



CYBER REALM

Juan Ford

Rules Reference Guide

Learn, Train, and Defend:

How to Use This Guide

This guide is designed to help you navigate and maximize your Cyber Realm Training Kit effectively. Follow these steps to get started:

- 1. Read the Game Instructions** - Understand the rules, turn structure, and how to engage in gameplay.
- 2. Explore the Training Scenario Booklet** –Dive into realistic cyber threats! The booklet will walk you through real-world situations, offering valuable insights into how to respond to each scenario.
- 3. Choose Your Training Mode -**
 - Red Team vs. Blue Team – Simulate cyber attacks and defense tactics.
 - Scenario Mode – Work through structured training exercises to reinforce learning.
- 4. Use the Industry-Specific Training** – Tailor your approach based on the specialized content for Government, Energy, Medical, and Financial sectors.

Scan the QR code inside to begin. Choose your role. Learn tactics. Defend systems. Welcome to the frontlines of cybersecurity training!



CYBERREALMTCG.COM



Table of Content

Section 1: The Basics

Anatomy of Cyber Realm	2
Card Types.	4
Cyber Range Setup.	8

Section 2: Important Concepts

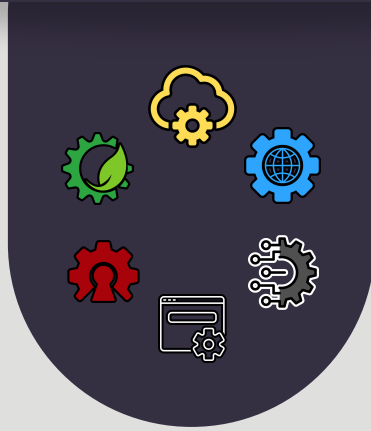
Turn Structure.	11
Game Actions.	16
Winning and Losing Conditions. . .	21
Training Scenarios.	25

Section 3: Deck Building

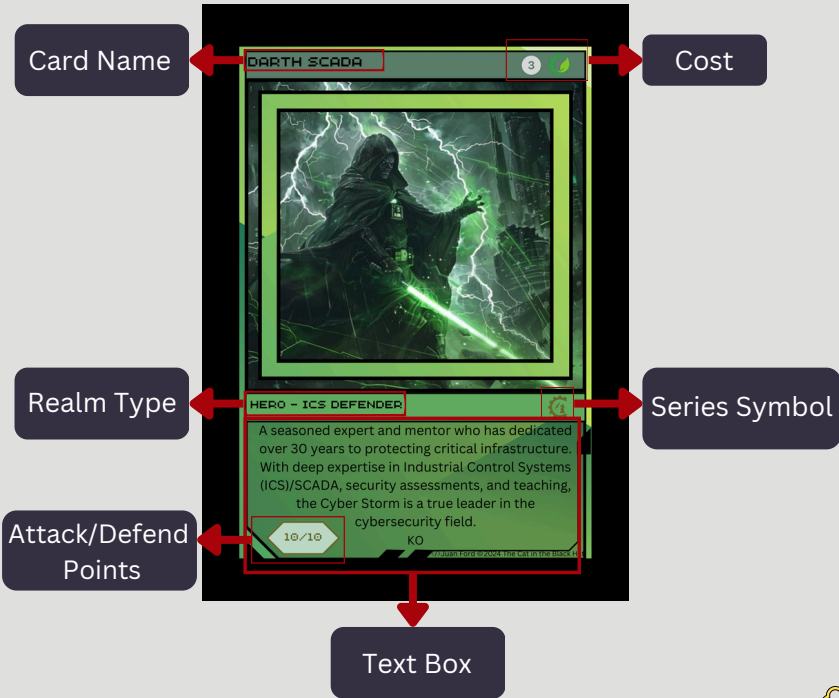
Deck Composition Rules	26
Strategy.	27
Themed Decks.	30

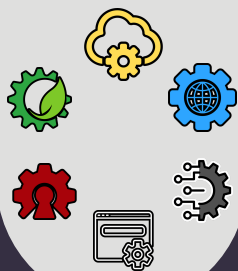


Section 1: The Basics



Anatomy of Cyber Realm Card






Card Name

- Description: The card's name is at the top of the card and identifies its unique function or character within the game. It represents either an offensive or defensive tactic, tool, attack, or hero. For example, a card might be called "Phishing Attack" or "Firewall Protection."
- Purpose: Helps players identify the card quickly and understand its role in gameplay.


Realm Type

- Description: The realm type specifies which Cyber Realm the card belongs to. There are six realms in your game: Cloud Security  Network Security  Endpoint Security 

Internet Security  App Security  Infrastructure Security 

- Purpose: This helps categorize the card and often influences the card's strategy or use during gameplay. Players may focus on certain realms for specific types of attacks or defenses.

Attack/Defend Points

- Description: These are numerical values that determine the effectiveness of a card's action in gameplay. For attack cards, these points represent how powerful the attack is, while for defense cards, they show how strong the defense is against incoming attacks. 

- Purpose: The attack and defense points are crucial for resolving conflicts between players, deciding whether an attack succeeds or whether a defense holds

Text Box



- Description: This box contains a detailed description of the card's special ability or effect, which can influence gameplay. It might describe how the card interacts with other cards, any additional rules or actions it can trigger, or special conditions for its use.
- Purpose: Provides additional information that gives the card its strategic value. It's essential for players to read and understand this part, as it can change the flow of the game

Series Symbol

- Description: The series symbol represents the specific series or edition of the card. It can be a small icon or symbol, often located at the center right of the card.
- Purpose: Helps players quickly identify the card's set and can be useful for organizing cards within a collection. It can also indicate the rarity or version of the card (e.g., common, uncommon, rare, or legendary).

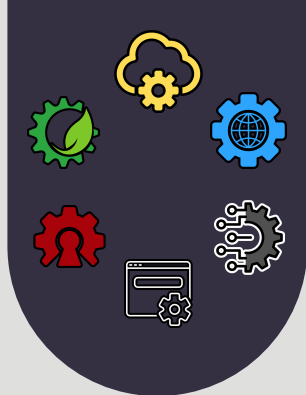
Common =  Uncommon =  Rare =  Legendary = 

Cost

- Description: The cost is represented by a number or symbol, often in the top right corner, indicating how many resources (realm cards) are required to play the card. Some cards may have a higher cost to use, while others may be cheaper.  
- Purpose: The cost is a strategic element in gameplay. It forces players to manage their resources wisely and adds a layer of complexity to how cards are played.



Card Types



Realms

Provide resources for playing other cards, some have special abilities.



Operators

Have attack/defense values and stay on the board to attack and defend.



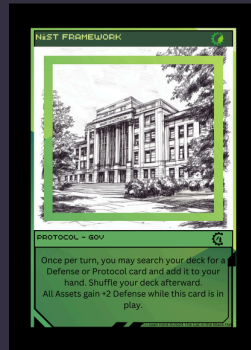
Tools

One-Time effects that are played and discarded immediately.



Protocols

Continuous effects that last multiple turns.



Assets

Important targets in the game that players attack or defend. Some generate benefits.





Events

Large-scale changes to the game state, played and discarded after resolving.



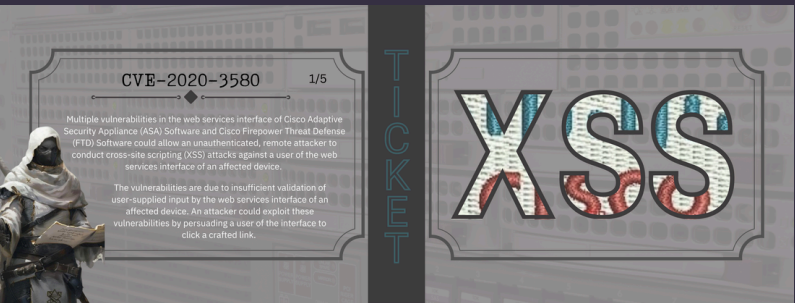
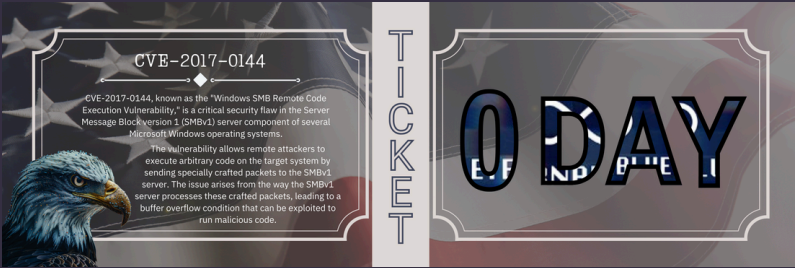
Attack/Defend

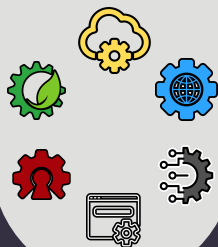
One-time offensive/defensive actions that boost an attack/defend card that exploits/mitigates in the game.



Special CVE Collectible Cards

Unique, limited-edition booklet cards representing real-world CVEs (Common Vulnerabilities and Exposures) with historical significance in cybersecurity. These add extra depth and strategy to gameplay.





Cyber Range Setup

Play Area (Active Cards Zone)

Discard

Deck

Realm Zone

Hand





Deck

- Description: Your deck consists of 60 cards, built before the game starts. It contains a mix of Realms, Operators, Tools, Protocols, Assets, Events, and Attack/Defend cards to create your strategy.
- Placement: The deck is placed face-down in your Deck Zone on the board. Players draw from this deck at the start of their turn.

Hand

- Description: The hand consists of cards drawn from your deck that are available for use. At the start of the game, players draw 7 cards.
- Limit: Players can hold as many cards as they want, but at the beginning of their turn, they must discard down to 7 cards if they exceed this number.
- Usage: Cards in hand can be played onto the board during the appropriate phase of the turn.

Discard Pile

- Description: This is where used, destroyed, or discarded cards go.
- Placement: The discard pile is placed next to the deck and is face-up. Some cards or abilities may allow players to retrieve cards from the discard pile.



Realm Zone

- Description: This is where players place their Realm Cards to establish their cyber environment. Each player can have up to 7 realms in play at a time.
- Function: Realms provide the foundation for deploying other cards, such as Operators, Tools, and Assets, and may grant special effects. Some cards require a matching realm type to be played.
- Example: A “Firewall” tool card may only be played if a Network Security Realm is in play.

Play Area (Active Cards Zone)

- Description: This is where active cards (Operators, Tools, Assets, Attack/Defend cards) are played onto the board.
- Attackers’ Play Area: This is where offensive cards (malware, exploits, attack actions) are placed.
- Defenders’ Play Area: This is where defensive cards (firewalls, endpoint protection, mitigation actions) are played.
- Interaction: Cards in this zone actively engage in combat, defend assets, or trigger effects.

Life Points

Each player starts the game with 20 life points by default. The goal is to reduce your opponent’s life points to 0 through attacks, card effects, and other strategies. If a player’s life points reach zero, they lose the game.



Section 2: Important Concepts



Turn Structure

Each turn follows a six-phase structure, with distinct paths for Attackers (Red Team) using the Cyber Kill Chain and Defenders (Blue Team) using MITRE ATT&CK. Players will need to account for Realm costs to deploy cards and take actions.

Phase	Attacker (Red Team) – Cyber Kill Chain	Defender (Blue Team) – MITRE ATT&CK
1. Draw Phase	Draw 1 card.	Draw 1 card.
2. Setup Phase	Deploy Tools, Protocols, or Assets.	Deploy Tools, Protocols, or Assets.
3. Execution Phase	Perform Recon, then launch Attacks.	Perform Detection, then launch Responses.
4. Impact Phase	Determine the success or failure of attacks.	Determine mitigation success or failures.
5. Recovery Phase	Establish persistence or escalate.	Recover and reinforce defenses.
6. End Phase	Discard if necessary and end turn.	Discard if necessary and end turn.

Detailed Breakdown Of Each Phase

1. Draw Phase (Both Players)

- Each player draws 1 card from their deck.
- If the deck is empty, shuffle the discard pile into a new deck.

2. Setup Phase (Both Players)

Players may deploy new cards into play during this phase.

- Deploy Tools, Protocols, Assets, or Realms onto the battlefield.
 - Realm Costs Apply: Players may only deploy cards that their available Realms can support. If a card requires multiple Realms, players must ensure they have the necessary resources.
- **Attackers (Red Team):**
 - Deploy Tools (exploit kits, malware, phishing kits).
 - Activate Protocols (botnets, C2 servers, spear-phishing frameworks).
 - Position Assets (compromised hosts, stolen credentials).
 - Play or swap Realms (cloud, on-prem, ICS, etc.).
 - **Defenders (Blue Team):**
 - Deploy Tools (firewalls, IDS/IPS, SIEM logs).
 - Activate Protocols (zero-trust, access controls, endpoint monitoring).
 - Position Assets (critical infrastructure, user accounts, endpoints).
 - Play or swap Realms (data centers, hospitals, financial networks).

3. Execution Phase (Attack & Defense Actions)

This is where players take their core actions, following either the **Cyber Kill Chain** (Attackers) or **MITRE ATT&CK** (Defenders).

- **Attackers (Red Team) – Cyber Kill Chain:**
 - **Reconnaissance:** Gather intelligence on the defender's setup.
 - Play scanning cards to identify vulnerabilities.
 - Use OSINT or social engineering cards for phishing/spear-phishing.
 - **Weaponization & Delivery:** Prepare and launch the attack.
 - Use exploit cards to target vulnerabilities.
 - Deploy malware, ransomware, or rootkits.
 - **Exploitation & Installation:** Gain access and execute payloads.
 - Trigger remote code execution (RCE), privilege escalation, or backdoors.
 - Establish persistence using C2 communication channels.
 - **Command & Control / Actions on Objective:** Achieve the attack goal.
 - Exfiltrate data, encrypt files, or destroy critical assets.

- **Defenders (Blue Team) – MITRE ATT&CK:**
 - **Detection & Analysis:** Identify potential threats.
 - Activate threat intelligence and logging tools.
 - Identify malware, suspicious network activity, or unauthorized access.
 - **Containment & Response:** Block or mitigate the attack.
 - Use incident response tools to isolate compromised assets.
 - Deploy endpoint protection and patch vulnerabilities.
 - **Eradication & Recovery:** Remove the threat and restore security.
 - Play rollback cards to restore system integrity.
 - Harden security by implementing new policies or security controls.

4. Impact Phase (Resolution & Consequences)

- If an attack is successful → The attacker executes their objective (data breach, ransomware, exfiltration, destruction).
- If the defender successfully blocks → The attack is mitigated or contained, preventing escalation.

5. Recovery Phase (Both Players)

- **Attackers (Red Team):**
 - Establish persistence through hidden backdoors.
 - Pivot to new targets if access is lost.
 - Deploy follow-up attacks if undetected.
- **Defenders (Blue Team):**
 - Deploy new security measures (patches, hardened defenses).
 - Activate forensics & threat-hunting to remove hidden threats.
 - Implement new compliance and incident response actions.

6. End Phase (Both Players)

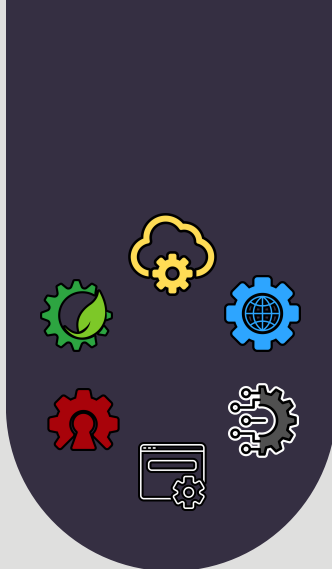
- Players discard excess cards (if over 7).
- Any end-of-turn effects trigger.
- The turn passes to the opponent.

Turn Flow Summary

1. **Draw** – Draw 1 card.
2. **Setup** – Deploy new tools, realms, and assets.
3. **Execution** – Attackers follow the Cyber Kill Chain, defenders follow MITRE ATT&CK.
4. **Impact** – Determine attack success or failure.
5. **Recovery** – Reinforce or escalate.
6. **End** – Discard and pass turn.



Game Actions



1. Playing Cards

To play cards in Cyber Realm, players need to meet certain conditions, such as having the required Realms and sufficient resources.

Action: Play Card

How to Play:

- From your hand, choose a card to play.
- Ensure you have enough Realms (resources) to pay for the card's cost.
- Place the card into the play area (field) and follow the effects or instructions on the card.
- Some cards may require you to sacrifice other cards or specific Realms to activate.

2. Activating Abilities

Cards may have abilities or effects that can be activated when certain conditions are met. This could involve launching attacks, triggering defense, or altering the game state.

Action: Activate Ability

How to Activate:

- After you've played a card, you may have the option to activate its ability (some abilities are passive and trigger automatically, while others require player action).
- Some abilities may need Realms or other cards to be active or in the play area to work.
- Important: Some abilities may cost additional resources to activate.

16

3. Attacking

Attack actions are where players initiate offensive moves to breach defenses or damage the opponent's assets. Attack actions are driven by the Cyber Kill Chain for Attackers and MITRE ATT&CK for Defenders.

Action: Attack

How to Attack:

- Attackers can target a Defender's Assets (e.g., endpoints, servers).
- Depending on the card used, attacking might involve direct damage (e.g., malware) or status effects (e.g., exfiltration).
- Attackers may need to pay Realm costs for tools or actions that launch an attack.

4. Defending

Defending is where players can block or prevent attacks from succeeding. Defensive actions are represented by Tools and Protocols used to contain, eradicate, or mitigate attacks.

Action: Defend

How to Defend:

- Defenders can deploy or activate cards that block or neutralize incoming attacks.
- Defenders may have the opportunity to activate tools like firewalls, IDS/IPS, or endpoint protection.
- Some defense cards are automatically triggered when specific conditions are met, while others need to be activated manually.

5. Resolving Effects

Many cards have ongoing or immediate effects. Resolving effects means figuring out the consequences of each action taken during the turn.

Action: Resolve Effect

How to Resolve Effect:

- When an attack, defense, or ability is triggered, you must resolve its effects as stated on the card. This may include damage to life points, status conditions, or temporary advantages (like control of a Realm).
- The effects will resolve either immediately or over time (depending on the card and action).
- Some effects require players to keep track of additional stats, like life points or success rates.

6. Paying Costs

In Cyber Realm, cards often require the player to spend Realms (resources) to play or activate.

Action: Pay Realm Costs

How to Pay Resolve:

- When a card is played or an action is performed, the player must check if they have the required Realms to meet the card's cost.
- Some actions may require multiple Realms to activate or combine specific types of Realms (e.g., cloud + data center).
- If a player cannot meet the required Realm cost, they cannot play or activate the card. This creates a resource management strategy for players.

7. End-of-Turn Effects

At the end of each turn, players must account for any end-of-turn effects or abilities that trigger after all actions have been resolved.

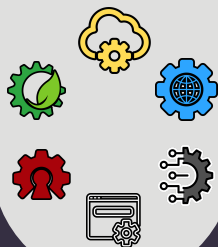
Action: Resolve End-of-Turn Effects

How to Pay Costs:

- Some cards and abilities specify that their effects only trigger at the end of a turn.
- For example, a malware card might continue to deal damage at the end of the opponent's turn, or a backdoor attack might activate, requiring a response.
- Players should also discard excess cards (keeping the hand at 7 cards) and prepare for the next turn.



winning and Losing Conditions



In Cyber Realm, achieving victory or suffering defeat depends on the actions taken throughout the game. Understanding these conditions helps shape strategy and focus on the key objectives of the game.

Winning the Game

There are multiple ways to achieve victory in Cyber Realm, depending on how you manage your offensive and defensive strategies.

Victory Condition 1: Deplete Opponent's Life Points

- **How to Win:**

- Each player starts with 20 life points, and through strategic card play—attacks, effects, and tactics—you aim to deplete the opponent's life points before they do the same to you.
- When an attack, defense, or ability is triggered, you must resolve its effects as stated on the card. This may include damage to life points, status conditions, or temporary advantages (like control of a Realm).
- The effects will resolve either immediately or over time (depending on the card and action).
- Some effects require players to keep track of additional stats, like life points or success rates.

Victory Condition 2: Complete Your Objective (Attackers)

- **How Attackers Win:**

- Attackers may have specific objectives to achieve, such as exfiltrating critical data, deploying malware, or destroying key assets.
- If the Attacker successfully achieves their objective (e.g., exfiltrating a set amount of data), they win the game even if the Defender still has Life Points remaining.
- These objectives are often tied to specific cards or combinations of cards played during the game.

Victory Condition 3: Overwhelm Opponent with Persistence (Defenders)

- **How Defenders Win:**

- Defenders can win by successfully mitigating all attacks and holding off the Attacker's advances until the Attacker can no longer mount an effective offensive.
- This can include maintaining sufficient defensive assets, continuously adapting to the Attacker's tactics, and preventing the completion of attack objectives.
- If the Attacker fails to achieve their attack objectives (like data exfiltration or system destruction) and their Life Points are sufficiently reduced, the Defender can claim victory.

Losing the Game

Losing conditions in Cyber Realm can occur in several ways, either by failure to defend effectively or by exhausting critical resources.

Defeat Condition 1: Life Points Depleted

- **How to Lose:**

- If your Life Points are reduced to zero, you lose the game immediately, regardless of other conditions, Each player starts with 20 life points.
- This could happen if the opponent successfully completes attack actions that deal direct damage or causes ongoing effects that chip away at your Life Points over time.

Defeat Condition 2: Failed Objective (Attackers)

- **How Attackers Lose:**

- Attackers lose if they fail to complete their attack objectives, such as exfiltrating critical data, destroying critical infrastructure, or achieving their ultimate mission goal.
- If the Attacker cannot successfully breach defenses or achieve their attack goals within a set number of turns (determined by game rules or scenario), they lose the game.

Defeat Condition 3: Insufficient Defenses (Defenders)

- **How Defenders Lose:**

- If the Defender's defenses are overwhelmed, and they can no longer prevent the Attacker from achieving their objectives, they lose.
- This could be due to insufficient defensive cards, the failure of key defensive tools, or being unable to mount a successful response to the Attacker's advances.

Draw Condition

In some cases, if both players are unable to win through the standard conditions (i.e., if time runs out or both players reach a standstill), a draw condition may occur. This is typically rare but could arise in specific scenarios (e.g., a stalemate in scenarios with strict time limits or specific objectives).

Winning and Losing Summary

Win Conditions:

- Deplete Opponent's Life Points to zero.
- Complete your objective (Attackers).
- Overwhelm Opponent with Persistence (Defenders).

Lose Conditions:

- Life Points Depleted to zero.
- Failed Objective (Attackers).
- Insufficient Defenses (Defenders).

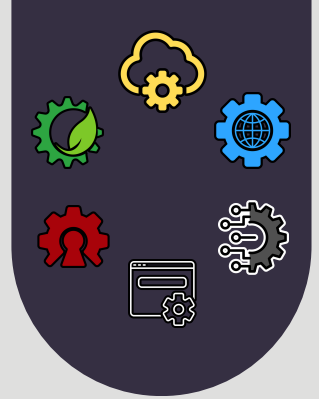
Draw Condition (Rare):

- Both players fail to achieve their victory conditions.



Training Scenarios

Cyber Realm offers Training Scenarios to boost offensive and defensive skills by simulating real-world cyber threats and strategic responses.



Types of Training Scenarios

1. Red Team vs. Blue Team

Players take on the roles of Attackers (Red Team) and Defenders (Blue Team). The Red Team attempts to breach defenses, while the Blue Team defends and mitigates attacks.

2. Scenario Mode

Engage in pre-scripted training exercises that mirror common cyber threats like ransomware or phishing. These scenarios guide players through various attack stages, testing response strategies.

3. Industry-Specific Training

Tailored to specific sectors like government, medical, and financial industries, these scenarios focus on sector-specific threats and vulnerabilities.

Why Use Training Scenarios?

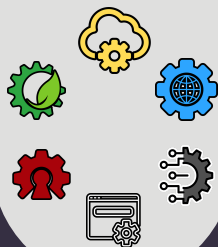
- **Skill Enhancement:** Develop technical and strategic skills.
- **Real-World Experience:** Simulate actual cyber threats.
- **Teamwork:** Build coordination in attack and defense roles.

Section 3: Deck Building



Deck Composition Rules

1. **Deck Size:** Each deck must contain exactly 60 cards.
2. **Card Types:** Players can include any combination of Realms, Operators, Tools, Protocols, Assets, Events, and Attack/Defend cards.
3. **Realm Cards:** At least 10 Realm cards must be included in your deck.
4. **No More Than 4 Copies:** Players can have a maximum of 4 copies of any single card in their deck, except for Basic Realms, which can have an unlimited number.
5. **Special Cards:** CVE Collectible cards are not part of the game deck and are for collection only. They cannot be used during gameplay.
6. **Balance:** It's recommended to balance your deck with offensive, defensive, and support cards for a strategic advantage.



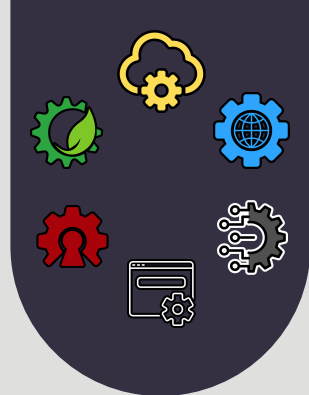
Strategy: Tips for Building a Balanced Deck

1. Balance Offense and Defense

- **Offensive Cards:** Include cards that help you exploit vulnerabilities, attack, and cause disruptions (e.g., Exploit Kits, Malware).
- **Defensive Cards:** Ensure you have tools to block, detect, and respond to attacks (e.g., Firewalls, IDS/IPS, Zero-Trust Protocols).
- Aim for a mix of Attack/Defend cards to ensure adaptability.

2. Include Realm Cards

- You must have at least 10 Realm cards. Choose a variety of cloud, on-prem, and critical infrastructure realms to ensure flexibility in both offense and defense.
- Switching Realms can be a key part of your strategy, so consider how each realm supports your offensive and defensive tools.

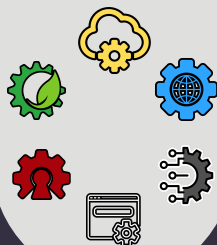


3. Leverage Utility Cards

- Assets: Use Assets to provide long-term advantages, such as Stolen Credentials or Compromised Hosts for attackers, or Critical Infrastructure and User Accounts for defenders.
- Protocols: Add Protocols to set up long-term strategies, like Botnets for attackers or Endpoint Monitoring for defenders.

4. Consider Cost and Resources

Remember that some cards have higher Realm costs. Make sure your deck includes a good balance of low-cost cards (easy to deploy early) and high-cost cards (powerful but requiring more resources).

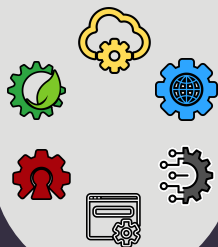


5. Adapt for the Meta

- Stay flexible and adapt your deck depending on your playstyle and the types of opponents you face. A solid understanding of the Cyber Kill Chain (for attackers) or MITRE ATT&CK (for defenders) will help you adjust your strategy.

6. Avoid Deck Clutter

- Keep your deck lean and focused. Too many cards can make it harder to execute your strategy and may leave you with excess cards in hand.



Strategy: Tips for Building a Balanced Deck

1. Balance Offense and Defense

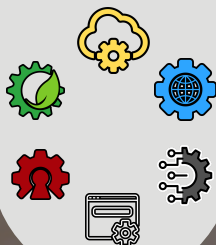
- **Offensive Cards:** Include cards that help you exploit vulnerabilities, attack, and cause disruptions (e.g., Exploit Kits, Malware).
- **Defensive Cards:** Ensure you have tools to block, detect, and respond to attacks (e.g., Firewalls, IDS/IPS, Zero-Trust Protocols).
- Aim for a mix of Attack/Defend cards to ensure adaptability.

2. Include Realm Cards

- You must have at least 10 Realm cards. Choose a variety of cloud, on-prem, and critical infrastructure realms to ensure flexibility in both offense and defense.
- Switching Realms can be a key part of your strategy, so consider how each realm supports your offensive and defensive tools.

Themed Decks:

Specializing in Realms or Cyber Tactics



1. Focus on Specific Realms

Build your deck around a particular Realm type.

Cryptomancers (Cloud Security)

Cryptomancers are technomagical wizards who manipulate cloud environments, virtualized systems, and digital constructs. They harness encrypted spells, AI-driven security, and cloud-based enchantments to wield immense power over distributed computing systems.



31

Net Pirates (Internet Security)

Net Pirates sail the vast digital ocean, navigating through the web, seizing control of domains, and exploiting online pathways. They specialize in manipulating internet traffic, securing or infiltrating web services, and harnessing the power of distributed networks to claim their treasure.



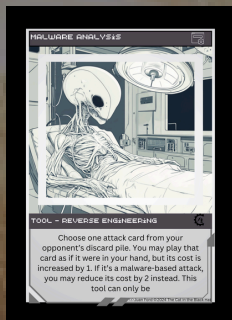
Shadow Nodes (Network Security)

Shadow Nodes thrive in the hidden corridors of cyberspace, where networks interconnect. These mysterious creatures manipulate traffic flow, establish hidden pathways, and control access points with stealth and precision. They move through digital shadows, unseen but always present.



Code Invaders (Application Security)

Code Invaders are alien entities fluent in the language of programming. They reshape applications, exploit or reinforce software, and alter the fabric of digital interactions. Their expertise lies in code manipulation, application behavior, and software integrity.



Cyber Knights (Endpoint Security)

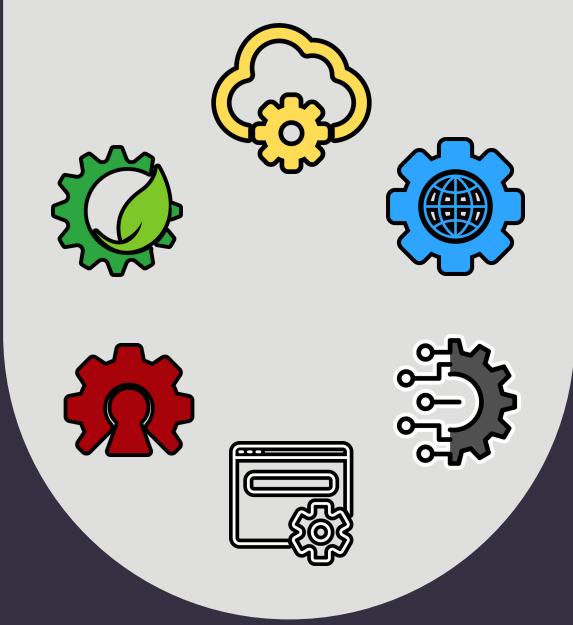
Cyber Knights are armored warriors of cyberspace, protecting or attacking individual devices, workstations, and personal technology. They stand at the frontlines, ensuring device integrity, system protection, and user security while wielding powerful digital weaponry.



Cyber Ninjas (Infrastructure Security)

Cyber Ninjas move in the shadows of critical systems, where the backbone of cyberspace is built. Their expertise lies in securing or infiltrating industrial control systems, IoT devices, and physical-digital infrastructure with precision and stealth. Each faction specializes in its own domain, influencing the strategies and tactics players use in Cyber Realm!





Thank You

Visit Us

CyberRealmTCG.com



