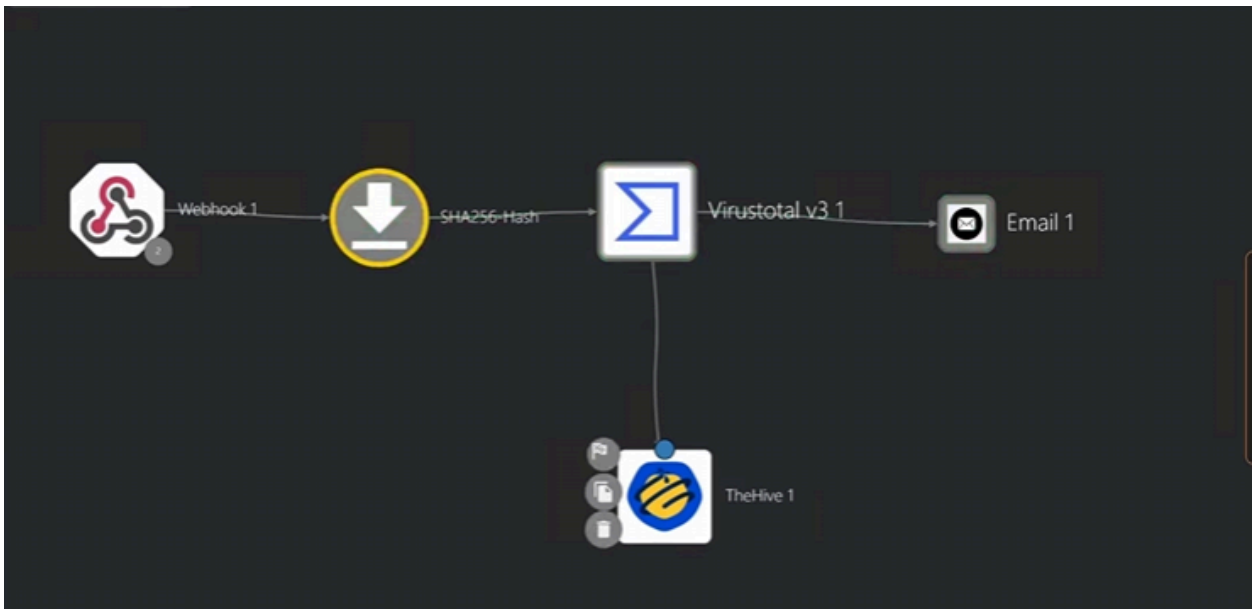
8. Automating Detection-to-Response with Shuffle SOAR

The SOAR pipeline automates enrichment and alert handling.



Workflow Steps:

1. Create a webhook trigger inside Shuffle.
2. Add a Regex Extraction step:
    - Pattern extracts SHA256 hashes from the Wazuh alert.
3. Add VirusTotal enrichment:
    - Uses extracted hash
    - Queries threat intelligence
4. Add a TheHive alert creation step:
    - Populates case title, description, severity, artifacts

5. Add an automated email notification:
    - Includes host info
    - Includes hash reputation
    - Links to the new TheHive case

This creates an end-to-end automated detection and response flow.