**Part 4: Blocking Attacks and Crafting Response Actions**

Part 4 focused on blocking attacks and implementing response actions to mitigate threats effectively. Here's a breakdown of what I accomplished and the skills I acquired:

1. **Understanding Attack Patterns:**
   * Explored common attack patterns, particularly the deletion of Volume Shadow Copies, which is a telltale sign of ransomware attacks.
   * Recognized the significance of identifying and blocking specific attack patterns to disrupt malicious activities effectively.
2. **Crafting Blocking Rules:**
   * Leveraging the LimaCharlie platform, I developed detection and response (D&R) rules to detect and block specific attack patterns.
   * Created a rule to detect the deletion of Volume Shadow Copies, a common precursor to ransomware attacks.
   * Configured the response action within the rule to terminate the parent process responsible for the deletion, effectively disrupting the attack.
3. **Testing Blocking Rules:**
   * Within the Sliver C2 session on the victim machine, I executed commands and performed actions that triggered the detection and response rules.
   * Observed the response actions in action, verifying that the parent process was successfully terminated, preventing further malicious activities.

