AN INTRODUCTION TO OSQUERY

WHO AM I ?

- Intern @ Practical DevSecOps
- Undergrad @ Vit Chennai
- Have interest over Mobile,Web,Cloud Security
- Currently Looking for Internship

TODAYS AGENDA

- What is Osquery
- Why Osquery
- Basic Queries
- Configuring Osquery
- What next?

PRE-REQUISTE

- Basic System Knowledge
- Basic SQL language

OS QUERY

- Tool to ask question about your System
- Developed by Facebook
- Opensource
- Based on SQL

COMPONENETS OF OS QUERY

- Osqueryi
- Osqueryd
- Osqueryctl

WHY OS QUERY ?

- Easy to use
- Supports almost all platform
- Easy to get information about different System

BASIC QUERIES

- Runs in `User-context` mode
- `.show` - shows basic configuration
- `.help` - shows help name
- `.table` - shows list of table
- `.schema <table>` - show the column

MODE

- pretty
- line
- csv
- List
- Line

```
SELECT * FROM uptime;

SELECT * FROM os_version;

SELECT * FROM system_info;
```

```
select count(*) from users;

select * from users limit 1;

select uid , username from users;

select uid , username from users where username like 's%';

select uid , username from users where username like '%s';
```

JOIN

- Used to join the table

```
select pid, name from processes limit 5;

select p.pid , p.name, u.username from processes p join users
```

OSQUERYD

- Option
- Schedule
- Packs
- Decarator

BASIC OS-QUERY CONFIGURATION

Should be stored in the

/etc/osquery/osquery.conf

```
{
    "options": {
        "config_plugin": "filesystem",
        "logger_plugin": "filesystem",
        "logger_path": "/var/log/osquery",
        "disable_logging": "false",
        "log_result_events": "true",
        "schedule_splay_percent": "10",
        "pidfile": "/var/osquery/osquery.pidfile",
        "events_expiry": "3600",
        "database_path": "/var/osquery/osquery.db",
        "verbose": "false",
        "worker_threads": "2",
        "enable_monitor": "true",
        "disable_events": "false",
```

DECARATOR

These are additional value need to be added in logs

There are 3 types

- load
- always
- interval

PACKS

- Packs are the way to group the query for Specific Task
- Default one can be found in `/usr/share/osquery/packs/`
- It has the following information

```
Intervals
Which platform to perform
Which action to use
```

BASIC USE CASE (FILE-INTEGRATION MONITORING)

```
sudo nano \etc\osquery\osquery.conf
```

```
{
   "options": {
       "config_plugin": "filesystem",
       "logger_plugin": "filesystem",
       "logger_path": "/var/log/osquery",
       "disable_logging": "false",
       "schedule_splay_percent": "10",
       "pidfile": "/var/osquery/osquery.pidfile",
       "events_expiry": "3600",
       "database_path": "/var/osquery/osquery.db",
       "verbose": "false",
       "worker_threads": "2",
       "disable_events": "false",
       "disable_audit": "false",
       "audit_allow_config": "true",
```

CREATING PACK

```
sudo nano /usr/share/osquery/packs/fim.conf
```

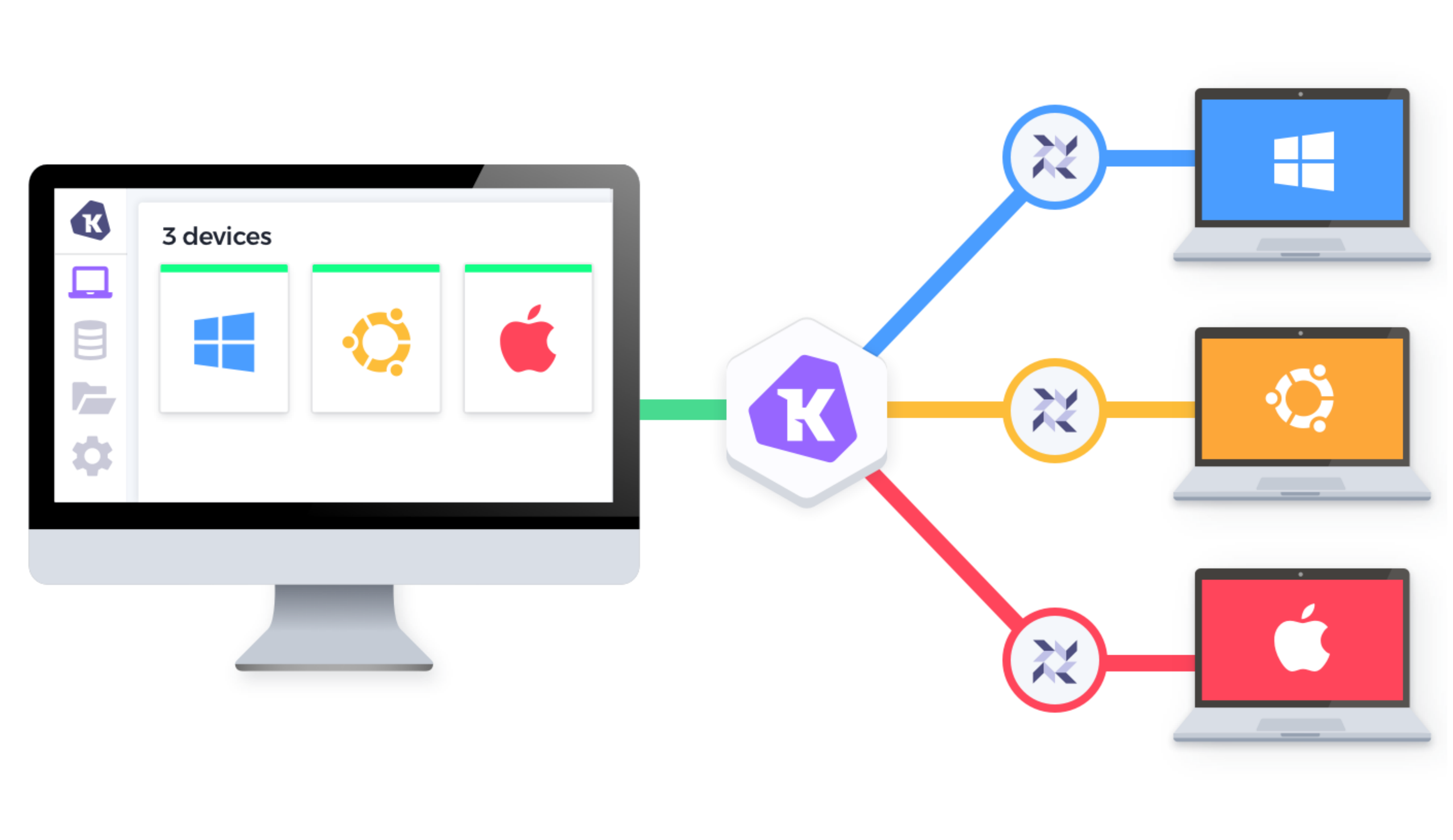
```
{
  "queries": {
    "file_events": {
      "query": "SELECT * FROM file_events;",
      "removed": false,
      "interval": 300
    }
  },
  "file_paths": {

      "important": [
      "/home/joshua/important/%%"
      ]
  }
```

OSQUERYCTL

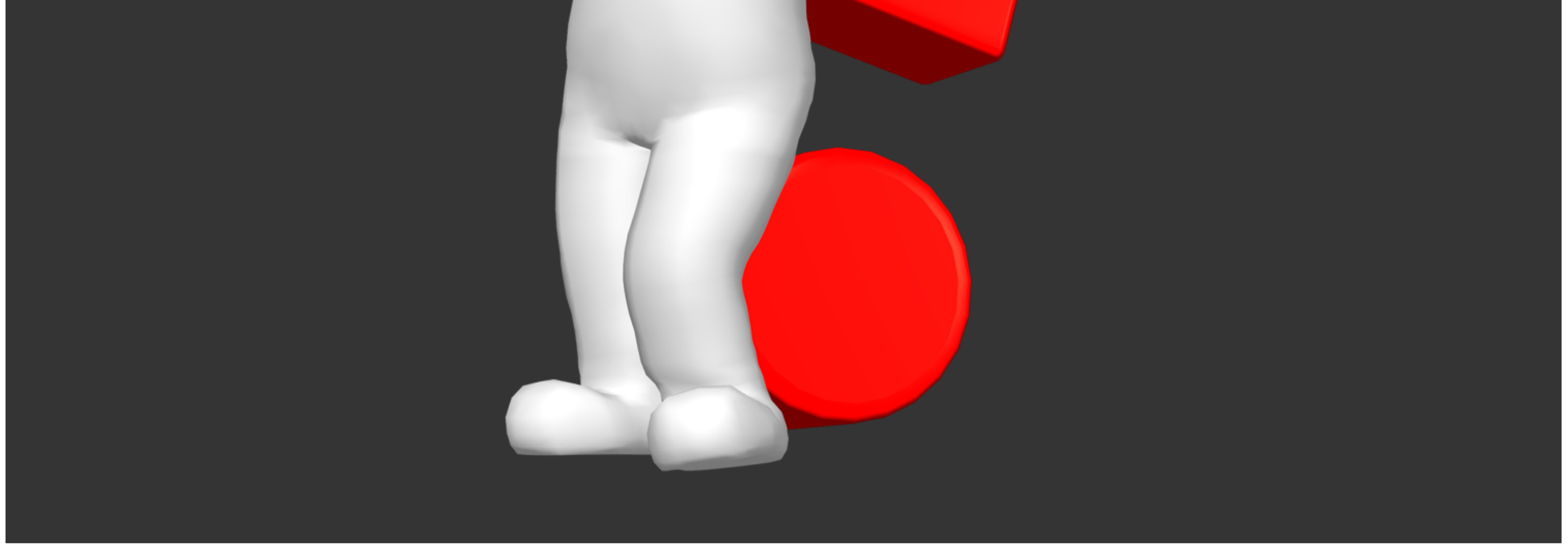
- Similar to systemctl
- Used to start,stop and check configuration of `osquery` configuration

```
$ osqueryctl config-check

$ osqueryctl start

$ osqueryctl stop osqueryd

$ osqueryctl restart osqueryd
```

WHAT NEXT



QUESTIONS & FEEDBACK



REFERENCES

- https://kifarunix.com/install-osquery-on-debian-10
  buster/
- https://www.digitalocean.com/community/tutorials
  to-monitor-your-system-security-with-osquery-on-
  ubuntu-16-04
- https://osquery.readthedocs.io/