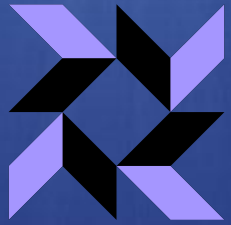
Endpoint Monitoring with Osquery



GTS São Paulo 2018

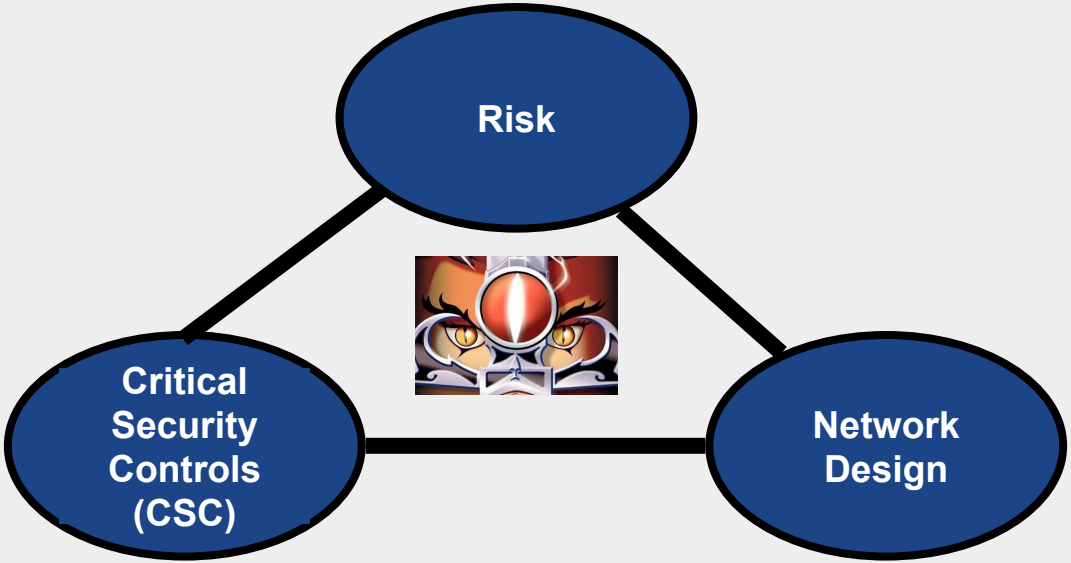
@BlueOpsBR @spookerlabs

About me

Rodrigo Montoro
@spookerlabs

Blue Ops

Motivation (1/2)



Attack Surface

Blue Ops

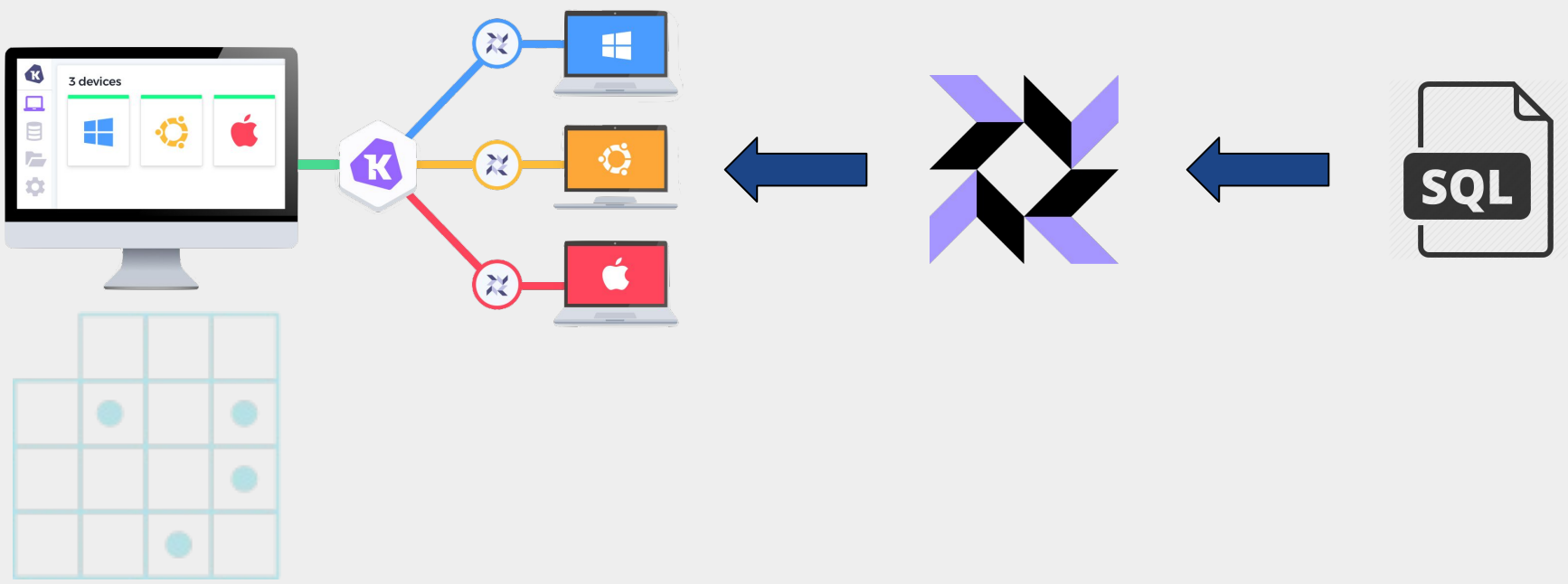
Motivation (2/2)

Blue Ops

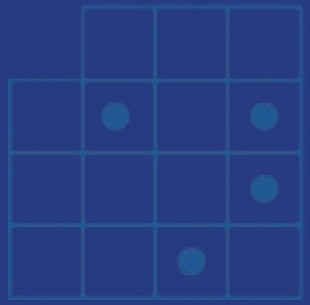
Agenda

- Intro {osquery, SQL Language}
- osquery{i,d}
- Kolide fleet

Workflow



Intro osquery



OSQUERY

- Created by Facebook 10/2014
- Multi Platform(Linux / Mac / Windows / FreeBSD)
- Operating System Database
- 200+ tables/Thousands of possible queries combination
- Current version 3.3.1 (Dec 10 2018)
- 2017 O’Reilly Defender Award for best project

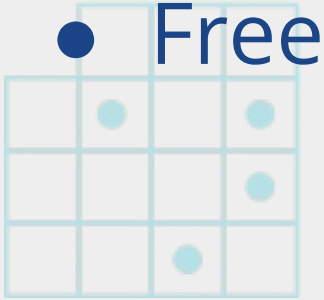
Unify sources of information

- Flat files (/etc/hosts, ~/.ssh/known_hosts)
- Applications API's (Docker, Carbon black)
- Filesystem (Shared folders, hashes, permissions)
- Event-based API's (OpenBSM, FSEvents, Audit)

Blue Ops

Platforms

- Linux
- MacOS
- Windows
- FreeBSD



.tables {Linux,Windows,MAC}

116 Tables

process_events
process_file_events
process_memory_map
process_open_files
process_open_sockets
processes
prometheus_metrics
python_packages
routes
rpm_package_files
rpm_packages
shadow
shared_memory
shell_history
smbios_tables
socket_events
sudoers
suid_bin
syslog_events
system_controls
system_info
time
uptime
usb_devices
user_events
user_groups
user_ssh_keys

68 Tables

osquery_schedule
patches
physical_disk_performance
pipes
platform_info
powershell_events NEW
process_memory_map
process_open_sockets
processes
programs
python_packages
registry
routes
scheduled_tasks
services
shared_resources
startup_items
system_info
time
uptime
user_groups
users
video_info
windows_crashes
windows_events
wmi_bios_info NEW
wmi_cli_event_consumers
wmi_event_filters

154 Tables

account_policy_data
acpi_tables
ad_config
alf
alf_exceptions
alf_explicit_auths
alf_services
app_schemes
apps
apt_sources
arp_cache
asl
augeas
authorization_mechanisms
authorizations
authorized_keys
block_devices
browser_plugins
carbon_black_info
carves
certificates
chrome_extensions
cpu_time
cpuid
crashes
crontab
cups_destinations NEW

schema tables

207 Tables

- mdfind NEW
- memory_devices NEW
- memory_info
- memory_map
- mounts
- msr
- nfs_shares
- npm_packages NEW
- nvram
- opera_extensions
- os_version
- osquery_events
- osquery_extensions
- osquery_flags

sudoers

Rules for running commands as other users via sudo.

Improve this Description on Github

COLUMN	TYPE	DESCRIPTION
header	TEXT	Symbol for given rule
rule_details	TEXT	Rule definition

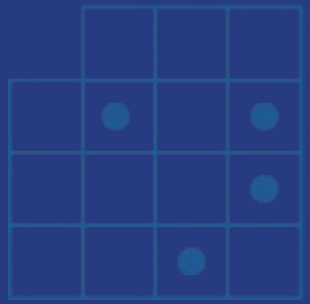
suid_bin

suid binaries in common locations.

Improve this Description on Github

COLUMN	TYPE	DESCRIPTION
path	TEXT	Binary path
username	TEXT	Binary owner username
groupname	TEXT	Binary owner group
permissions	TEXT	Binary permissions

SQL Language



Data Query Language

SELECT home, id, user **FROM** tables **WHERE** available=1;

What you want?

where is stored?

Predicate

Condition

Average()
Count()
Distinct()

ORDER BY var DESC;

Blue Ops

Advanced...

file

Interactive filesystem attributes and metadata.

Improve this Description on Github

COLUMN	TYPE	DESCRIPTION
path	TEXT	Absolute file path
directory	TEXT	Directory of file(s)
filename	TEXT	Name portion of file path
inode	BIGINT	Filesystem inode number
uid	BIGINT	Owning user ID
gid	BIGINT	Owning group ID

hash

Filesystem hash data.

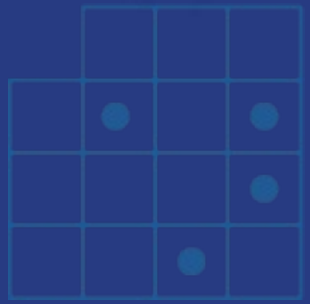
Improve this Description on Github

COLUMN	TYPE	DESCRIPTION
path	TEXT	Must provide a path or directory
directory	TEXT	Must provide a path or directory
md5	TEXT	MD5 hash of provided filesystem data
sha1	TEXT	SHA1 hash of provided filesystem data
sha256	TEXT	SHA256 hash of provided filesystem data

```
SELECT path, mtime, sha256 FROM file
JOIN hash USING (path) WHERE file.directory = '/etc'
ORDER BY mtime DESC LIMIT 1;
```

Blue Ops

osquer{i,d}



osqueryi


```
[root@blueopslabs lab]# osqueryi
Using a virtual database. Need help, type '.help'
osquery> .help
Welcome to the osquery shell. Please explore your OS!
You are connected to a transient 'in-memory' virtual database.

.all [TABLE]     Select all from a table
.bail ON|OFF     Stop after hitting an error
.echo ON|OFF     Turn command echo on or off
.exit            Exit this program
.features        List osquery's features and their statuses
.headers ON|OFF  Turn display of headers on or off
.help            Show this message
.mode MODE       Set output mode where MODE is one of:
                   csv      Comma-separated values
                   column   Left-aligned columns see .width
                   line     One value per line
                   list     Values delimited by .separator string
                   pretty   Pretty printed SQL results (default)
.nullvalue STR   Use STRING in place of NULL values
.print STR...    Print literal STRING
.quit            Exit this program
.schema [TABLE]  Show the CREATE statements
.separator STR   Change separator used by output mode
.socket          Show the osquery extensions socket path
.show            Show the current values for various settings
.summary         Alias for the show meta command
.tables [TABLE]  List names of tables
.width [NUM1]+   Set column widths for "column" mode
.timer ON|OFF      Turn the CPU timer measurement on or off
osquery>
```

query

```
osquery> .schema wifi_status
CREATE TABLE wifi_status(`interface` TEXT, `ssid` TEXT, `bssid` TEXT, `network_name` TEXT, `country_code` TEXT, `securi
ty_type` TEXT, `rssi` INTEGER, `noise` INTEGER, `channel` INTEGER, `channel_width` INTEGER, `channel_band` INTEGER, `tr
ansmit_rate` TEXT, `mode` TEXT);
osquery> select interface, network_name,security_type, mode from wifi_status ;
+-----------+--------------+---------------+---------+
| interface | network_name  | security_type | mode    |
+-----------+--------------+---------------+---------+
| en0       | FIBRA-9788-5G | WPA2 Personal | Station |
+-----------+--------------+---------------+---------+
osquery>
```

```
osquery> SELECT  p.name, h.md5, local_address, remote_address, local_port, remote_port FROM process_open_sockets s JOIN
 processes p ON s.pid = p.pid  JOIN hash h ON h.path = p.path WHERE remote_port NOT IN (80, 443) AND family =2 AND remo
te_address NOT like '0.0.0.0';
+---------------+----------------------------------+---------------+----------------+------------+-------------+
| name          | md5                              | local_address | remote_address | local_port | remote_port |
+---------------+----------------------------------+---------------+----------------+------------+-------------+
| Google Chrome | ae2922cf9fd2539cdf5b4a6479c99210 | 192.168.25.3  | 74.125.192.188 | 51616      | 5228        |
| rapportd      | 642766fab51796754fc3fef3737ffa7e | 192.168.25.3  | 192.168.25.4   | 55941      | 52689       |
| GlobalProtect | a3dbcb334ee87f6a7e62d6a953e85d0a | 127.0.0.1     | 127.0.0.1      | 49194      | 4767        |
| Spotify       | c8e7f1a477bf951ae9c16445f2e657c5 | 192.168.25.3  | 104.154.126.206 | 52711      | 4070        |
| firefox       | 4b7bca0132c37f8a13bfa6738a843052 | 192.168.25.3  | 138.68.62.104  | 51599      | 8080        |
| ssh           | 1b270f15270378ccf5e74a9ced55baae | 192.168.25.3  | 138.68.62.104  | 63874      | 22          |
| ssh           | 1b270f15270378ccf5e74a9ced55baae | 192.168.25.3  | 138.68.62.104  | 63874      | 22          |
+---------------+----------------------------------+---------------+----------------+------------+-------------+
osquery>
```

osqueryi parameters

```
[root@blueopslabs lab]# osqueryi -h | wc -l
164
[root@blueopslabs lab]#
```

```
osquery shell-only CLI flags:

    --A VALUE                           Select all from a table
    --L                                 List all table names
    --csv                               Set output mode to 'csv'
    --extension VALUE                   Path to a single extension to autoload
    --header                            Toggle column headers true/false
    --json                              Set output mode to 'json'
    --line                              Set output mode to 'line'
    --list                              Set output mode to 'list'
    --pack VALUE                        Run all queries in a pack
    --planner                           Enable osquery runtime planner output
    --profile VALUE                     Enable profile mode when non-0, set number of iterations
    --separator VALUE                   Set output field separator, default '|'
```

osqueryd

- Continuous monitoring
- Queries
  - packs
  - schedule
  - distributed
- Standalone or Central management

Blue Ops

schedule

```
// Define a schedule of queries:
"schedule": {
  "user_info": {
    // The exact query to run.
    "query": "SELECT * FROM users;",
    // The interval in seconds to run this query, not an exact interval.
    "interval": 10
  }
},
```


Blue Ops

pack

```
{
  "platform": "windows",
  "queries": {
    "OpenType_Font_Driver_Vulnerability": {
      "query" : "select * from registry where path like 'HKEY_LOCAL_MACHINE\\SOFTWARE\\Microsoft\\Windows NT\\CurrentVe
rsion\\Windows\\%' AND name = 'DisableATMFD' AND data != '1';",
      "interval" : "3600",
      "version": "2.2.1",
      "description" : "Determine if Adobe Type Manager Font Driver is disabled (https://technet.microsoft.com/en-us/lib
rary/security/ms15-078)"
    },
    "Protecting_Against_Weak_Crypto_Algo": {
      "query" : "select * from registry where path like 'HKEY_LOCAL_MACHINE\\SOFTWARE\\Microsoft\\Cryptography\\OID\\En
codingType 0\\CertDllCreateCertificateChainEngine\\Config\\Default\\%' AND name IN ('WeakSha1ThirdPartyFlags','WeakMd5T
hirdPartyFlags') AND type = 'REG_DWORD' AND data not like '-2%';",
      "interval" : "3600",
      "version": "2.2.1",
      "description" : "Determine if Windows is configured to log certificates with weak crypto (https://technet.microso
ft.com/library/dn375961(v=ws.11).aspx)",
      "value" : "Artifact used by this malware"
    },
    "UAC_Disabled": {
      "query": "SELECT * FROM registry WHERE path='HKEY_LOCAL_MACHINE\\Software\\Microsoft\\Windows\\CurrentVersion\\Po
licies\\System\\EnableLUA' AND data=0;",
      "interval": 3600,
      "version": "2.2.1",
      "description": "Controls UAC. A setting of 0 indicates that UAC is disabled."
    },
    "SecureBoot": {
      "query" : "select * from registry where key='HKEY_LOCAL_MACHINE\\SYSTEM\\CurrentControlSet\\Control\\SecureBoot\\
State\\UEFISecureBootEnabled'",
      "interval": "86400",
```

ue Ops

FIM (File Integrity Monitoring)

```yaml
apiVersion: v1
kind: options
spec:
  config:
    decorators:
      load:
      - SELECT uuid AS host_uuid FROM system_info;
      - SELECT hostname AS hostname FROM system_info;
    options:
      disable_distributed: false
      distributed_interval: 10
      distributed_plugin: tls
      distributed_tls_max_attempts: 3
      distributed_tls_read_endpoint: /api/v1/osquery/distributed/read
      distributed_tls_write_endpoint: /api/v1/osquery/distributed/write
      logger_plugin: tls
      logger_tls_endpoint: /api/v1/osquery/log
      logger_tls_period: 10
      pack_delimiter: /

    file_paths:
      tmp:
        - /tmp/bsideslv/%%

  overrides: {}
```

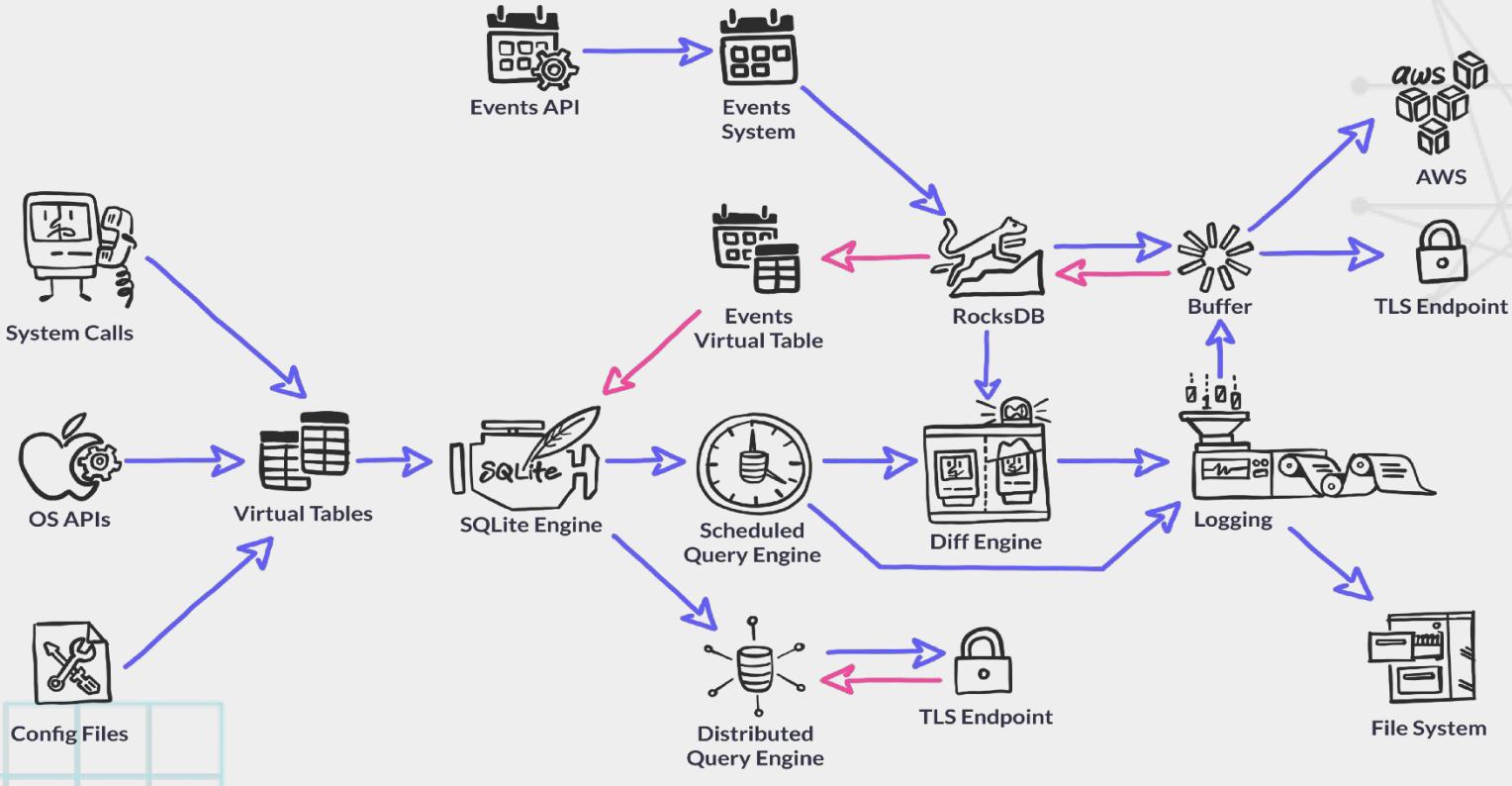
```yaml
apiVersion: v1
kind: query
spec:
  description: Select key fields from file_events to be used at FIM pack
  name: FileEvents
  query: SELECT action, uid, category, target_path, md5 FROM file_events
```

```yaml
apiVersion: v1
kind: pack
spec:
  description: Rule to monitor file integrity from sensitive locations
  id: 4
  name: FIM-FileIntegrityMonitoring
  queries:
  - description: ""
    interval: 30
    name: File Events
    platform: ""
    query: File Events
    removed: true
    snapshot: false
    version: ""
  targets:
    labels:
    - All Hosts
```

```json
{
  "name": "pack/FIM - File Integrity Monitoring/File Events",
  "hostIdentifier": "DF485792-3B3D-4E5F-A178-221CC9557C80",
  "calendarTime": "Mon Jul 30 14:10:21 2018 UTC",
  "unixTime": 1532959821,
  "epoch": 0,
  "counter": 0,
  "decorations": {
    "host_uuid": "DF485792-3B3D-4E5F-A178-221CC9557C80",
    "hostname": "BlueOpsLabs"
  },
  "columns": {
    "action": "CREATED",
    "category": "tmp",
    "md5": "d41d8cd98f00b204e9800998ecf8427e",
    "target_path": "/tmp/bsideslv/blueops_bsidesLV",
    "uid": "0"
  },
  "action": "added"
}
```

Process Events

```
osquery> select pid,uid,auid,path,cmdline from process_events ;
+-------+-----+------+--------------+-----------------------------------------------------+
| pid   | uid | auid | path         | cmdline                                             |
+-------+-----+------+--------------+-----------------------------------------------------+
| 12436 | 0   | 0    | /usr/bin/curl | "curl" "-v" "https://www.blueops.com.br/bsideslv" |
+-------+-----+------+--------------+-----------------------------------------------------+
osquery> select pid,auid,path, remote_address,remote_port from socket_events ;
+-------+------+--------------+----------------+-------------+
| pid   | auid | path         | remote_address | remote_port |
+-------+------+--------------+----------------+-------------+
| 12436 | 0    | /usr/bin/curl | 67.207.67.2    | 53          |
| 12436 | 0    | /usr/bin/curl | 104.24.124.5   | 443         |
| 12436 | 0    | /usr/bin/curl | 104.24.125.5   | 443         |
+-------+------+--------------+----------------+-------------+
osquery> select se.pid,se.action,pe.cmdline,se.remote_address,se.remote_port from socket_events se JOIN proces
s_events pe ON se.pid = pe.pid WHERE remote_port != 0;
+-------+---------+-----------------------------------------------------+----------------+-------------+
| pid   | action  | cmdline                                             | remote_address | remote_port |
+-------+---------+-----------------------------------------------------+----------------+-------------+
| 12436 | connect | "curl" "-v" "https://www.blueops.com.br/bsideslv" | 67.207.67.2    | 53          |
| 12436 | connect | "curl" "-v" "https://www.blueops.com.br/bsideslv" | 104.24.124.5   | 443         |
| 12436 | connect | "curl" "-v" "https://www.blueops.com.br/bsideslv" | 104.24.125.5   | 443         |
+-------+---------+-----------------------------------------------------+----------------+-------------+
osquery>
```

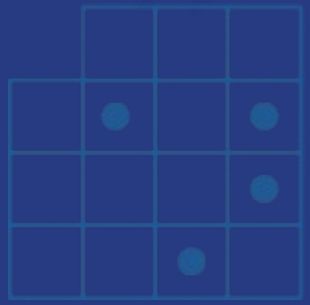

Events API
Events System
AWS
System Calls
Events Virtual Table
RocksDB
Buffer
TLS Endpoint
OS APIs
Virtual Tables
SQLite Engine
Scheduled Query Engine
Diff Engine
Logging
Config Files
Distributed Query Engine
TLS Endpoint
File System

Blue Ops

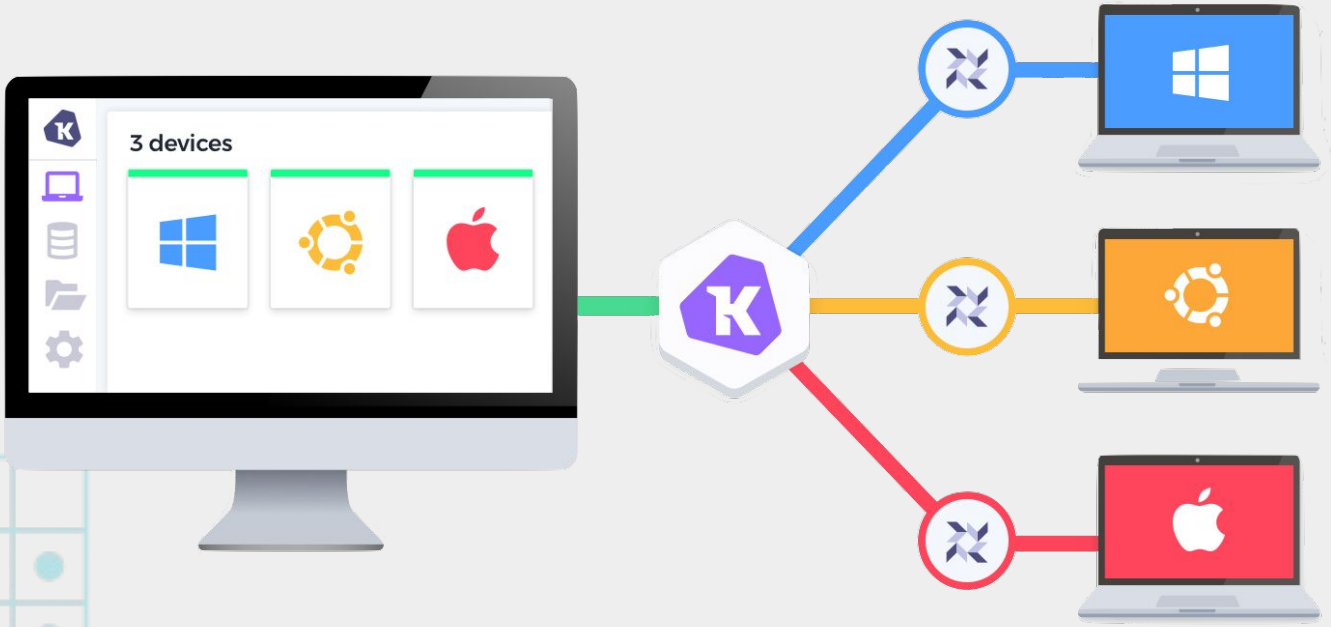
What to monitor ?

- Browser plugins ?
- Sudoers ? Crontab ?
- Programs installed ? Patches ?
- MD5/SHA1, process and listening ports ?
- Users / Groups created ?
- Docker: images ? processes ? ports ?
- Certificates ? File Integrity ?
- System Startup ?
- Firewall configs?

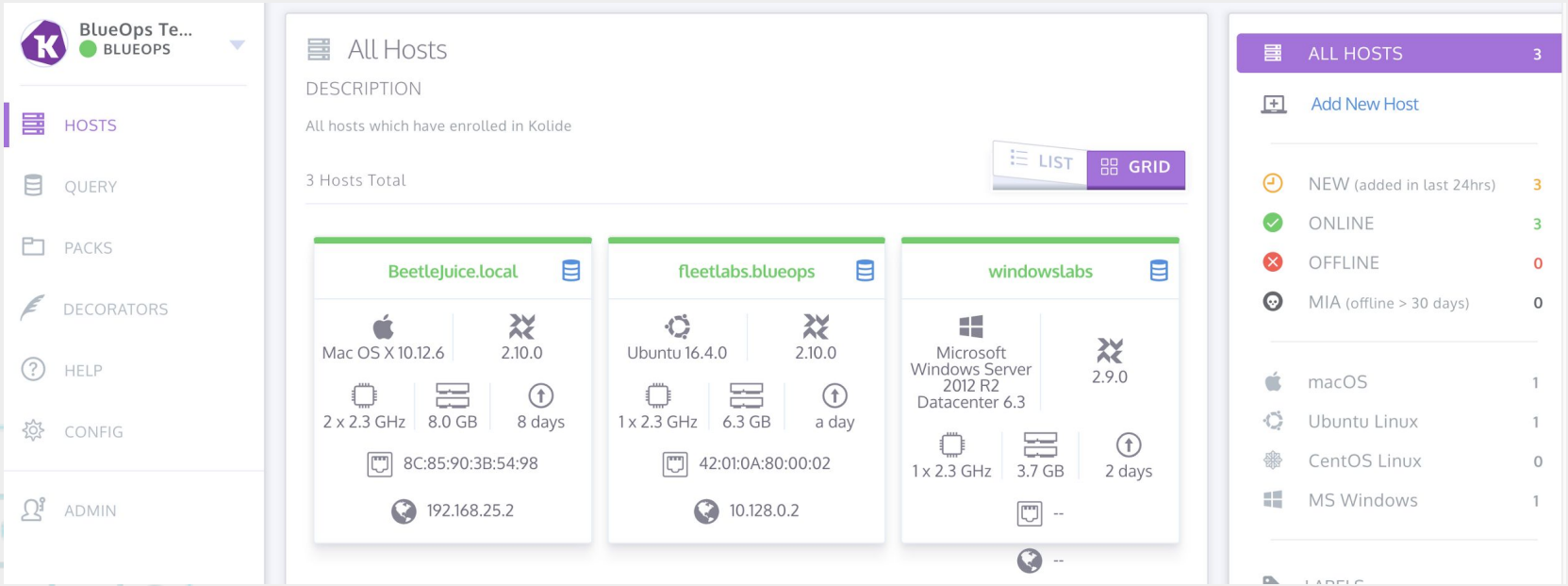
Kolide Fleet



About Kolide Fleet



General hosts view



Query Fleet

Edit Query

Query Title

FileEvents

SQL

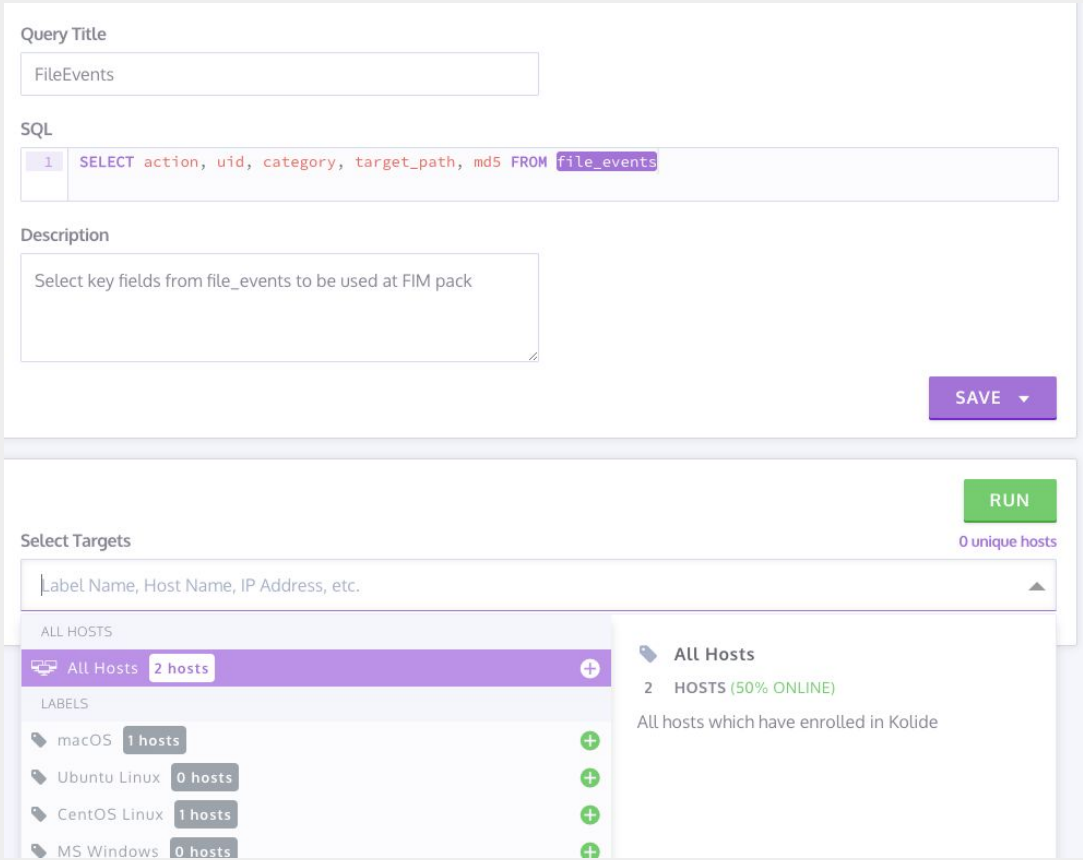
```
1  SELECT action, uid, category, target_path, md5 FROM file_events
```

Description

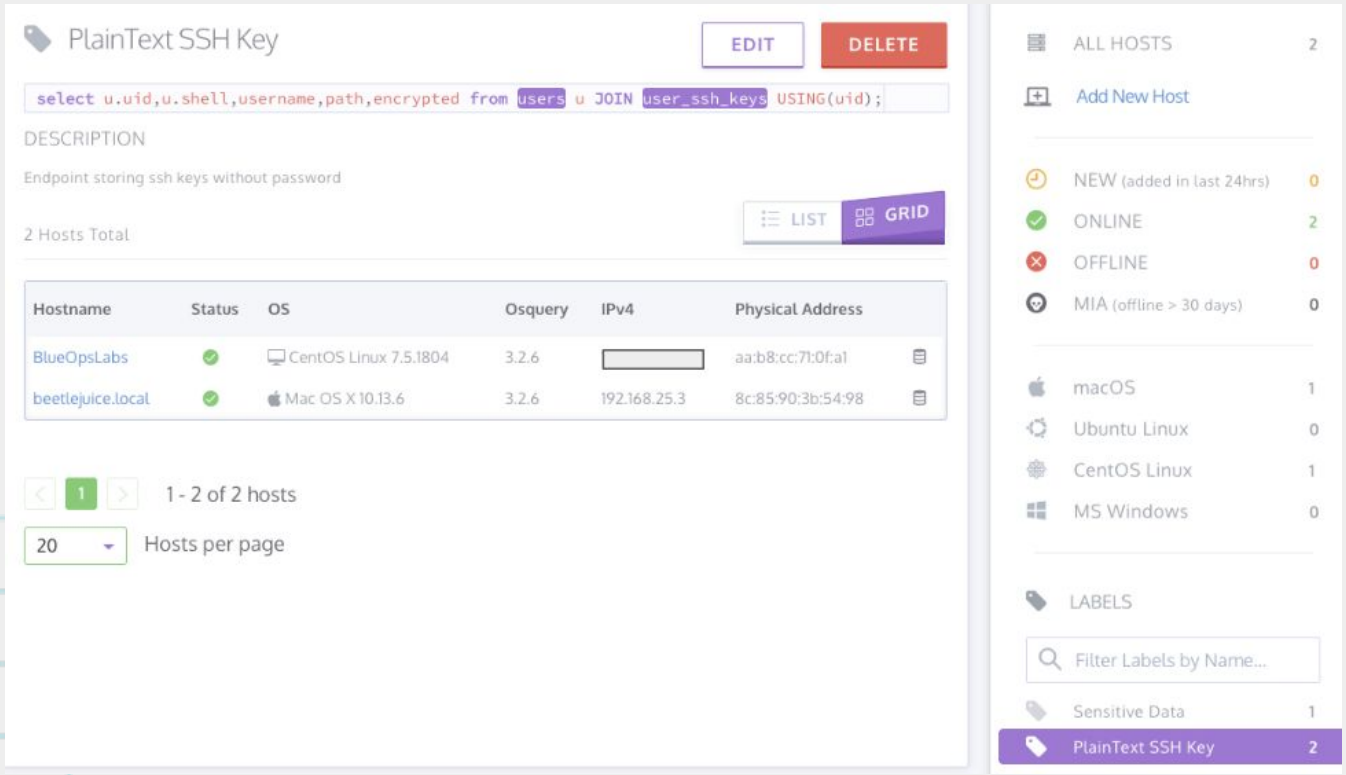
Select key fields from file_events to be used at FIM pack

SAVE

Distributed Query



Labels


PlainText SSH Key
EDIT
DELETE
select u.uid,u.shell,username,path,encrypted from users u JOIN user_ssh_keys USING(uid);
DESCRIPTION
Endpoint storing ssh keys without password
2 Hosts Total
LIST
GRID
Hostname
Status
OS
Osquery
IPv4
Physical Address
BlueOpsLabs
CentOS Linux 7.5.1804
3.2.6
aa:b8:cc:71:0f:a1
beetlejuice.local
Mac OS X 10.13.6
3.2.6
192.168.25.3
8c:85:90:3b:54:98
1 - 2 of 2 hosts
20
Hosts per page
ALL HOSTS 2
Add New Host
NEW (added in last 24hrs) 0
ONLINE 2
OFFLINE 0
MIA (offline > 30 days) 0
macOS 1
Ubuntu Linux 0
CentOS Linux 1
MS Windows 0
LABELS
Filter Labels by Name...
Sensitive Data 1
PlainText SSH Key 2

FleetCTL

```
BeetleJuice:~ rodrigomontoro$ fleetctl -h
NAME:
   fleetctl - CLI for operating Kolide Fleet

USAGE:
   fleetctl [global options] command [command options] [arguments...]

COMMANDS:
     apply    Apply files to declaratively manage osquery configurations
     delete   Specify files to declaratively batch delete osquery configurations
     setup    Setup a Kolide Fleet instance
     login    Login to Kolide Fleet
     logout   Logout of Kolide Fleet
     query    Run a live query
     get      Get/list resources
     config   Modify how and which Fleet server to connect to
     convert  Convert osquery packs into decomposed fleet configs
     help, h  Shows a list of commands or help for one command

GLOBAL OPTIONS:
   --help, -h     show help
   --version, -v  print the version
```

Obrigado

rodrigo.montoro@blueops.com.br

rodrigo.montoro@neoway.com.br

https://www.blueops.com.br

@spookerlabs

@blueopsbr