Data-Driven IT

aka, “Why are we doing this thing?”

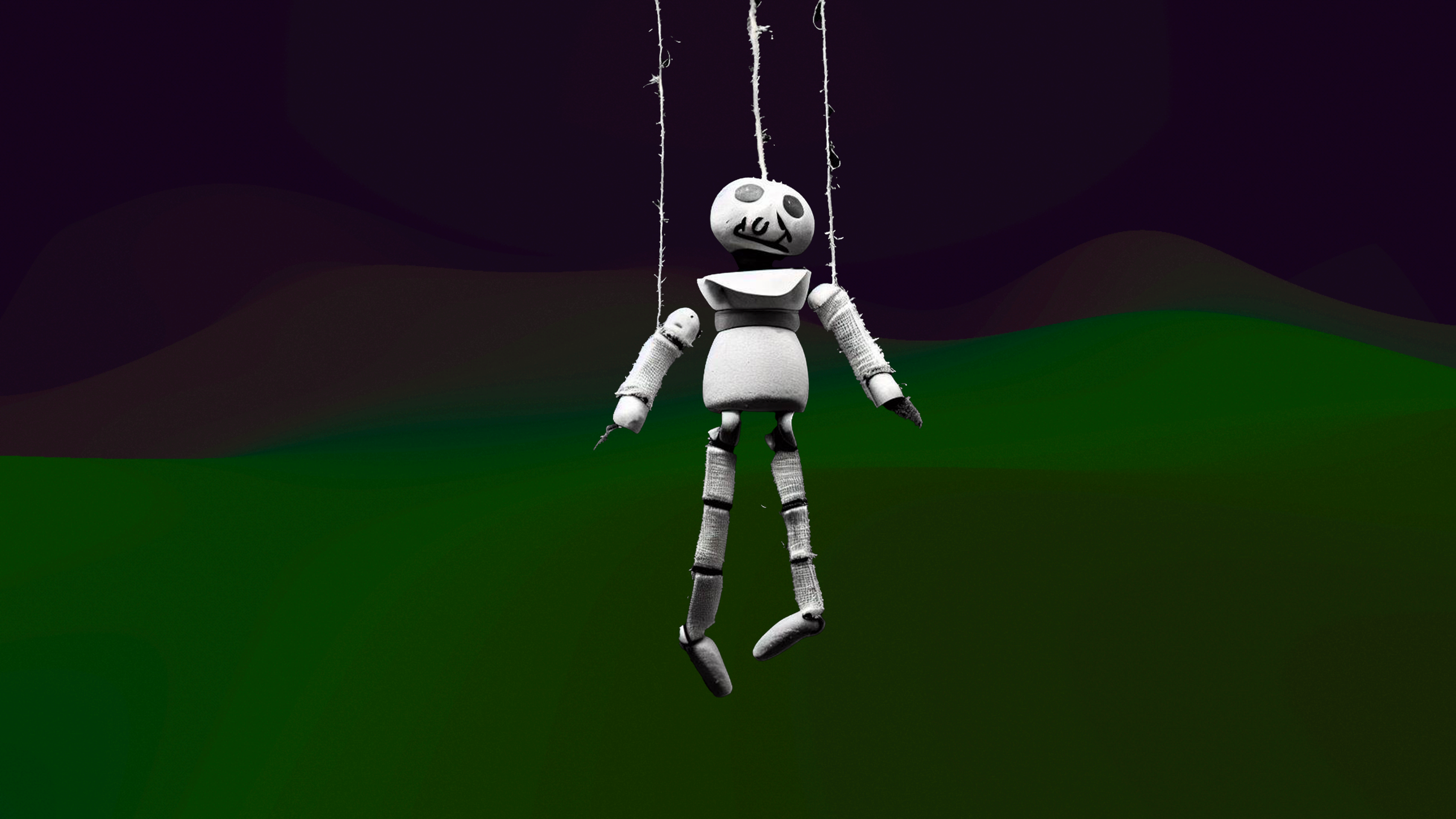
Edward Marczak 2023-10-05

M: @marczak@mastodon.social

Slack: marczak

https://www.icloud.com/pages/01d4oW6bojyK4uiY08MkqPSyQ#Marczak-MSA2023-Data_Driven_IT

Why?

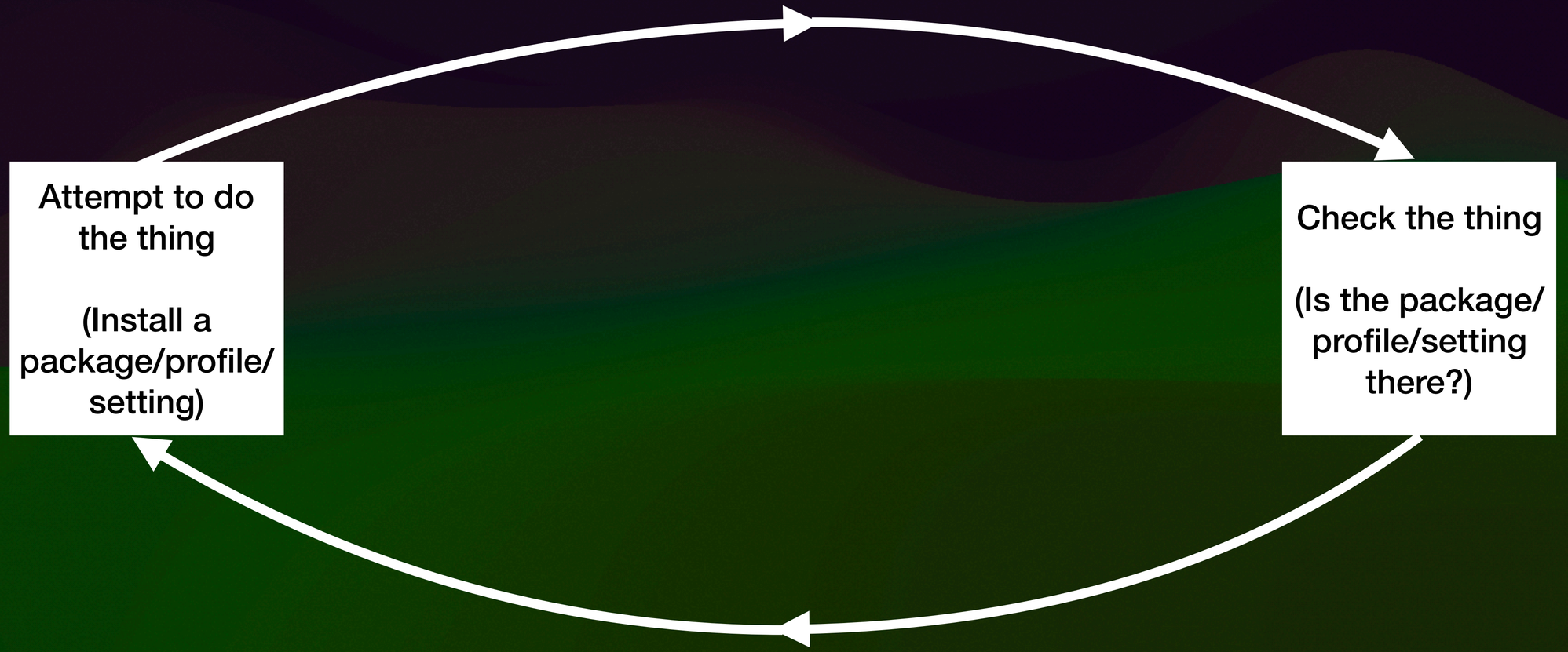


How quickly can you affect your fleet?

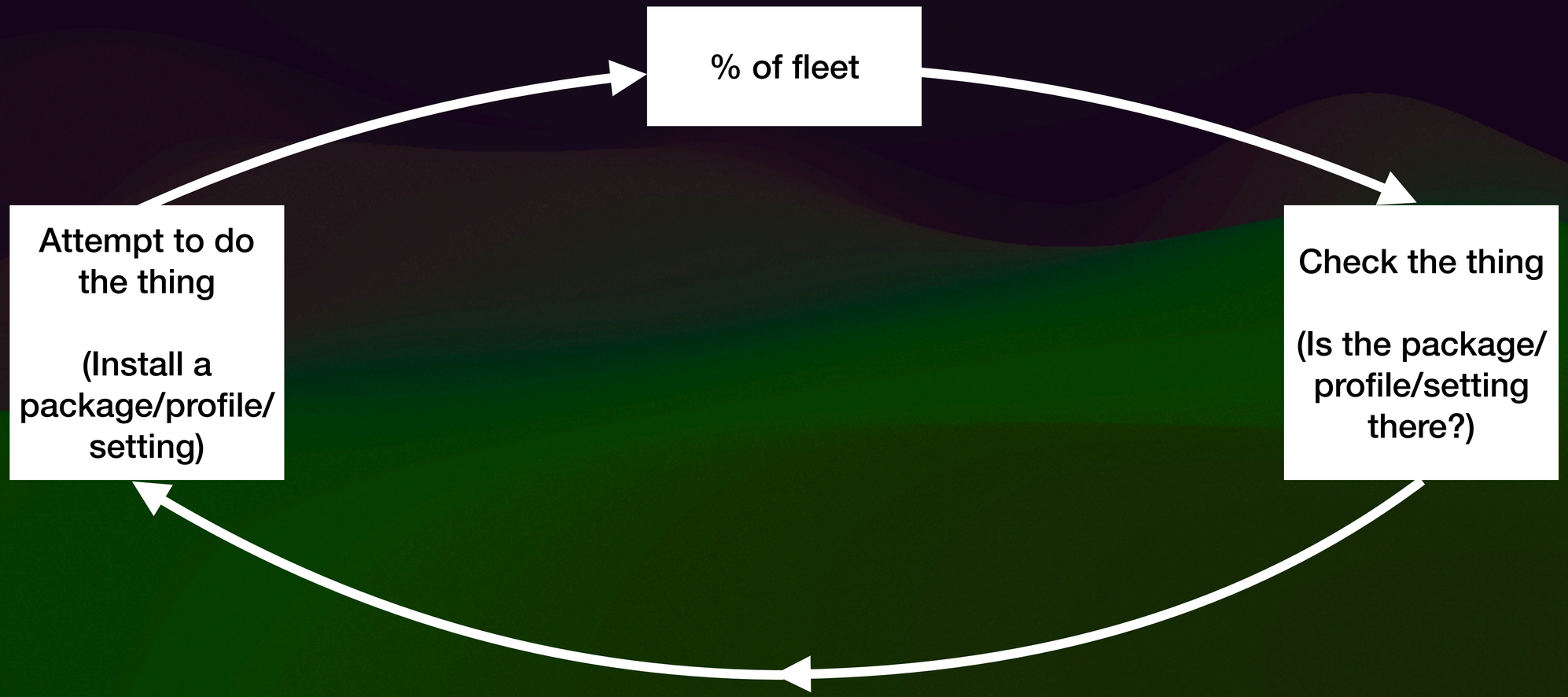
How do you know?

Close the loop

Close the loop



Close the loop



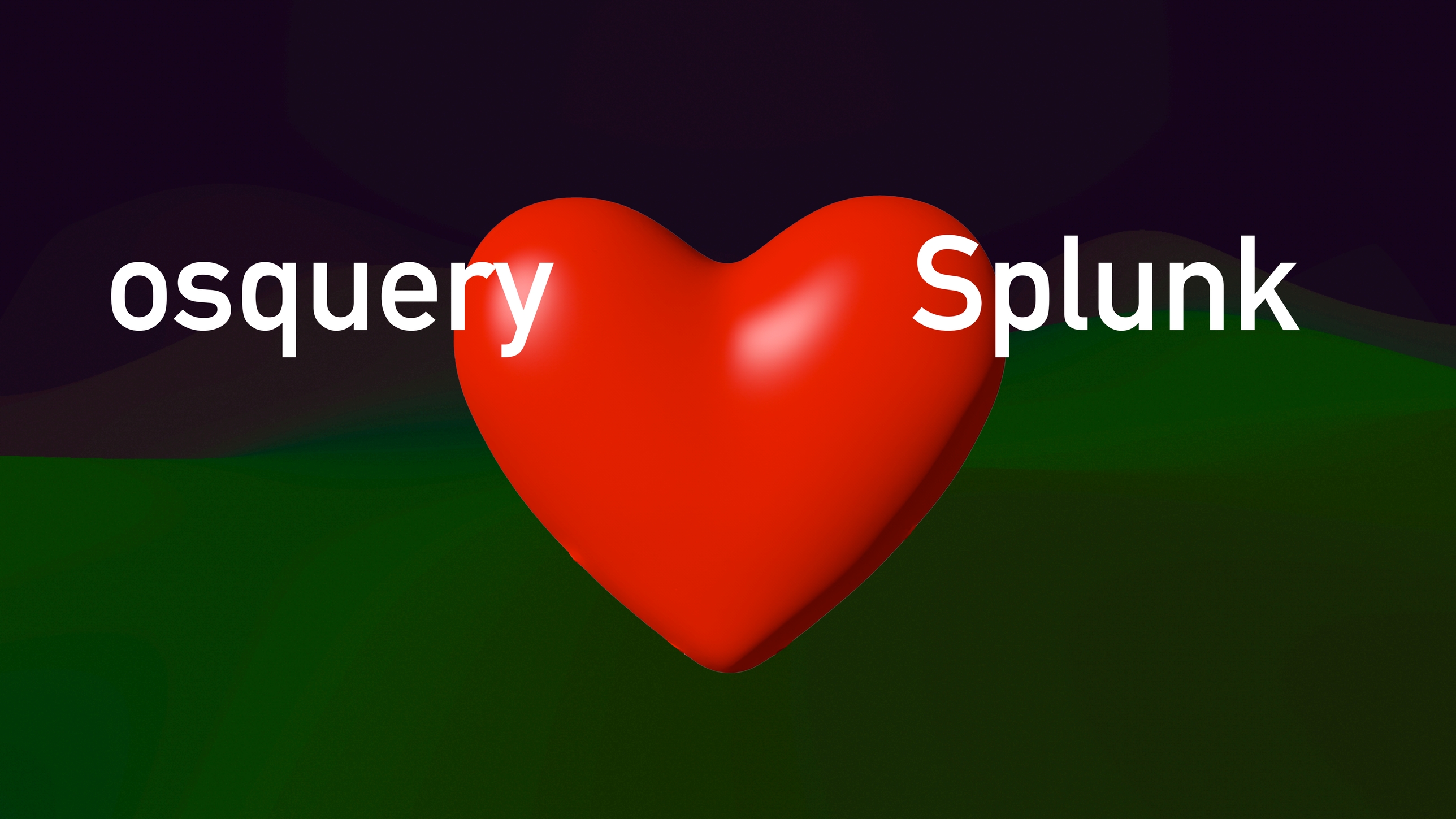
Monitoring

Do everything manually

Use an MDM/ Management Product

AI!

How?


osquery
Splunk

Log collection

Log collection

- fluentd
- fluentbit
- Splunk universal forwarder
- Vector
- sal-scripts
- Custom agent of your writing

Your Management Agent(s)

Munki

JAMF

(Your product here)

Munki

- /Library/Managed Installs/Logs
  - appusage logs
  - Install.log
  - error.log
  - warning.log

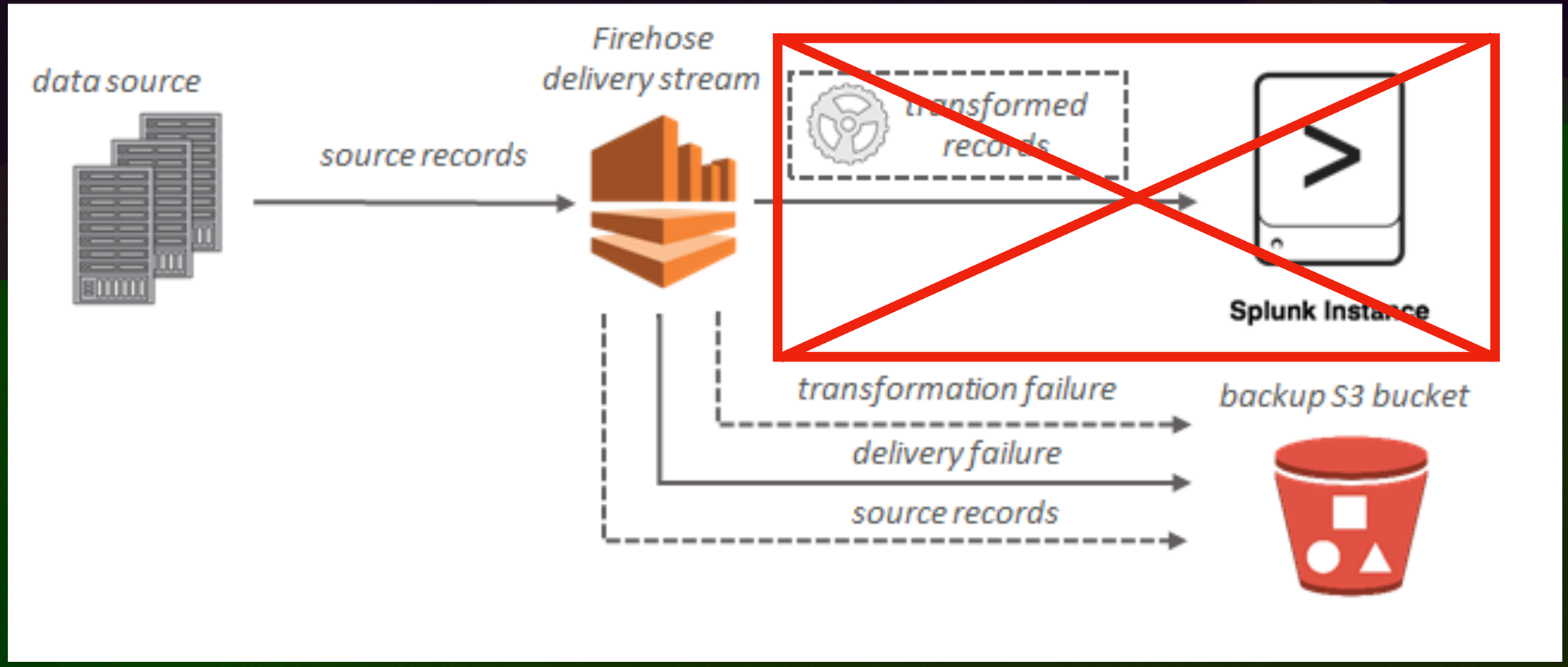
JAMF

- Server: server logs/activity
- Clients: JAMF has a reasonable API (aka - we want data about our endpoints)
  - Use the JAMF Add-on for Splunk (ok-ish)
  - Webhook (nice-ish)
  - Better: do it yourself

(Your product here)

- Look for a product that can ship server logs/activity
- Webhooks are…nice (use Firehose for reliability)

Firehose for Reliability



(Your product here)

- Look for a product that can ship server logs/activity
- Webhooks are…nice (use Firehose for reliability)
- Ideally, look for a good API
  - This benefits you: build what you want!
  - This also helps you move from click-ops to DevOps

Posture Collection

- osquery
- ~~Extended Attributes (JAMF)~~
- ~~Custom agent of your writing~~
- Additional agents already on the machine

osquery

- Open source “operating system instrumentation framework for Windows, macOS, and Linux”
- Exposes the OS as an SQL database
- Ships the results of your queries to a server
  - Zentral, FleetDM, Kolide
- From the server, you ship the centralized logs to your logging infrastructure

osquery

- Open source “operating system instrumentation framework for Windows, macOS, and Linux”
- Exposes the OS as an SQL database
- Ships the results of your queries to a server
  - Zentral, FleetDM, Kolide
- From the server, you ship the centralized logs to your logging infrastructure

What?

os version

os version: osquery

```
osquery>  select * from os_version;
+-------+---------+-------+-------+-------+---------+----------+---------------+----------+-------+
| name  | version | major | minor | patch | build   | platform | platform_like | codename | arch  |
+-------+---------+-------+-------+-------+---------+----------+---------------+----------+-------+
| macOS | 14.0    | 14    | 0     | 0     | 23A339 | darwin   | darwin        |          | arm64 |
+-------+---------+-------+-------+-------+---------+----------+---------------+----------+-------+
```

os version: Splunk/JAMF

```
index="your_index" source=“your_source" | bin span=1d _time
| dedup _time,event.computer.serialNumber
| rename event.computer.osVersion as osVer
| eval temp=split(osVer,".") | eval major=mvindex(temp,0)| eval
minor=mvindex(temp,1) | eval patch=mvindex(temp,2) | fields - temp
| eval p=if(isnull(patch), "0", patch)
| eval semver=major + "." + minor + "." + p
| timechart span=1d count(semver) as "macOS Version" by semver
```

os version: Splunk/JAMF

```
index=    Your index     source="    Your source    " | bin span=1d _time
| dedup _time,event.computer.serialNumber
| rename event.computer.osVersion as osVer
| eval temp=split(osVer,".") | eval major=mvindex(temp,0)| eval minor=mvindex(temp,1) | eval patch=mvindex(temp,2) | fields - temp
| eval p=if(isnull(patch), "0", patch)
| eval semver=major + "." + minor + "." + p
| timechart span=1d count(semver) as "macOS Version" by semver
```

Last 14 days

✓ **7,098 events** (8/24/23 11:31:18.000 AM to 9/7/23 11:31:18.000 AM) Job standard_perf (search default) Fast Mode

No Event Sampling

Events Patterns **Statistics (15)** Visualization

20 Per Page Format Preview

_time	10.15.6	11.6.0	12.0.0	12.6.8	13.0.1	13.4.0	13.4.1	13.5.0	13.5.1	14.0.0	OTHER
2023-08-24	1	2	1	1	0	1	7	457	38	2	0
2023-08-25	1	2	1	1	0	1	7	459	42	2	0
2023-08-26	1	0	1	1	0	1	6	330	27	2	0
2023-08-27	0	2	1	1	0	1	6	336	37	2	0
2023-08-28	1	2	1	3	1	1	6	448	53	2	1
2023-08-29	1	2	1	1	1	1	6	455	58	2	1
2023-08-30	1	2	1	1	1	1	8	455	65	2	0

G⚠️⚠️ D⚡⚡⚡

M#####F#####

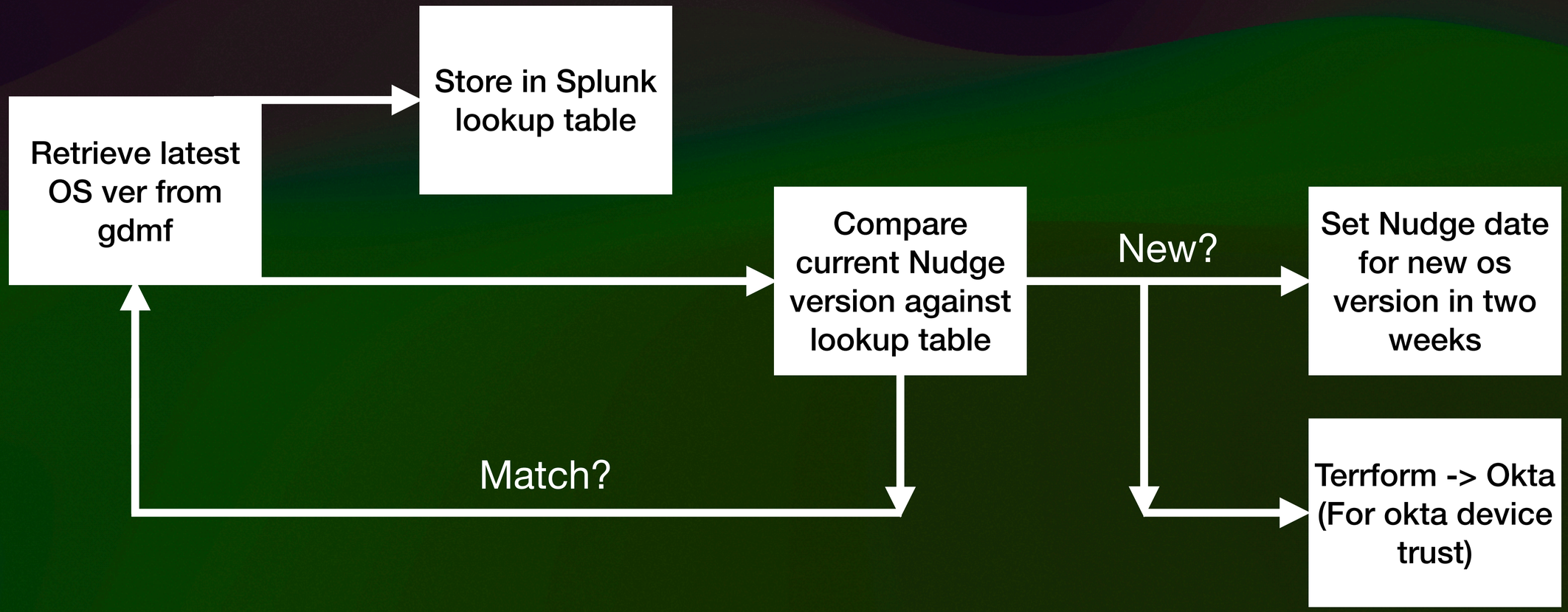
Apple‼️

https://gdmf.apple.com

```python
#!/usr/bin/python3

import json
import semver
import urllib.request

def get_feed(feed_url):
    req = urllib.request.Request(feed_url, headers={"User-Agent": "pg/noleather"})
    response = urllib.request.urlopen(req)
    body = response.read()
    jsonbody = json.loads(body)
    return jsonbody

feed = get_feed("https://gdmf.apple.com/v2/pmv")

highver = "0.0.1"
releases = {}

pdb.set_trace()

for k in feed["PublicAssetSets"]["macOS"]:
    ver = k["ProductVersion"]
    releases[ver] = k["PostingDate"]
    if semver.compare(ver, highver) > 0:
        highver = ver

print(highver + ": " + releases[highver])
```

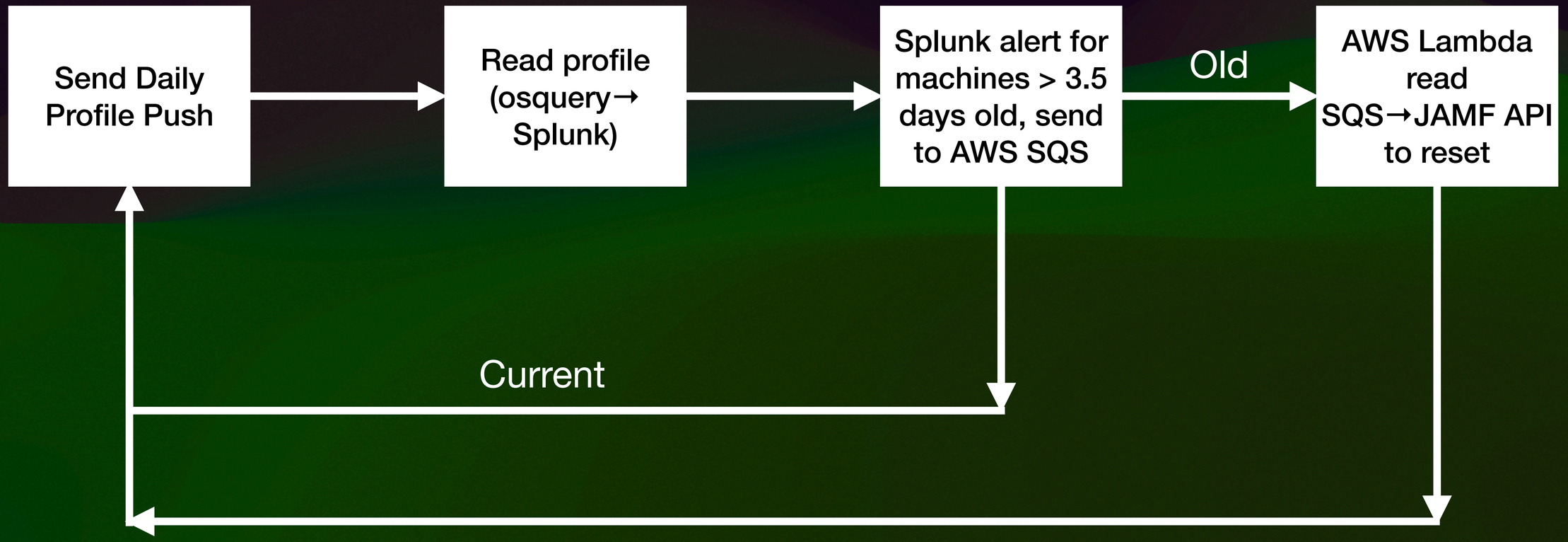
```
% ./parsegdmf.py
13.5.2: 2023-09-11
```

OS Version


Retrieve latest OS ver from gdmf
Store in Splunk lookup table
Compare current Nudge version against lookup table
New?
Set Nudge date for new os version in two weeks
Match?
Terrform -> Okta (For okta device trust)

MDM “Hiccups”

MDM “Hiccups”: osquery



MDM “Hiccups”: osquery

```
osquery> select value as mdm_push_date from plist where
key="Jamf Telemetry Daily" and path="/Library/Managed
Preferences/com.example.daily.plist";
+----------------------------+
| mdm_push_date              |
+----------------------------+
| 2023-09-14 12:01:19.367233 |
+----------------------------+
```

MDM “Hiccups”: Splunk

```
index="your_index" source=“osquery_source” name="pack/fleet_mgmt/daily_mdm_push"
| dedup hostIdentifier
| join left=L right=R where L.hostIdentifier=R.hostIdentifier [ search
index="endpoint_audit" source="http:osqueryprod_results_hec__json" name="pack/Essential/
system_info" ] | rename R.snapshot{}.computer_name as Computer_Name
| rename L.snapshot{}.mdm_push_date as push_date
| eval today=now()
| eval report_time=strftime(_time, "%Y-%m-%d %H:%M")
| eval u_push_date=strptime(push_date, "%Y-%m-%d %H:%M:%S.%6Q")
| eval diff=today-u_push_date
| where diff>302400
| table report_time, L.hostIdentifier, Computer_Name, push_date, diff | sort -diff
```

MDM “Hiccups”: Splunk

```
index="your_index" source=“osquery_source” name="pack/fleet_mgmt/daily_mdm_push"
| dedup hostIdentifier
| join left=L right=R where L.hostIdentifier=R.hostIdentifier [ search
index="endpoint_audit" source="http:osqueryprod_results_hec__json" name="pack/Essential/
system_info" ] | rename R.snapshot{}.computer_name as Computer_Name
| rename L.snapshot{}.mdm_push_date as push_date
| eval today=now()
| eval report_time=strftime(_time, "%Y-%m-%d %H:%M")
| eval u_push_date=strptime(push_date, "%Y-%m-%d %H:%M:%S.%6Q")
| eval diff=today-u_push_date
| where diff>302400
| table report_time, L.hostIdentifier, Computer_Name, push_date, diff | sort -diff
```

MDM “Hiccups”: Splunk/JAMF

```
index="endpoint_audit" source="http:osqueryprod_results_hec__json" name="pack/fleet_mgmt/daily_mdm_push"
| dedup hostIdentifier
| join left=L right=R where L.hostIdentifier=R.hostIdentifier [ search index="endpoint_audit" source="http
    :osqueryprod_results_hec__json" name="pack/Essential/system_info" ] | rename R.snapshot{}.computer_name as Computer_Name
| rename L.snapshot{}.mdm_push_date as push_date
| eval today=now()
| eval report_time=strftime(_time, "%Y-%m-%d %H:%M")
| eval u_push_date=strptime(push_date, "%Y-%m-%d %H:%M:%S.%6Q")
| eval diff=today-u_push_date
| where diff>302400
| table report_time, L.hostIdentifier, Computer_Name, push_date, diff | sort -diff
```

Last 72 hours

✓ **19 events** (9/4/23 11:28:34.000 AM to 9/7/23 11:28:34.000 AM) Job standard_perf (search default) Fast Mode

No Event Sampling

Events Patterns **Statistics (19)** Visualization

20 Per Page Format Preview

report_time	L.hostIdentifier	Computer_Name	push_date	diff
2023-09-07 03:07	86E540EF-33		2023-04-28 12:00:32.154918	11402881.845082
2023-09-07 11:15	C083A21D-CD		2023-05-05 12:00:48.145856	10798065.854144
2023-09-06 16:36	1CA6F30E-84		2023-05-10 12:01:20.154551	10366033.845449
2023-09-07 11:17	09586871-2E		2023-06-01 12:01:22.222118	8465231.777882
2023-09-07 04:57	B284265E-AE		2023-06-15 12:01:35.431690	7255618.568310
2023-09-06 16:24	79760206-27		2023-06-16 12:01:16.503203	7169237.496797
2023-09-07 10:51	9E6006DF-6B		2023-06-22 12:00:34.943593	6650879.056407

Software Installs

tware
stalls


SOC 2
TYPE 2
AICPA
SOC
aicpa.org/soc4so
SOC for Service Organizations | Service Organizations
tw
sta
Information Security Management
ISO
27001
Certified

Software Installs: osquery

```
osquery>  select name, path, bundle_executable,
bundle_identifier, bundle_name,
bundle_short_version, bundle_version,
development_region, applescript_enabled,
last_opened_time from apps;
```

Software Installs: osquery

```
osquery>  select name, path, bundle_executable, bundle_identifier, bundle_name,
bundle_short_version, bundle_version, development_region, applescript_enabled,
last_opened_time from apps;
```

name	path	bundle_executable	bundle_identifier	bundle_name	bundle_short_version	bundle_version	development_region	applescript_enabled	last_opened_time
1Password 7.app	/Applications/1Password 7.app	1Password 7	com.agilebits.onepassword7	1Password 7	7.9.11	70911000	en	0	1694688636.97074
1Password Extension Helper.app	/Applications/1Password 7.app/Contents/Library/LoginItems/1Password Extension Helper.app	1Password Extension Helper	2BUA8C4S2C.com.agilebits.onepassword7-helper	1Password Extension Helper	7.9.11	70911000	en	0	1692316171.86541
osquery.app	/opt/osquery/lib/osquery.app	osqueryd	io.osquery.agent	osqueryd	5.8.1	5.8.1			1678918092.55241
pinentry-mac.app	/usr/local/MacGPG2/libexec/pinentry-mac.app	pinentry-mac	org.gpgtools.pinentry-mac	pinentry-mac	1.1.1.1	100	English		-1.0
Python.app	/usr/local/munki/Python.framework/Versions/3.10/Resources/Python.app	Python	org.python.python	Python	3.10.11	3.10.11	English	1	-1.0

Software Installs: osquery

```
osquery> select n
bundle_short_versi
last_opened_time f
+-----------------------------------+-----------------------------------
| name                              | path
+-----------------------------------+-----------------------------------
| 1Password 7.app                   | /Applications/1Password 7.app
| 1Password Extension Helper.app    | /Applications/1Password 7.app/Co
| osquery.app                       | /opt/osquery/lib/osquery.app
| pinentry-mac.app                  | /usr/local/MacGPG2/libexec/pinen
| Python.app                        | /usr/local/munki/Python.framewor
+-----------------------------------+-----------------------------------
```

Software Installs: osquery

```
select name, path, bund
hort_version, bundle_vers
ed_time from apps;
```

```
---+-----------------------------------------------------------------------------------------------
   | path
---+-----------------------------------------------------------------------------------------------
   | /Applications/1Password 7.app
   | /Applications/1Password 7.app/Contents/Library/LoginItems/1Password Extension Helper.app
   | /opt/osquery/lib/osquery.app
   | /usr/local/MacGPG2/libexec/pinentry-mac.app
   | /usr/local/munki/Python.framework/Versions/3.10/Resources/Python.app
---+-----------------------------------------------------------------------------------------------
```

Software Installs: osquery

```
e_executable, bundle_ide
on, development_region, c
```

	bundle_executable	bundle_identifier	bund
	1Password 7	com.agilebits.onepassword7	1Pass
	1Password Extension Helper	2BUA8C4S2C.com.agilebits.onepassword7-helper	1Pass
	osqueryd	io.osquery.agent	osque
	pinentry-mac	org.gpgtools.pinentry-mac	piner
	Python	org.python.python	Pytho

Software Installs: osquery

```
identifier, bundle_name,
n, applescript_enabled,
```

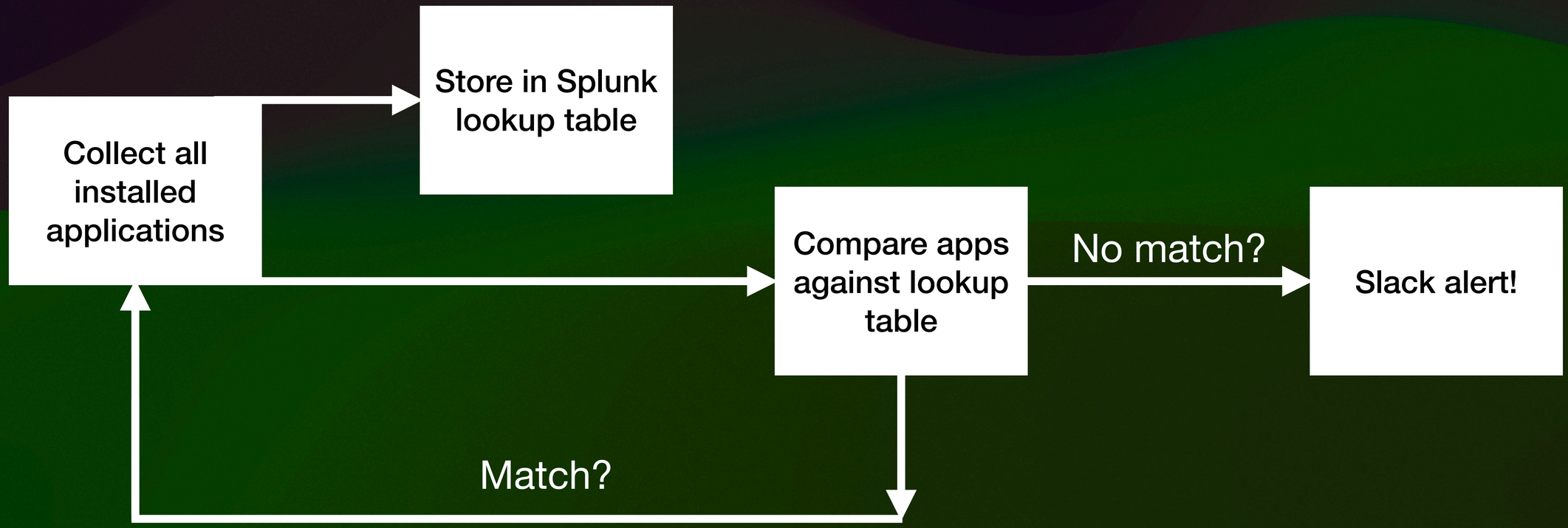
```
+-----+-----------------------------+-------------------------+-----------------+-----------------+
|     | bundle_name                 | bundle_short_version    | bundle_version  | development_reg |
+-----+-----------------------------+-------------------------+-----------------+-----------------+
|     | 1Password 7                 | 7.9.11                  | 70911000        | en              |
| per | 1Password Extension Helper  | 7.9.11                  | 70911000        | en              |
|     | osqueryd                    | 5.8.1                   | 5.8.1           |                 |
|     | pinentry-mac                | 1.1.1.1                 | 100             | English         |
|     | Python                      | 3.10.11                 | 3.10.11         | English         |
+-----+-----------------------------+-------------------------+-----------------+-----------------+
```

Software Installs: osquery

```
le_name,
nabled,
```

bundle_version	development_region	applescript_enabled	last_opened_time
70911000	en	0	1694688636.97074
70911000	en	0	1692316171.86541
5.8.1			1678918092.55241
100	English		-1.0
3.10.11	English	1	-1.0

Software Installs



Install Errors

Software Installs: Splunk/sal-scripts

```
index="your_index" | spath sourcetype | search sourcetype="macos:munki"
| spath "event.munki_data.serial_number" | dedup "event.munki_data.serial_number"
| spath "event.munki_data.munki.messages{}.Warnings.text"
| search "event.munki_data.munki.messages{}.Warnings.text"!=""
| rename "event.munki_data.munki.messages{}.Warnings.text" as message
| append
    [ search index="your_index" | spath sourcetype | search sourcetype="macos:munki"
    | spath "event.munki_data.serial_number" | dedup
"event.munki_data.serial_number"
    | spath "event.munki_data.munki.messages{}.Errors.text"
    | search "event.munki_data.munki.messages{}.Errors.text"!=""
    | rename "event.munki_data.munki.messages{}.Errors.text" as message ]
| search message!="Could not retrieve *"
| stats count, values(event.munki_data.serial_number) by message | sort - count
```

Software Installs: osquery

```
index="your_index" | spath sourcetype | search sourcetype="macos:munki"
| spath "event.munki_data.serial_number" | dedup "event.munki_data.serial_number"
| spath "event.munki_data.munki.messages{}.Warnings.text"
| search "event.munki_data.munki.messages{}.Warnings.text"!=""
| rename "event.munki_data.munki.messages{}.Warnings.text" as message
| append
    [ search index="your_index" | spath sourcetype | search sourcetype="macos:munki"
    | spath "event.munki_data.serial_number" | dedup
"event.munki_data.serial_number"
    | spath "event.munki_data.munki.messages{}.Errors.text"
    | search "event.munki_data.munki.messages{}.Errors.text"!=""
    | rename "event.munki_data.munki.messages{}.Errors.text" as message ]
| search message!="Could not retrieve *"
| stats count, values(event.munki_data.serial_number) by message | sort - count
```

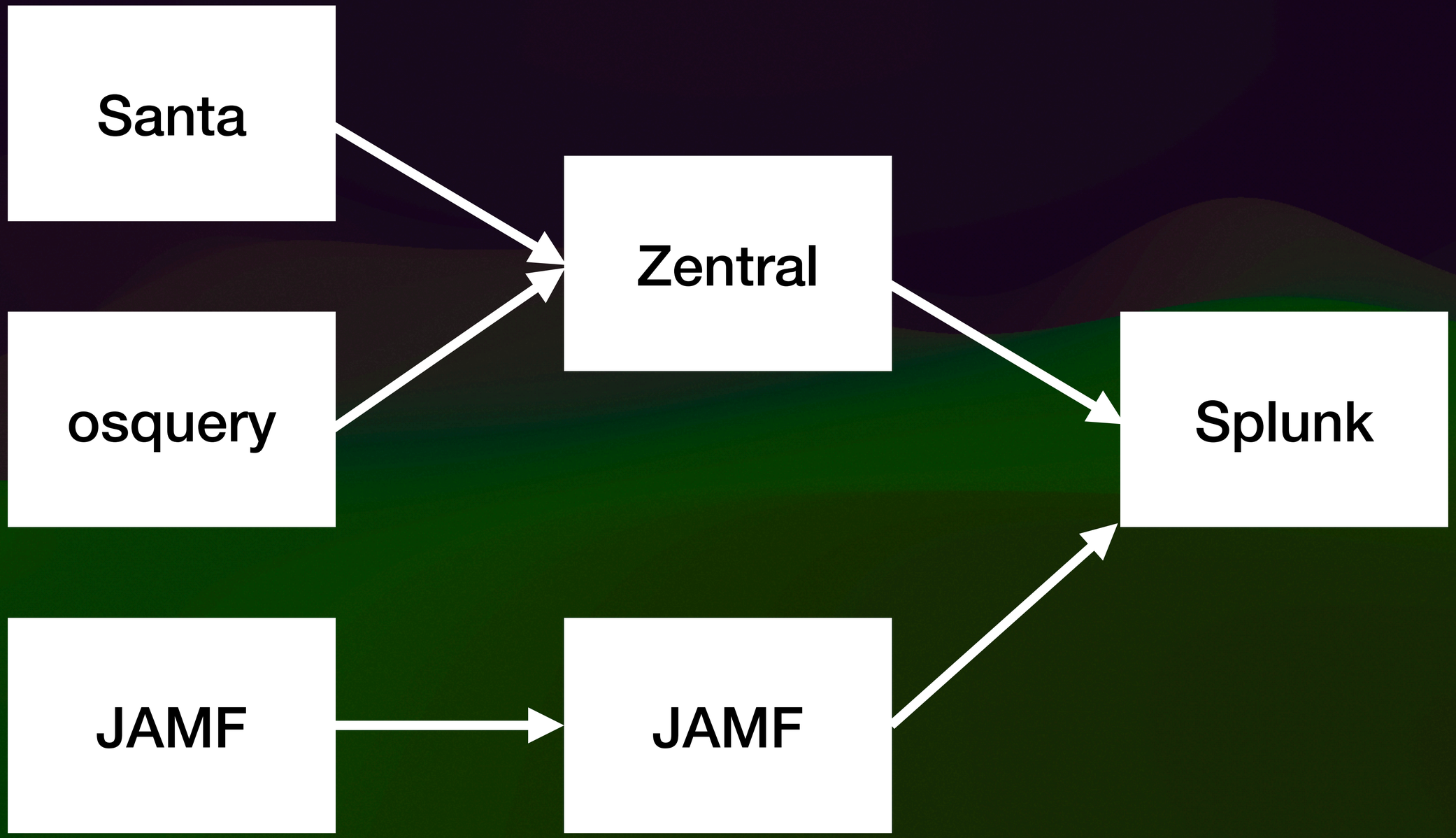
Software Installs: osquery

```
index="your_index" | spath sourcetype | search sourcetype="macos:munki"
| spath "event.munki_data.serial_number" | dedup "event.munki_data.serial_number"
| spath "event.munki_data.munki.messages{}.Warnings.text"
| search "event.munki_data.munki.messages{}.Warnings.text"!=""
| rename "event.munki_data.munki.messages{}.Warnings.text" as message
| append
    [ search index="your_index" | spath sourcetype | search sourcetype="macos:munki"
    | spath "event.munki_data.serial_number" | dedup
"event.munki_data.serial_number"
    | spath "event.munki_data.munki.messages{}.Errors.text"
    | search "event.munki_data.munki.messages{}.Errors.text"!=""
    | rename "event.munki_data.munki.messages{}.Errors.text" as message ]
| search message!="Could not retrieve *"
| stats count, values(event.munki_data.serial_number) by message | sort - count
```

Cross-Checking


MORRIS
4


N243SP
MANEUVERING SPEED
105 KIAS
WARNING
ASSURE THAT ALL CONTAMINANTS, INCLUDING WATER ARE REMOVED FROM FUEL AND FUEL SYSTEM BEFORE FLIGHT. FAILURE TO ASSURE CONTAMINANT FREE FUEL AND HEED ALL SAFETY INSTRUCTIONS AND OWNER ADVISORIES PRIOR TO FLIGHT CAN RESULT IN BODILY INJURY OR DEATH.
D.A.T.
VOLTS
SELECT
CONTROL
DAYTRON
KNOTS
TAS
VACUUM
ALTIMETER
CALIBRATE TO 20
D.C. ELEC.
TURN COORDINATOR
2 MIN.
NO PITCH INFORMATION
VERTICAL SPEED
100 FEET PER MIN
OIL
QTY
RPM
HOURS
WARNING
ASSURE THAT SEAT IS LOCKED IN POSITION PRIOR TO TAXI, TAKE-OFF AND LANDING. FAILURE TO PROPERLY LATCH SEAT AND HEED ALL SAFETY INSTRUCTIONS CAN RESULT IN BODILY IN JURY OR DEATH.
AVN FAN
XPNDR
AUTO PILOT
GYRO
AVIONICS
FLAP
INST
AVN BUS 1
BCN
LAND
TST
BRT
DIM
HSI
NAV
GPS APR
ENGINE ON
PROTECT YOUR STARTER!
THIS AIRCRAFT IS EQUIPPED WITH A HIGH PERFORMANCE SKY-TEC STARTER.
DO NOT CRANK STARTER FOR MORE THAN 10 SECONDS!
ALLOW 20 SECONDS TO COOL DOWN BETWEEN ATTEMPTS. REPEAT UP TO 6 TIMES. THEN LET STARTER COOL FOR 30 MINUTES.
COMM
ADF
BFO
MIX
PULL
LEAN
GLARESHIE
PEDESTAL L


Santa
osquery
JAMF
Zentral
JAMF
Splunk

Cross-Check Agents: Splunk

```
index=your_index source="jamf_json" "webhook.webhookEvent"=ComputerCheckIn
| dedup "event.computer.udid"
| eval jamf_time=strftime(_time, "%Y-%m-%dT%H:%M:%S")
| rename event.computer.deviceName as hostName, event.computer.udid as hostIdentifier
| table hostName, jamf_time, osq_time, hostIdentifier
| append
  [ search index="your_index" source="osquery_json" name="pack/fleet_mgmt/osquery_info"
  | fields _time, hostIdentifier
  | eval osq_time=strftime(_time, "%Y-%m-%d %H:%M:%S")
  | dedup hostIdentifier
  | table osq_time, hostIdentifier ]
| stats count,values(*) as * by hostIdentifier
| where count=1 AND jamf_time!=""
| fields - count, osq_time
```

Cross-Check Agents: Splunk

```
index=your_index source="jamf_json" "webhook.webhookEvent"=ComputerCheckIn
| dedup "event.computer.udid"
| eval jamf_time=strftime(_time, "%Y-%m-%dT%H:%M:%S")
| rename event.computer.deviceName as hostName, event.computer.udid as hostIdentifier
| table hostName, jamf_time, osq_time, hostIdentifier
| append
  [ search index="your_index" source="osquery_json" name="pack/fleet_mgmt/osquery_info"
  | fields _time, hostIdentifier
  | eval osq_time=strftime(_time, "%Y-%m-%d %H:%M:%S")
  | dedup hostIdentifier
  | table osq_time, hostIdentifier ]
| stats count,values(*) as * by hostIdentifier
| where count=1 AND jamf_time!=""
| fields - count, osq_time
```

Cross-Check Agents: Splunk

```
index=your_index source="jamf_json" "webhook.webhookEvent"=ComputerCheckIn
| dedup "event.computer.udid"
| eval jamf_time=strftime(_time, "%Y-%m-%dT%H:%M:%S")
| rename event.computer.deviceName as hostName, event.computer.udid as hostIdentifier
| table hostName, jamf_time, osq_time, hostIdentifier
| append
  [ search index="your_index" source="osquery_json" name="pack/fleet_mgmt/osquery_info"
  | fields _time, hostIdentifier
  | eval osq_time=strftime(_time, "%Y-%m-%d %H:%M:%S")
  | dedup hostIdentifier
  | table osq_time, hostIdentifier ]
| stats count,values(*) as * by hostIdentifier
| where count=1 AND jamf_time!=""
| fields - count, osq_time
```

Cross-Check Agents: Splunk

```
index=your_index source="jamf_json" "webhook.webhookEvent"=ComputerCheckIn
| dedup "event.computer.udid"
| eval jamf_time=strftime(_time, "%Y-%m-%dT%H:%M:%S")
| rename event.computer.deviceName as hostName, event.computer.udid as hostIdentifier
| table hostName, jamf_time, osq_time, hostIdentifier
| append
  [ search index="your_index" source="osquery_json" name="pack/fleet_mgmt/osquery_info"
  | fields _time, hostIdentifier
  | eval osq_time=strftime(_time, "%Y-%m-%d %H:%M:%S")
  | dedup hostIdentifier
  | table osq_time, hostIdentifier ]
| stats count,values(*) as * by hostIdentifier
| where count=1 AND jamf_time!=""
| fields - count, osq_time
```

JAMF not osquery

Save | Save As | View | Create Table View | Close

```
index=     Your index      source="     Your source      " "webhook.webhookEvent"=ComputerCheckIn

| dedup "event.computer.udid"
| eval jamf_time=strftime(_time, "%Y-%m-%dT%H:%M:%S")
| rename event.computer.deviceName as hostName, event.computer.udid as hostIdentifier
| table hostName, jamf_time, osq_time, hostIdentifier
| append
  [ search index="   Your index   " source="            Your source            " name="pack/fleet_mgmt/osquery_info"
  | fields _time, hostIdentifier
  | eval osq_time=strftime(_time, "%Y-%m-%d %H:%M:%S")
  | dedup hostIdentifier
  | table osq_time, hostIdentifier ]
| stats count,values(*) as * by hostIdentifier
| where count=1 AND jamf_time!=""
| fields - count, osq_time
```

Last 1 week

✓ **569 events** (8/27/23 12:00:00.000 AM to 9/7/23 11:37:50.000 AM)

Job | standard_perf (search default) | Verbose Mode

No Event Sampling

Events (569) | Patterns | **Statistics (23)** | Visualization

20 Per Page | Format | Preview

< Prev 1 2 Next >

hostIdentifier	hostName	jamf_time
021197		2023-09-05T11:27:35
10F7C2		2023-09-06T17:07:45
2DE1A8		2023-09-07T11:36:33
32AA60		2023-09-07T01:00:31
39E7C0		2023-09-07T11:16:31

Failed IDP Auth

Failed IDP Login: Splunk

```
eventtype=okta “outcome.result"=DENY outcome.reason="Sign-on policy*"
| dedup actor.id
| table _time, actor.*, target{}.displayName, device.*, outcome.*
| sort -_time
```

Tea Pause

What ?

```
[ ~ ]% osqueryi
Using a virtual database. Need help, type '.help'
osquery> .tables
```

```
[ ~ ]% osqueryi
Using a virtual database. Need help, type '.help'
osquery> .tables
  => account_policy_data
  => acpi_tables
  => ad_config
  => alf
  => alf_exceptions
  => alf_explicit_auths
  => app_schemes
  => apps
  => arp_cache
  => asl
  => atom_packages
  => augeas
  => authorization_mechanisms
  => authorizations
  => authorized_keys
  => azure_instance_metadata
  => azure_instance_tags
  => battery
  => block_devices
  => browser_plugins
  => carbon_black_info
  => carves
```

=> suid_bin
=> system_controls
=> system_extensions
=> system_info
=> temperature_sensors
=> time
=> time_machine_backups
=> time_machine_destinations
=> ulimit_info
=> unified_log
=> uptime
=> usb_devices
=> user_events
=> user_groups
=> user_interaction_events
=> user_ssh_keys
=> users
=> virtual_memory_info
=> wifi_networks
=> wifi_status
=> wifi_survey
=> xprotect_entries
=> xprotect_meta
=> xprotect_reports
=> yara
=> yara_events
=> ycloud_instance_metadata

What?

What Else?

Who?

User Stories

Device Posture

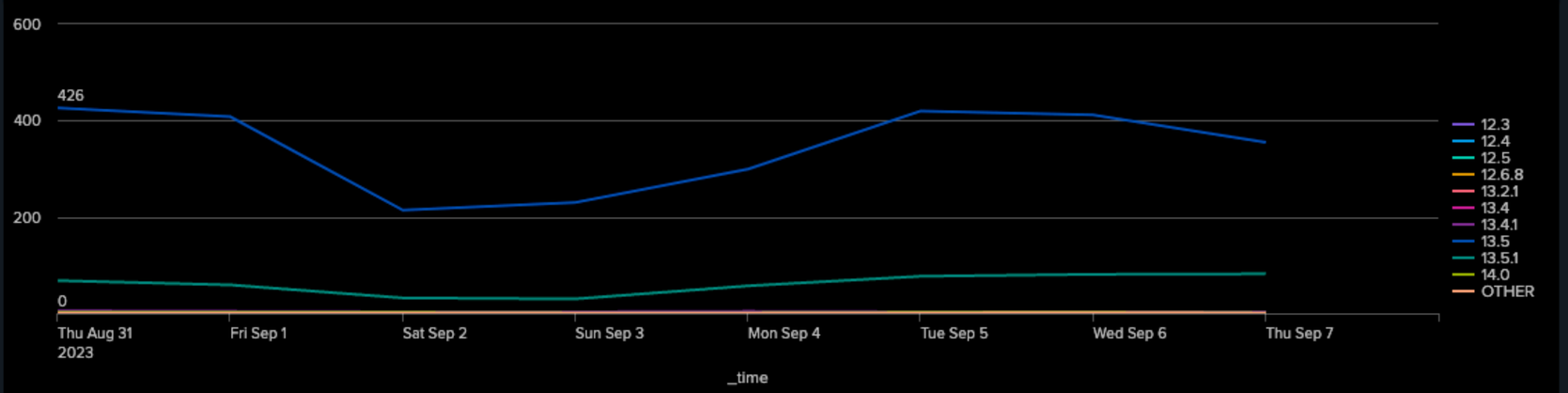
Security

Dashboards

macOS Endpoint Patching

Actions Edit

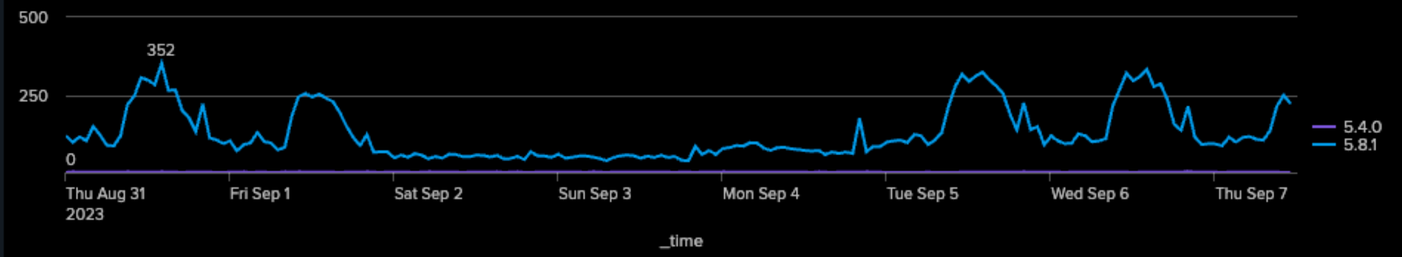
macOS Versions-7-day active, by Day



Outdated macOS-24-hour

13

osquery Versions-7-day active, by Hour



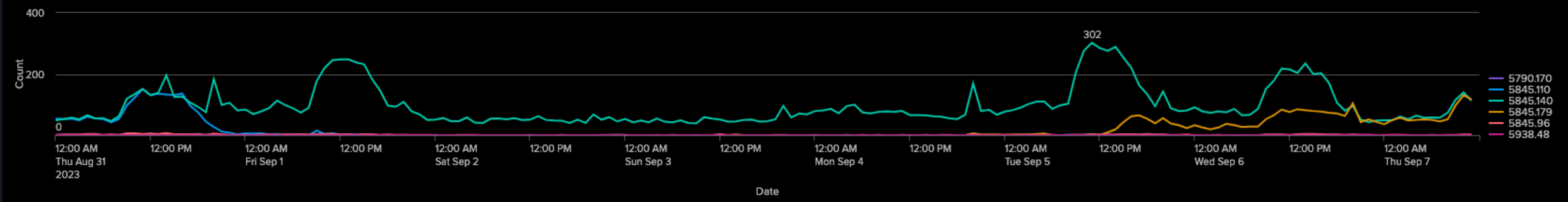
osquery 24-Hour checkins

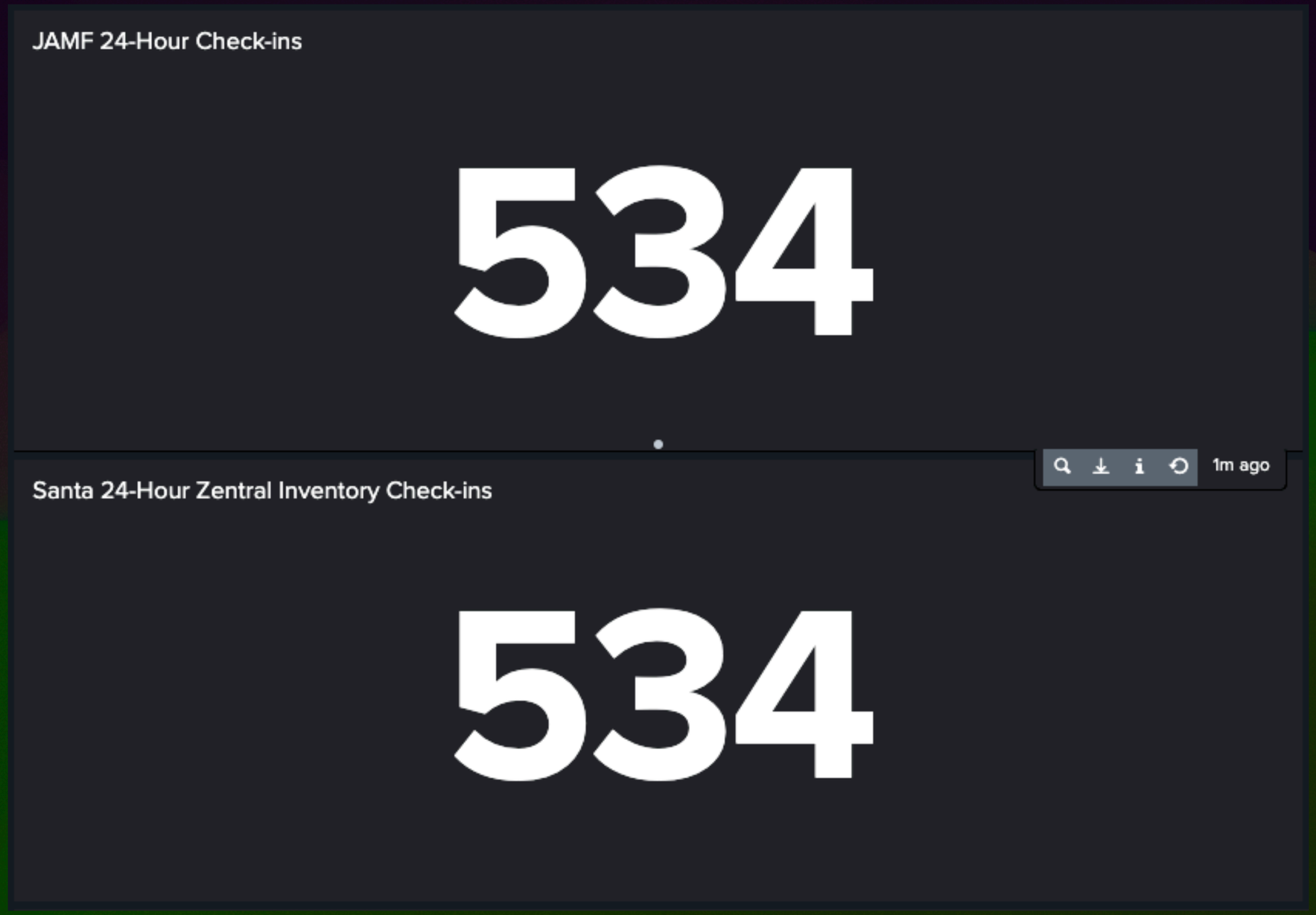
521

JAMF 24-Hour checkins

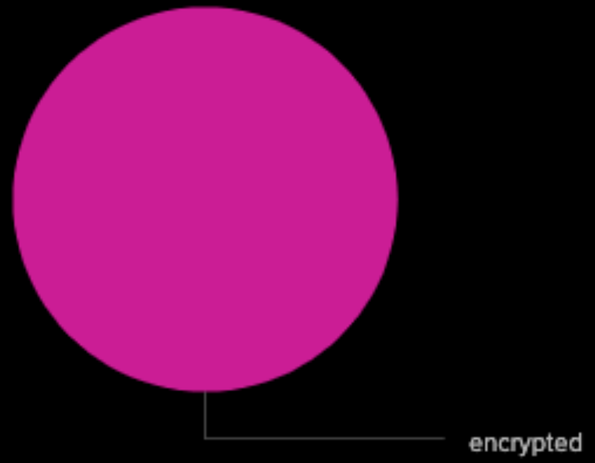
529

Chrome Versions-7-Day

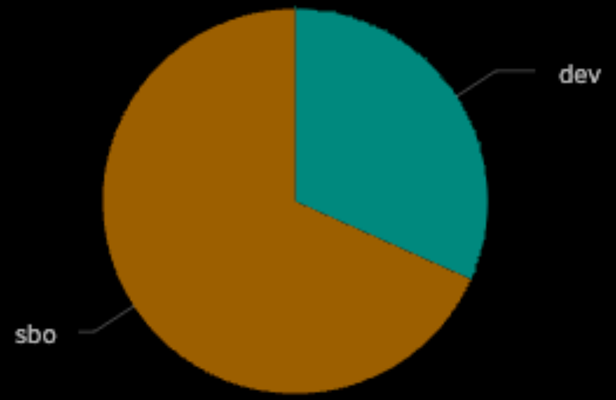



JAMF 24-Hour Check-ins
534
1m ago
Santa 24-Hour Zentral Inventory Check-ins
534

FileVaulted



24-Hour Fleet Composure

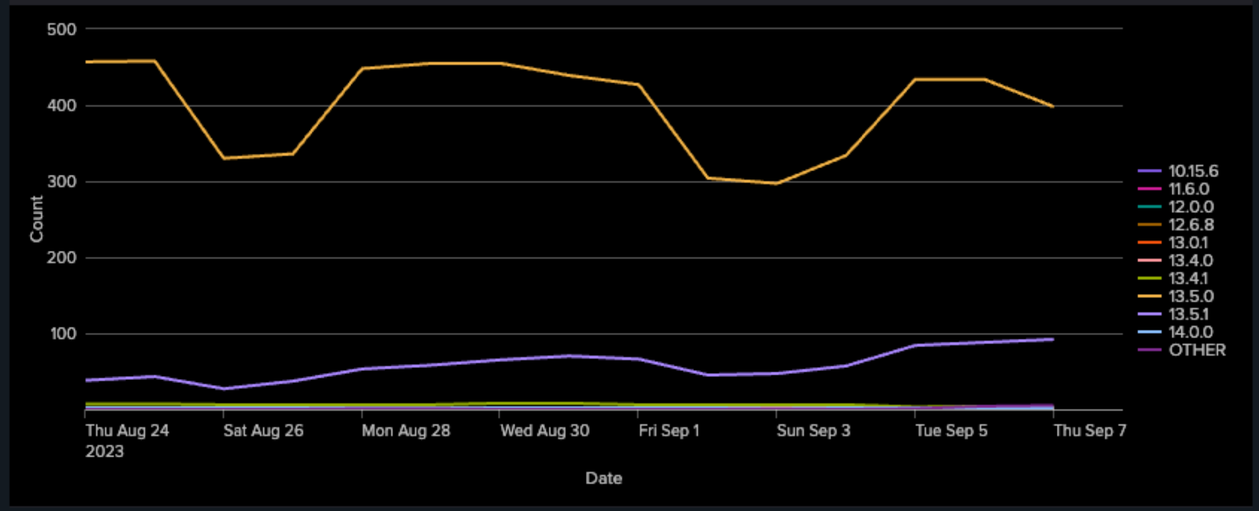


macOS Endpoint Stats

Edit | Export | ...

Mac endpoint 14-day averages

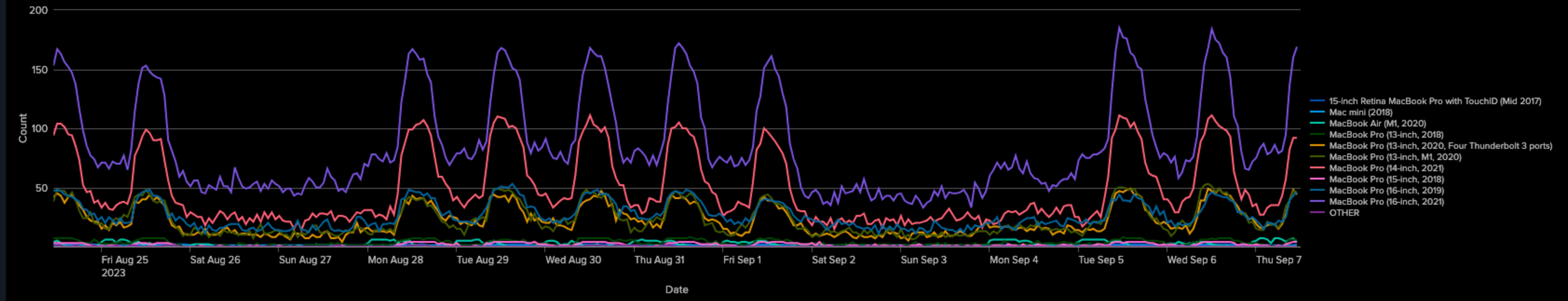
macOS Version via JAMF



24-Hour MDM Push Failing

15

Mac Hardware Models



Alerts

Alerts

- Send to:
  - Email
  - Slack
  - Pager Duty
  - Automations
  - All/some of the above

Alerts on your Alerts

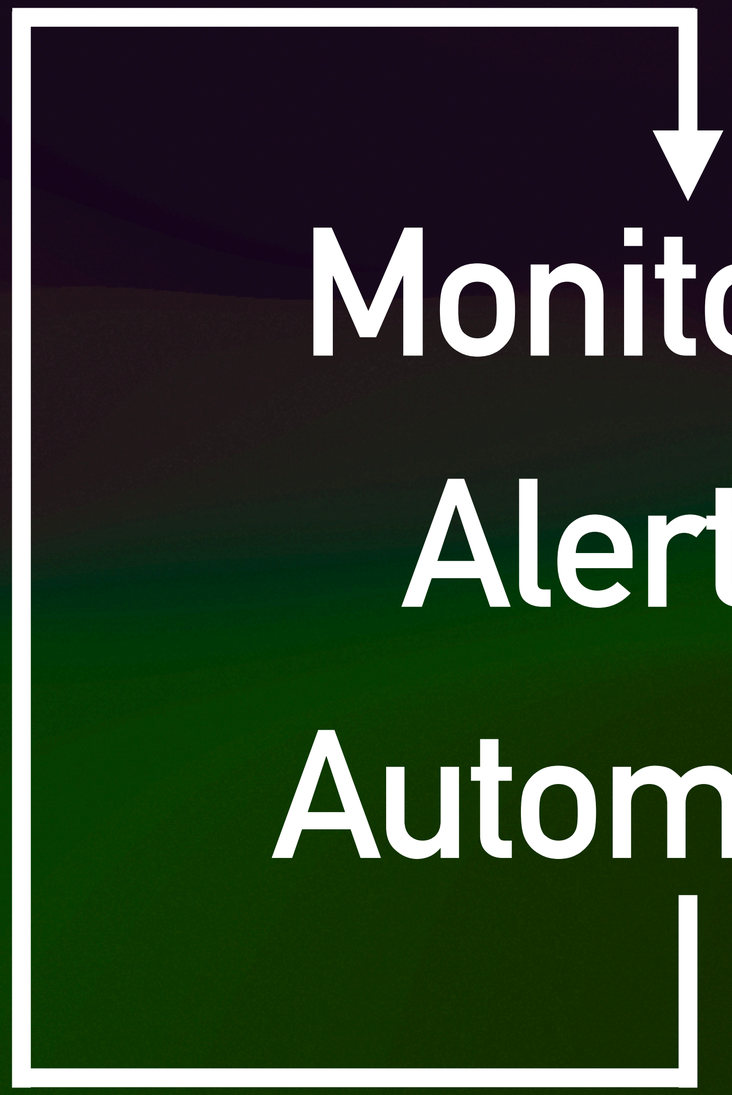
Alerts on your Alerts

```
index=your_index source="jamf_json"
"webhook.webhookEvent"=ComputerCheckIn
| dedup "event.computer.udid"
| table *
```

Get the foundations right

. . . fancy stuff comes later

Monitoring
Alerting
Automation


Monitoring
Alerting
Automation

Data-Driven IT

aka, “Why are we doing this thing?”

Edward Marczak 2023-10-05

M: @marczak@mastodon.social

Slack: marczak