Threat Intelligence Integration

Import AlienVault OTX into Wazuh:

Edit Wazuh Configuration:

Commands: sudo mousepad /var/ossec/etc/ossec.conf

Add integration to the configuration file,

```
          <!-- Intergration of Virusvault otxx -->
 <integration>
   <name>otx</name>
   <api_key>1aad0db556711b0d0fdfe3b743d821fafad6e1a6567ea8a2c6c3b5703822edf7</api_key>
   <group>syscheck,authentication,firewall</group>
   <alert_format>json</alert_format>
 </integration>
```

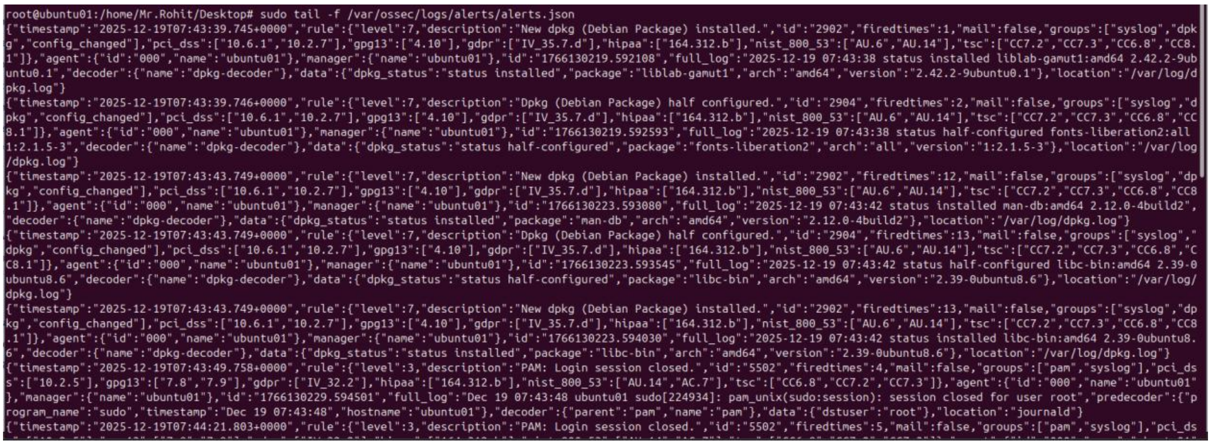
Then Restart the Wazuh-manager:

Command: sudo systemctl restart wazuh-manager

Let’s Verify that wazuh is creating alert,

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

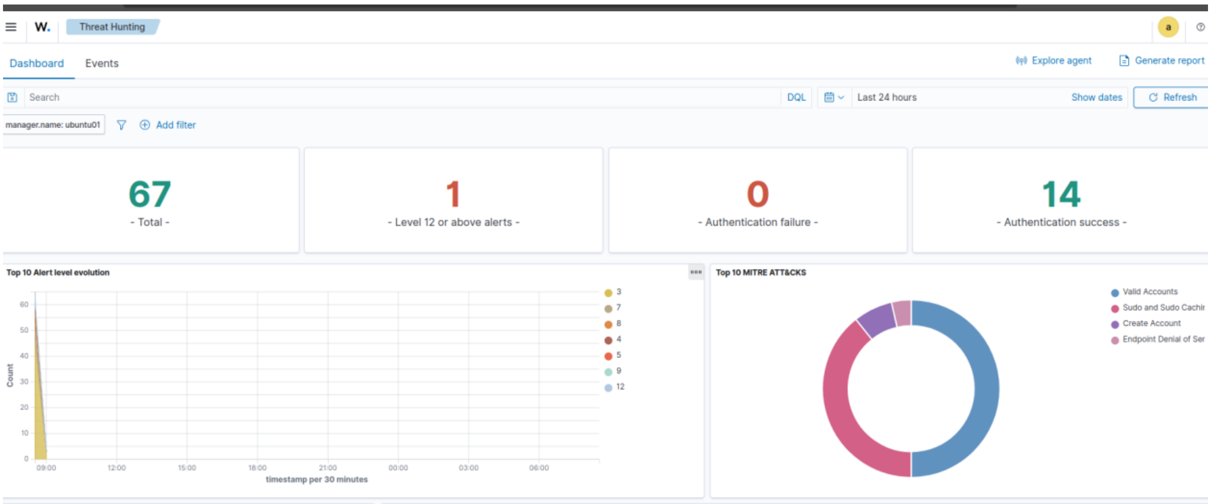
Screenshot:



```
root@ubuntu01:/home/Mr.Rohit/Desktop# sudo tail -f /var/ossec/logs/alerts/alerts.json
{"timestamp":"2025-12-19T07:43:39.745+0000","rule":{"level":7,"description":"New dpkg (Debian Package) installed.","id":"2902","firedtimes":1,"mail":false,"groups":["syslog","dpk
g","config_changed"],"pci_dss":["10.6.1","10.2.7"],"gpg13":["4.10"],"gdpr":["IV_35.7.d"],"hipaa":["164.312.b"],"nist_800_53":["AU.6","AU.14"],"tsc":["CC7.2","CC7.3","CC6.8","CC8.
1"]},"agent":{"id":"000","name":"ubuntu01"},"manager":{"name":"ubuntu01"},"id":"1766130219.592108","full_log":"2025-12-19 07:43:38 status installed liblab-gamut1:amd64 2.42.2-9ub
untu0.1","decoder":{"name":"dpkg-decoder"},"data":{"dpkg_status":"status installed","package":"liblab-gamut1","arch":"amd64","version":"2.42.2-9ubuntu0.1"},"location":"/var/log/d
pkg.log"}
{"timestamp":"2025-12-19T07:43:39.746+0000","rule":{"level":7,"description":"Dpkg (Debian Package) half configured.","id":"2904","firedtimes":2,"mail":false,"groups":["syslog","d
pkg","config_changed"],"pci_dss":["10.6.1","10.2.7"],"gpg13":["4.10"],"gdpr":["IV_35.7.d"],"hipaa":["164.312.b"],"nist_800_53":["AU.6","AU.14"],"tsc":["CC7.2","CC7.3","CC6.8","CC
8.1"]},"agent":{"id":"000","name":"ubuntu01"},"manager":{"name":"ubuntu01"},"id":"1766130219.592593","full_log":"2025-12-19 07:43:38 status half-configured fonts-liberation2:all
1:2.1.5-3","decoder":{"name":"dpkg-decoder"},"data":{"dpkg_status":"status half-configured","package":"fonts-liberation2","arch":"all","version":"1:2.1.5-3"},"location":"/var/log
/dpkg.log"}
{"timestamp":"2025-12-19T07:43:43.749+0000","rule":{"level":7,"description":"New dpkg (Debian Package) installed.","id":"2902","firedtimes":12,"mail":false,"groups":["syslog","dp
kg","config_changed"],"pci_dss":["10.6.1","10.2.7"],"gpg13":["4.10"],"gdpr":["IV_35.7.d"],"hipaa":["164.312.b"],"nist_800_53":["AU.6","AU.14"],"tsc":["CC7.2","CC7.3","CC6.8","CC8
.1"]},"agent":{"id":"000","name":"ubuntu01"},"manager":{"name":"ubuntu01"},"id":"1766130223.593080","full_log":"2025-12-19 07:43:42 status installed man-db:amd64 2.12.0-4build2",
"decoder":{"name":"dpkg-decoder"},"data":{"dpkg_status":"status installed","package":"man-db","arch":"amd64","version":"2.12.0-4build2"},"location":"/var/log/dpkg.log"}
{"timestamp":"2025-12-19T07:43:43.749+0000","rule":{"level":7,"description":"Dpkg (Debian Package) half configured.","id":"2904","firedtimes":13,"mail":false,"groups":["syslog","
dpkg","config_changed"],"pci_dss":["10.6.1","10.2.7"],"gpg13":["4.10"],"gdpr":["IV_35.7.d"],"hipaa":["164.312.b"],"nist_800_53":["AU.6","AU.14"],"tsc":["CC7.2","CC7.3","CC6.8","C
C8.1"]},"agent":{"id":"000","name":"ubuntu01"},"manager":{"name":"ubuntu01"},"id":"1766130223.593545","full_log":"2025-12-19 07:43:42 status half-configured libc-bin:amd64 2.39-0
ubuntu8.6","decoder":{"name":"dpkg-decoder"},"data":{"dpkg_status":"status half-configured","package":"libc-bin","arch":"amd64","version":"2.39-0ubuntu8.6"},"location":"/var/log/
dpkg.log"}
{"timestamp":"2025-12-19T07:43:43.749+0000","rule":{"level":7,"description":"New dpkg (Debian Package) installed.","id":"2902","firedtimes":13,"mail":false,"groups":["syslog","dp
kg","config_changed"],"pci_dss":["10.6.1","10.2.7"],"gpg13":["4.10"],"gdpr":["IV_35.7.d"],"hipaa":["164.312.b"],"nist_800_53":["AU.6","AU.14"],"tsc":["CC7.2","CC7.3","CC6.8","CC8
.1"]},"agent":{"id":"000","name":"ubuntu01"},"manager":{"name":"ubuntu01"},"id":"1766130223.594030","full_log":"2025-12-19 07:43:42 status installed libc-bin:amd64 2.39-0ubuntu8.
6","decoder":{"name":"dpkg-decoder"},"data":{"dpkg_status":"status installed","package":"libc-bin","arch":"amd64","version":"2.39-0ubuntu8.6"},"location":"/var/log/dpkg.log"}
{"timestamp":"2025-12-19T07:43:49.758+0000","rule":{"level":3,"description":"PAM: Login session closed.","id":"5502","firedtimes":4,"mail":false,"groups":["pam","syslog"],"pci_ds
s":["10.2.5"],"gpg13":["7.8","7.9"],"gdpr":["IV_32.2"],"hipaa":["164.312.b"],"nist_800_53":["AU.14","AC.7"],"tsc":["CC6.8","CC7.2","CC7.3"]},"agent":{"id":"000","name":"ubuntu01"
},"manager":{"name":"ubuntu01"},"id":"1766130229.594501","full_log":"Dec 19 07:43:48 ubuntu01 sudo[224934]: pam_unix(sudo:session): session closed for user root","predecoder":{"p
rogram_name":"sudo","timestamp":"Dec 19 07:43:48","hostname":"ubuntu01"},"decoder":{"parent":"pam","name":"pam"},"data":{"dstuser":"root"},"location":"journald"}
{"timestamp":"2025-12-19T07:44:21.803+0000","rule":{"level":3,"description":"PAM: Login session closed.","id":"5502","firedtimes":5,"mail":false,"groups":["pam","syslog"],"pci_ds
```

Now the wazuh is creating alert

let’s move to the Threat Hunting Integration,



67
- Total -

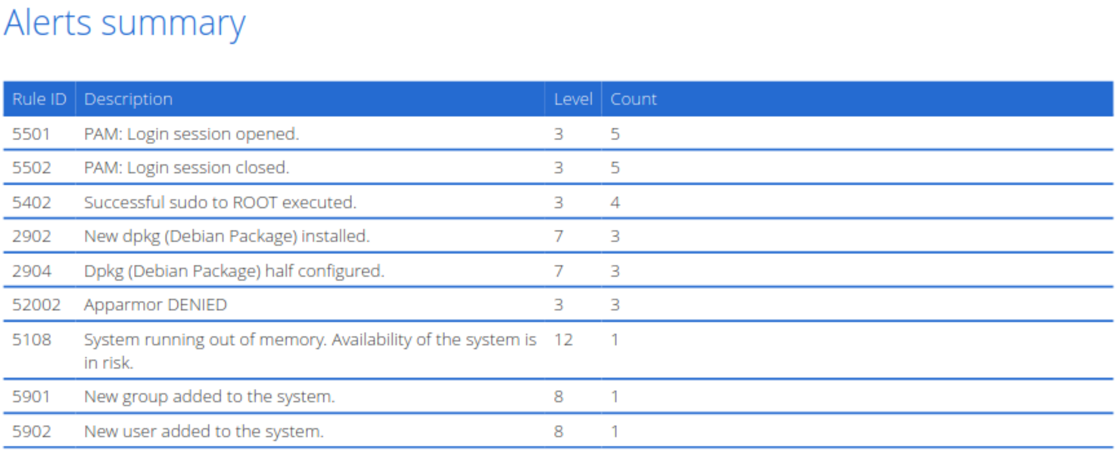
1
- Level 12 or above alerts -

0
- Authentication failure -

14
- Authentication success -

Based on this analysis, I Generated the report:

Alert summary:



Alerts summary

Rule ID	Description	Level	Count
5501	PAM: Login session opened.	3	5
5502	PAM: Login session closed.	3	5
5402	Successful sudo to ROOT executed.	3	4
2902	New dpkg (Debian Package) installed.	7	3
2904	Dpkg (Debian Package) half configured.	7	3
52002	Apparmor DENIED	3	3
5108	System running out of memory. Availability of the system is in risk.	12	1
5901	New group added to the system.	8	1
5902	New user added to the system.	8	1