Red vs Blue

Red vs Blue is a cyber security focused card game that pits opposing players or teams of players against each other in a cyber-attack scenario. Both Red and Blue teams purchase assets to develop their cyber capabilities.

The Red team takes the position of the cyber threat actor, developing assets to enable them to launch cyber-attacks against the Blue Team. As the Red Team cyber offensive abilities grows so does the sophistication of the attacks they can launch against the Blue Team.

The Blue Team acts as the cyber defence team of their company. Purchasing and developing assets to mitigate and defend against attacks from the Red Team. As the Blue Team cyber defence posture improves it opens potential business opportunities based upon the various combinations of assets they currently possess.

How to Play:

There are two game modes for Red vs Blue, Single Player and Two Player mode. Both of which are explained below:

Single Player:

In Single Player mode a single player or team takes charge of the Blue Team and builds Assets whilst facing random Attacks each round. By purchasing and developing Assets, the Blue Team can mitigate more sophisticated attacks, and in doing so acquire Business Contracts that provide them with more Capital and Reputation with which to buy more assets.

The game ends when one of these 2 scenario's occurs:

The Blue Team successfully builds a Security Operations Centre (SOC)

OR

The Blue Team is reduced to zero Capital or zero Reputation by failing to mitigate the cyber-attacks they face.

How to get started:

In Single Player Mode the Blue Team get the help of a Chief Information Security Officer or CISO from the purple CISO Deck. Shuffle the CISO Deck and select a card at random from the Deck. That card is your CISO, and for the duration of the game you gain the benefits granted by your CISO.

The Blue Team begins with 75,000 in startup capital to purchase assets from a list of starting assets, and 3 Reputation. The Blue Team startup assets are:

Security Analyst, Firewall, Intrusion Detection System, Intrusion Prevention System.

Once you have purchased as many Assets as you want, return the remaining Assets to your Asset pile and the game is ready to begin.

Order of Play:

The game is broken up into a series of turns, each turn has four distinct phases:

Asset Phase: At the start of each round the Blue Team can purchase or sell assets to develop their cyber security capabilities. The Blue Team can buy as many assets as they desire, and they can afford.

Attack Phase: At the start of the Attack Phase, shuffle the gold-coloured Attack Deck and randomly choose a card. That is the cyber attack you face that round.

Mitigation Phase: Once the Attack Card has been drawn, check to see if any of your Blue Team Assets can mitigate the Attack. If they cannot then you suffer the impact as described on the Attack card.

Once the mitigation phase has ended return the attack card to the Attack deck unless it states it is a Persistent Attack. Persistent Attacks remain in play until mitigated. Follow the instructions on the card.

Contract Phase: Once the Attack and Mitigation phases have been resolved, the Blue Team can check to see if they have the necessary assets to obtain a business contract. The Blue Team may only acquire 1 Contract per turn. Once a Contract is acquired the Blue Team gains Capital and Reputation equal the values stated on the card.

Once the Contract Phase ends the turn is over and the next turn begins with the Asset Phase.

Two Player Mode:

Two Player Mode pits two players or teams of players against each other in a Red vs Blue scenario. Where the Blue Team purchases Assets to build their companies cyber security, whilst the Red Team builds Assets to launch a variety of Cyber Attacks against the Blue Team.

Getting Started: Both Teams start with £75,000 in startup capital to purchase assets from a list of startup assets, and 3 Reputation. Once both teams have purchased assets, they deduct the cost from their startup funds and the game begins. The Red Team chooses from the Red Team Asset Deck and the Blue Team from the Blue Team Asset Deck.

Red Team Start Up Assets:

OSINT Officer, Hacker Laptop, Port Scanner, Command and Control (C2) Server.

Blue Team Start Up Assets:

SOC Analyst, Firewall, Intrusion Detection System (IDS), Intrusion Prevention System (IPS).

Once each team has purchased all the assets they want, return the remaining Assets to their respective Asset piles. With this done the 1st round of the game begins. Note: You do not have to spend all your startup money to begin with.

Domains:

In Red vs Blue there are 2 domains:

The Public Domain: These are cards played out on the table that all players can see. Some cards will force either team to reveal cards and place them in the public domain. Once an asset is deployed in either an attack by the red team or defence by the Blue Team it becomes part of the public domain.

Private Domain: These are cards held by the players and have yet to be placed in the public domain. Adding an element of strategy and surprise to the game play.

Order of Play:

The game is broken up into a series of turns, each turns has four distinct phases:

Asset Phase: At the start of each round both Red and Blue teams can purchase or sell assets to develop their attack or defence capabilities. Each team can buy as many assets as they desire, and they can afford. Except for the first round.

Attack Phase: At the start of each attack phase, the Red Team goes first and decides whether they want to launch a cyber-attack against the Blue Team by deploying Red Team Assets. The Red Team must have the necessary Assets in the Public Domain to launch an Attack. It is not compulsory for the Red Team to attack. If the Red Team does play an Attack Card, then the Blue Team may deploy Assets into the Public Domain to attempt to mitigate them.

The Mitigation Phase: If the Blue Team cannot mitigate the Attack by deploying an Asset, then they suffer the impact on the Attack Card. Where in the single player mode the loss of capital is removed from the game. In Two Player mode on a successful Attack the loss of Capital and Reputation is captured by from the Blue Team by the Red Team. Transfer any capital or reputation from the Blue Team to the Red Team.

If the Red Team plays a Persistent Threat, that threat remains in play in the Public Domain. Otherwise at the end of each mitigation phase return all attack cards to the Attack Deck.

Contract Phase: Once the mitigation phase is complete, the Blue Team may look to see if it has the necessary assets to boost its capital and reputation to enable to defences. During the Contract Phase, the Blue Team may choose to sale assets to boost its capital or stop it from going bankrupt. It may sale a maximum of 2 Assets per turn. The Blue Team cannot sale an Asset and acquire a Contract in the same turn.

With the Contract Phase at an end the turn ends, and we return to the top of the next turn.

For example:

The Red Team and Blue Team purchase their Assets and hold them in their hands. Then each

The Red Team plays the Distributed Denial of Service (DDOS) Attack Card, the Blue Team lacks the necessary Assets and is unable to mitigate the attack. As such the Blue Team must pay the Red Team £40,000 to stop the attack and loses 2 reputation for the disruption to their service.

At the end of each round all non-persistent attacks are returned to the Red Teams hand.

Contract Phase: Each Round the Blue Team can pick up new Business Contract based on the various Cyber Defence Assets they possess. Each Contract has varying requirements as determined by the Business Opportunity Card. The Blue Team can only gain 1 new Contract per round.

Should the Blue Team fail to maintain the Assets requirement for a Contract they lose the Contract and any benefit it may offer. The card is returned to the Blue Teams Contract deck.

At the end of the Contract Phase the turn ends.

Winning the Game:

The game can be played in multiple ways:

Over a set number of rounds, with the winner being the Team with the most money and reputation at the end of the allotted number of rounds.

OR

The game can be played out in full, and is decided as follows:

Either the Red Team succeeds in launching enough successful cyber-attacks to reduce the Blue Teams finances or Reputation to 0.

OR

The Blue Team successfully fends off all the Red Team attacks and can acquire all its assets, and in doing so fully develop its cyber defence capabilities.