**Wazuh + AlienVault OTX — IOC Enrichment & Hunting (GitHub README)**

**Objective:** Practical walkthrough on feeding AlienVault OTX indicators into Wazuh (v4.12), enriching alerts with IOC context, and performing a hunt for MITRE ATT&CK T1078 (Valid Accounts). This guide is structured so anyone can reproduce the setup from scratch.

**Summary**

This lab shows how to:

1. Grab IOCs from AlienVault OTX (manual export)
2. Format the list into Wazuh’s CDB lookup format
3. Hook the list into Wazuh for enrichment
4. Add detection rules for IOC hits and T1078 activity
5. Verify the pipeline (logtest, logger, agent events)
6. Simulate activity with Hydra to validate detection

Tested with **Wazuh 4.12** (manager + indexer + dashboard on Debian 22.x, IP 192.168.204.137) and a **Windows 11 VM agent** (192.168.204.138). No use of the old alienvaultotx integrator.

**Requirements**

* Wazuh Manager + Indexer + Dashboard up and running on **Debian 22.x (192.168.204.137)**
* Wazuh Agent deployed to a **Windows 11 VM (192.168.204.138)**
* sudo access on the manager host
* AlienVault OTX account (or access to manually downloaded IOC feeds)
* Install jq for JSON parsing if needed:

sudo apt install jq

**Directory Layout**

We will create the following:

* /var/ossec/etc/lists/otx-iocs.txt → raw IOC list
* /var/ossec/etc/lists/otx-iocs.txt.cdb → compiled lookup file
* /var/ossec/etc/rules/local\_rules.xml → custom detection rules
* Optional scripts for automation (keep outside repo if sensitive)

**Security Reminder**

* Do not commit OTX API keys, credentials, or private configs.
* Use .gitignore to exclude secrets.
* Keep any automation scripts that handle API keys outside of public repos.

**1) Extract IOCs from AlienVault OTX**

1. Log in at <https://otx.alienvault.com/>
2. Subscribe to a Pulse and choose **Export → CSV** (or copy IPs from the UI).
3. Collect IPv4 indicators.

**Example set:**

185.220.101.1

45.33.32.156

207.210.121.148

**2) Format IOC List for Wazuh**

On the Wazuh Manager (Debian 22.x, IP 192.168.204.137):

sudo -s

cat > /var/ossec/etc/lists/otx-iocs.txt <<'EOF'

185.220.101.1:1

45.33.32.156:1

207.210.121.148:1

EOF

* Each line follows the indicator:value format.
* The value can simply be 1 for all.

**3) Compile into CDB File**

Wazuh requires compiled CDB lists.

**Method A: Using Wazuh helper (preferred)**

Check available scripts:

ls -l /var/ossec/framework/scripts | grep cdb

If available, run:

sudo /var/ossec/framework/scripts/wazuh-cdbsync /var/ossec/etc/lists/otx-iocs.txt

This should output: /var/ossec/etc/lists/otx-iocs.txt.cdb.

**Method B: Existing .cdb**

Some packages autogenerate otx-iocs.txt.cdb. If present, just reference that in your rules.

**4) Register the List in ossec.conf**

Edit /var/ossec/etc/ossec.conf and add to <ruleset>:

<ruleset>

<decoder\_dir>ruleset/decoders</decoder\_dir>

<rule\_dir>ruleset/rules</rule\_dir>

<list>etc/lists/otx-iocs.txt.cdb</list>

<decoder\_dir>etc/decoders</decoder\_dir>

<rule\_dir>etc/rules</rule\_dir>

</ruleset>

**5) Custom Rules (local\_rules.xml)**

Add IOC detection and T1078 logic. Edit /var/ossec/etc/rules/local\_rules.xml:

<group name="local,syslog,sshd,">

<!-- IOC match -->

<rule id="100100" level="10">

<if\_sid>5760</if\_sid>

<list field="srcip">etc/lists/otx-iocs.txt.cdb</list>

<description>Source IP present in OTX IOC feed</description>

<mitre>

<id>T1071</id>

</mitre>

</rule>

<!-- Valid Accounts -->

<rule id="100110" level="8">

<match>Accepted password for</match>

<description>SSH successful login — potential Valid Accounts abuse (T1078)</description>

<mitre>

<id>T1078</id>

</mitre>

</rule>

</group>

**6) Validate & Restart**

sudo /var/ossec/bin/wazuh-analysisd -t

sudo systemctl restart wazuh-manager

Check logs:

sudo tail -n 200 /var/ossec/logs/ossec.log

sudo tail -n 200 /var/ossec/logs/alerts/alerts.json

**7) Testing (with Hydra & log injection)**

**A) Hydra attack simulation**

On Debian VM (192.168.204.137) run against Windows 11 agent (192.168.204.138):

sudo apt update && sudo apt install -y hydra

hydra -l admin -P /usr/share/wordlists/rockyou.txt -t 4 ssh://192.168.204.138 -s 22

This will flood SSH login attempts, creating logs that Suricata/Wazuh should detect.

**B) Using wazuh-logtest**

sudo /var/ossec/bin/wazuh-logtest

Sep 05 00:10:15 debian sshd[9999]: Failed password for root from 207.210.121.148 port 4444 ssh2

**C) Using logger**

logger "sshd[1234]: Accepted password for testuser from 203.0.113.5 port 5555 ssh2"

Check alerts:

sudo tail -f /var/ossec/logs/alerts/alerts.json

**8) Wazuh Dashboard Queries**

* IOC hits:

rule.id:100100

* Valid Accounts (T1078):

rule.id:100110

* Combine IOC + login:

rule.id:100100 AND rule.id:100110

**9) Example Evidence Table**

| **Rule ID** | **IP** | **Source** | **Notes** |
| --- | --- | --- | --- |
| 100100 | 207.210.121.148 | OTX Pulse | Known malicious SSH scanner |

**50-word hunt summary:**  
Hydra-generated brute force attempts from known OTX-listed IPs were detected by Wazuh. One simulated login succeeded, mapping to MITRE T1078. This confirms potential credential abuse tied to malicious infrastructure. Recommended response: enforce MFA, reset affected credentials, and expand IOC correlation to lateral movement detection.