SEACAT

Table of Contents:

(order for game manual)

Welcome to the SEACAT game manual! SEACAT is a gamified variation of the commonly used Cyber Tabletop (CTT) exercise, often used to test the cyber security of certain systems. However, despite the numerous benefits of conducting the CTT exercise, one major downfall is the experience of the CTT itself generally being described as an unstimulating, dreary, uninspiring, tedious, exuberating, miserable task. Therefore, the only logical solution was to gamify the Cyber Tabletop to make the exercise a more bearable experience. And the end result was the SEACAT game, an awe-inspiring, delightful, beneficial, and heart-healthy exercise.

Pre-Game/Set-up:

Before the execution of this game/exercise, everyone should have an understanding of the Cyber Tabletop (CTT) manual.

Review the optional rules section (Page #) for additional variations on the CTT game.

1. Follow "Exercise preparations" (Pages 8–28 in the CTT manual), such as, but not limited to
    a. Define Teams: The teams in the CTT game are synonymous with the CTT; however, there are some additional tasks for the groups included:
        i. Control: The main purpose of the Control Team is similar to the CTT. They are meant to facilitate the entirety of the exercise; however, in the gamified version of the CTT, the Control Team is also tasked with operating the computer interface (Page #).
        ii. Blue (Operational): The Blue Team is tasked with presenting the system defense; however, in the gamified CTT, the Blue Team takes less of a passive role and is met with some opportunities to prevent the advance of attackers (Page # for defensive opportunities).
        iii. Red (OPFOR): The Red Team is tasked with designing a chain of attacks to successfully accomplish their mission in the operational system. However, in the CTT game, there are opportunities for adaptation in the attack chain if it were to fail.
    b. Construct team missions and scenarios: Blue Team mission timeline, Red Team objective, etc. Ex: The Blue Team mission timeline is around three days

    (theoretical time). The Red Team needs to breach the defenses and accomplish their goal (exfiltration, impact, etc.) before the Blue Team knows what is happening.

        i. Red Team assumptions, TTPs (Tactics, Techniques, and Preparations), and pre-exercise infiltration: The Control Team informs the Red Team about Blue defenses, Red Team weaponization, and any pre-mission variables implemented by the Red Team, such as malware.

2. Attacker and Defender Cards: Both the Red and Blue Teams have cards assigned to them. These are merely for illustrating the attacks and defenses employed and making the process of using and arranging certain techniques easier. At the start of the game, each team will add a brief description of a specific attack (Red) or defense (Blue) they plan to use. Card templates can be found on GitHub and are fully customizable.

        i. (Template will be shown here of both teams)
        ii. (Example of completed card of both teams with resources and cost filled in and one with both blank)

    b. The colors of the cards are assigned accordingly to the teams. Additionally, the Red Team’s cards have a section titled “resources” and "time." Go to page # for an explanation of the resource system and page # for the time system, then fill out the card accordingly. Blue Team’s cards also have a section for "maturity" to fill out; more on that in a bit. The Control Team will read over these cards and work with Red and Blue before the game begins.
    c. As stated earlier, the purpose of the physical objects in this game is to have tangible representations of the computer interface. Nonetheless, the Attack and Defense teams will set those up after the cards have been made, taking note of where to put cards that have been played, where resources can be found, etc.

3. The Control Team decides the resource level of the Red Team and starts setting resources accordingly (resource system on page #). Cards will have a plastic protective sleeve and stickers that can be placed and peeled away when done that display cost and

attack/defense. The cost of each card is measured in time (time system on page #), and the resource level limits the complexity of the attack as well.

4. The Blue Team determines the maximum maturity level (1-5) of the defenses in the system in use and will represent it by placing one star for each maturity level on the sleeve of the card. The Control Team will verify and change this maturity level to fit the actual capabilities of the system.
5. The Control Team will input commands into the computer interface (mission timeline, list of attacks and defenses, resources, etc.). Go to page # for the computer interface.

Computer Interface: The computer interface is a way for the teams to see a virtual representation of the CTT. The game has many different features to make the experience as useful as possible.

1. Options Menu: The options menu, accessible from the start screen, allows the user to change the audio levels of music and sound effects, as well as select between three different themes.
2. Help screen: The help screen gives information on how to use the game. There is also a help button available in the bottom left corner of nearly every screen, denoted by a question mark.
3. Mission Statements: The following screen allows the user to manually input OPFOR and Defense mission statements, which will be displayed later. Additionally, the game can save these statements ahead of time. If there is a .txt file in the game's directory specifically named "mission statments," then the first line will be read as the OPFOR statement, and the second will be read as the defense mission statement. This allows for a smooth transition to the following screens.
4. Create profiles screen: This screen allows the user to download a template for the OPFOR and Defense profiles, as well as the mission timeline. Ideally, this should be downloaded ahead of time, edited, and then reuploaded in future steps. This page also contains the ATT&CK and D3FEND databases for download.
5. Profile Upload: After editing the templates with the necessary components, upload each of them to their respective locations. The interface will store them and use the data on the gameplay screen.

6. Mission Statement Scrolling Screen: The previously inputted mission statements will scroll up from the bottom. This can be skipped, paused, or sped up.
7. Gameplay screen: This screen is where the game will be played. After pressing the start button in the center of the screen, a variety of options will open up. The timer at the top works like a chess clock and can be paused or played with the button in the middle. Additionally, the mission timeline is visible through the animated progress bar at the top, customizable with the theme settings. The Attack Team can select anywhere from 1-3 cards using the drop-down menu. Below each card is an expand button to size up the card, and a delete option to remove it from the current cards. After the Attack Team has selected the desired cards, the timer will pause for them and start for the Defense Team. The Defense Team's interface is identical to that of the Attack Team. After the Defense Team has submitted their chosen attacks, the discussion time will commence. After the Control Team has reached a conclusion about the viability of the attack they will input an attack result (success or failure), and an attack success likelihood. The Attack Team's timer will start again, and the game will continue. Once the game has reached a finishing point, select the end game button and progress to the end. Here you can download the game's data as a csv file, which can easily be imported into Microsoft Excel or Google Sheets for clean visibility. To play the game again, select either "Play again same profiles" or "Play again Change profiles." Press quit to close the game.

Resources

Resources allow for a realistic depiction of how accessible certain techniques are for certain adversaries. However, it does not necessarily indicate the success or strength of an attack. Techniques will be ranked on a 10-point scale, where 1 is the easiest to develop and 10 is the most complex to develop. The amount of resources techniques will cost is debated amongst the 3 groups based on the 10 number scale. For example, a phishing virus may be scaled at 3, while malware developed from scratch may be scaled at 8. At the beginning of the game, the Control Team will determine the development level of the adversaries. The Control Team will decide how many resources to give the Red Team relative to the longevity of the mission and traits of adversaries. In other words, the Control Team will give the Red Team a realistic amount of resources based on who they are meant to represent. The given resources should allow the Red Team to create the pre-planned attack chain; however, they should also allow them to switch attack chains if the first one fails or they see a better opening.

Note: The amount of resources needed to develop an attack does NOT preface its strength or effectiveness.

Time:

Similarly to the resource system, the factor of time is supposed to further implement constraints on the adversaries by taking into account the amount of time it would realistically take to complete an action.

Like the resource system, players will have a high degree of freedom in choosing how much time they have. The Control Team will be in charge of assigning a realistic value of progression per specific attack or technique. For example, a firewall breach could potentially take up to 15 minutes. It is recommended to use multiples of 5 minutes to keep it simple, but this is only a recommendation, not a rule.

Game:

1. Following the preparation state of the game, the Control Team will begin the mission timeline in the computer interface and begin the game.
2. Turn order
    1. The Red Team will begin their attack chain and present their first point of conflict. After selecting the attack card, the Red Team will "buy" the technique with their resource points (Page #) and place the card relative to where it belongs on the mission timeline. Techniques will also require a certain amount of time on the mission timeline to complete, and during the duration of that period, no other attacks can be initiated (Page # for the time system).
        1. Note: If attackers use 2 techniques to accomplish a task, they will be combined into 1 card with both the sum of resource costs and the time of

the 2 cards. This new card will function as the representation of those attacks.

    2. The Blue Team presents the appropriate defense(s) for the attack and states the maximum maturity level (1 through 5) of the defense system to the group.
        1. Note: It is recommended that the Control Team restrict the number of defenses Blue can use at a time to 3 (page # for multiple defenses).
        2. Note: If no appropriate defense can be presented, assume the Red attack is successful.
    3. Determining whether the attack will be successful (Page # for determining the success of an attack). Additionally, determine the attack success percentage and take note of it for the final analysis later on (Page # for attack success percentage).

3. Depending on the outcome of the attack, the Red Team has a few choices. If Red's attack is higher than the maturity level of the Blue Team, they may continue with their attack chain. If the number is below the maturity level, they must change their attack chain and spend resources on new techniques.
   Note: If an attack fails, a penalty will be enacted against the Red Team. Bringing the Blue Team's mission time closer to completion (for example, by 5 minutes).
4. The Control Team takes note of the attack chain used, possibly offers some advice or their opinion on a given defense or attack, and inputs the values given into the computer interface.
5. The game continues until the situation in which the Red Team reaches their objective, the Red Team's attack is stopped, or the Blue Team's mission timeline is complete.

Multiple Defenses:

If multiple defenses are presented, this process must be completed differently, depending on how the defenses work. If the defenses work in collaboration with one another, all teams will debate the total maturity level of the systems, similar to combining attacks. However, if defenses work in sequence, or one after another, they will each be presented one at a time, and the maturity level will remain individual.

Note: If defenses work in sequence, the attack will only take a singular amount of time to execute, rather than spending time on each defense.

Determining the success of an attack:

The maximum maturity level (1 through 5) is adjusted to a 1–20 scale, giving its armor value—if a maturity level of 4 was decided, it would turn into an armor value of 16. Various variables (Page #) for the defense are debated by all teams, and they will decide what the “actual” maturity level or armor is in the current situation. For example, if the attackers planted malware in the system before the operation, it could potentially bring down a system with an armor level of 12 to 10 by -16%. All teams will then debate both the likelihood of the success of a particular attacker technique against the presented defense and the attacker variables (page # for debates). The outcome of the debate should be in the form of a percentage. This percentage will then be used to decide how many additional points will be added to the attack relative to the defense's defense. For example, all teams reach the conclusion that the attack percentage is 50% and the defense armor is 10. This means that 5 (50% of 10) will be the base value of the attack. The Red Team will then roll a 20-sided die to determine the attack, along with the additional points, with the example being 5 from earlier. This will decide whether the attackers will be able to continue with this course of attack if they get a total value of the attack above the defense armor.

How well the attack works	Percent armor change
Amazing	-90%
Great	-75%
Good	-50%
Ok	-25%
Neutral	0%

Attack success percentage:

To determine the attack success likelihood, the Control Team must determine the probability of the Red Team rolling a number above the defense armor to account for the attacker percentage. For example, if attackers have a 50% against a defense armor of 10 (that was originally 12), that gives them a base of 5. Then, based on a 20-sided die, the probability of achieving a number above 10 (5+dice roll) is 75%; therefore, that would be the attack success likelihood percentage.

Note: If multiple defenses are presented, this process must be individually completed for each defense.

Note: If there is something assisting the attack, take that into account when determining the percentage.

Formula for determining percentage: *1-(M*4/20)*(1-V1)*(1-V2)...*(1-Vn)*

M=Maximum Maturity

V=Variable

The formula simplifies the process of analysis. Input the maximum maturity level (1-5), then account for variables that can affect both the maturity and the success of an attack. Taking the example from earlier, this would be .16 and .5—16% & 50%—and input the values for V1 & V2, respectively. And then taking the maximum maturity level of 3, and substituting that value for M. 1-(3*4/20)*(1-.5)*(1-.16)= roughly outputs to .75 or 75%

Note: When inputting variables into the computer software, (1-V*n*), etc. must be determined beforehand.

Variables:

Variables not only include a factor of randomization in the game, but they also allow for a realistic representation of real-world scenarios where a variety of factors can affect the success of an operation. Variables are highly customizable and can be positive or negative; however, they should be made to appropriately convey the scenario.

Attacker: Examples of attacker variables could include pre-mission malware, the number of adversaries, or a poor internet connection.

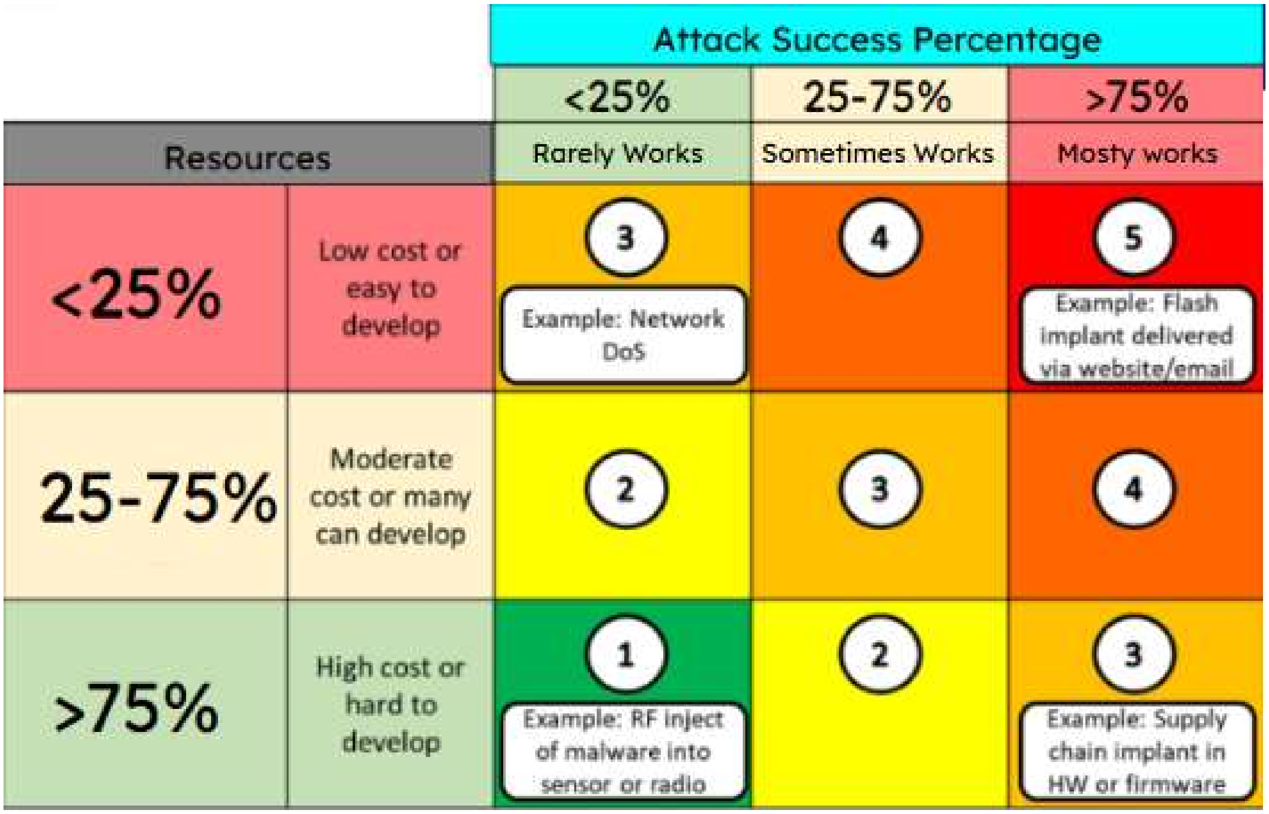
Defense: Examples of defender variables could include how long a system has been in use, a lack of cyber security employees, or a power outage.

Debate: To maintain the realistic aspects of the game, teams must justify their reasoning for success likelihood to the Control group. There are two main types of debate: the one at the beginning of the game to establish the action cards, resource allotment, maturity, etc., and the other debates that follow an attack. For this reason, it would help if the Control group was familiar with both teams as well as the techniques they are putting to use (manual). When conducting a debate, each team should be able to present their ideas like a case before a judge and be allowed to respectfully argue back and forth. At the end of any debate, the Control group makes the final decision.

Post-game analysis

1. Conducting the Likelihood Assessment (Page #).
    1. Determine the overall attack success likelihood (page #).
    2. Determine overall resource usage and conduct analysis (page #).
2. Conduct impact analysis (page #).
3. Determine the operation risk analysis; refer to the risk matrix in the CTT manual.

Likelihood assessment: The likelihood assessment is one of the post-exercise analyses of the CTT. For this gamified CTT, we use a similar concept; however, there are some changes to the table that is used.



		Attack Success Percentage		
		<25%	25-75%	>75%
Resources		Rarely Works	Sometimes Works	Mosty works
<25%	Low cost or easy to develop	3 Example: Network DoS	4	5 Example: Flash implant delivered via website/email
25-75%	Moderate cost or many can develop	2	3	4
>75%	High cost or hard to develop	1 Example: RF inject of malware into sensor or radio	2	3 Example: Supply chain implant in HW or firmware

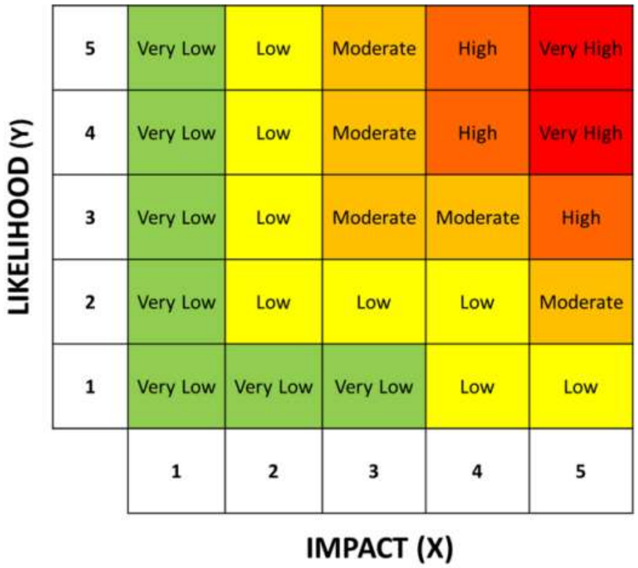
As shown in the table, attack success percentage and resource use are vital for determining the outcome.

Overall Attack Success Percentage: At the end of the game, all attack success percentages will be multiplied out, and the product will be used for the likelihood assessment.
Attack success likelihood scale: bottom 25% is “rarely works," middle 50% is “sometimes works," and top 25% is “always works.”

Resource Analysis: The resource analysis gives the players a system to understand to what extent the Red Team was able to efficiently conduct their attack.
To conduct this analysis, at the end of the game, players will determine what percentage of their total resource count they used. For example, if 10 resource points were used out of 15, the percentage would be 66%.
Similarly to attack success analysis, the percentage will be grouped into 3 groups. The bottom 25% will be “low cost," the middle 50% will be “moderate cost," and the top 25% will be “high cost.”.

Impact Analysis: Following the completion of the exercise, all teams will decide what the overall impact of the Red Team’s attack is. This will be done through a debate and use of the Impact Methodology table in the CTT, with consideration for the CIA triad (confidentiality, integrity, and availability).

Risk analysis: The risk analysis is one of, if not the most significant, reasons for conducting a CTT exercise. Thus, the overall risk analysis of the operation is also a crucial concept included in this game. To determine this, no changes were made to the risk matrix used in the CTT; however, there were a few crucial changes made to the likelihood assessment that should be understood.



LIKELIHOOD (Y)

5	Very Low	Low	Moderate	High	Very High
4	Very Low	Low	Moderate	High	Very High
3	Very Low	Low	Moderate	Moderate	High
2	Very Low	Low	Low	Low	Moderate
1	Very Low	Very Low	Very Low	Low	Low
	1	2	3	4	5

IMPACT (X)

DOD CTT Manual

Backstory: Add backstory comic from Graphic Design/Rulebook Design/Comic in order.

Optional Rules: As said in the name, these variations of the CTT game are optional; however, they are variations of the SEACAT that can further gamify or make the exercise truer to the CTT.

Card deck: The card deck system adds further randomization to the game, confining the Red Team to use techniques provided by their card draws.

The cards are split into 3 sections: technique cards, initial access, entry point, and final exfiltration. The Red Team has the option to draw 5 cards from whichever deck they want to use against Blue; however, they can only draw from 1 deck at a time. After each attack, the Red Team will have the opportunity to draw again. All other rules stay the same.

Note: If the cards that are drawn cannot be used in sequence with previous attacks, the mission timeline automatically progresses by 10%, and the Red Team is able to draw again.

Counter Defending: In the situation where attackers roll a low enough value to trigger the count"

> Note: On the chance that attackers roll less than or equal to 10% of the maturity level +1, defenders have an opportunity to fully counter the attackers (Page # for counter defense). For example, 10% of a maturity level of 10 would be 1, plus an additional point, making it 2. In this situation, if attackers rolled a 2 or below, it

would trigger the counter-defense opportunity for the Blue Team if that failure could lead to them being detected.

For a counterdefense to be successful, both teams must roll the dice. If Blue rolls a number higher than or equal to half of what Red rolls, the game ends. If not, the game continues. For example, if Red rolls a 10, Blue must roll a 5 or higher.

Adversary advancement levels:

At the beginning of the game, the Control Team decides the adversary's advancement level from 1-10. The advancement level limits what cards the Red Team can use. For example, if the Red Team's level is 7, then they are confined to using cards that cost 7 or fewer resource points and are not allowed to use any cards that cost 8, 9, or 10 resource points.

Increase time length

You can increase the length of attacks by 50% and give a reason, such as that the Attack Team does not have coffee. This can be used to limit the length of attacks.

How to make an optional rule:

1. Make it relevant. It should represent a condition that could be affecting the attack or Defense Team, or if it does not represent a condition or situation, it should make the Attack Team think about a new way to exploit the system.
2. If it includes a random element, it should change the game slightly and not be overly present.
3. Don't use a special rule in every game, switch it up. The Attack Team should have to think in many different ways so that you can get more varied attack plans.