WATER SECTOR EDITION

RULEBOOK

A Red Team vs. Blue Team cybersecurity card game set inside a water utility.

Defend the water. Walk the cyber kill chain. The system is the prize.

PLAYERS	TEAMS	AGES	TIME
2–6	**Red vs. Blue**	**13+**	**30–45 min**

GOAL OF THE GAME

Red Team breaks into a water utility and tries to disrupt service. **Blue Team** stands up the utility's assets and defends them with the five functions of the NIST Cybersecurity Framework. The scoreboard is **SCP**.

WHAT IS SCP?

SCP stands for **System Control Points** — the operational health of the water system, tracked from 20 down to 0. Blue wants to keep SCP high. Red wants to drive SCP down into Service Disruption.

RED WINS IF…

SCP reaches Service Disruption (2–0) at any time.

BLUE WINS IF…

SCP is 7 or higher when the turn cap is reached.

ASYMMETRY BY DESIGN

This is not a mirror match. Red races a timed attack; Blue absorbs, detects, and recovers. The tension between an attacker's tempo and a defender's trade-offs is the game — and the lesson.

TEAMS, PLAYERS & SETUP

Cyber Realm is always **Red Team** vs. **Blue Team**. From 2 to 6 players split across the two teams. Teammates share their team's cards, decisions, and strategy.

PLAYERS	TEAM SPLIT
2 players	1 Red, 1 Blue.
3 players	2 v 1 (either side takes the extra player).
4 players	2 v 2.
5–6 players	Split as evenly as possible.

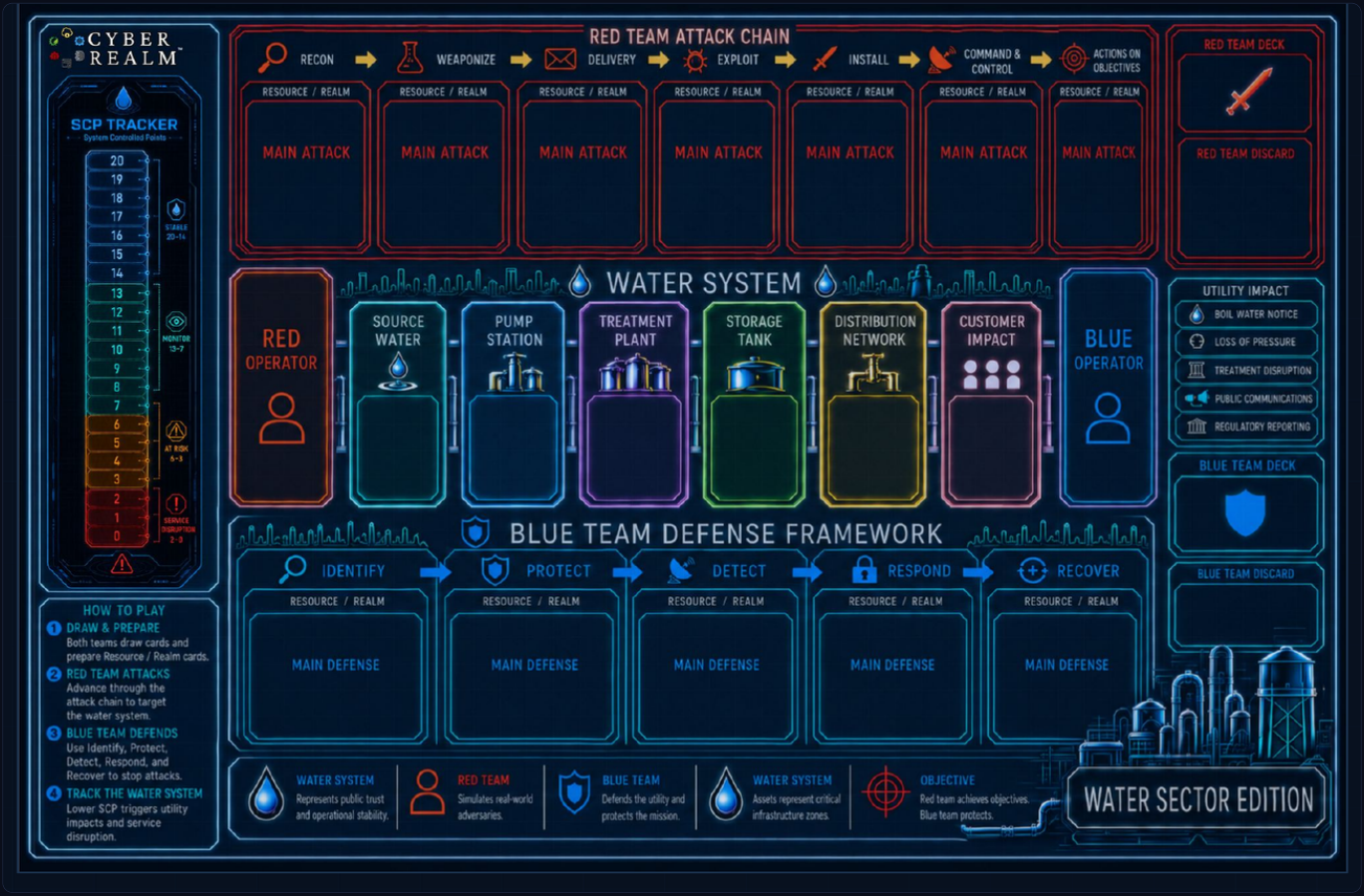
SETUP

1. **CHOOSE SIDES & DECKS**
   Pick a Red threat tier and a Blue org tier (Script Kiddie / Hacktivist / Nation-State vs. Small / Medium / Large Org). Place both Objective cards face-up.
2. **SET THE GAUGE**
   Place the SCP marker at 20 — the top of Stable.
3. **SHUFFLE & DRAW**
   Each team draws 7. One mulligan allowed if you have no Realm cards.
4. **FIRST TURN**
   Blue goes first and skips their first Draw.

> **DECKS**
> Demo games use smaller prebuilt decks. Full play uses the Red 162-card pool and the Blue 162-card pool (324 cards total). Higher tiers include all lower-tier cards plus their own.

THE PLAY MAT

One double-sided mat holds the whole game: Red's attack chain on top, Blue's NIST defense on the bottom, the shared Water System in the middle, and the SCP gauge down the left.



TOP — RED ATTACK CHAIN

Seven phase slots, Recon to Actions on Objectives, each with a Resource/Realm row and a Main Attack row.

BOTTOM — BLUE DEFENSE

Five NIST slots, Identify to Recover, each with a Resource and Main Defense row.

CENTER — WATER SYSTEM

Six zones (Source → Customer Impact) flanked by the Red and Blue Operator zones, where combat happens.

LEFT — SCP TRACKER

20 down to 0, in four bands: Stable / Monitor / At Risk / Service Disruption.

CARD TYPES & ANATOMY

Card types: **Realm** (resources), **Asset**, **Operator**, **Hero**, **Tool**, **Protocol**, and **Event**. Most cards show up to five things.

PUMP STATION — A BLUE ASSET

NAME + COST

The card name runs across the top. The icons near the corner show the card's required Realm/resource cost. Each icon must be paid with one matching resource unless the card says otherwise. The card frame and icons also help show the card's Realm or category.

TYPE LINE

The card's subtype/subclass plus its Realm or category — e.g. Asset – Cyber Systems (AWIA-C), Asset – Storage (AWIA-ST), Tool – Network, Operator – Nation-State, Protocol – Protect.

RULES TEXT

What the card does when it's played or while it's in play.

PHASE / FUNCTION

Red cards show an Attack-Chain phase; Blue cards show a NIST function.

STAT LINE — ATTACK / DEFENSE

Operators, Heroes & Assets only. *Example: an APT at 10/9 attacks for 10 and has 9 Defense.*

CARD COST EXAMPLE

Low Orbit Ion Cannon — a Red Tool, not the Pump Station shown above — requires 1 Network resource to play.

CONNECTION LINE

Many Water assets list a Connection. Connected assets that are both active strengthen each other.

RULE OF THUMB

A healthy asset survives one hit and falls to a two-card combo — giving the defender a reaction window.

REALMS & PAYING COSTS

Realm cards generate resources in six colors that mirror an enterprise attack surface. Play a Realm to your budget; spend the budget on cards.

REALM	COVERS
ENDPOINT	Laptops, workstations, servers.
APPLICATION	Portals, APIs, billing, SCADA UI.
NETWORK	Segments, ports, traffic.
INTERNET	The exposed perimeter.
CLOUD	Hosted identity, storage, services.
INFRASTRUCTURE	Pumps, valves, PLCs, water.

PAYING A COST

To play a card, you must have the matching Realm resources available. Each Realm icon in a cost must be paid with one resource of that color; a gray (generic) cost may be paid with any color. Cards with no cost are free. Wild resources count as any color.

STAYS IN PLAY VS. ONE-SHOT

Cards that stay in play (Assets, Operators, Protocols) keep their resources committed until they leave play. One-shot cards (Tools, Attacks) are discarded after use, and their resources free up at the start of your next turn.

EVENTS

Events resolve once and are discarded. If an Event shows a cost, pay it normally. If it shows no cost, it is free.

WHY COLORS MATTER

The six Realms are the domains a defender must fund and an attacker must cover. Starved on a color? That's the lesson — you under-invested there.

TURN SEQUENCE

Teams alternate turns. Each turn has five steps, in order.

1. **DRAW**
   Draw 1 card at the start of your turn. Your hand limit is 7. (The first player skips their very first Draw.)
2. **RESOURCES**
   Play up to one Realm card and resolve any "generate resource" abilities. Resources spent last turn on one-shot cards refresh now; resources locked by cards still in play stay locked.
3. **MAIN**
   Play cards by paying their cost. Your Operators may attack. Red follows the Attack Chain; Blue may play any NIST function.
4. **RESOLVE & REACT**
   Apply damage and effects. The defender may play reveal / reduce / cancel cards from their free (unspent) resources.
5. **END**
   Resolve end-of-turn triggers (SCP gains, per-turn damage, scenario timers). Discard down to 7 cards. Check win conditions.

TURN CAP

Standard play ends after turn 20. Demo and conference play uses a cap of 10 turns.

PLAY THE DIGITAL DEMO

Practice against a Script Kiddie AI, free in your browser: play.cyberrealmtcg.com

RED TEAM — THE ATTACK CHAIN

Red's seven phases follow the classic cyber kill chain. The chain is a strategy, not a straitjacket.

RECON	WEAPONIZE	DELIVERY	EXPLOIT	INSTALL	C2	OBJECTIVES
Find targets	Prep payload	Reach target	Break in	Persist	Maintain	Impact

FLEXIBLE ORDER + CHAIN BONUS

Red may play attack-chain cards in any order, as long as each card's text requirements are met. When you play the next phase *in sequence*, that card earns a Chain Bonus — choose one as you play it: cost 1 less, +1 damage, +1 Attack, or draw 1.

OBJECTIVE RESTRICTION

Actions on Objectives cards may only be played if Red has C2, Persistence, or a Compromised Asset. You can't cause impact without a foothold.

OPERATOR COMBAT

Operators have an Attack / Defense stat. Once per turn, each Operator or Hero may attack. The defending team may defend with an Operator or Hero. Both cards deal damage to each other's Defense simultaneously. If the attack is undefended, the defending team loses SCP equal to the attacker's Attack, to a maximum of 4 SCP per Operator or Hero per turn. Heroes are treated as Operators for combat and card effects.

EXAMPLE ATTACK-CHAIN CARDS

PASSWORD CRACKER · WEAPONIZE

FIREWALL MISCONFIGURATION · OBJECTIVES

BLUE TEAM — NIST DEFENSE

Blue's cards carry one of five NIST CSF functions. Unlike Red, Blue is not order-locked — defenders prepare and respond out of sequence.

IDENTIFY	PROTECT	DETECT	RESPOND	RECOVER
See your surface	Harden	Reveal early	Stop it	Restore

CHEAP EARLY, EXPENSIVE LATE

Identify, Protect, and Detect stop attacks before they cost SCP. Recover works after the damage — slower and pricier, just like real life. Front-load the left of the framework.

HOLD A RESERVE

Reaction cards (reveal / reduce / cancel) are played on Red's turn and paid from your free, unspent resources. A defender who spends everything every turn has no answers when the exploit lands.

DAMAGE & STATES

Defense is an asset's health, in counters. At **0 Defense** an asset is **Destroyed** and discarded. A successful Exploit marks a specific asset **Compromised** — Red has access (not destroyed), which enables follow-on attacks. Recovery on that asset clears the Compromised state.

EXAMPLE NIST DEFENSE CARDS

ENCRYPTED BACKUPS · RECOVER

PATCH MANAGEMENT · PROTECT

THE WATER SYSTEM & AWIA-STYLE ZONES

The heart of the game. Blue's water assets carry **AWIA-style classifications** and a Connection line — connected, active assets strengthen each other.

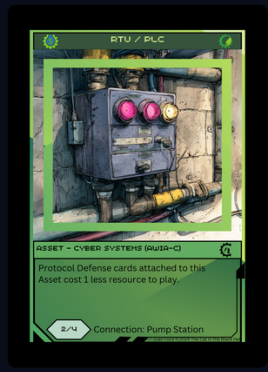
BOARD ZONE	EXAMPLE CARD	LABEL
Source Water	Well	AWIA-S
Pump Station	Pump Station	AWIA-D / Conveyance
Treatment Plant	Chlorination Unit	AWIA-T
Storage Tank	Water Tower	AWIA-ST
Distribution / Control Network	RTU/PLC, SCADA, Gateway	AWIA-C
Customer Impact	Pressure loss, outage, overflow	Consequence

WELL · S

PUMP · D

CHLORINATION · T

WATER TOWER · ST



RTU/PLC · C

CYBER SYSTEMS ARE CROSS-CUTTING

Cyber Systems cards — RTU/PLC, HMI, SCADA, Gateway, Active Directory, and Firewalls — use AWIA-C. These cards may connect to or affect multiple Water System zones, not just distribution. The IT/OT bridge (Gateway ▸ SCADA Web Interface ▸ RTU/PLC ▸ Pump Station) is the path Red most wants to cross.

DISCLAIMER

AWIA-style labels in Cyber Realm are simplified educational categories used for gameplay. They are inspired by water utility risk and resilience concepts and are not official regulatory designations.

WINNING, DEMO PLAY & GLOSSARY

SCP BAND	RANGE	STATE
STABLE	20–14	The plant runs normally.
MONITOR	13–7	Pressure on the system; watch closely.
AT RISK	6–3	Degraded service; a near-miss in progress.
SERVICE DISRUPTION	2–0	The system fails — Red wins.

RED WINS

SCP reaches Service Disruption (2–0) at any time.

BLUE WINS

SCP is 7 or higher when the turn cap is reached.

AT RISK (3–6) — TRAINING RESULT

If SCP ends between 3 and 6, the system is At Risk. In training play, treat it as a Red near-miss and discuss which control, one turn earlier, would have changed the outcome.

DEMO PLAY

Use prebuilt ~40-card decks and a turn cap of 10. Warm-up: Script Kiddie vs. Small Org. Main event: Nation-State vs. Large Org.

QUICK GLOSSARY

SCP — System Control Points; the 0–20 health of the water system. · **Realm** — a resource card in one of six colors. · **Resource** — what Realms produce to pay costs. · **Asset** — a card with Defense that holds the board. · **Operator / Hero** — cards that attack and defend. Heroes are treated as Operators for all rules purposes, but represent heroes of the industry. · **Tool** — one-time effect, then discarded. · **Protocol** — continuous effect that stays in play. · **Compromised** — Red has access to an asset (not destroyed). · **Destroyed** — an asset at 0 Defense; discarded. · **Chain Bonus** — the reward for playing the next kill-chain phase in sequence. · **AWIA-style Category** — Cyber Realm's educational shorthand for water-utility asset areas; not official regulatory designations.