Buttendorf, Abijah
Project 1, OSQuery
SEC-350
02/23/2023

- Step 1: Install OS query on the Host
  Starting with the host system, web01, assuming its rocky:

  curl -L https://pkg.osquery.io/rpm/GPG | tee
  /etc/pki/rpm-gpg/RPM-GPG-KEY-osquery
  yum install yum-utils
  yum-config-manager --add-repo https://pkg.osquery.io/rpm/osquery-s3-rpm.repo
  yum-config-manager --enable osquery-s3-rpm-repo
  yum install osquery

```
[root@web01-thomsen ~]# yum install osquery
name=osquery RPM repository - x86_64           1.1 MB/s | 376 kB     00:00
Dependencies resolved.
================================================================================
 Package       Architecture Version            Repository                 Size
================================================================================
Installing:
 osquery       x86_64       5.7.0-1.linux      osquery-s3-rpm-repo        17 M

Transaction Summary
================================================================================
Install  1 Package
```

-

- Step 2:
  Enter the /etc/osquery directory
  Create osquery.conf and append the following:

Unset

```
{
      "options": {
      "config_plugin": "filesystem",
      "logger_plugin": "filesystem",
      "utc": "true"
      },
      "schedule": {
      "system_info": {
      "query": "SELECT hostname, cpu_brand, physical_memory FROM
system_info;",
      "interval": 60
      },
      "processes_binding_to_ports": {
      "query": "SELECT DISTINCT process.name, listening.port,
listening.address, process.pid FROM processes AS process JOIN
listening_ports AS listening ON process.pid = listening.pid;",
      "interval": 60
      },
   "high_load_average": {
        "query": "SELECT period, average, '70%' AS 'threshold' FROM
load_average WHERE period = '15m' AND average > '0.7';",
        "interval": 900,
        "description": "Report if load charge is over 70 percent."
      },
    "low_free_memory": {
        "query": "SELECT memory_total, memory_free, CAST(memory_free AS
real) / memory_total AS memory_free_perc, '10%' AS threshold FROM
memory_info WHERE memory_free_perc < 0.1;",
        "interval": 1800,
        "description": "Free RAM is under 10%."
            }
      }
}
```

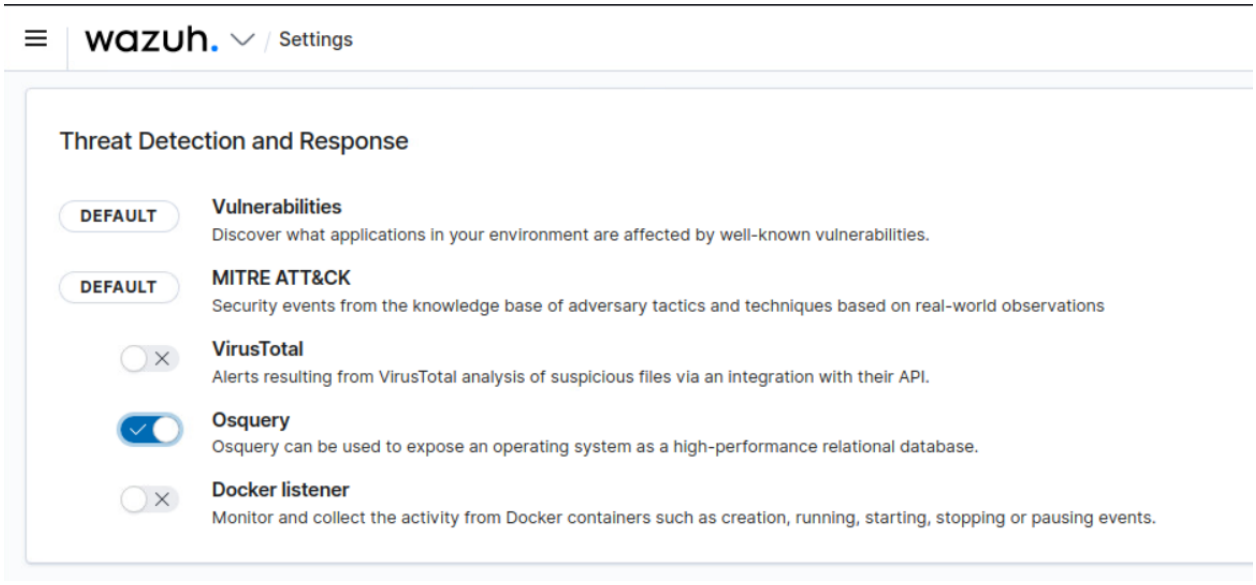
Step 3: Enable OS Query on wazuh agent:

Open /var/ossec/etc/ossec.conf and modify the following section:

```
Unset
<ossec_config>
    <wodle name="osquery">
        <disabled>no</disabled>
        <run_daemon>yes</run_daemon>
        <bin_path>/usr/bin</bin_path>
        <log_path>/var/log/osquery/osqueryd.results.log</log_path>
        <config_path>/etc/osquery/osquery.conf</config_path>
        <add_labels>no</add_labels>
    </wodle>
</ossec_config>
```

Step 4: Enable OS Query on Wazuh Server:

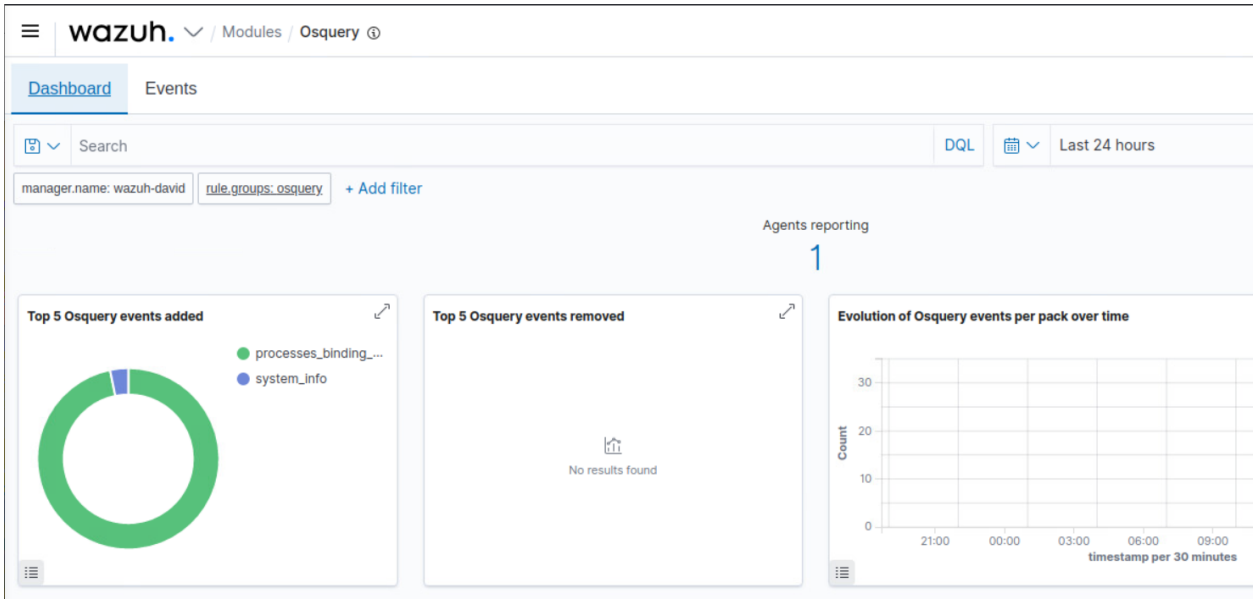
Go to Wazuh > Settings > Modules and enable OSquery



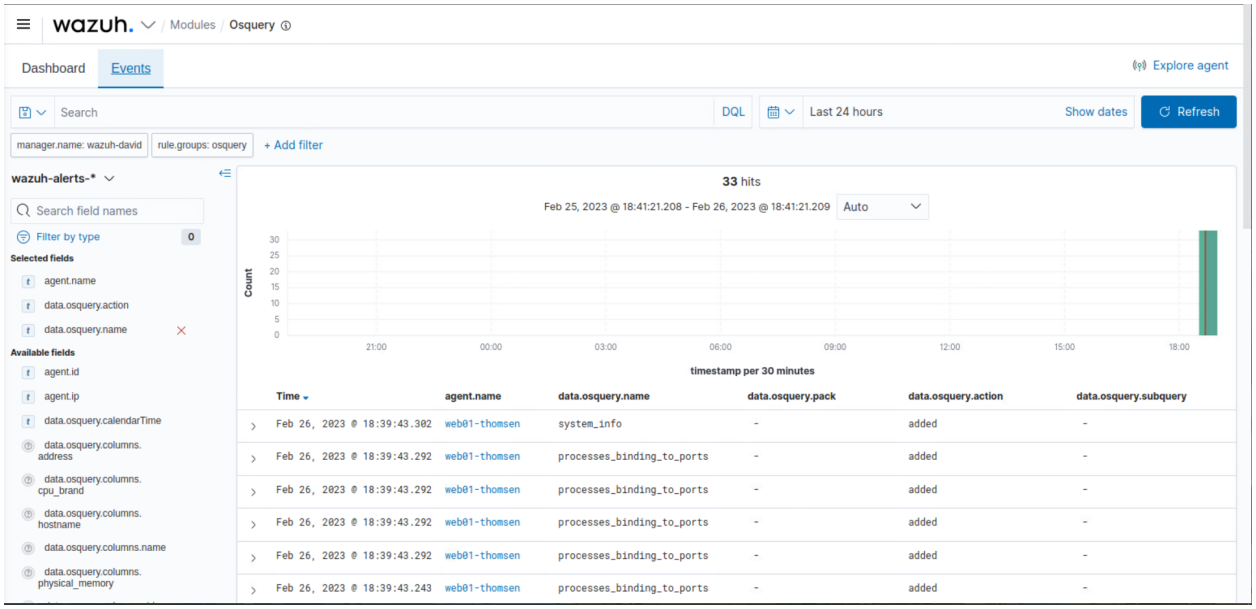
Step 5: Restart Wazuh agent on Host:

```
[root@web01-thomsen etc]# sudo systemctl restart wazuh-agent.service
```

Now you should be able to see the agent reporting for ossec:



Go to modules > osquery > events:



https://drive.google.com/file/d/167yj4o-rfjr6zImtqEBf-YpOrwOXxqXa/view?usp=sharing