What I learned from deploying...

osquery@scale

explore from home

Brendan Shaklovitz

@nyanshak

ATLASSIAN

Origin Story

2016/2017

One Small Step for Security Posture

- hard-coded config in pre-built packages

Guiding Principles

- Maintain employee autonomy over their computing environment
- Pursue an unobtrusive approach to osquery data collection
- Be transparent

Ghostscript Vulnerability

CVE-2017-8291

Lesson: Set up alerts!

- long-running processes from /tmp, ~/.Trash, in-memory
- VNC servers
- "interesting" processes / connections
- processes attempting to access /etc/shadow
- processes searching for writeable directories
- making hidden executable files

Lesson: Use an osquery fleet manager

Broader rollout

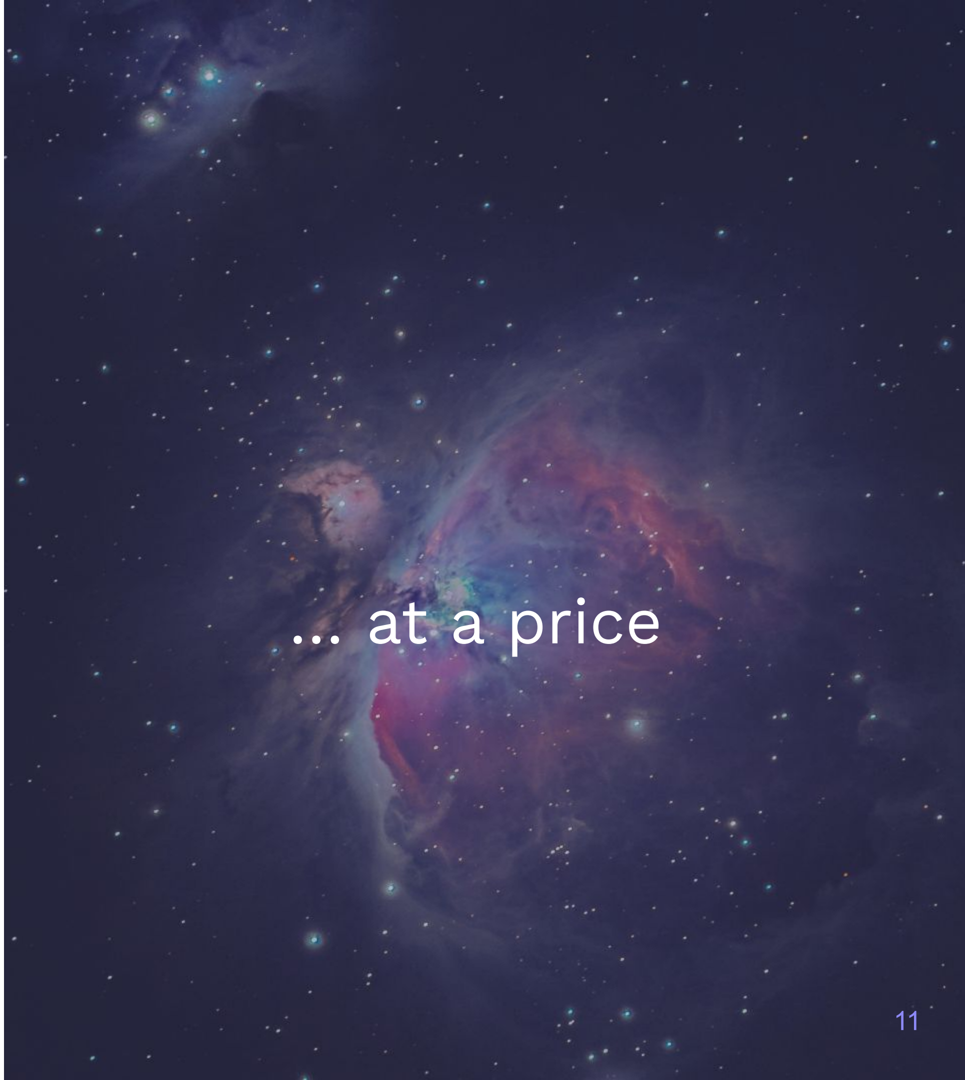
2018/2019

Prioritizing Deployment

- workstations
  - Linux
  - **macOS**
  - Windows
- servers
  - primarily **Linux**
  - Windows

Process Auditing

Great way to gain visibility…

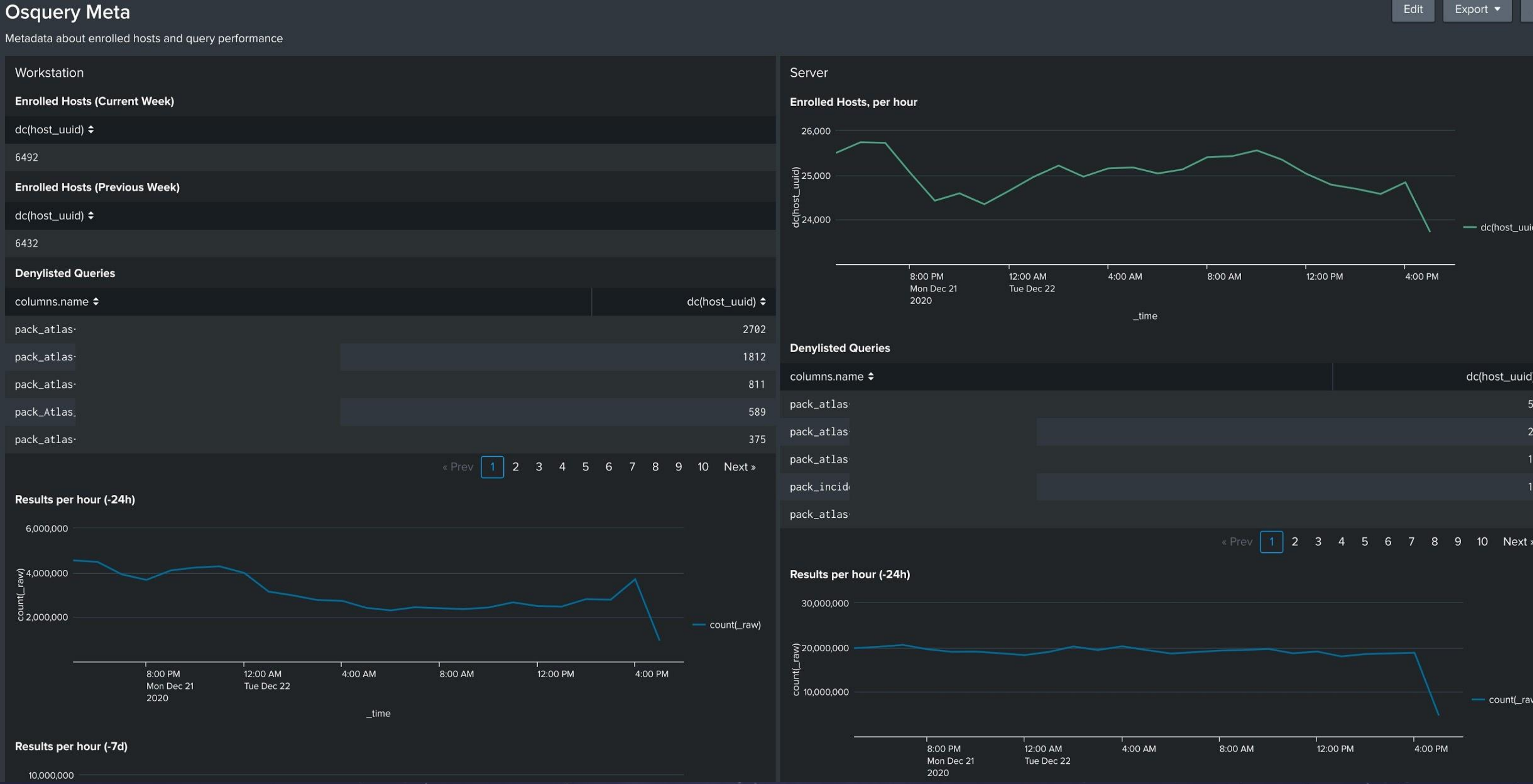


… at a price

Lesson: Test & measure everything!

Measure for Success

2020



Osquery Meta

Metadata about enrolled hosts and query performance

Workstation

Enrolled Hosts (Current Week)

dc(host_uuid) ⬍
6492

Enrolled Hosts (Previous Week)

dc(host_uuid) ⬍
6432

Denylisted Queries

columns.name ⬍	dc(host_uuid) ⬍
pack_atlas-	2702
pack_atlas-	1812
pack_atlas-	811
pack_Atlas_	589
pack_atlas-	375

« Prev 1 2 3 4 5 6 7 8 9 10 Next »

Results per hour (-24h)

Results per hour (-7d)

Server

Enrolled Hosts, per hour

Denylisted Queries

columns.name ⬍	dc(host_uuid
pack_atlas	5
pack_atlas	2
pack_atlas	1
pack_incid	1
pack_atlas	

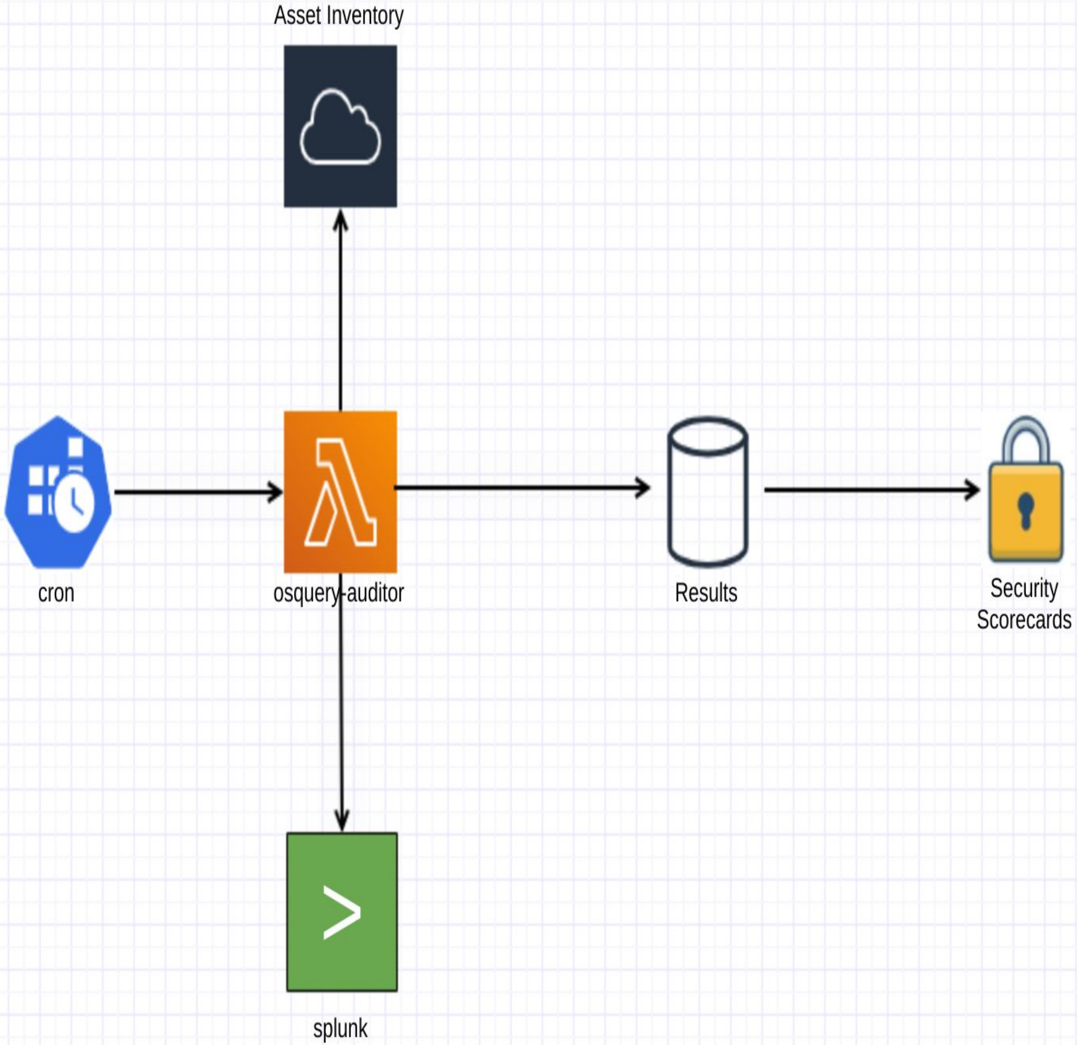
« Prev 1 2 3 4 5 6 7 8 9 10 Next »

Results per hour (-24h)

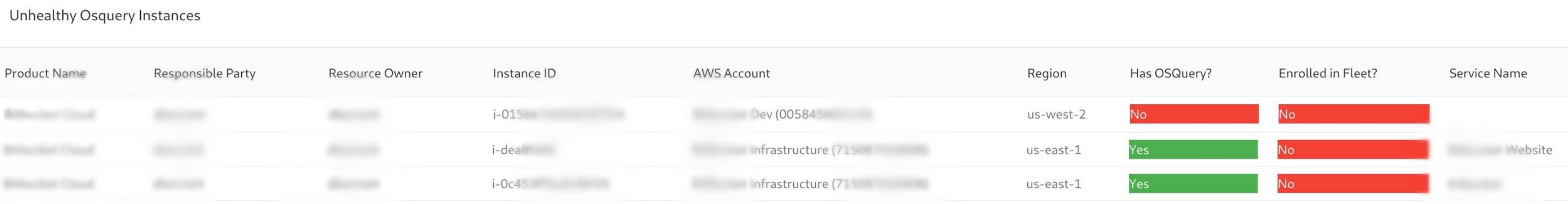
Automate query perf testing

- fail builds if queries are too expensive

How do I know if it's working?

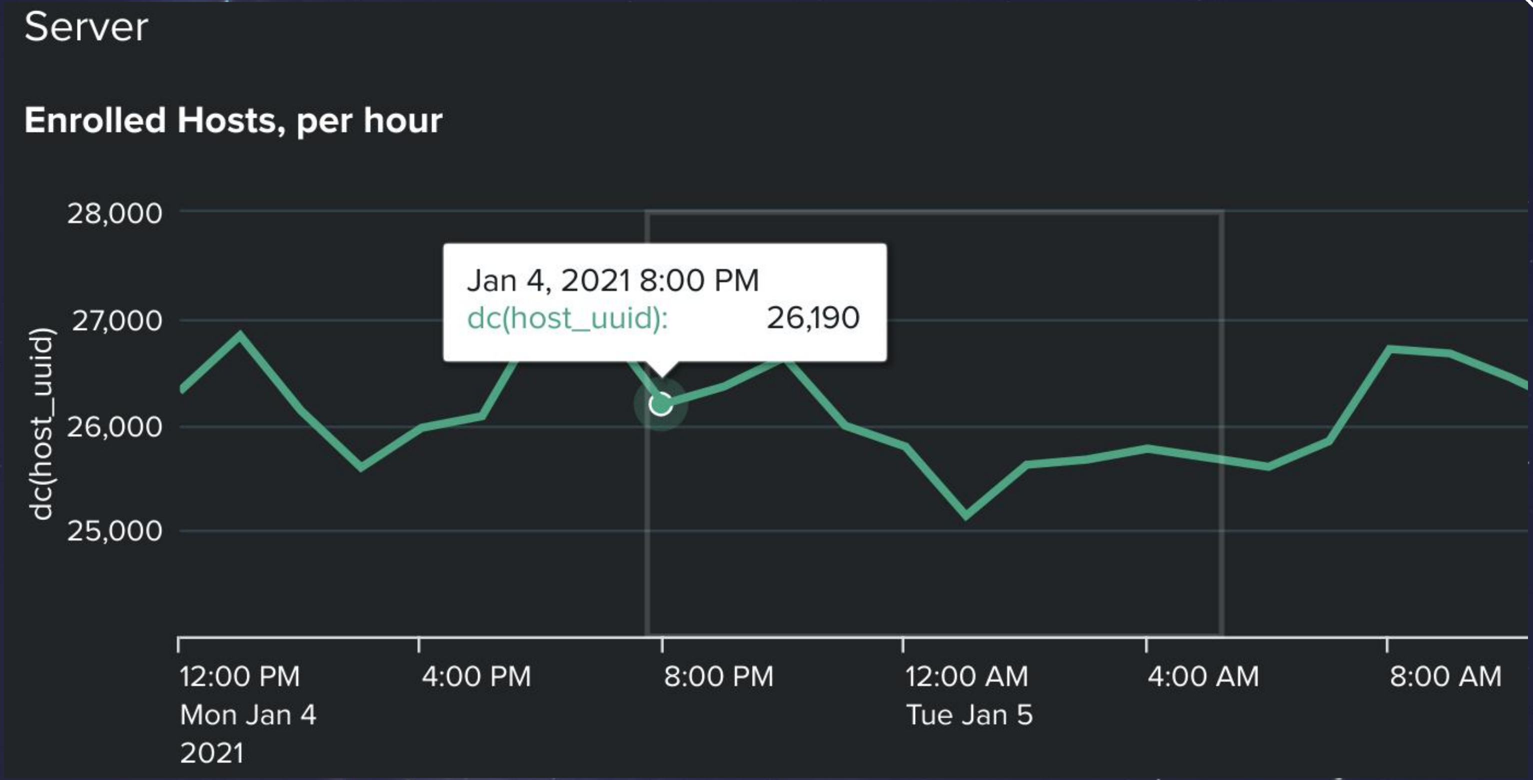


Osquery Auditor



Unhealthy Osquery Instances

Product Name	Responsible Party	Resource Owner	Instance ID	AWS Account	Region	Has OSQuery?	Enrolled in Fleet?	Service Name
[redacted]	[redacted]	[redacted]	i-015[redacted]	[redacted] Dev (00584[redacted]	us-west-2	🟥 No	🟥 No	
[redacted]	[redacted]	[redacted]	i-dea[redacted]	[redacted] Infrastructure (715[redacted]	us-east-1	🟩 Yes	🟥 No	[redacted] Website
[redacted]	[redacted]	[redacted]	i-0c45[redacted]	[redacted] Infrastructure (71[redacted]	us-east-1	🟩 Yes	🟥 No	[redacted]



Server

Enrolled Hosts, per hour

Jan 4, 2021 8:00 PM
dc(host_uuid): 26,190

What's Next?

2021 & Beyond

-- **mission statement** --

osquery installed on **all** systems, running **useful** queries, while having **limited** impact

osquery
@scale

Better tracking for non-EC2 assets

- Azure
- GCP
- EKS
- and more!

Better Configuration Management

- More granular controls & gradual rollout
- Launcher

Other Ideas

- ZeroTrust
- Auto-isolate / shut down
- Query & schedule optimization
- Extensions
- BPF & ESF process auditing

Community Involvement

- Contributions to osquery & Fleet
  - features
  - bug fixes
  - documentation
  - issues
- Getting & giving help in Slack
- Chat with other osquery using companies

Lessons Learned

- start with why
- measure and test everything
- use an osquery fleet manager
- set up automated alerts

Brendan Shaklovitz

@nyanshak

ATLASSIAN