

Defend Against Ransomware Attack

(Cyber Kill Chain)

Asset

Recon

Weaponize

Delivery

Exploit

Install









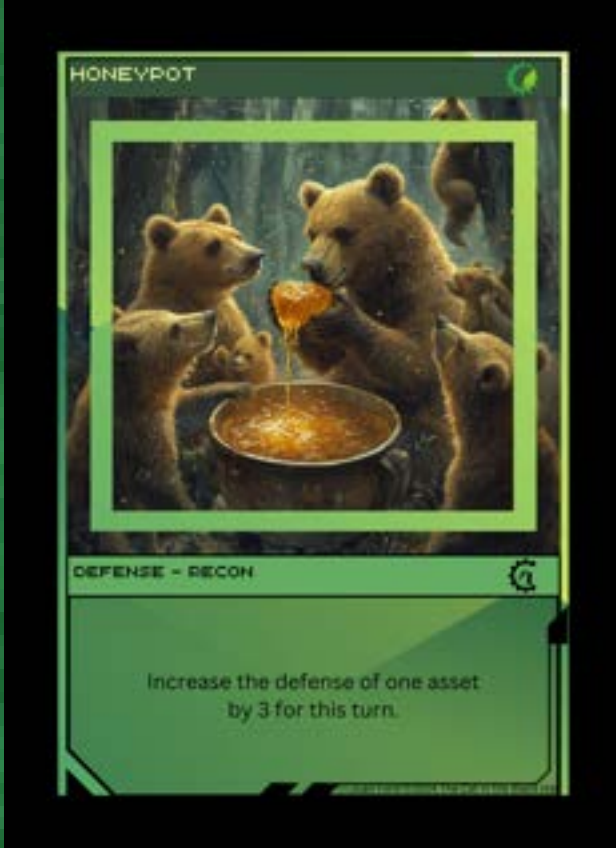






C2

Actions



Defend Against SSH Attack

(Cyber Kill Chain)

Asset	Recon	Weaponize	Delivery	Exploit	Install	C2	Actions		
	 <p>PORT HARDENING</p> <p>DEFENSE - RECON</p> <p>Increase the defense of one asset by 2 for this turn.</p>	 <p>RATE LIMITS LOGINS</p> <p>DEFENSE - WEAPONIZATION</p> <p>During the Weaponize or Delivery Phase, if an attacker attempts a brute-force login, they must skip their next attack phase unless they roll a 14 or higher on a d20.</p>	 <p>ACCOUNT LOCKOUT POLICY</p> <p>DEFENSE - DELIVERY</p> <p>After 3 failed login attempts, lock the attacker out for 1 turn.</p> <p>Roll a d20.</p> <p>15+ Block the attack.</p> <p>14 or lower: Reduce attack by 2 points.</p>	 <p>INTRUSION DETECTION SYSTEM</p> <p>DEFENSE - EXPLOITATION</p> <p>When an attacker plays an Exploit card, roll a dice. If you roll 12 or higher, negate the exploit and force the attacker to discard 1 random card from their hand.</p>	 <p>SIEH</p> <p>DEFENSE - EXPLOITATION</p> <p>Draw 1 card. For each exploit or attack card played by the attacker this turn, reduce its attack by 2. If the attacker has no exploit or attack cards in hand, draw an additional card.</p>	 <p>SSH SESSION TIMEOUT</p> <p>DEFENSE - INSTALL</p> <p>Play during the attacker's Weaponize phase.</p> <p>Roll a d20.</p> <p>15+ Force attacker to discard a Weaponize card and end their turn early.</p> <p>14 or lower: Reduce the attack's effectiveness by 2 for this turn.</p>	 <p>SSH KEY ROTATION</p> <p>DEFENSE - C2</p> <p>Roll a d20.</p> <p>15+ Prevent attacker from using old SSH keys; attacker must reattempt login.</p> <p>14 or lower: Attacker can bypass with old SSH keys, reducing defense by 2 for this turn.</p>	 <p>ENCRYPTED BACKUPS</p> <p>DEFENSE - ACTIONS ON OBJECTIVES</p> <p>Roll a d20.</p> <p>11+ restores all lost data.</p> <p>10 or lower: reduces damage by half.</p>	
 <p>EXPOSED LINUX SERVER</p> <p>DEFENSE - ASSET</p> <p>An exposed Linux server configured with weak credentials, leaving it vulnerable to unauthorized access. Attacker can exploit its open SSH service on port 2222 to launch brute force attempts.</p>	 <p>FIREWALL RULE ENFORCEMENT</p> <p>DEFENSE - RECON</p> <p>Increase your asset's defense by 1 for the turn.</p>	 <p>SSH BANNER OBFUSCATION</p> <p>DEFENSE - RECON</p> <p>If the attacker plays a Recon card, they must discard it without effect unless they roll a 15 or higher on a d20.</p>	 <p>STRONG PASSWORD POLICY</p> <p>DEFENSE - WEAPONIZATION</p> <p>Increase the defense of all your asset cards by 2 against brute-force and credential-based attacks.</p> <p>If an attacker attempts a credential-based attack, they must discard 3 card from their hand.</p>	 <p>DISABLE PASSWORD AUTH</p> <p>DEFENSE - DELIVERY</p> <p>Negate any attack relying on password-based authentication. If the attacker does not have an SSH key-based attack in play, their turn ends immediately.</p> <p>Add 2 defense to any asset.</p>	 <p>SECURITY PATCH</p> <p>DEFENSE - EXPLOITATION</p> <p>Play this card when an Exploit card is used.</p> <p>Roll a d20: if you roll 15 or higher, the exploit is fully blocked, and the attacker skips their Weaponize phase. If you roll 14 or lower, the exploit still occurs, but its attack power is reduced by 2.</p>	 <p>FILE INTEGRITY MONITORING</p> <p>DEFENSE - EXPLOITATION</p> <p>Monitor file changes for unauthorized alterations.</p> <p>Roll a d20 during an attack.</p> <p>15+ Block attack and reveal next card.</p> <p>14 or lower: Reduce damage by 3 and detect future changes for 2 turns.</p>	 <p>DISABLE ROOT LOGIN</p> <p>DEFENSE - INSTALL</p> <p>Prevent root login access.</p> <p>Roll a d20.</p> <p>11+ Block the attacker's root access attempt.</p> <p>10 or lower: Reduce attack by 3 points for this turn.</p>	 <p>ZERO TRUST ACCESS</p> <p>DEFENSE - C2</p> <p>Block all unauthorized access attempts, regardless of network origin. Any attack that requires access to an asset is automatically denied unless explicitly verified.</p> <p>Once per turn, reduce the effectiveness of an exploit by 3 during an attack.</p>	 <p>LOG MONITORING</p> <p>DEFENSE - ACTIONS ON OBJECTIVES</p> <p>Reveal the top card of the attacker's deck. If it's an exploit or attack card, prevent its activation for this turn.</p>
 <p>HONEYPOT</p> <p>DEFENSE - RECON</p> <p>Increase the defense of one asset by 3 for this turn.</p>	 <p>HONEYTOKEN</p> <p>DEFENSE - WEAPONIZATION</p> <p>During the Weaponize, reveal the top card of the attacker's deck and decide to discard or leave in deck.</p>	 <p>MULTI-FACTOR AUTHENTICATION</p> <p>DEFENSE - DELIVERY</p> <p>When an attacker successfully bypasses a login attempt, roll a dice. If you roll 10 or higher, negate the attack. If the attacker has a 'Credential Harvesting' or similar setup card in play, they must roll twice and take the lower result.</p>	 <p>THREAT HUNTING</p> <p>DEFENSE - EXPLOITATION</p> <p>Look at the top 3 cards of the attacker's deck. Discard one and return the rest in any order.</p>	 <p>NETWORK SEGMENTATION</p> <p>DEFENSE - EXPLOITATION</p> <p>Roll a d20.</p> <p>11+ Block attack from scanning certain segments.</p> <p>10 or lower: Attacker can scan one segment, but reduces next scan success by 1.</p>	 <p>ENDPOINT DETECTION & RESPONSE</p> <p>DEFENSE - INSTALL</p> <p>Play when an attack targets an asset.</p> <p>Roll a d20.</p> <p>11+ Prevent attack and expose one attacker card.</p> <p>10 or lower: Reduce attack damage by 2 and reveal the top 2 cards of the</p>	 <p>INTRUSION PREVENTION SYSTEM</p> <p>DEFENSE - C2</p> <p>Block one attack per turn. Roll a d20 when an exploit is played.</p> <p>11+ Block the exploit.</p> <p>10 or lower: Reduce damage by 3.</p>	 <p>DATA LOSS PREVENTION</p> <p>DEFENSE - ACTIONS ON OBJECTIVES</p> <p>Block an exfiltration attempt. If an attacker plays a Data Exfiltration card, roll a d20.</p> <p>15+ cancels the attack, 14 or lower reduces its effect by half.</p>		

Defend Against Data Breach

(Cyber Kill Chain)

Asset

Recon

Weaponize

Delivery

Exploit

Install

C2

Actions

