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
- SQL Query:
  ```sql
  SELECT * FROM programs;
  ```
- Run button
What We Learned

MVP
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

[Graph showing data trends over time]
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

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

- IT Hygiene: 37.8%
- Vulnerability: 24.4%
- Compliance: 31.1%
- Threat Hunting: 6.7%
How Did We Get Here? Revisited

FIRST FOCUS

Advanced Users

Incident Response

CURRENT USERS

IT/Security

New to Data

IT Hygiene

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
Goal: Make Users...

1. Not Comfortable
2. Not Confident
3. Not Hooked
Thank You

Carbon Black.