Would you recognize a cyber kill chain as it’s happening? Explore the Account Takeover Kill Chain cyberattack stages and learn how to stop them.

1. **RECONNAISSANCE**
   - **What to Expect**: Identify vulnerabilities, exploit them.
   - **How to Defend**:
     - Implement:
       - Web application firewall
       - Encryption
       - Credential checks against known breaches
       - Strong security policies

2. **WEAPONIZATION**
   - **What to Expect**: Tool or toolset designed.
   - **How to Defend**:
     - Confirm:
       - Whether logins are legitimate users
       - Bot management software is tuned
       - Login endpoints are protected with MFA

3. **DELIVERY**
   - **What to Expect**: Small spike in failed logins.
   - **How to Defend**:
     - Validate:
       - Rate controls
       - MFA
       - User behavior anomalies
       - Advanced detections from bot management software

4. **EXPLOITATION**
   - **What to Expect**: Single request coming from a human; small increase in logins.
   - **How to Defend**:
     - Inspect:
       - User behavior anomalies

5. **ACTION**
   - **What to Expect**: Spike in customer reports of accounts being taken over.
   - **How to Defend**:
     - Monitor:
       - User risk continuously until user logs out

Attacks can’t do anything at scale. For individual attempts, criminals may search for the account owner on social networks.

Possible Attacker Reaction:
- Attack is stopped. Kill chain is disrupted. Very sophisticated bots may temporarily evade detection.
- Attackers may tune bot software if bot is detected.
- Attackers may try another site or buy credentials, since billions are available on the dark web.

Learn how Akamai can help you prevent account takeover.