DETECTION AND RESPONSE GAME

You are a lone IT Security Expert on the noble quest of defending your company from evil hackers. On the line are a lot of overtime, the wrath of your fellow IT colleagues and an unpleasant talk with management, so be ready to prove your knowledge.

You need:

- Detection and Response game cards (Initial Access, Privilege Escalation, Persistence, Lateral Movement & C2 & Exfiltration, Impact, Event)
- Defenderpoints
- A 6-sided die
- Pen and worksheets

The player with the most knowledge is assigned the roll of the Hacker, he shuffles the deck and sorts the cards face down by color, he draws a card from every stack (Initial Access, Privilege Escalation, Persistence, Lateral Movement & C2 & Exfiltration, Impact) besides the black Eventcards. The Hacker then precedes to create an incident situation based on the Attackcards and relates as much as possible to his own work environment. The Hacker will then reveal the scenario of the first card and the IT Security Experts have time to write down a way to mitigate and detect this kind of attack. When everyone is finished every IT Security Expert rolls a die, if the number is a 1-3 (this can change with Eventcards) the attack was successfully mitigated, otherwise the player has a second chance to do the same with the detection method. If the attack was successfully mitigated or detected the player gets a Defenderpoint. After every Attackcard the hacker must draw an Eventcard and give it to the IT Security Expert who is the biggest threat. This continues until all Attackcards are processed and the attack is finished. The IT Security Expert with the most Defenderpoints is the winner and has successfully defended the Hacker's attack.

After the Game all participants should work together to determine if the played attack would be possible in their environment and what incident response processes should be taken if such an attack would be successful.