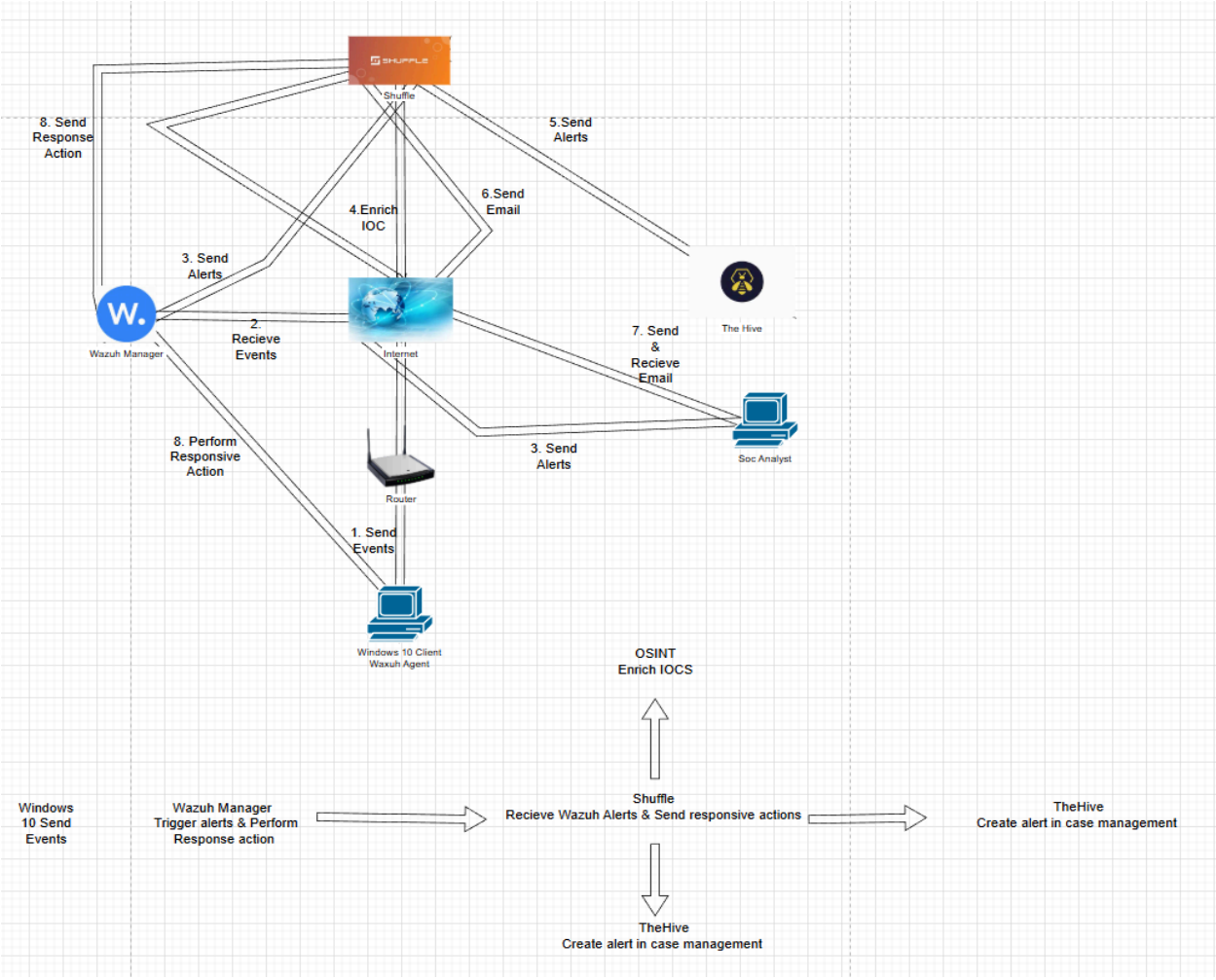
SOC Home Lab – Attack & Defense Simulation Architecture

The SOC Home Lab simulates a real-world security operations environment using virtual machines, SIEM technology, endpoint telemetry, and automated incident response. The environment features dynamic interaction between an attacker or malicious tool (Mimikatz) and the defensive monitoring stack (Sysmon → Wazuh →Shuffle → TheHive).



Architecture Components:

1. **Windows 11 Endpoint (Victim Machine)**
    - Runs Sysmon for detailed event logging
    - Runs Wazuh agent to send logs to SIEM
    - Used to execute simulated attacks (Mimikatz)
2. **Wazuh Manager (SIEM Platform)**
    - Receives Sysmon telemetry from the Windows endpoint
    - Parses logs, applies detection rules, triggers alerts
    - Sends alerts to SOAR via webhook integration
3. **TheHive (Incident Response Platform)**
    - Receives alerts from Shuffle
    - Creates cases with artifacts (hashes, process info, host data)
    - Used to track triage, incident documentation, and remediation steps
4. **Shuffle (SOAR – Automation Layer)**
    - Receives Wazuh alerts from webhook
    - Extracts hashes
    - Performs VirusTotal enrichment
    - Automatically creates alerts in TheHive
    - Sends email alerts to the analyst
5. **VirtualBox Host Machine**
    - Runs the Windows VM
    - Local testing ground for endpoint detections and attacks

6. **Cloud VMs (Vultr, DigitalOcean, etc.)**
    - Host Wazuh
    - Host TheHive
    - Publicly reachable for agent communications (1514, 1515, 9000, etc.)

Workflow Summary:

● Step 1 – Sysmon logs a process creation event
● Step 2 – Wazuh agent forwards event to Wazuh Manager
● Step 3 – Custom rule detects Mimikatz execution
● Step 4 – Wazuh triggers a webhook to Shuffle
● Step 5 – Shuffle enriches data with VirusTotal
● Step 6 – Shuffle creates a case in TheHive
● Step 7 – Analyst receives automated email notification

This architecture mimics a modern enterprise SOC pipeline — endpoint telemetry, SIEM correlation, SOAR automation, and IR case management.