

Scenario 1: Ransomware Attack on a Power Grid

Narrative:

The grid is under attack. SCADA servers are locking up, RTUs are going offline, and the clock is ticking. Can you stop the ransomware before the lights go out?

Active Realm: Energy & Utilities

Key Assets:

- SCADA Master Server
- Vulnerable Linux Server
- Gateway

Starting Hands:

- **Attacker:** Ransomware Gang (Operator), Ransomware (Attack Card)
- **Defender:** Incident Response and any three cards in deck

Setup:

1. Both players must have a least one realm card in play before playing operators, attacks, defenses, or tools.
2. Place all three key assets face-up in play
3. Attacker starts first

Questions to Think About

- How would a ransomware gang follow the cyber kill chain to carry out this attack, and how could defenders break it?
- when should either side pivot, attackers to a new asset or defenders to a new strategy to win?

Win Condition:

- Defenders win if SCADA operations are restored within 6 turns.
- Attackers win if the grid remains compromised after 6 turns.

Scenario 2: SSH Attack on Vulnerable Linux Server

Narrative:

A threat actor has discovered a vulnerable Linux server with weak SSH credentials. They are attempting to brute-force access and establish persistence. Can the defender detect and block the intrusion before privilege escalation occurs?

Active Realm: Energy & Utilities

Key Assets:

- Vulnerable Linux Server

Starting Hands:

- **Attacker:** APT (Operator), SSH Exploit (Attack Card).
- **Defender:** Firewall, and any three cards in deck.

Setup:

Place the vulnerable Linux Server asset card in play. The attacker begins with recon in play and may attempt to compromise the server on turn one if possible.

Questions to Think About

- What steps would an attacker take to compromise the server, and which detection/mitigation strategies would be most effective?
- How would you prioritize defensive actions to protect critical assets while maintaining uptime?

Win Condition:

- Defender wins if the server remains uncompromised for 5 turns or if the attacker's operator is neutralized.
- Attacker wins if they gain root access (compromise the server) and maintain persistence for 2 consecutive turns.

Scenario 3: Data Breach

Narrative:

A data breach is underway in an ICS network. Attackers aim to steal sensitive data while avoiding detection. Can defenders stop them in time?

Active Realm: Energy & Utilities

Key Assets:

- SCADA Master Server
- Gateway

Starting Hands:

- **Attacker:** Choose 1 Insider Threat (Operator), APT (Operator), or Hacker (Operator), plus an attack card for exfiltration or intrusion.
- **Defender:** Firewall/IPS Protocol, any three additional cards from deck.

Setup:

- Place the ICS Gateway in play as the main asset.
- Attacker deploys one operator to start intrusion.
- Defender draws 4 cards and prepares defenses.

Questions to Think About

- How might attackers steal data, and what steps can you take to stop them?
- Which defenses would you prioritize first, and why?

Win Condition:

- Defender wins: Prevent sensitive data exfiltration for 6 turns or reduce attacker SCP to 0.
- Attacker wins: Exfiltrate sensitive operational or design data or reduce defender SCP to 0.