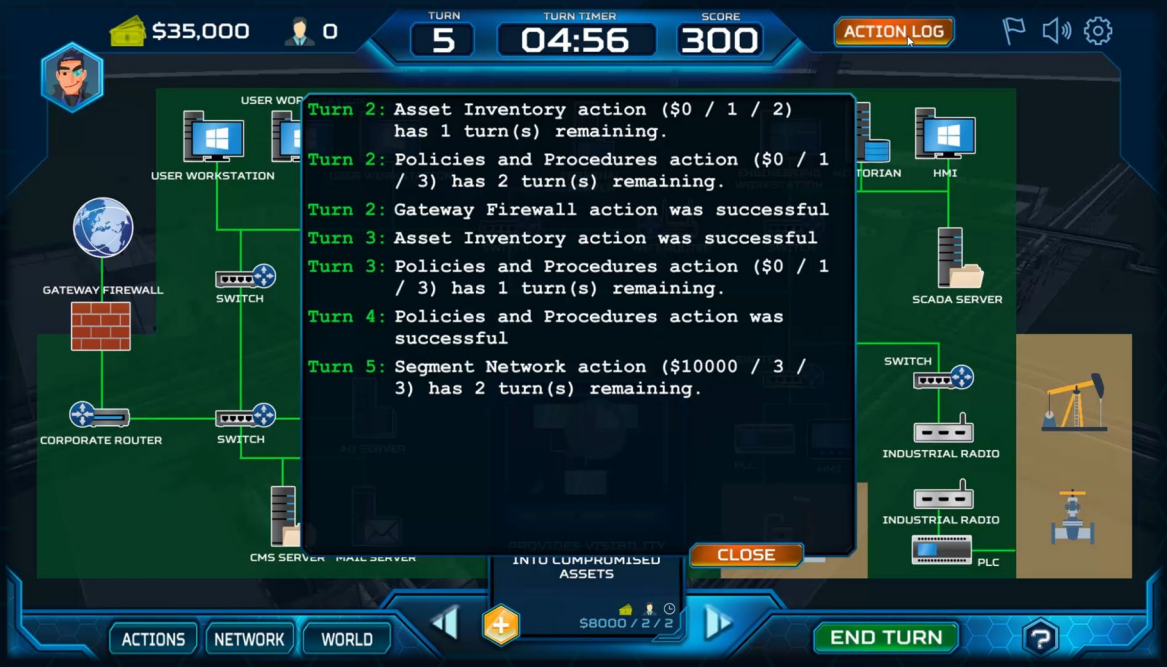


ACTION QUEUE

When you select an Action to play, that Action will appear in the Action Queue and the resource cost (Money and Staff) of that Action will immediately be subtracted from your resource balance. If you choose not to play an Action that has already been selected, you can click on the resource 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 as long as you have the Resources to pay for the Action selected. You can display the Action Queue at any time by clicking on any resource icon at the top right corner of the interface for both Blue Team and Red Team.

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 completions.



Assets

Assets are the second most important aspect of the game. 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 different characteristics, functions, operating systems… and Vulnerabilities. They also have different advantages to attackers in the event they are compromised. Further details about each Asset can be found under the Assets Tab in the Game Wiki or in the Assets List in the Appendixes of the *ThreatGEN Game Guide*.

Win Conditions

It's hard to win a game without Win Conditions. That said, you can disable all Win Conditions and set the maximum number of turns to 0, and the game will go on perpetually, like a simulation. However, for those that do desire the thrills of victory, 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.

Around the World (Red Team Win) –
Maintain simultaneous control of at least one Asset in each network zone.

Damage ICS (Industrial Control Systems) Process (Red Team Win) –
The default scenario takes place in a refinery. Therefore, the ultimate victory (for the Red Team) would be to damage an industrial control systems process. The opposite of that would be a Blue Team win by preventing such a condition.

Play for Score (Blue Team or Red Team Win) –
Simply put, you play until you reach the maximum turn limit and the player with the highest score wins. Scoring is achieved by completing Milestones. See Milestones.

Weather the Storm (Blue Team Win) –
When both this Win Condition and the Damage ICS Process Win Condition are both enabled, this is the ultimate win for the Blue Team. Otherwise, this serves as the default Win Condition when the maximum turns have expired. If the Red Team hasn't achieved a victory, and the Play for Score Win Condition is disabled, Blue Team Wins by virtue of preventing the Red Team from achieving a victory.

Milestones

You increase your score by completing Milestones. Milestones represent significant events, tasks, or achievements similar to their comparable real-world counterparts. They are awarded based on a number of factors including completing specific Actions, special sequences and/or a combination of Actions, and completing Actions under special circumstances or with special conditions. Further details about each Milestone can be found under the Game Concepts Tab in the Game Wiki or in the Milestones List in the Appendixes of the *ThreatGEN Game Guide*.