Game Setup

1. For teams - split by your choice
    a. Make sure equal number of seniors and juniors on each team
2. For role: have team team draw 3 cards and pick 1
3. For defense: draw ½ of cards per vulnerability tier and layout on their table
4. Have each team assign their roles to their players
    a. Team roles can be found on the powerpoint slides
5. Setup market: 3 in market per side
6. Assign starting cash - $1000
7. Each team assigned a moderator (watches the cash flow and helps you out if needed)
    a. This can be the threat intel leads or people who want to help with this if lots of people participating
8. Offense - setup APT market: 3
9. Defense knows what the possible apts are attacking them
10. Split teams by tables/divider
    a. Lower dividers and put timer/rules on screens
    b. 2-3 min timer : keep on screen

Game Rules:

1. Defense goes first
2. 3 min timer per turn - bonus 2min if go over
    a. Penalties for not finishing in time:
        i. Offense: defense gets a successful block = losing hp
            1. 20 sided die to decide loss
        ii. Defense: successful attack = offense moves one step
    b. As the game progresses, reduce the timer length - increase pressure
3. Team team has a set income per round (updates later in game)
    a. Defense: $200
    b. Offense: $100
        i. As the game progresses, increase the income of both teams
4. Per turn(one action):
    a. Each team collects their income for the turn
    b. Action one (pick one)
        i. Pay $100 to draw an inject card
        ii. Play inject card
        iii. Pay $100 to reset market
        iv. Defense: purchase tool
        v. Collect an extra $100
    c. Action two (pick one)
        i. Defense: pay double for a custom tool
        ii. Card abilities
        iii. Market card purchase (everyone)

5. Required to develop resources for offense to make initial attack
    a. Also when purchase new APT to join team
    b. If fail initial access, required to develop a new resource to try new attack
6. Reconnaissance - both teams roll a D20
    a. The offense does not need to complete the reconnaissance level of the mitre framework, this only applies when they use the ability to find a vulnerability in the defense (via market cards)
        i. Defense: their roll plus the current tier level the attacker has gotten to
            1. Ex: on persistence so they roll a D20 and get 15 + 5 = 20
        ii. If critical success for offense then get to see ½ of vulnerabilities
        iii. If fail for offense then they are detected and roll a D20 to lose health
        iv. If normal success for offense then get to see one vulnerability
        v. If critical success for defense then roll 2 d20 for offense to lose health
7. Winning:
    a. Offense reaches impact
    b. Defense defeats APT -aka lose all health
        i. Successfully block attack or detect active scan for offense to lose health via a D20 roll