

06-21-19

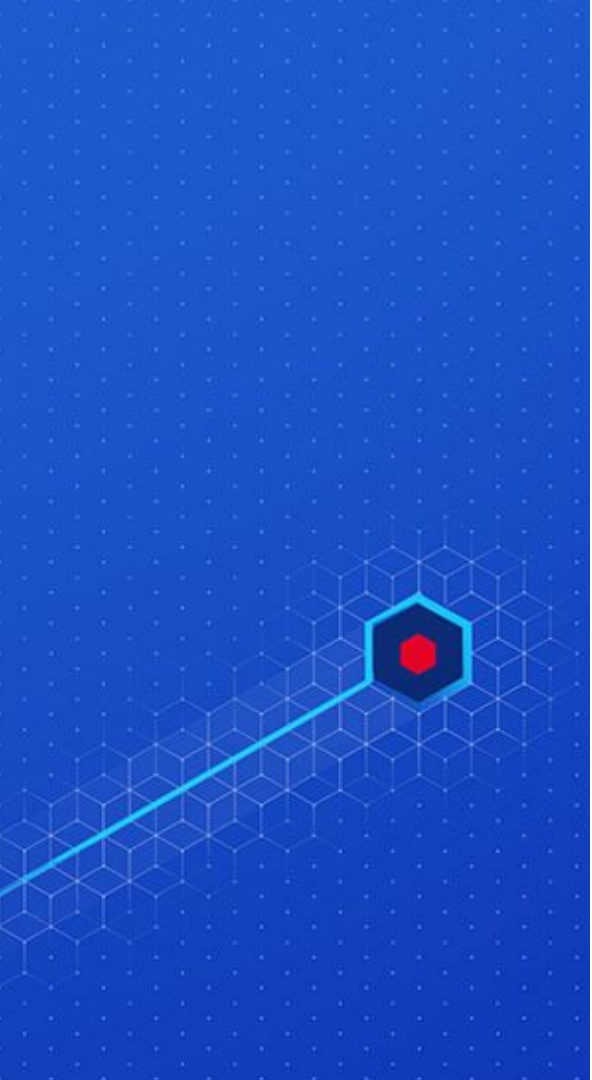
# QueryCon

Taking Osquery to the Mainstream  
to Benefit Us All

Tania McCormack

Carbon Black.

A decorative graphic on the right side of the slide. It features a cyan line that starts from the bottom left and extends diagonally upwards to the right. At the end of this line is a hexagonal shape with a red dot in the center. The background of the slide is a dark blue grid of small dots, with a larger, lighter blue grid of hexagons in the bottom right corner.



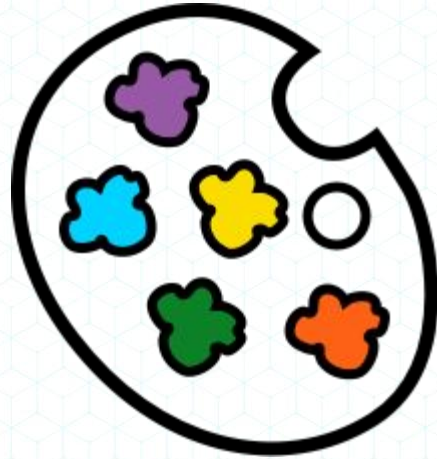
1. We Built Something
2. Research Time
3. Research Summary
4. Experiments
5. Community Recommendations

## Why Carbon Black Joined the Osquery Train

To provide an **easy path**  
for our customers to  
**valuable** real time data.

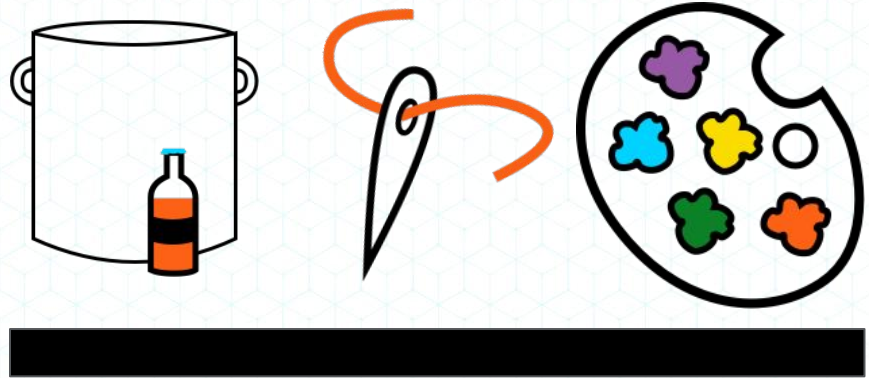
# What We Gave Them

---

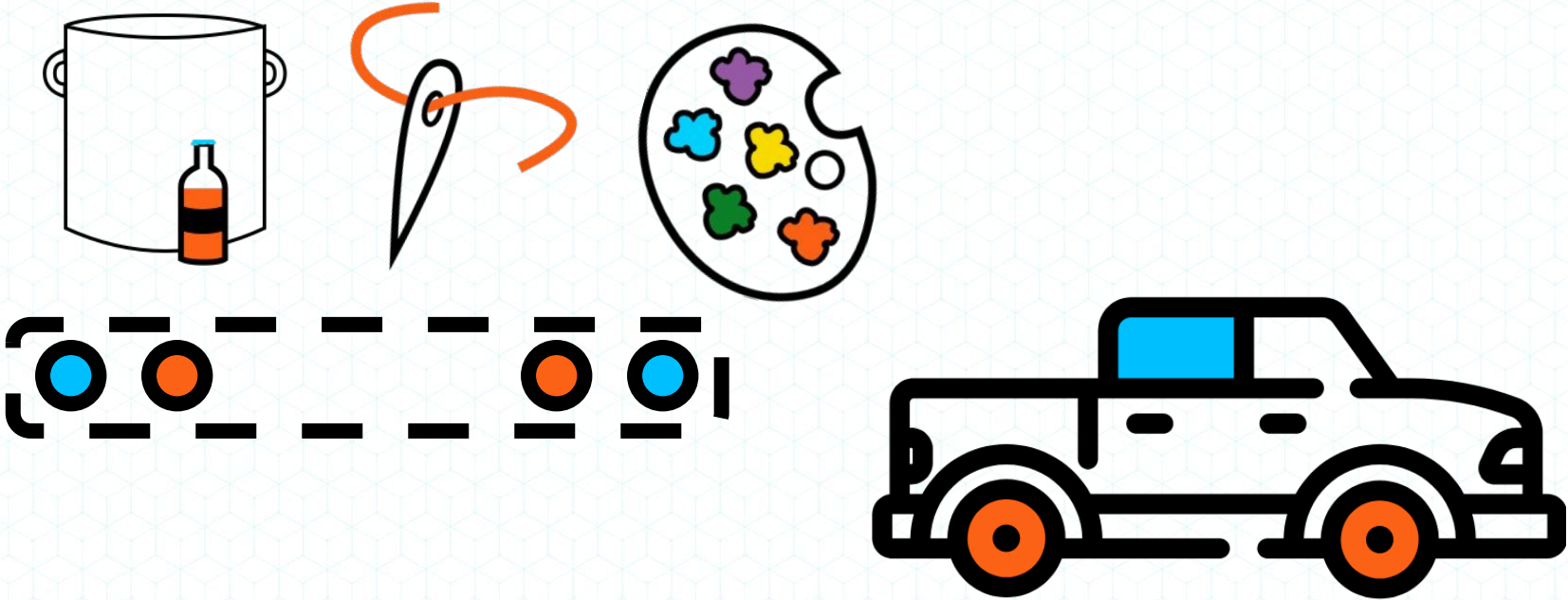


# What We Learned

---



# Oh No...What If?



# How Did We Get Here?

## R1 RESEARCH

Prototypes

Shared Screen

Cust. Interviews

## FIRST FOCUS

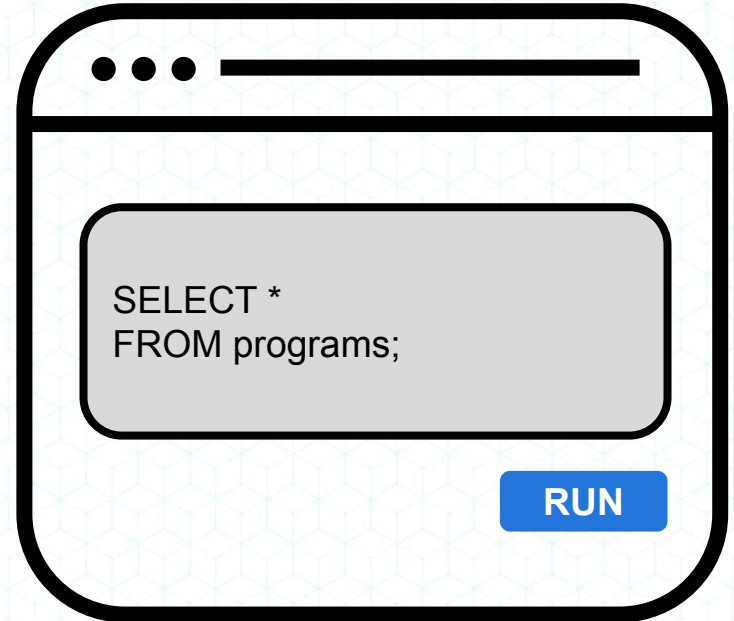


Advanced Users



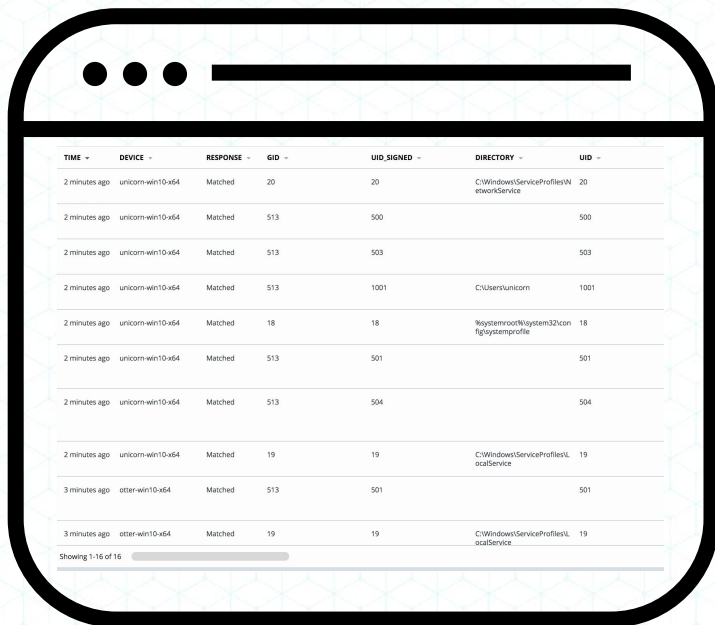
Incident Response

## MVP



# What We Learned

## MVP



TIME	DEVICE	RESPONSE	GID	UID_SIGNED	DIRECTORY	UID
2 minutes ago	unicom-wm10-x64	Matched	20	20	C:\Windows\ServiceProfiles\NetworkService	20
2 minutes ago	unicom-wm10-x64	Matched	513	500		500
2 minutes ago	unicom-wm10-x64	Matched	513	503		503
2 minutes ago	unicom-wm10-x64	Matched	513	1001	C:\Users\unicom	1001
2 minutes ago	unicom-wm10-x64	Matched	18	18	%systemroot%\system32\config\systemprofile	18
2 minutes ago	unicom-wm10-x64	Matched	513	501		501
2 minutes ago	unicom-wm10-x64	Matched	513	504		504
2 minutes ago	unicom-wm10-x64	Matched	19	19	C:\Windows\ServiceProfiles\LocalService	19
3 minutes ago	otter-wm10-x64	Matched	513	501		501
3 minutes ago	otter-wm10-x64	Matched	19	19	C:\Windows\ServiceProfiles\LocalService	19

Showing 1-16 of 16





Research Time

# Asking The Right Questions

## WHAT DON'T WE KNOW?

What is your background?

How can this data help their day to day?

How often do they need it?

How do we surface the need?

When do you need this data?

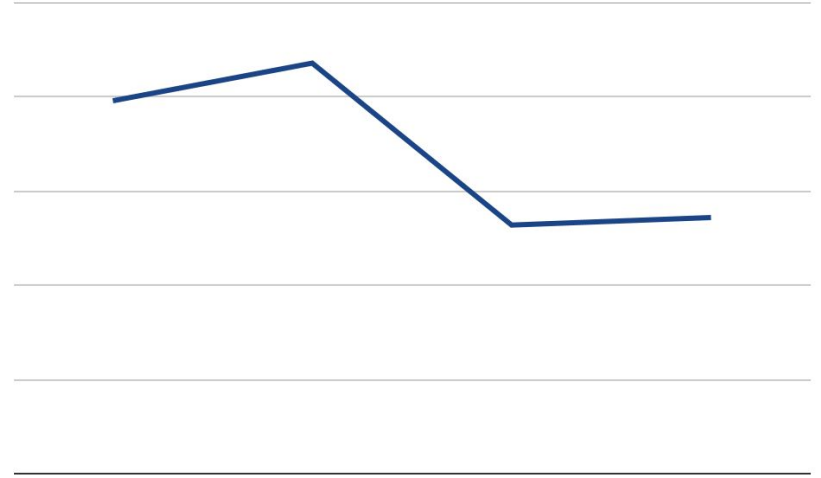
Where do you want to view it?

Why should you care about this data?

What are the best queries for my team needs?

## WHAT WE KNOW

Queries Ran Weekly



# Answering The Questions

---

## Usability Calls

First impressions  
One month later

## Internal Team feedback

SecOps  
Infrastructure  
IT/Help Desk

## User Analytics

User activity  
Storage with new AWS

## Market Check-In

Where does Osquery fit

# Who Are They

---

## What is your role & background?

Security Analyst  
Came from IT

## What's your team like?

1-3 People  
Mix of IT/Security folks

## Have you heard of Osquery?

I think, but never used  
Know “some” SQL

## Why did you try this?

It seemed like something I  
might need to help  
productivity

## Have you been using it?

Not really

# Summary: Current Users

What, why, & when should I query?



What do the results mean?



This doesn't fit my workflow...



# Summary: CB Secops

Hard to get going,  
hard to manage.



Data returned is  
hard to consume.



I just want to set  
and forget.



# Summary: CB IT/Help Desk

It's yet another tool...



If you can get us to root cause faster...



Are there IT focused packs for benchmarking?



# Research Conclusions



# Top Problem Statements

1

Not Comfortable

2

Not Confident

3

Not Hooked

# Goal: Make Users...

1

~~Not~~ Comfortable

2

~~Not~~ Confident

3

~~Not~~ Hooked

# How Did We Get Here? Revisited

FIRST FOCUS



Advanced Users



Incident Response

VS

CURRENT USERS



IT/Security



New to Data



Use Case Unsure

Experiment Time

# Popularity Contest: Recommended Queries



Incident Response



IT Hygiene



Compliance

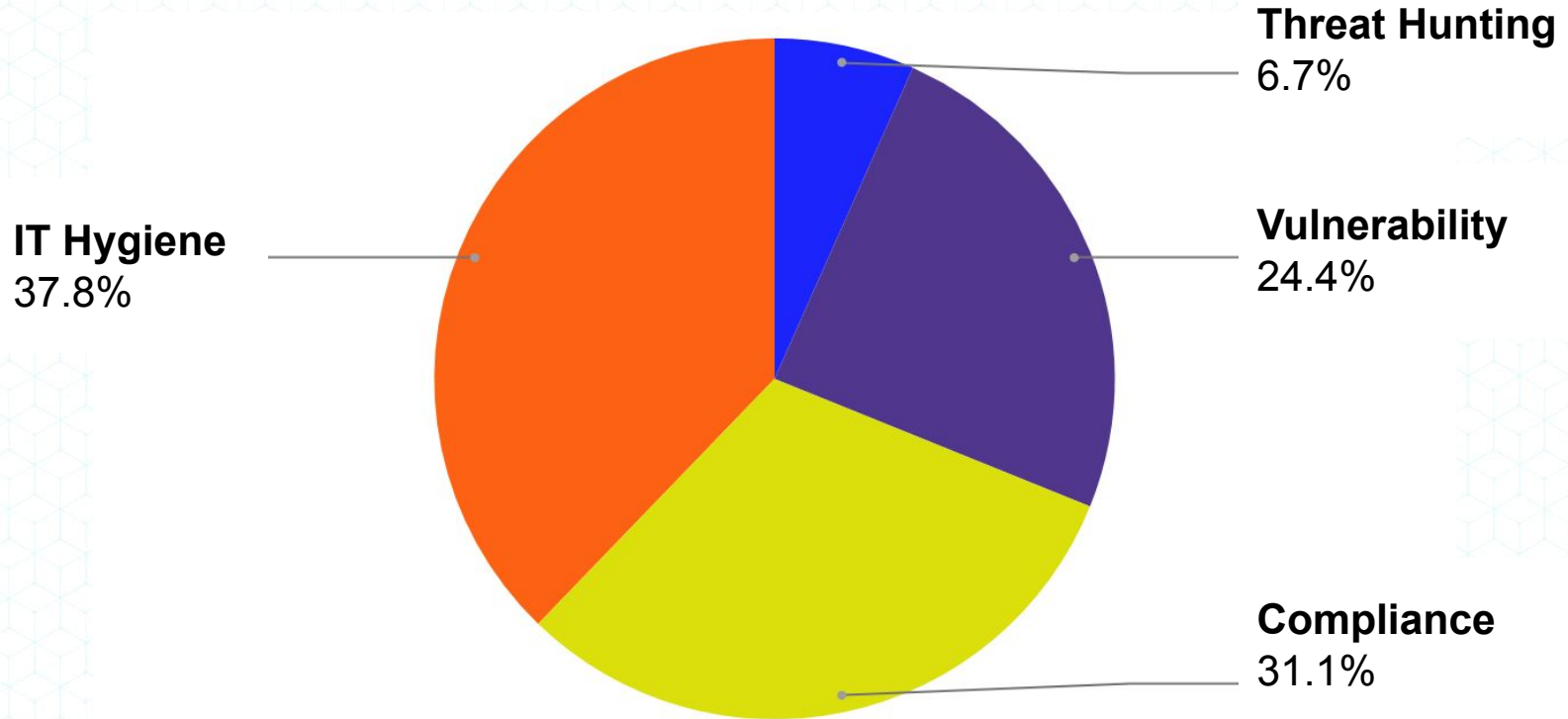


Vulnerability Mgt



Threat Hunting

# Popularity Contest: Results



# How Did We Get Here? Revisited

FIRST FOCUS



Advanced Users



Incident Response

VS

CURRENT USERS



IT/Security



IT Hygiene



New to Data



Compliance

# We Still Have More To Learn

## WHAT DON'T WE KNOW?

~~What is your background?~~

~~How can this data help their day to day?~~

How often do they need it?

How do we surface the need?

When do you need this data?

Where do you want to view it?

Why should you care about this data?

~~What are the best queries for my team needs?~~



**Continue:**  
experiments, interviews,  
and data monitoring



Dear Community

# Top Priority: Improve Barrier of Entry

BETTER DESCRIPTIONS



LOGICAL JARGON



GIVE SOME WHY



CONSIDER A NEW PERSON



REQUIRED COLUMNS



# Cool Ideas

---



Query  
Sharing  
Space



Osquery  
Mentorship



More  
Query  
Hackathons

# Public Query Space

Hosted by Carbon Black

Easily find and share queries

## Query Contest

One query each month wins \$100 Amazon card

Search Query Exchange...



Share a Query

### QUERIES

Use Case



Operating System



Source



#### Query Submission Windows Patch Level

**CB Approved** 2 Comments

Submitted by [coreymaygard](#) 6 hours ago

Description: Cname and patch level of windows hosts  
What The Data Shows: gives a full accountin...

Community

IT Hygiene

Windows



0 Votes



#### Check if Credential Guard is enabled

**Under Review** 3 Comments

Submitted by [mjomha](#) Friday

Description: What does this query look for? Looks for machines that  
have credential guard enabled (Wi...

Community

IT Hygiene

Vulnerability Management

Windows



0 Votes



#### Bitlocker not enabled

**CB Approved** 2 Comments

Submitted by [ksnihur](#) Friday

Description: Looks for Bitlocker is not enabled.  
What The Data Shows: machines where bitlocker i...

Community

Compliance

Windows



0 Votes

# Goal: Make Users...

1

~~Not~~ Comfortable

2

~~Not~~ Confident

3

~~Not~~ Hooked

The background is a solid blue color. It features a subtle pattern of binary code (0s and 1s) scattered across the top half. In the bottom half, there are several faint, semi-transparent hexagonal shapes of varying sizes, some overlapping each other.

**Thank You**

**Carbon Black.**