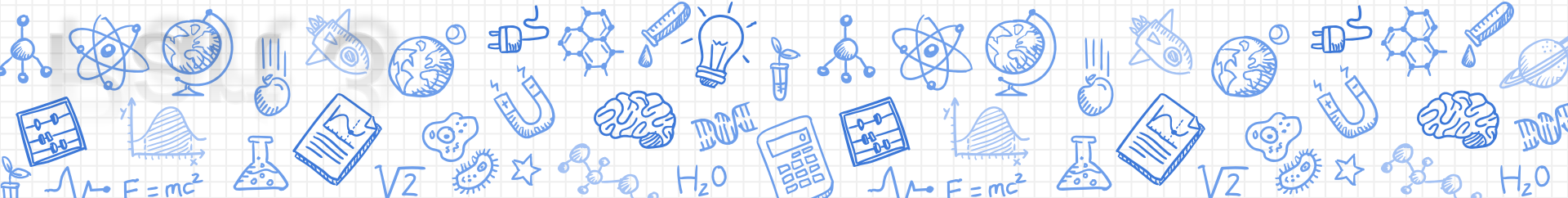
Digital Forensics and Incident Response in the Cloud

Part 3

Dr. Michael Cohen
Velocidex Innovations.
https://www.velocidex.com/

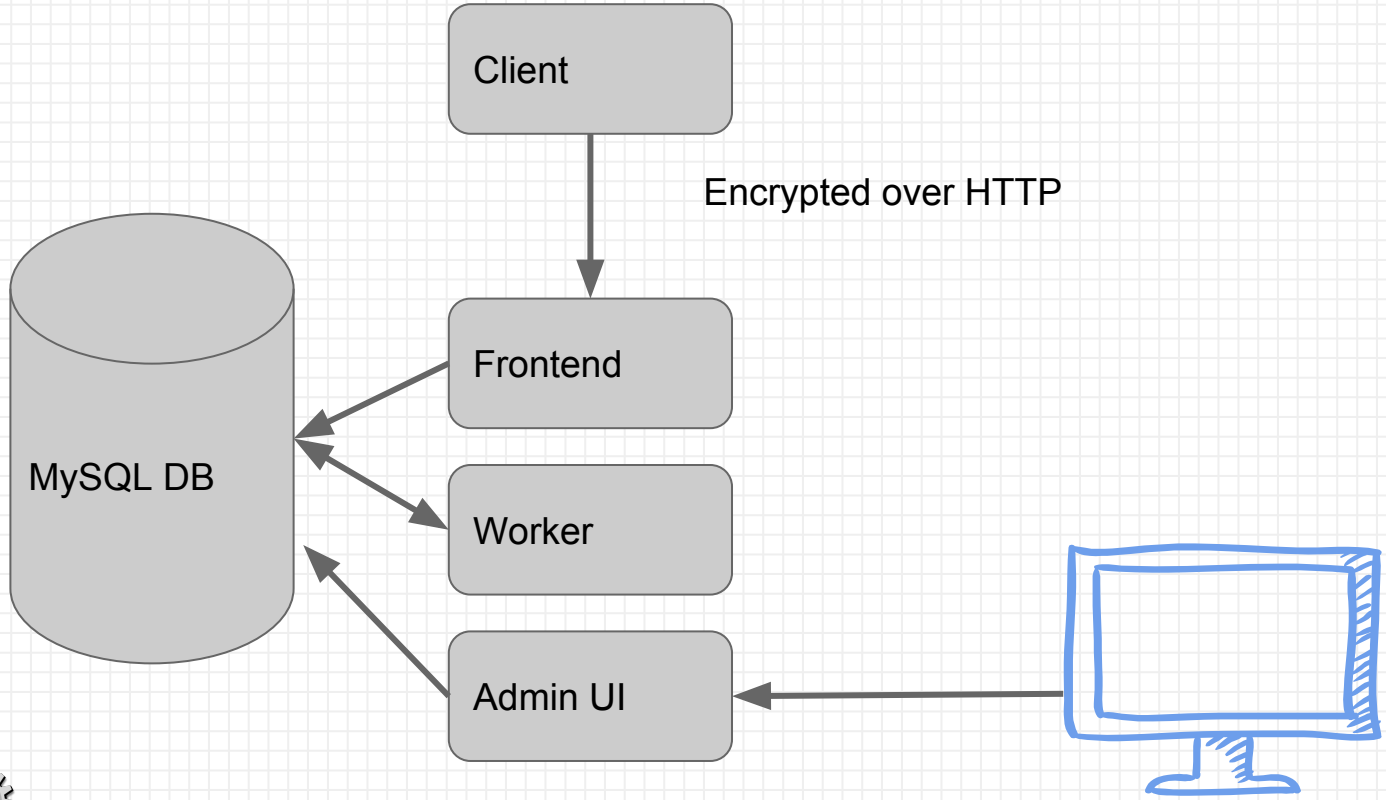


Part 3: GRR and Velociraptor

What is GRR?

- ✘ Incident response tool developed by Google
- ✘ Agent based
- ✘ Written in Python
- ✘ Opensource
- ✘ Used internally by Google - battle tested
  - ✗ Although not in quite the same configuration as open source.

Main GRR architecture



GRR Strengths

- ✘ Artifacts - a collaborative way of specifying and sharing forensic artifacts
- ✘ Very easy to install
- ✘ Ability to do a “hunt” - collect the same data across every node
  - ✗ Can group hunts by label.
- ✘ Very good and intuitive UI
  - ✗ This also has an external API surface.

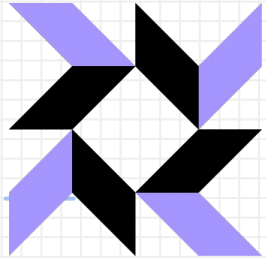
GRR – Weaknesses

- ✘ Very intensive on DB
  - ✗ Lots of traffic between components
  - ✗ No clear data expiration path (policy is to collect everything on all clients forever).
- ✘ Large files are stored in DB
- ✘ Building clients is hard due to Python.
  - ✗ The GRR team has done lots of great work on making this slightly easier but it's hard to modify the client.
  - ✗ GRR client is inflexible but can run arbitrary code.

What is Velociraptor

- ✘ Still an immature project!
- ✘ The aim is to improve and build on GRR
  - ✗ Client written in GO:
    - Makes it easier to deploy, package and rebuild.
  - ✗ Supports VQL as the main mode of operation
    - Easier to adapt to changing requirements.
    - Very flexible.
- ✘ Open source, supported by Velocidex Innovations.

What is OSQuery?



- ✘ A flexible tool that makes your OS look like a database
- ✘ Use SQL SELECT queries to query the host OS

```
osquery> SELECT name, path, pid FROM processes WHERE on_disk = 0;
name = Drop_Agent
path = /Users/jim/bin/dropage
pid = 561
```

OSQuery

- Very flexible
  - Can join 2 or more tables to make really powerful queries.

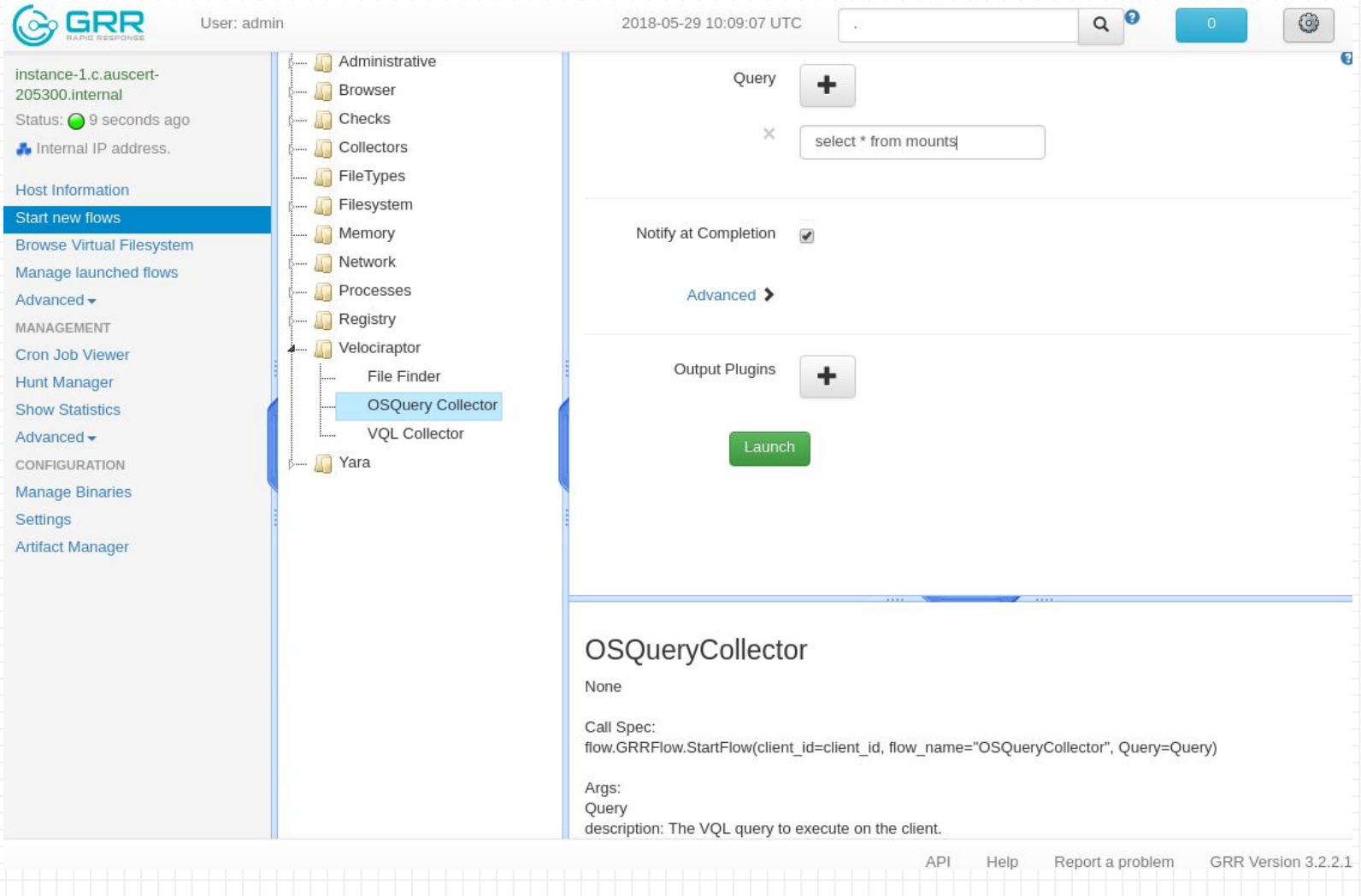

```
  "logged_in_users": {
    "query" : "select liu.*, p.name, p.cmdline, p.cwd, p.root from logged_in_users liu, processes p where liu.pid = p.pid;",
    "interval" : "3600",
    "platform": "posix",
    "version" : "1.4.5",
    "description" : "Retrieves the list of all the currently logged in users in the target system.",
    "value" : "Useful for intrusion detection and incident response. Verify assumptions of what accounts should be accessing what systems and identify machines accessed during a compromise."
  }
```

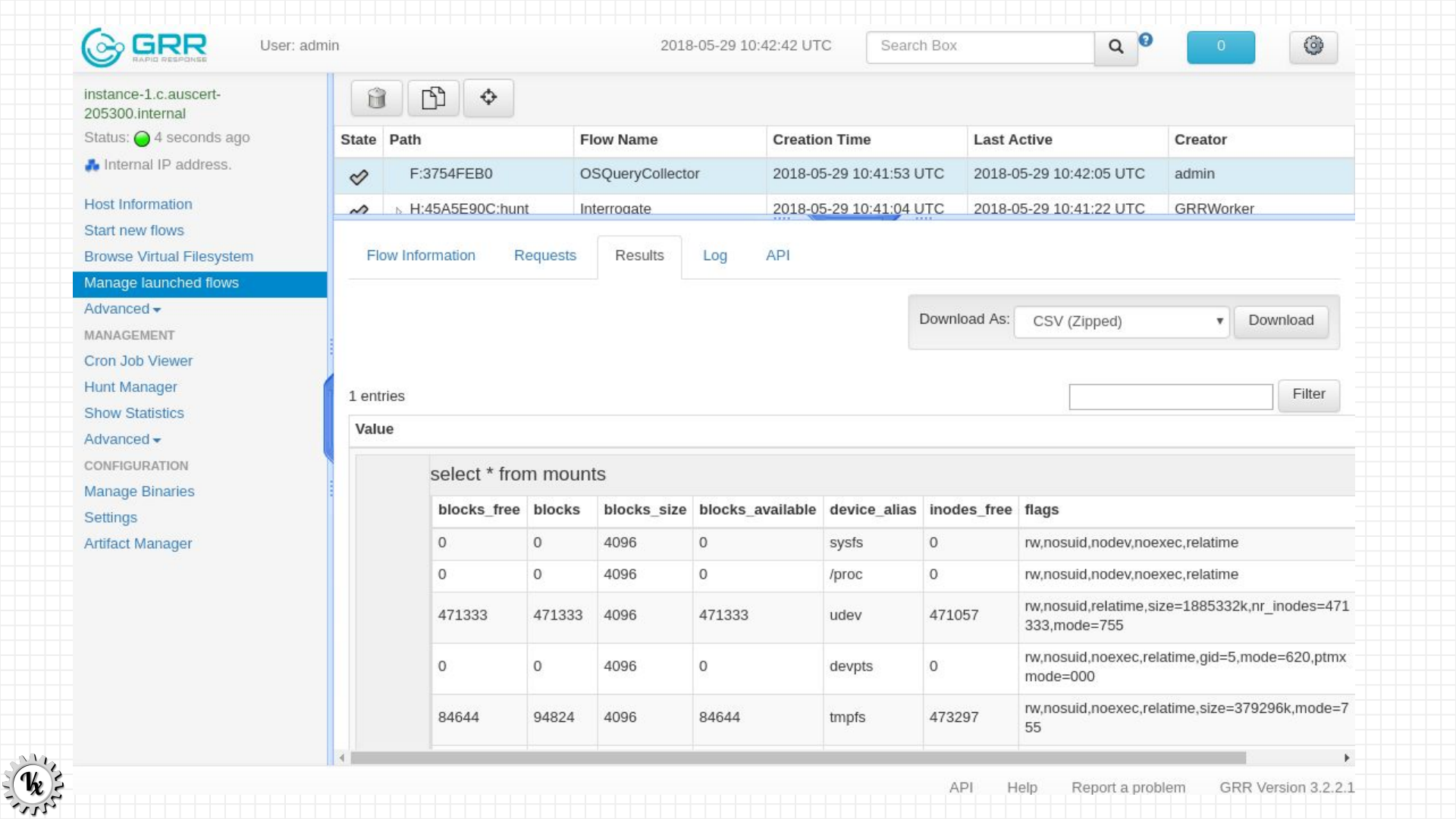

What is VQL?

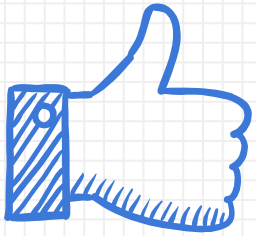
- ✘ An extension of SQL based on EFilter:
  - ✗ Instead of tables, provides plugins which can take arguments.
  - ✗ Has a more natural progression of joining outputs into input of plugins.

```
+-------------------------------+-------------------------------+
|          FS CREATION          |            FULLPATH           |
+-------------------------------+-------------------------------+
| 2018-01-23 15:47:16 +1000 AEST | "/home/lost+found"           |
+-------------------------------+-------------------------------+
SELECT ModTime AS FS_Creation, FullPath FROM glob(globs= { SELECT
mountpoint + '/lost+found' FROM filesystems()})
```

Subselect result is presented as a plugin arg


GRR
RAPID RESPONSE
User: admin
2018-05-29 10:09:07 UTC
0
instance-1.c.auscert-205300.internal
Status: 9 seconds ago
Internal IP address.
Host Information
Start new flows
Browse Virtual Filesystem
Manage launched flows
Advanced
MANAGEMENT
Cron Job Viewer
Hunt Manager
Show Statistics
Advanced
CONFIGURATION
Manage Binaries
Settings
Artifact Manager
Administrative
Browser
Checks
Collectors
FileTypes
Filesystem
Memory
Network
Processes
Registry
Velociraptor
File Finder
OSQuery Collector
VQL Collector
Yara
Query
select * from mounts
Notify at Completion
Advanced
Output Plugins
Launch
OSQueryCollector
None
Call Spec:
flow.GRRFlow.StartFlow(client_id=client_id, flow_name="OSQueryCollector", Query=Query)
Args:
Query
description: The VQL query to execute on the client.
API
Help
Report a problem
GRR Version 3.2.2.1


GRR
RAPID RESPONSE
User: admin
2018-05-29 10:42:42 UTC
Search Box
0
instance-1.c.auscert-205300.internal
Status: 4 seconds ago
Internal IP address.
Host Information
Start new flows
Browse Virtual Filesystem
Manage launched flows
Advanced
MANAGEMENT
Cron Job Viewer
Hunt Manager
Show Statistics
Advanced
CONFIGURATION
Manage Binaries
Settings
Artifact Manager
State
Path
Flow Name
Creation Time
Last Active
Creator
F:3754FEB0
OSQueryCollector
2018-05-29 10:41:53 UTC
2018-05-29 10:42:05 UTC
admin
H:45A5E90C:hunt
Interrogate
2018-05-29 10:41:04 UTC
2018-05-29 10:41:22 UTC
GRRWorker
Flow Information
Requests
Results
Log
API
Download As:
CSV (Zipped)
Download
1 entries
Filter
Value
select * from mounts
blocks_free
blocks
blocks_size
blocks_available
device_alias
inodes_free
flags
0
0
4096
0
sysfs
0
rw,nosuid,nodev,noexec,relatime
0
0
4096
0
/proc
0
rw,nosuid,nodev,noexec,relatime
471333
471333
4096
471333
udev
471057
rw,nosuid,relatime,size=1885332k,nr_inodes=471333,mode=755
0
0
4096
0
devpts
0
rw,nosuid,noexec,relatime,gid=5,mode=620,ptmxmode=000
84644
94824
4096
84644
tmpfs
473297
rw,nosuid,noexec,relatime,size=379296k,mode=755
API
Help
Report a problem
GRR Version 3.2.2.1



THANKS!

Any questions?

You can find me at

- mike@velocidex.com
- https://www.velocidex.com