Operating System Analytics & Tools

A tour of the osquery ecosystem and how to take advantage of it

About me

Mike Arpaia
marpaia

Co-Founder & CTO of **@kolide**. Creator of **@osquery**. Formerly employed by **@facebook**, **@etsy**, **@iSECPartners**.

Block or report user

Developer Program Member

@kolide
Boulder, Colorado
https://twitter.com/mikearpaia

Organizations

Overview | Repositories 22 | Stars 108 | Followers 199 | Following 18

Pinned repositories

facebook/osquery
SQL powered operating system instrumentation, monitoring, and analytics.
C++ ★ 10.5k 1.2k

kolide/launcher
Osquery launcher, autoupdater, and packager
Go ★ 75 10

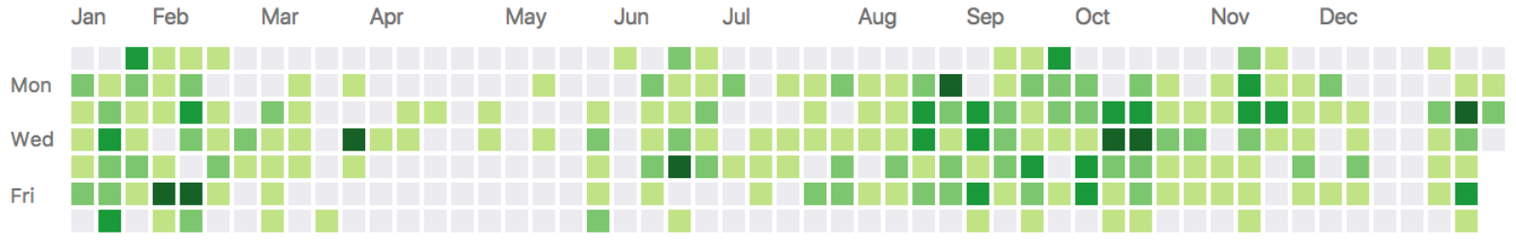
kolide/fleet
A flexible control server for osquery fleets
Go ★ 170 32

kolide/updater
Autoupdate binaries with Docker Notary and TUF
Go ★ 26 5

kolide/osquery-go
Go bindings for Osquery
Go ★ 67 10

osquery/osquery-python
python bindings for osquery
Python ★ 75 18

1,097 contributions in the last year



Learn how we count contributions.

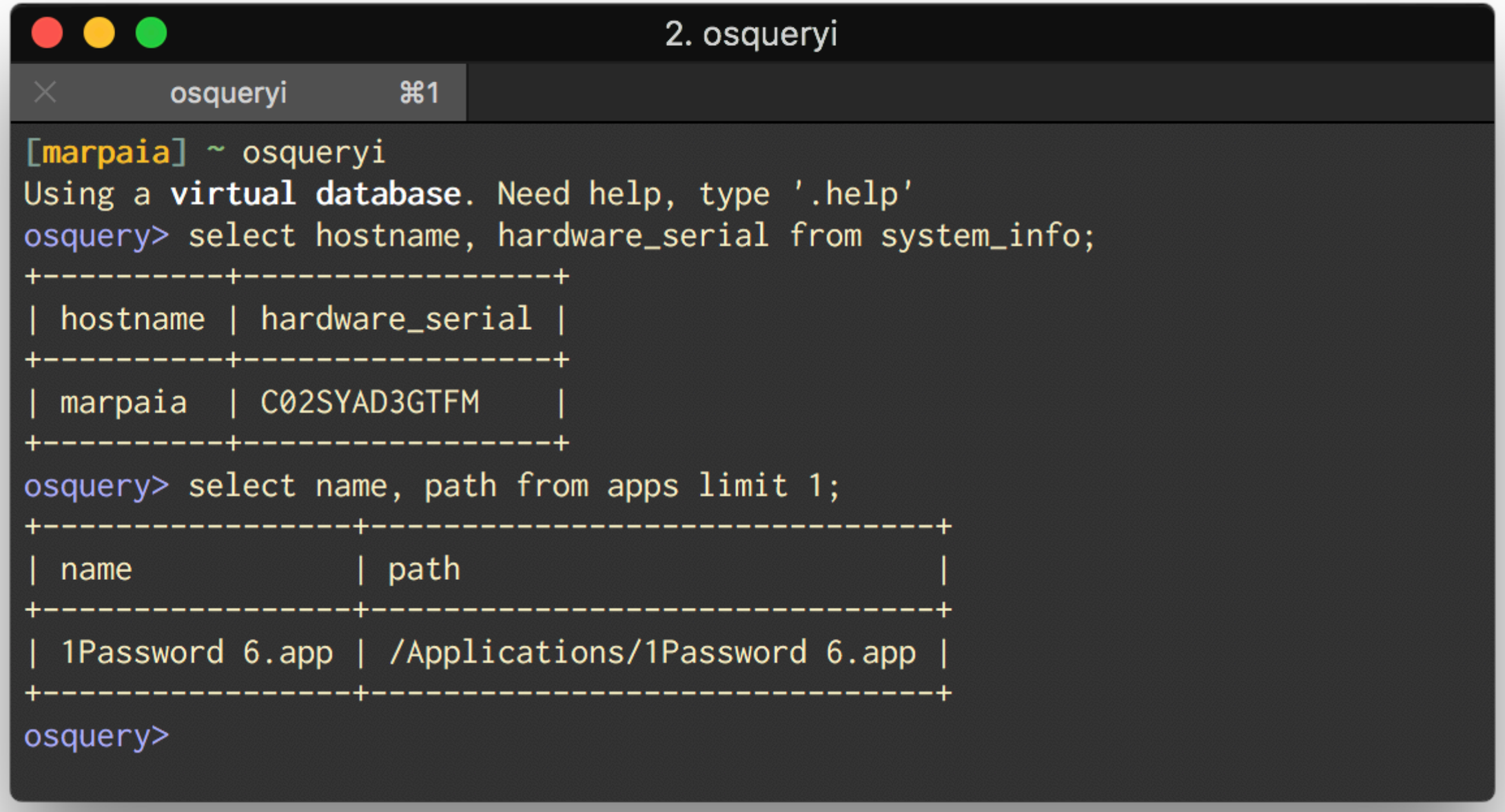
Less More

Agenda

- Osquery introduction and background
- Architecture of an osquery deployment
- Kolide Fleet as an osquery control server
- Kolide Launcher for packaging and updating osquery

facebook/osquery

Performant endpoint visibility


2. osqueryi
osqueryi ⌘1
[marpaia] ~ osqueryi
Using a virtual database. Need help, type '.help'
osquery> select hostname, hardware_serial from system_info;
+----------+-----------------+
| hostname | hardware_serial |
+----------+-----------------+
| marpaia | C02SYAD3GTFM |
+----------+-----------------+
osquery> select name, path from apps limit 1;
+-----------------+--------------------------------+
| name | path |
+-----------------+--------------------------------+
| 1Password 6.app | /Applications/1Password 6.app |
+-----------------+--------------------------------+
osquery>

147 Tables

Osquery Version: 2.10.2 (current)

Show only Tables compatible with: macOS

Restore Default View

acpi_tables

Firmware ACPI functional table common metadata and content.

Improve this Description on Github

COLUMN	TYPE	DESCRIPTION
name	TEXT	ACPI table name
size	INTEGER	Size of compiled table data
md5	TEXT	MD5 hash of table content

ad_config

OS X Active Directory configuration.

Improve this Description on Github

COLUMN	TYPE	DESCRIPTION
name	TEXT	The OS X-specific configuration name
domain	TEXT	Active Directory trust domain
option	TEXT	Canonical name of option
value	TEXT	Variable typed option value

alf

OS X application layer firewall (ALF) service details.

SQL powered operating system instrumentation, monitoring, and analytics. https://osquery.io

security | monitoring | intrusion-detection | sql

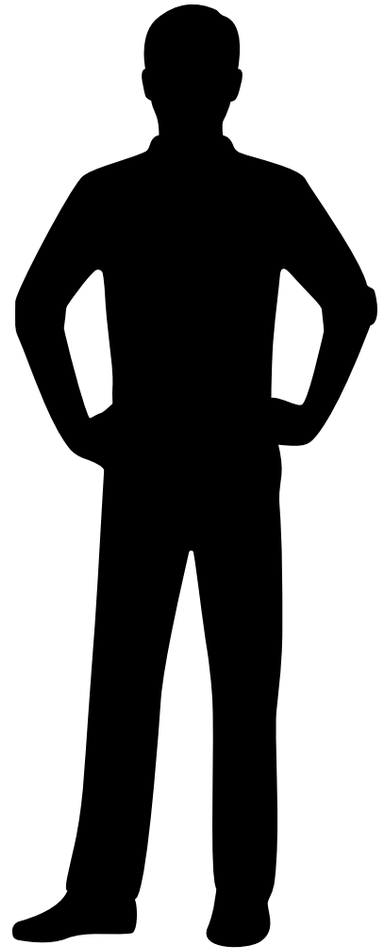
4,168 commits | **2** branches | **81** releases | **182** contributors

Branch: **master** | New pull request | Create new file | Upload files | Find file | Clone or download

alessandrogario committed with **theopolis** process_file_events: Add fields euid and egid and cleanup logs — Latest commit 44e03ba on Dec 12, 2017

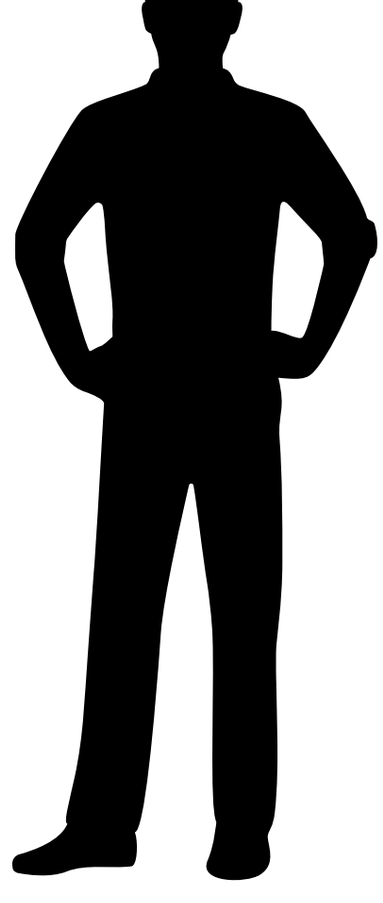
CMake	deps: Improve native (non-deps) builds (#4060)	2 days ago
docs	website: Upload dark version of logo for README (#4065)	a day ago
external	external: Enable external applications through make external (#3023)	11 months ago
include/osquery	feature: URI parsing from folly (#4035)	10 days ago
kernel	license: Change license to Apache 2.0 and GPLv2 (#4007)	29 days ago
osquery	process_file_events: Add fields euid and egid and cleanup logs	22 hours ago
packs	added IOCs to query for OSX_MaMi malware (#4055)	4 days ago
specs	process_file_events: Add fields euid and egid and cleanup logs	22 hours ago
third-party @ 4ef099c	deps: Build linenoise locally (third-party) (#4058)	2 days ago
tools	deps: Improve native (non-deps) builds (#4060)	2 days ago
.clang-format	format: Remove Cpp restriction (#3521)	6 months ago
.gitignore	audit-based file integrity monitoring (#3492)	23 hours ago
.gitmodules	removing lib submodule	3 years ago
.watchmanconfig	watcher: Do not initialize the config in watcher (#3403)	7 months ago
CMakeLists.txt	build: Fix OSQUERY_BUILD_SHARED linkage (#4062)	2 days ago

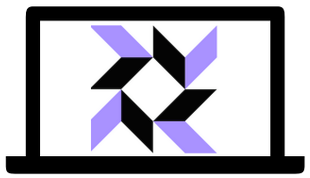
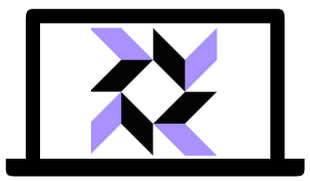
this is you

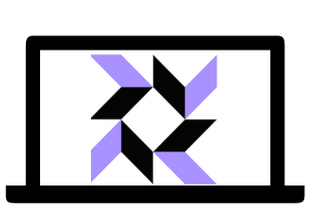
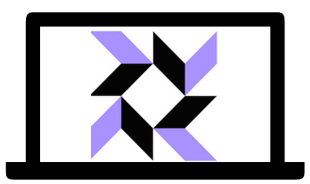
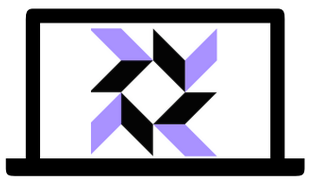
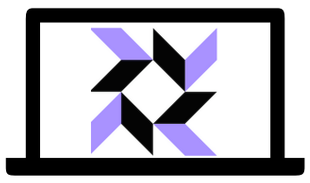


these are the macs

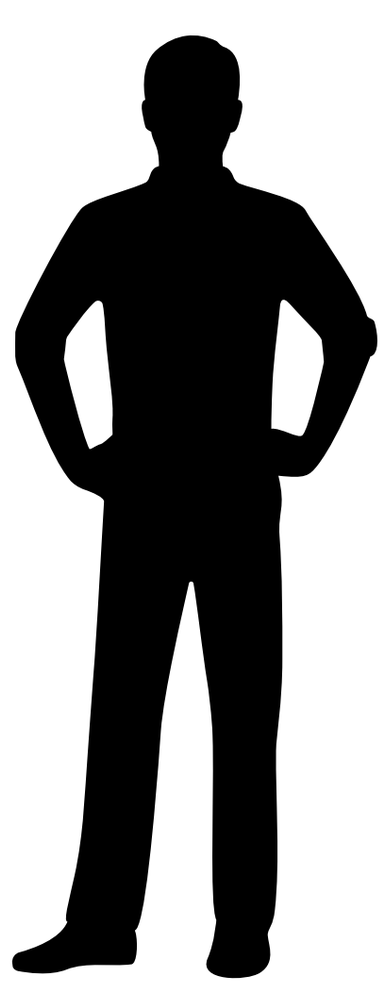
that you manage

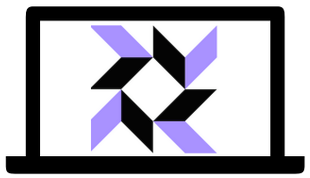


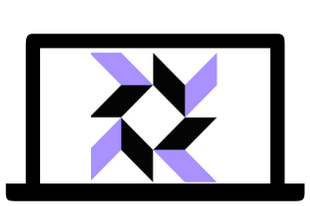



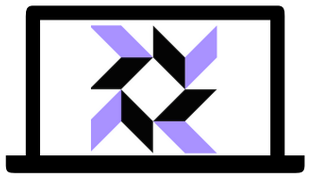





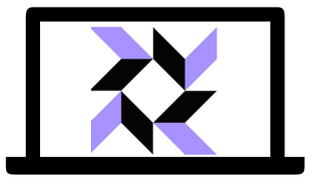
you want to install
osquery on your Macs



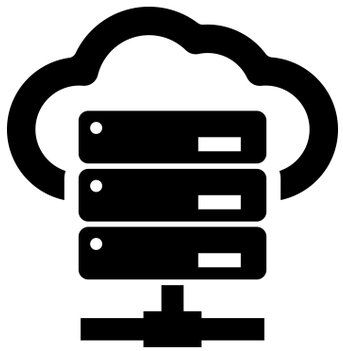


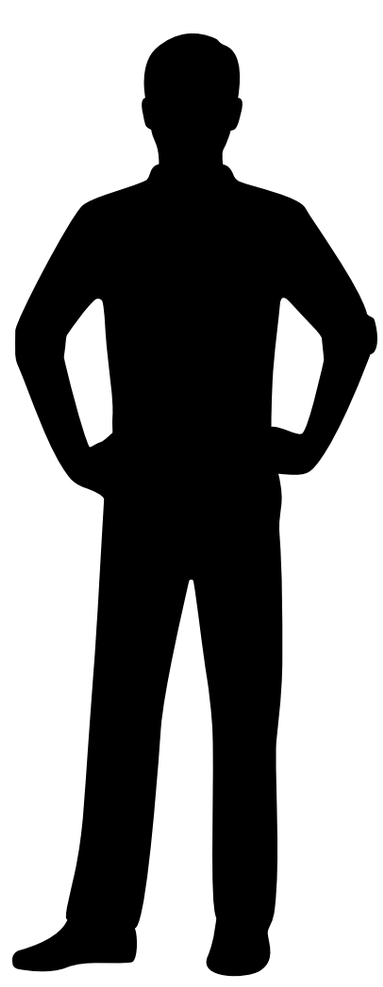


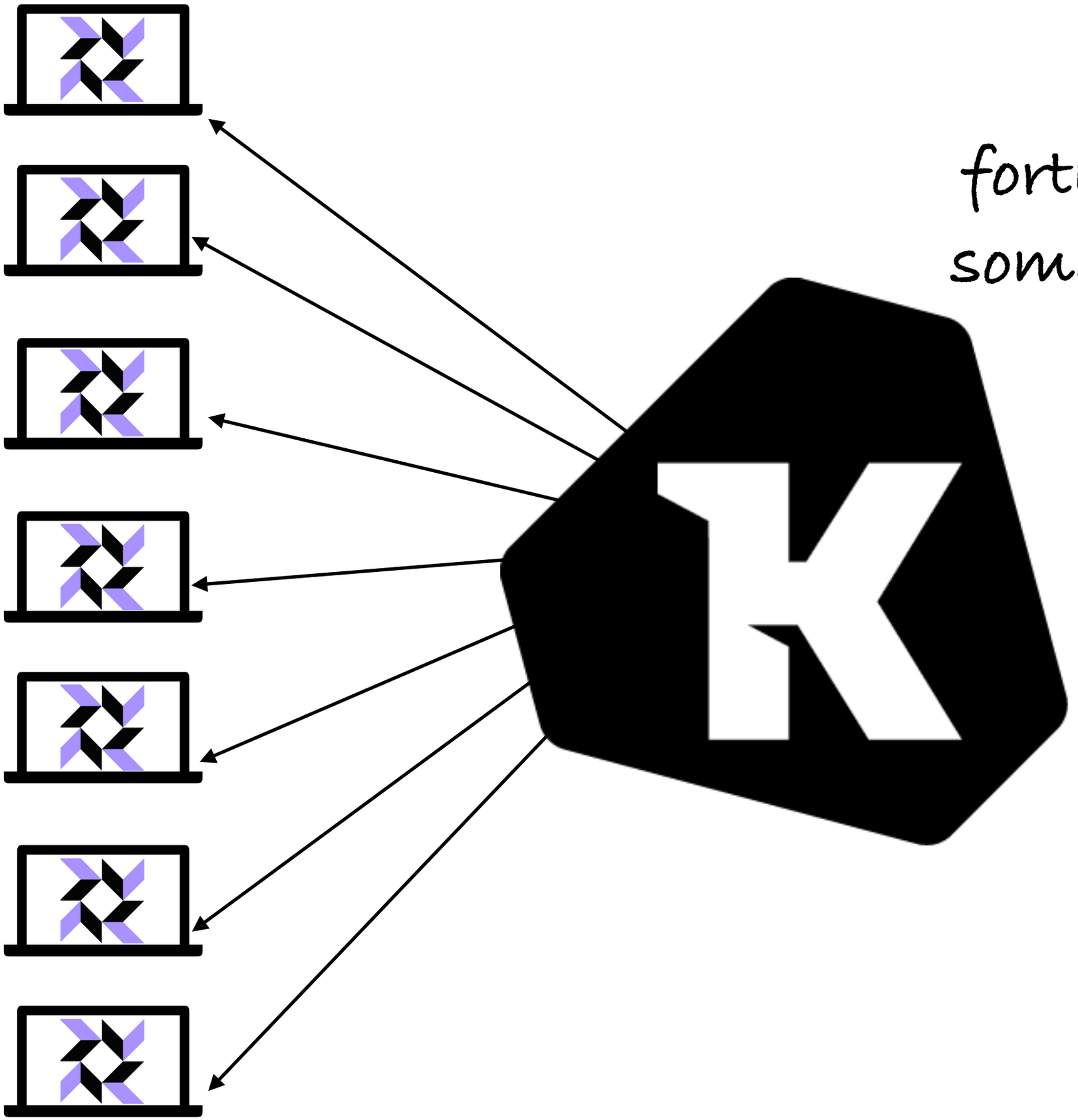




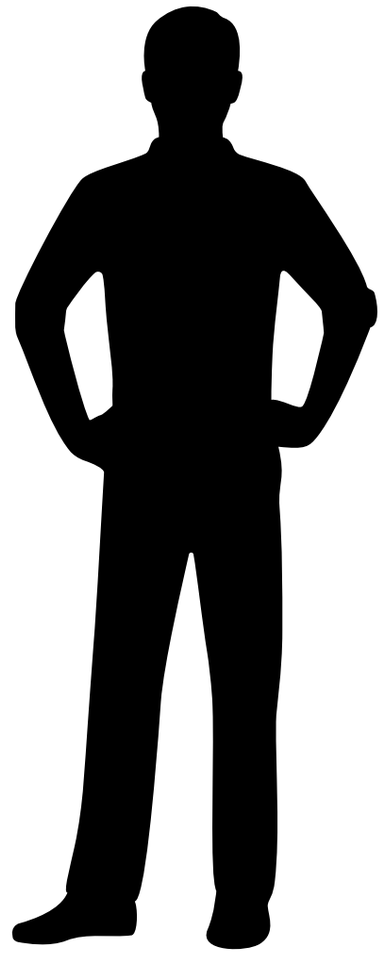
but first you need a
server for your osquery
nodes to connect to

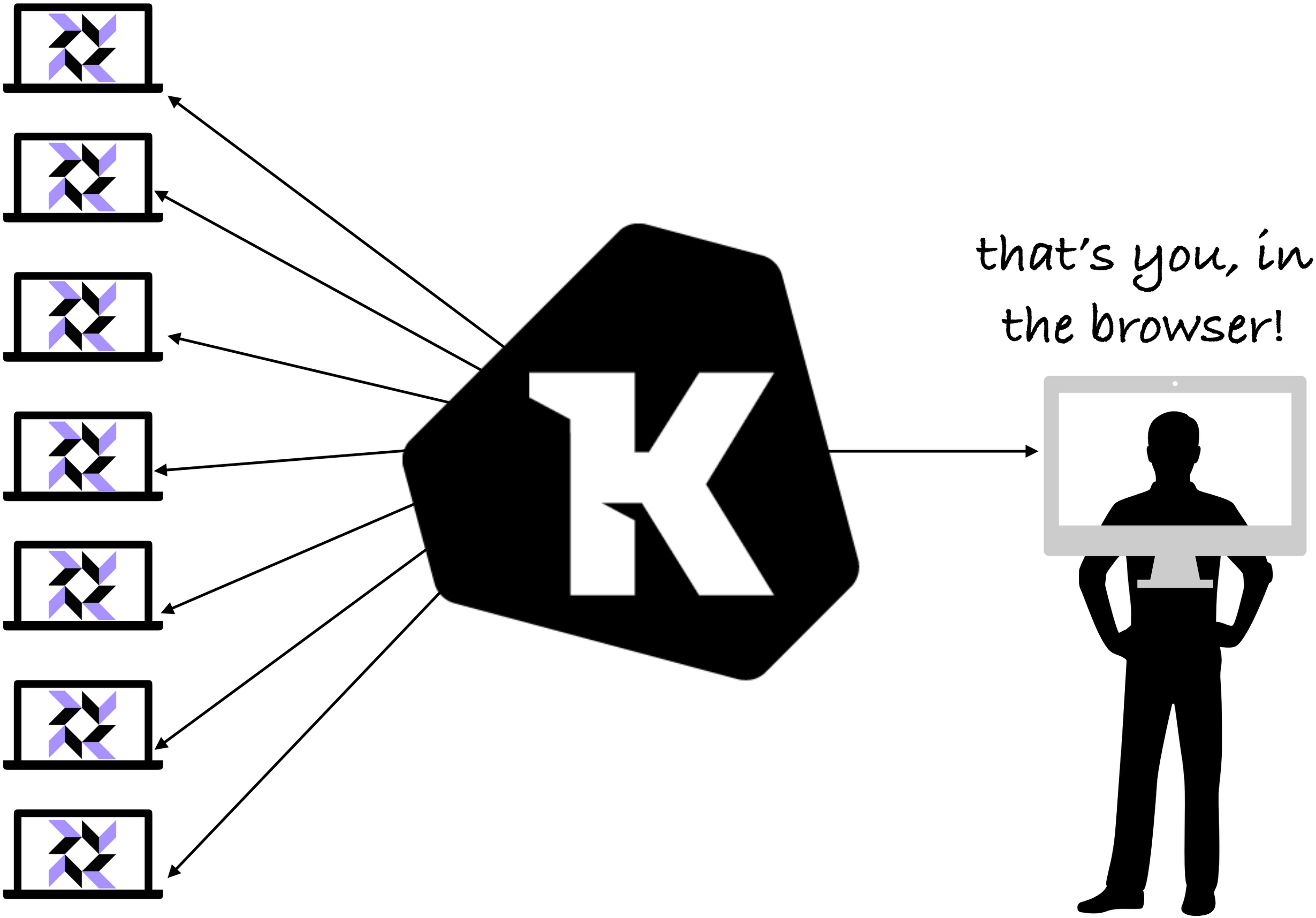






fortunately I have
something for that




that's you, in
the browser!

There are two things that are hard about deploying osquery

- The osquery binary lifecycle
    - Packaging osquery
    - Configuring it to connect to your server
    - Keeping it up to date
- Connecting your fleet of osquery nodes
    - Running live queries
    - Logically grouping hosts into labels
    - Scheduling queries to run on an on-going basis
    - Saving and iterating on your favorite queries

Kolide Launcher for Osquery

STREAMLINE YOUR OSQUERY DEPLOYMENT

Built for Kolide, 100% Open Source

Launcher is the result of hard-won experience, building products and supporting organizations, making long term investments in the **Osquery** ecosystem.

Osquery possesses an incredible range of features and utility but getting it up and running across your fleet can be a daunting task. That's why we built **Kolide Launcher**, an open-source project aimed to remove the hurdles of installing, updating and using osquery at scale.

Key Osquery Improvements

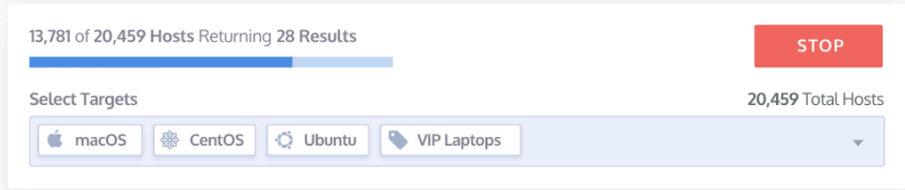
Always Up to Date

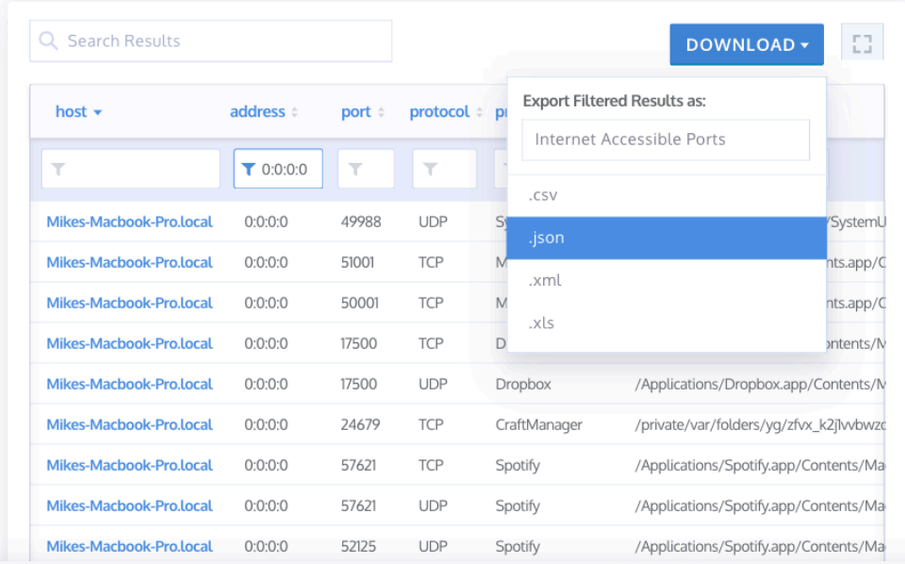
Easy Packaging & Deployment

gRPC Remote API

Kolide Fleet

Open Source Osquery Manager

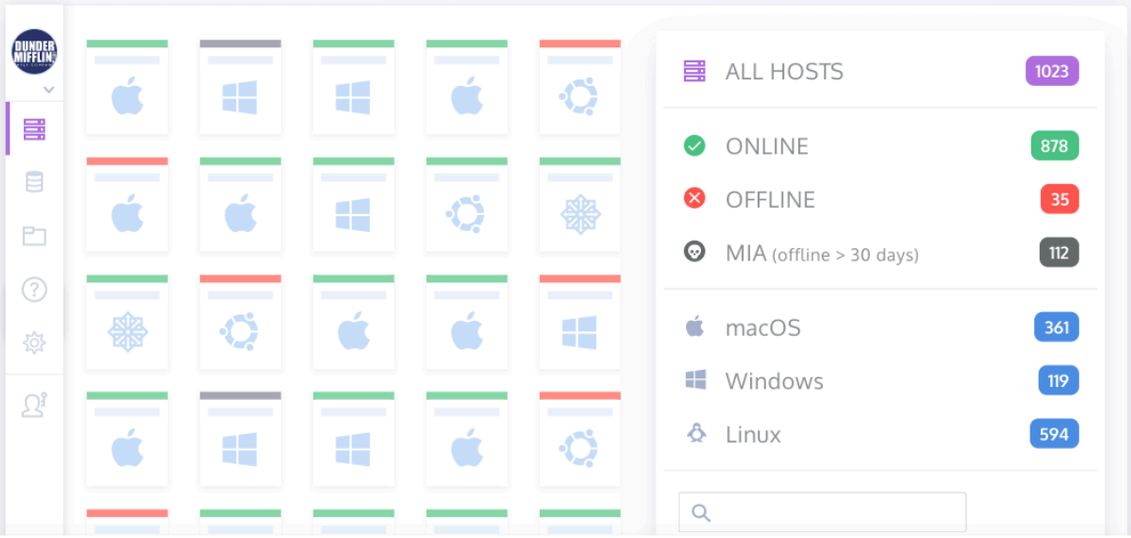




WRITE QUERIES ON THE FLY
EXPLORE LIVE STREAM RESULTS

Curious as to what listening ports have active connections? What hosts are currently unencrypted? The scope and breadth of your searches are totally customizable.

- Query individual targets, groups or your entire fleet.
- Drill into results, filter and export for further analysis.
- Query processes, files, packages, user access and more...



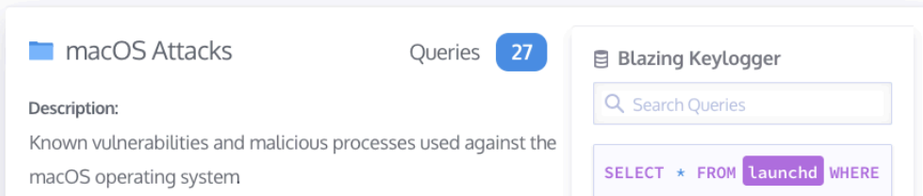
EVERY MACHINE AT A GLANCE, ORGANIZED YOUR WAY

Track, manage and monitor your entire infrastructure from a single screen. Whether you want to see machines with low disk space, overheating or simply running vulnerable software. Labels will help you group your fleet in an organized and intelligible way.

- Create dynamic labels that are automatically populated.
- Organize your fleet by status, platform or custom criteria.
- Use labels as targets in queries and packs.

GROUP & RUN QUERIES ON A RECURRING BASIS WITH PACKS

Group queries together by any common purpose or function you can imagine. Run them on a scheduled basis and output the logs together. Craft packs of



Demo!

Kolide Customer Reliability Engineering

This is macOS administration role and a customer support role combined into one. *This role requires broad internal coordination to respond to customer inquiries and provide advice on macOS management strategy to customers. You will use your macOS administration skills to help customers use Kolide Cloud to create a successful macOS management and insight function in their organization. This is a remote role, open to candidates anywhere in US.*

https://kolide.com/jobs