
apfelwerk

Henry Stamerjohann

Apfelwerk GmbH & Co. KG

@head_min

#macadmins

Combine the power of osquery + Santa

Zentral

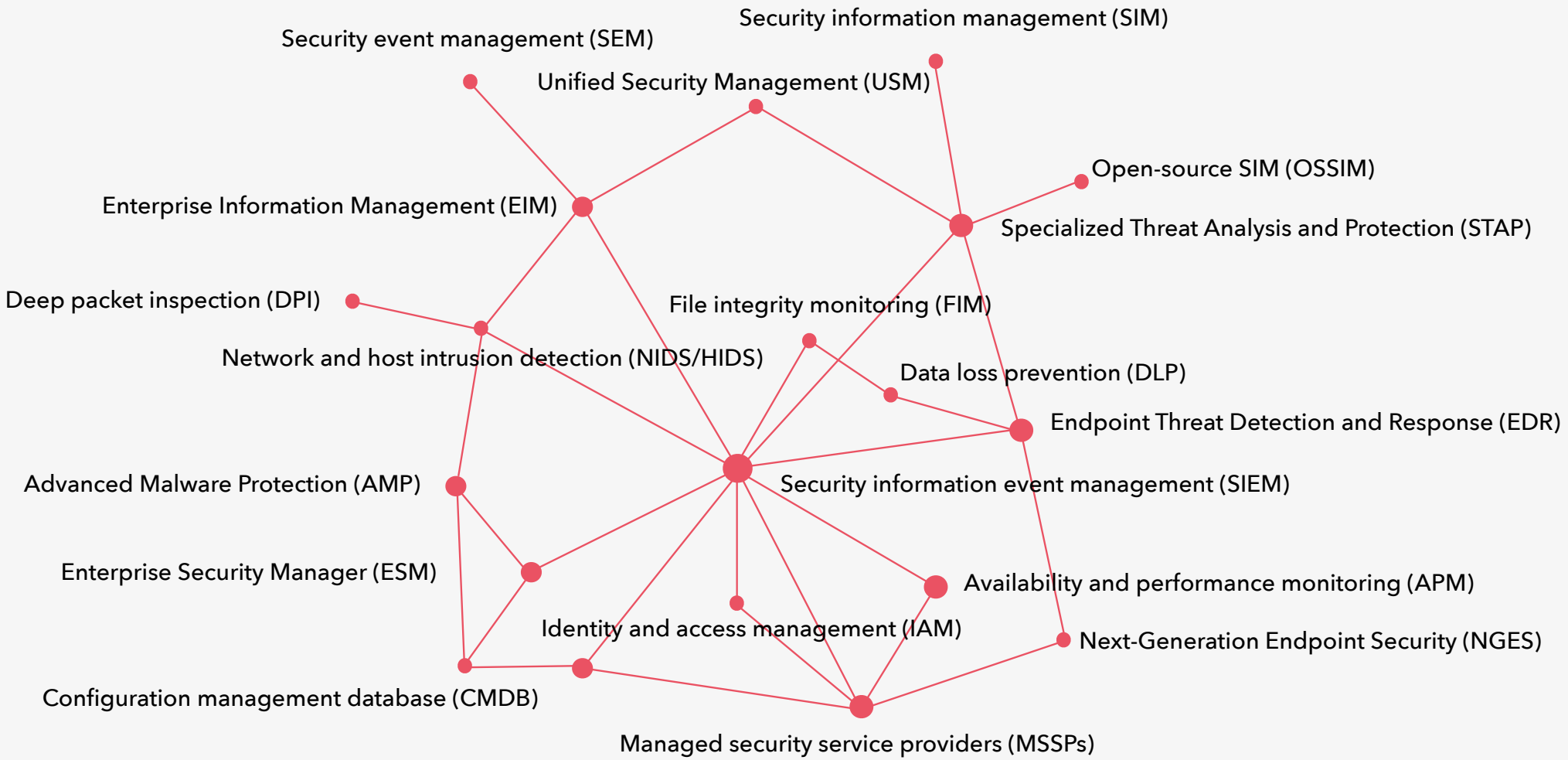
Security

Monitoring

Security

IT Security Market

Security Acronyms and Abbreviations



Management

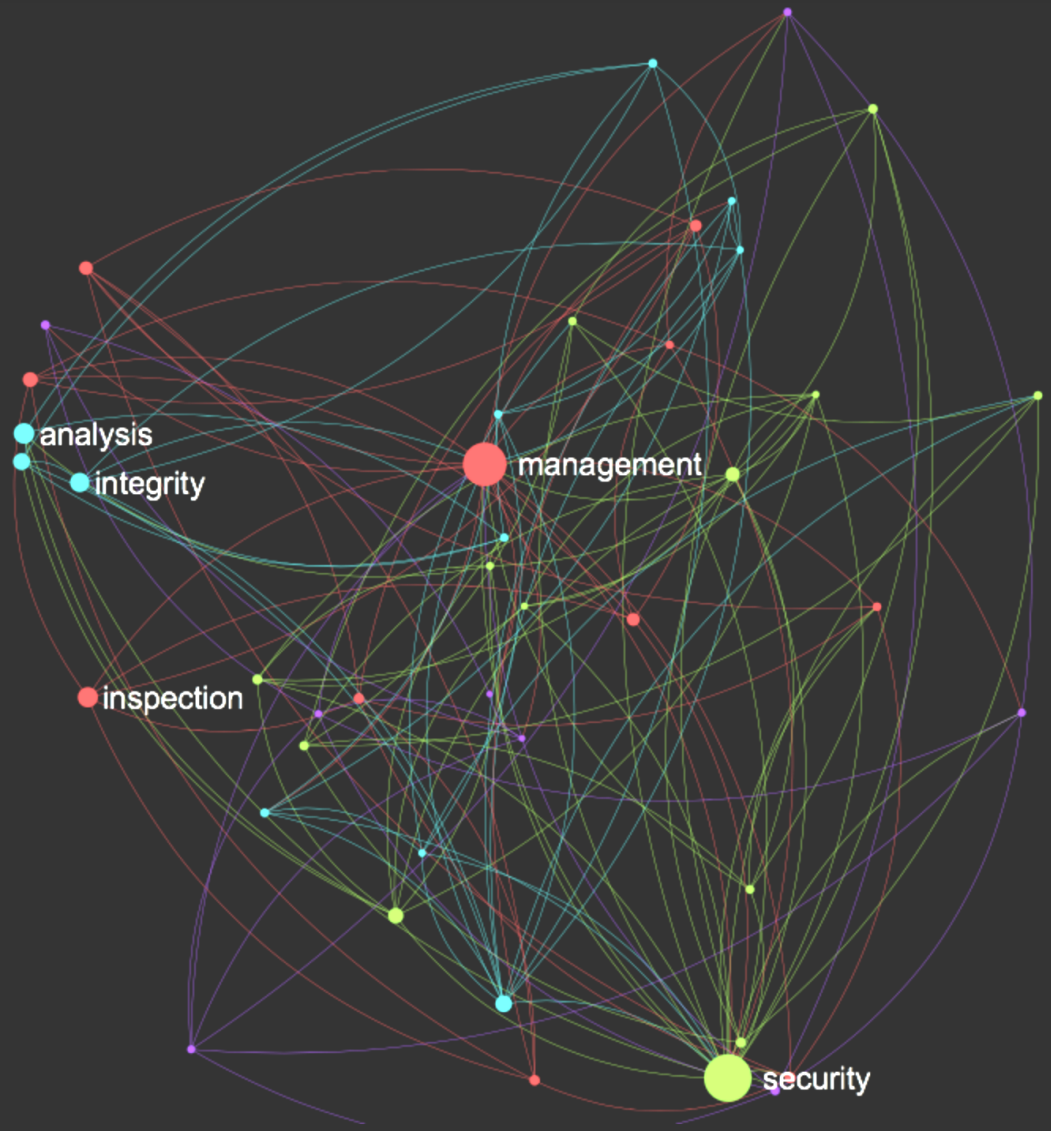
Inspection

Analysis

+

Integrity

Security



Management

Monitoring

Inspection

Analysis

Integrity

Stability

Security

Monitoring

Reasons

Growing need to **measure** and **manage** IT Systems

Support the **business operations**

Know **state** of your technology environment

Help to **resolve** faults, **detect** issues, **vulnerabilities**, etc.

Mitigate risks and help to remediate systems

Methods

~~No monitoring~~

Manual - inspection (non automated)

Reactive - automated (threshold based)

Proactive - automated (collect data, analyse, alert with context)

Modern Architectures

Fully **searchable** databases

Enable to search **metrics** with granularity or resolution

Use of **time-series** events

Follow changes in a **chronological** window

Correlate events and **alert** upon specific issues

Tools

Open Source:

ELK Stack, Prometheus,

Graphite / Grafana

Commercial:

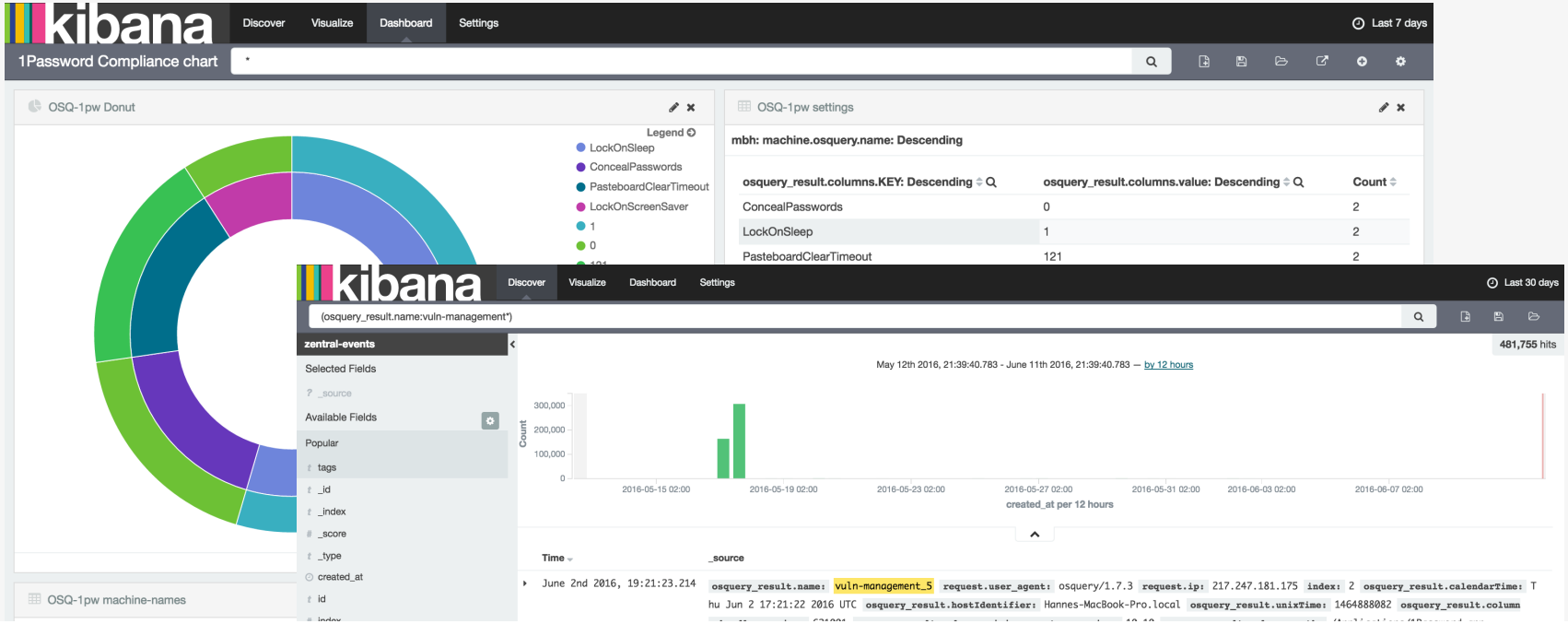
DataDog, Splunk

Metrics Visualization

ElasticSearch / Kibana (ELK)

Time-series metrics, indexed, full-text search DB (ES)

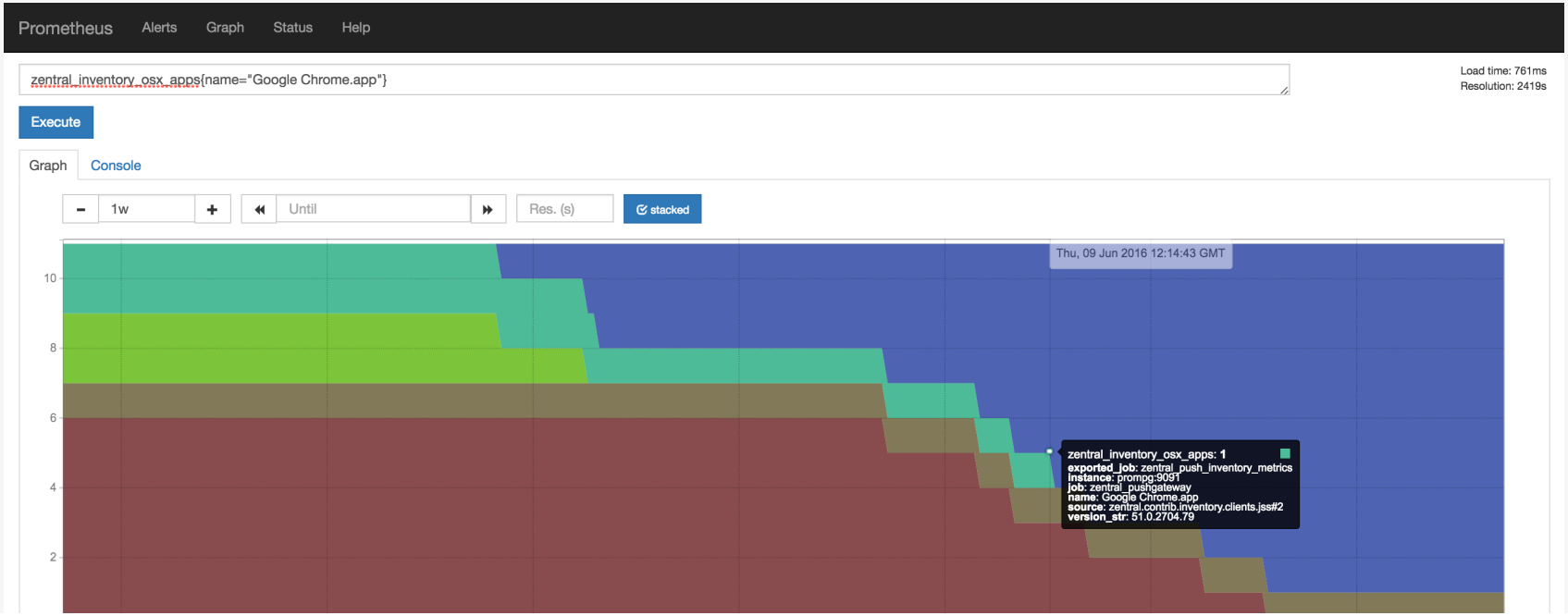
Discover and visualize data over time (Kibana 4)



Prometheus / TimeSeries

Event data transformed into TimeSeries

See streams of timestamped values on same Metric



Why ?

Visually understand the **changes**

Track **how long** something took

Apply **statistical functions** on Metrics

Quickly **answer questions** about compliance

Discover metrics for **ad hoc** areas of interest

Challenge

Process data to business needs

Measure **quality** and **performance** of IT (not availability)

Take responsibility for **all endpoints**

Routines for servers may not **automatically**

apply for all endpoints

Discovery ?!

Discovery

Broad Scale for General Overview &

Narrow, Focused for **in Depth Metrics**

(T-shaped information)

Standout Information from existing IT infrastructure

Focus **not limited** to fault detection

Culture & Velocity

Endpoints (COPE) - Corporate owned, personally enabled device - **don't break trust** with end-users

(this is critical for acceptance and success)

Responsiveness is crucial for specific issues, incidents, and changes in your environment

Automate and **notify** where needed

Challenge

Integrate **new tools** with existing ones

Implement procedures to log and monitor **proactively**

(but do not go into big brother mode)

There's different **objectives** and **concerns**

for IT in SMB and Enterprise

Adaptation and **customization** is required

Synergy

osquery

Ask questions about your Linux and macOS infrastructure

Query system state with a SQL syntax

Multi platform support

Not hidden (like other tools)

No restrictions on the users or system

Great community

Google Santa

Event logging to sync server (API)

A binary whitelisting/blacklisting system

Keeps **track** of binaries in macOS

(naughty and nice)

Kernel Extension and daemon

MONITOR and LOCKDOWN (default deny)

Zentral

Coordinate and control **osquery**

Control and event sync with **Santa**

TLS Server and **Event / Processing / Action -** Framework

Connect inventory from **multiple sources**

IFTTT like event **processing** based on

conditional and behavioural **Metrics**

Organize alerting **efficiently**

Zentral

Web service, written in **Python3**

Django 1.9 Framework

Event **aggregator** with extendable

modules for event **processing**

Crafted API support and **integrations**

Store events in full-text **search** database

Backend based on **modular & scalable** components

Event Processing

Zentral - Events

zentral | Inventory | Probes | Munki | Osquery | Santa | Extra links

Home / Inventory machines / C02QM01AGCN2 / Events

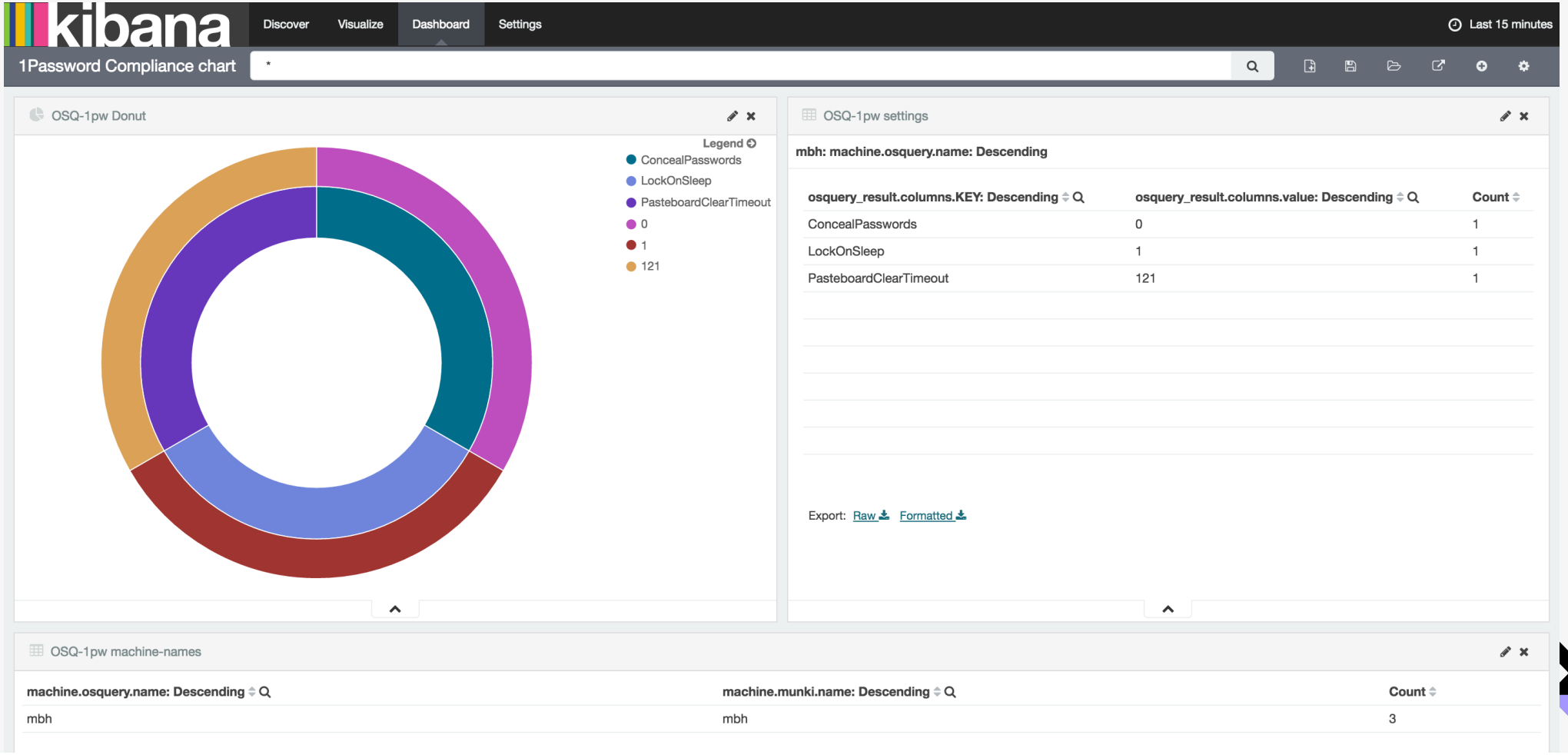
mbh / C02QM01AGCN2 Events

Event type All (145784) OK

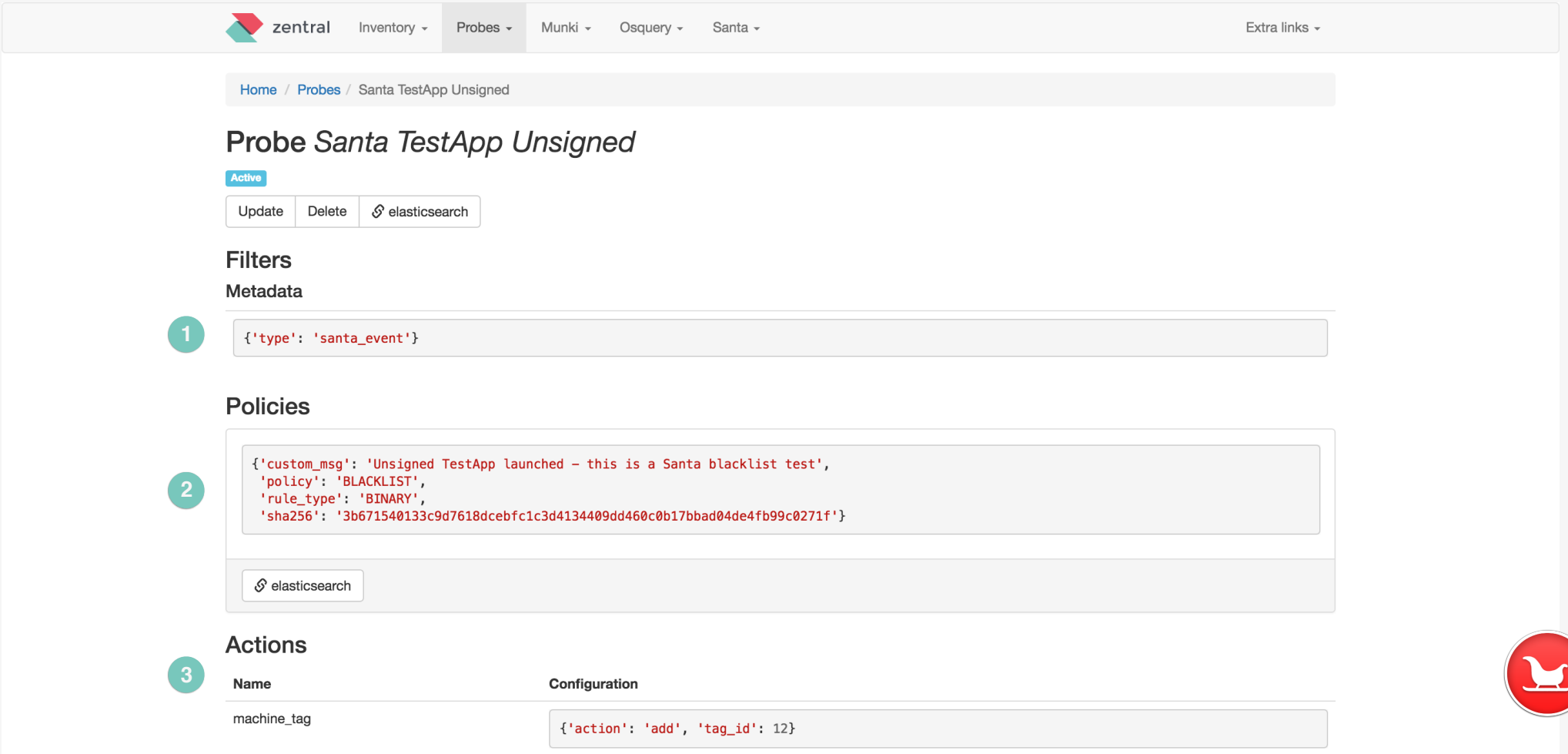
Older →

Type	Created at	Data
osquery_request	June 8, 2016, 6:19 p.m.	`{'request_type': 'config'}`
santa_event	June 8, 2016, 6:18 p.m.	`{'current_sessions': ['head@ttys001', 'head@ttys000', 'head@console'], 'decision': 'ALLOW_UNKNOWN', 'executing_user': 'root', 'execution_time': 1465409329.630623, 'file_name': 'jamfAgent', 'file_path': '/usr/local/jamf/bin', 'file_sha256': 'efa39e542620418fbf2d96da4f95e41e8a2a3cd6861cfff45a59cebc1ffaedfb', 'logged_in_users': ['head'], 'parent_name': 'launchd', 'pid': 46723, 'ppid': 1, 'quarantine_timestamp': 0, 'signing_chain': [{'cn': 'Developer ID Application: JAMF Software', 'org': 'JAMF Software', 'ou': '483DWKW443', 'sha256': '0caf42ad5cf856f4125a1e174692fce7d49a8f6acb70568f3bb53b69acdc979c',`

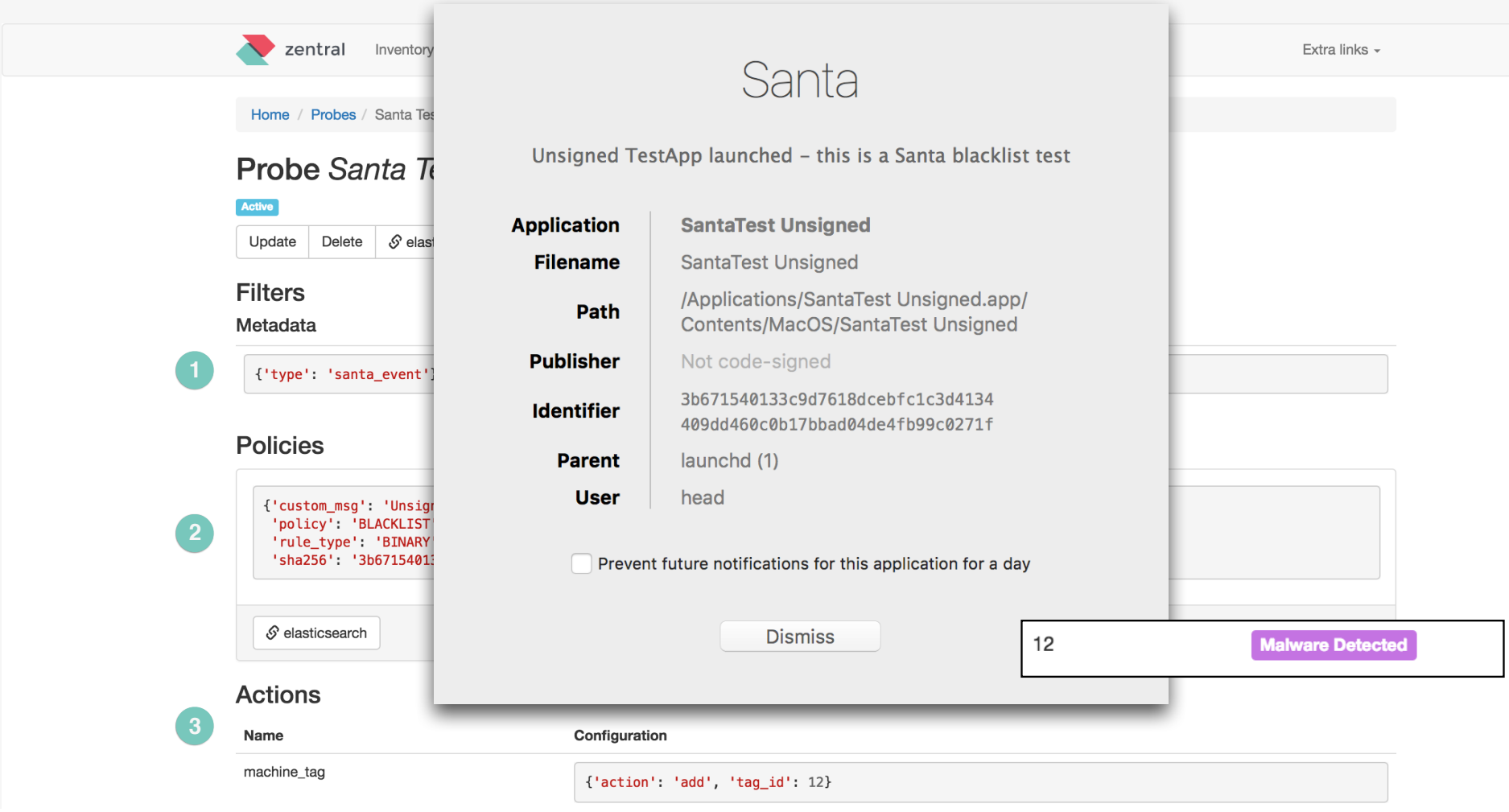
Zentral - Probe / osquery compliance



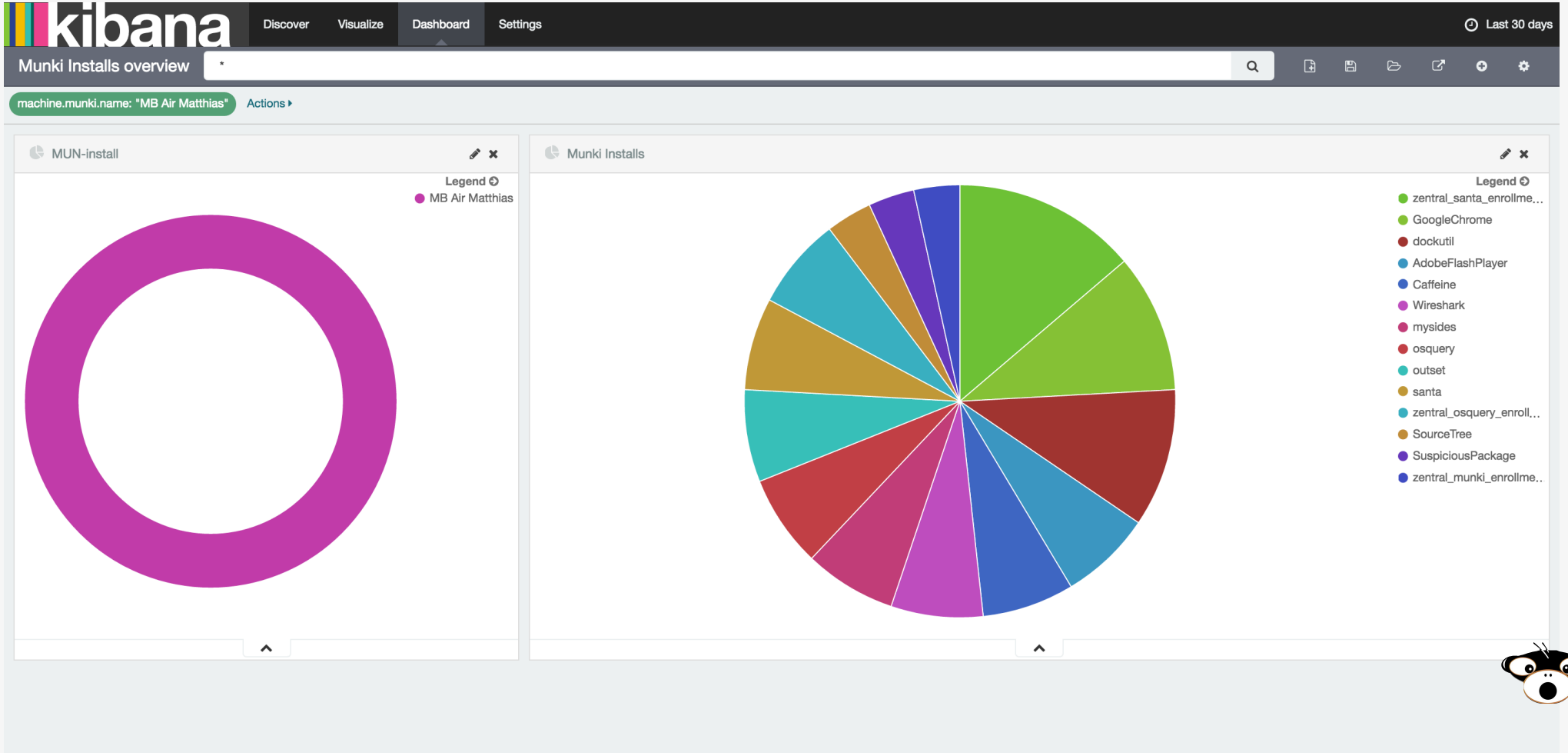
Zentral - Probe / Santa Blacklist



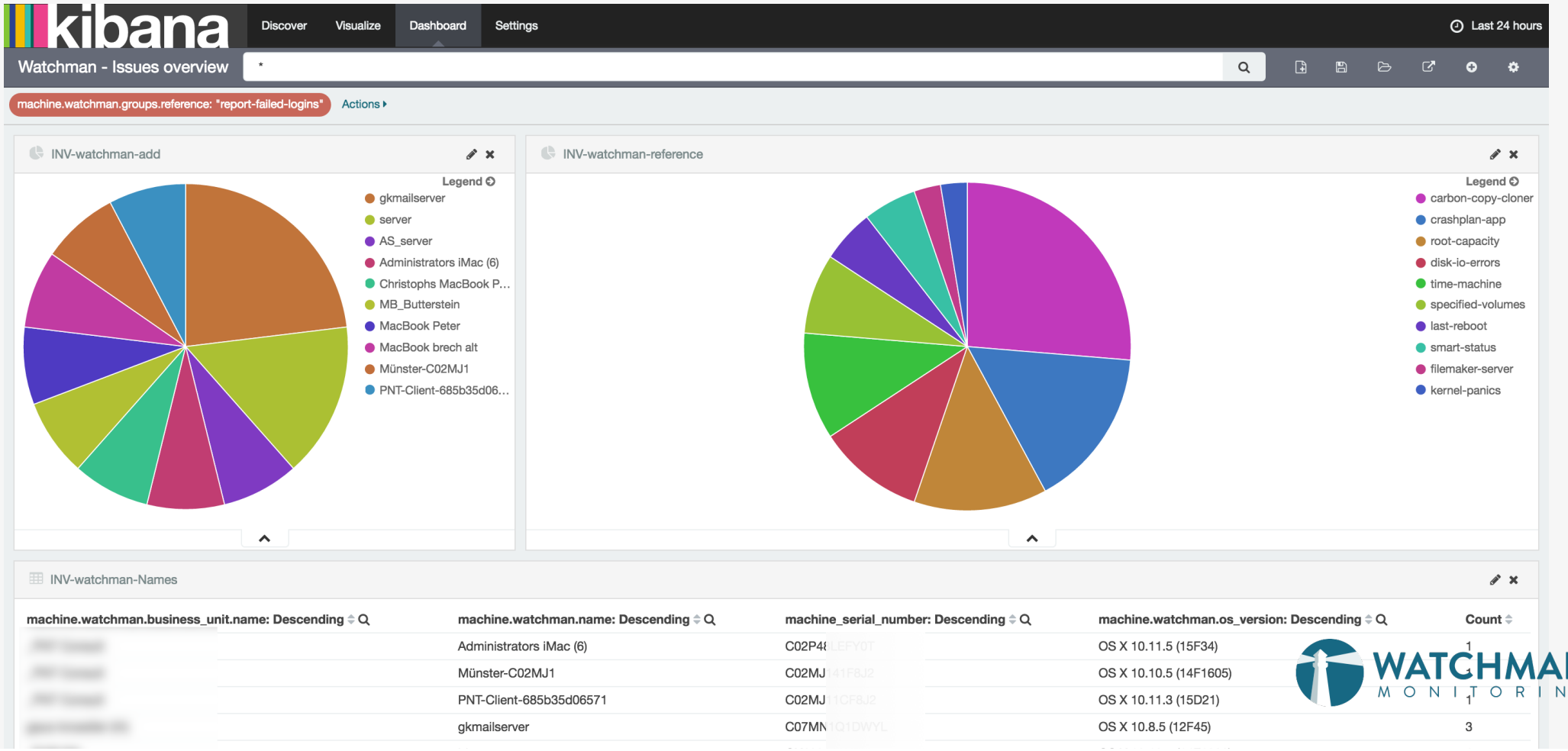
Zentral - Probe / Santa Blacklist



Zentral - Inventory / Munki installs



Zentral - Inventory / Watchman



WATCHMAN MONITORING

Modular Monitoring

Modular Monitoring

Scan based monitoring

Distributed queries

Trigger-based monitoring

Probes: osquery scheduled checks, inventory events

Continuous monitoring

Probes: osquery FIM, santa events

Discovery-based monitoring

Kibana, search, visualize correlating Metrics

Event Lifecycles

Example Lifecycle

IFTTT conditional event processing

- Endpoint = **Emitter** Zentral = **Collector**
- Events, Metrics are **pushed** unidirectional
- Store **near real-time** for continuous/historical visibility
- **Proactive** monitoring, look for **patterns** (anomalies)
- Flexible **response**, auto-activate in depth **mitigation**
- **Search**, event **correlation,** and historical investigation

Flexible

Measure and **collect** standard events

Send ad hoc **distributed queries** to devices

Quickly **Identify** anomalies in context

Automate with tags, filtering, and collision detection

Alert & **notify** with additional **information**

Progressively build escalation & **response** strategies

Response

See **trends**, act upon them (semi) automated

Notify and automate via **MDM** (JAMF JSS)

Santa LOCKDOWN mode

OSQuery - **File Integrity Monitoring** (FIM),

Investigate historical data, change-logs **post-mortem**

Subsequently **mitigate** / **remediate** in context

Integrations

Input

Endpoint Security Tools

osquery

Google Santa

Endpoint Managed Software Solutions

Munki

JAMF software

Casper Suite

Inventory, Events, Metrics

WATCHMAN MONITORING

casper SUITE

REST API

Sal

Input

Endpoint Security Tools

osquery

Google Santa

Endpoint Managed Software Solutions

Munki

JAMF software

Casper Suite

Inventory, Events, Metrics

WATCHMAN MONITORING

casper SUITE

REST API Sal

Output

MDM

JAMF software

REST API

Notifications

Email

zendesk

Trello

GitHub

freshdesk

twilio

slack

Pushover

webhooks

Sub-Systems

kibana

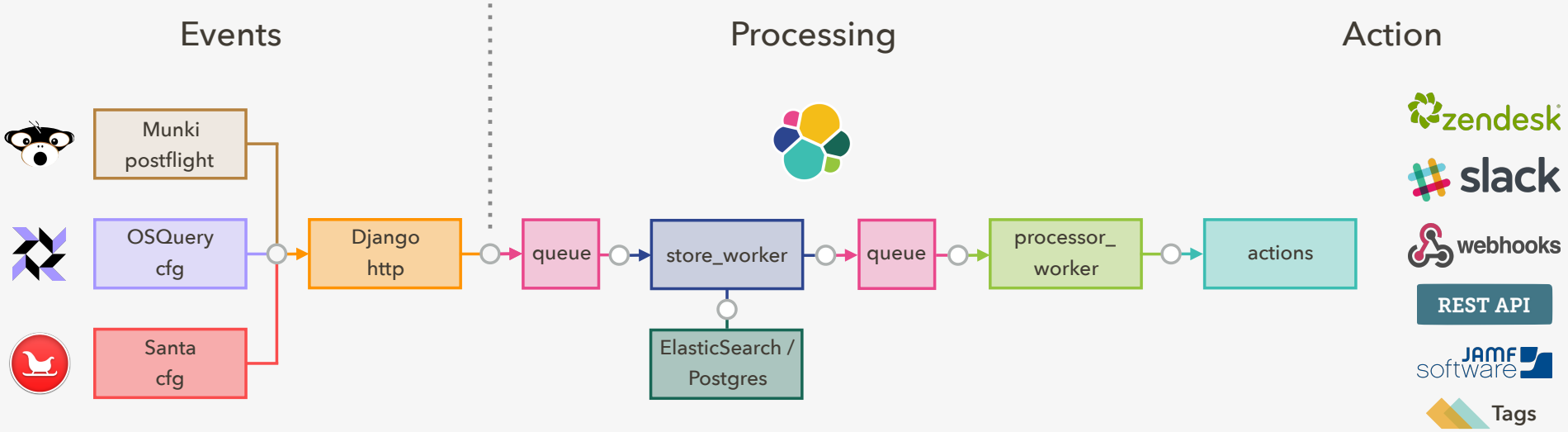
ElasticSearch

Prometheus

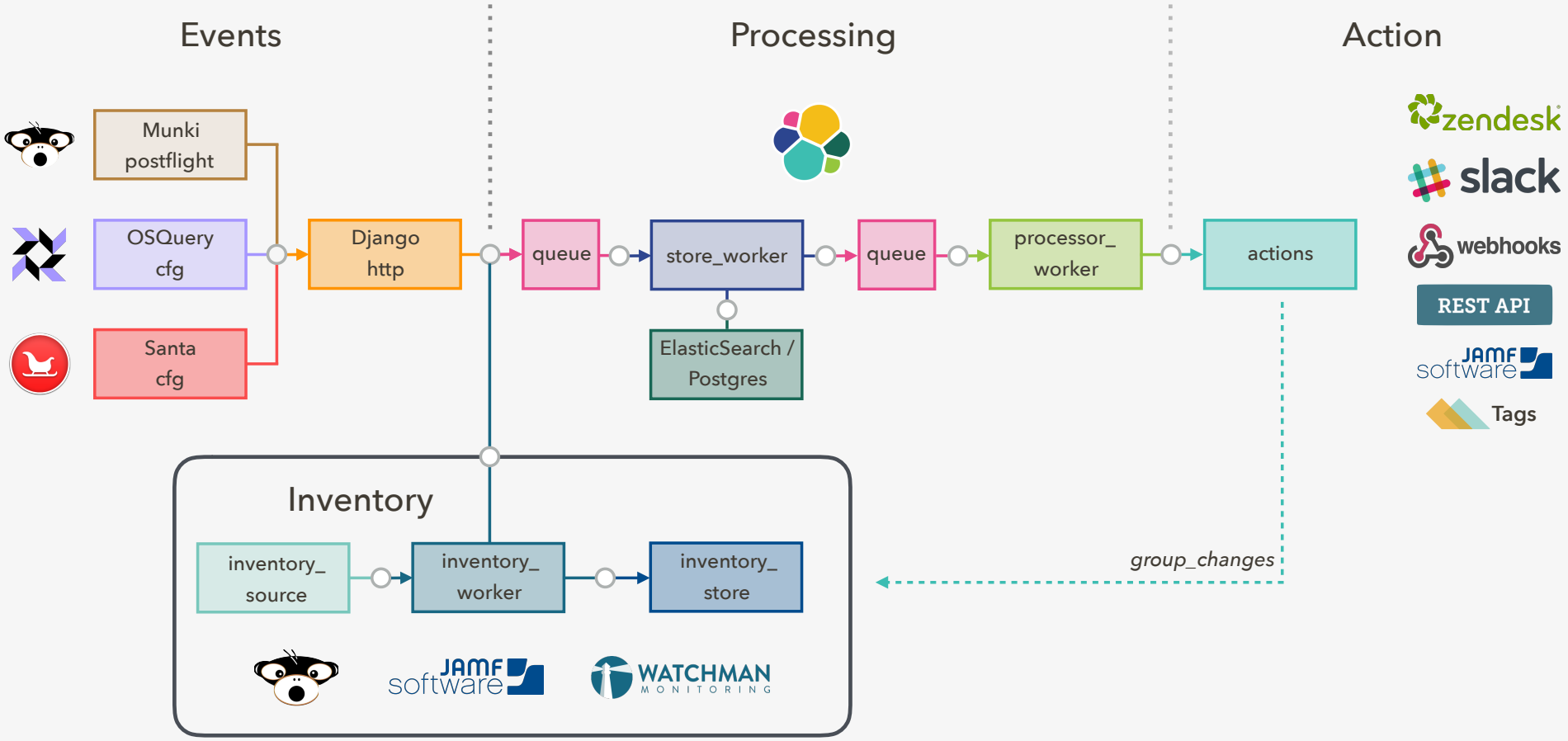
Grafana

Processing Workflow

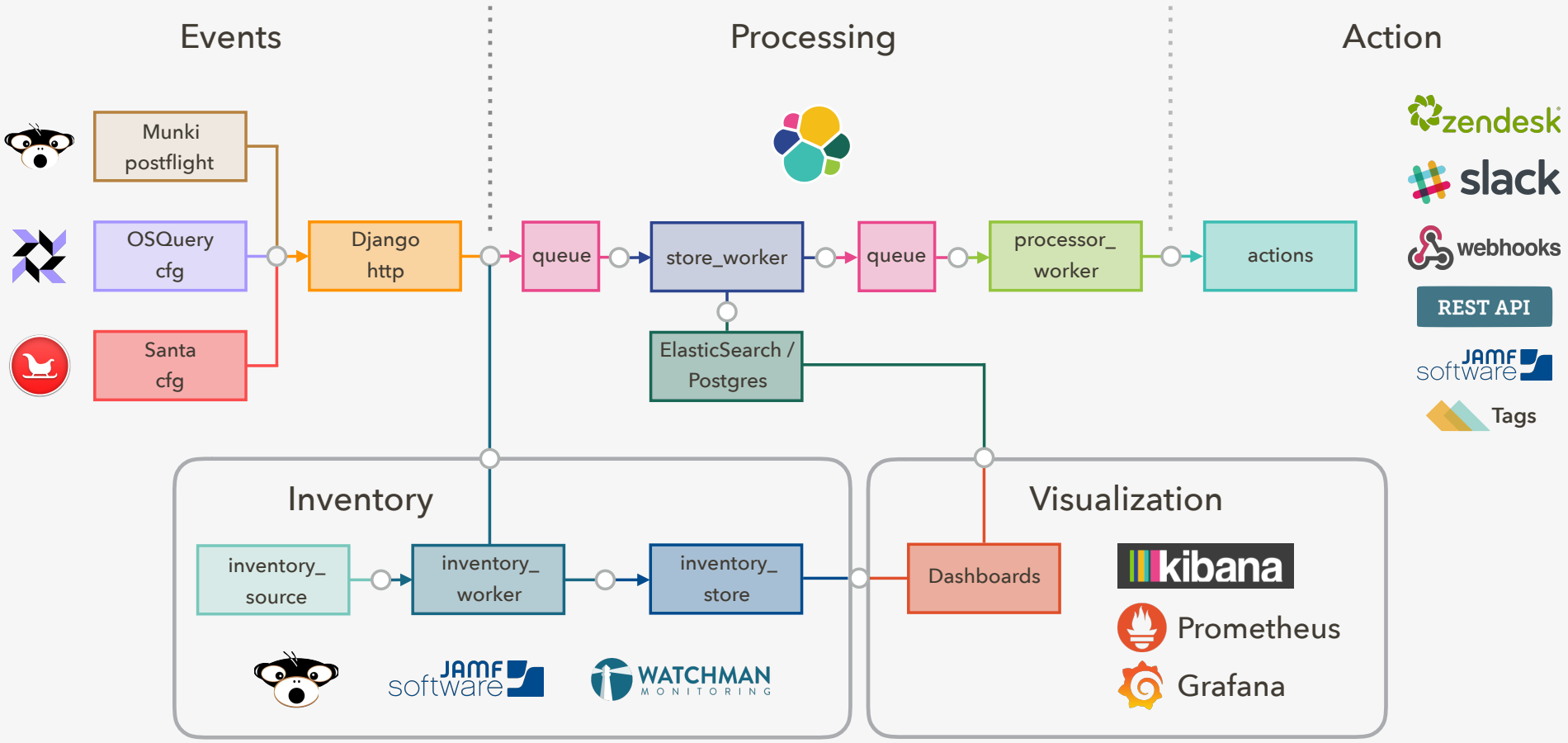
Zentral - Event Processing



Zentral - Event Processing



Zentral - Event Processing



Zentral Features

June 2016

Device Enrollment & Business Units

Device Enrollment / BUs

Enrollment packages pre-build

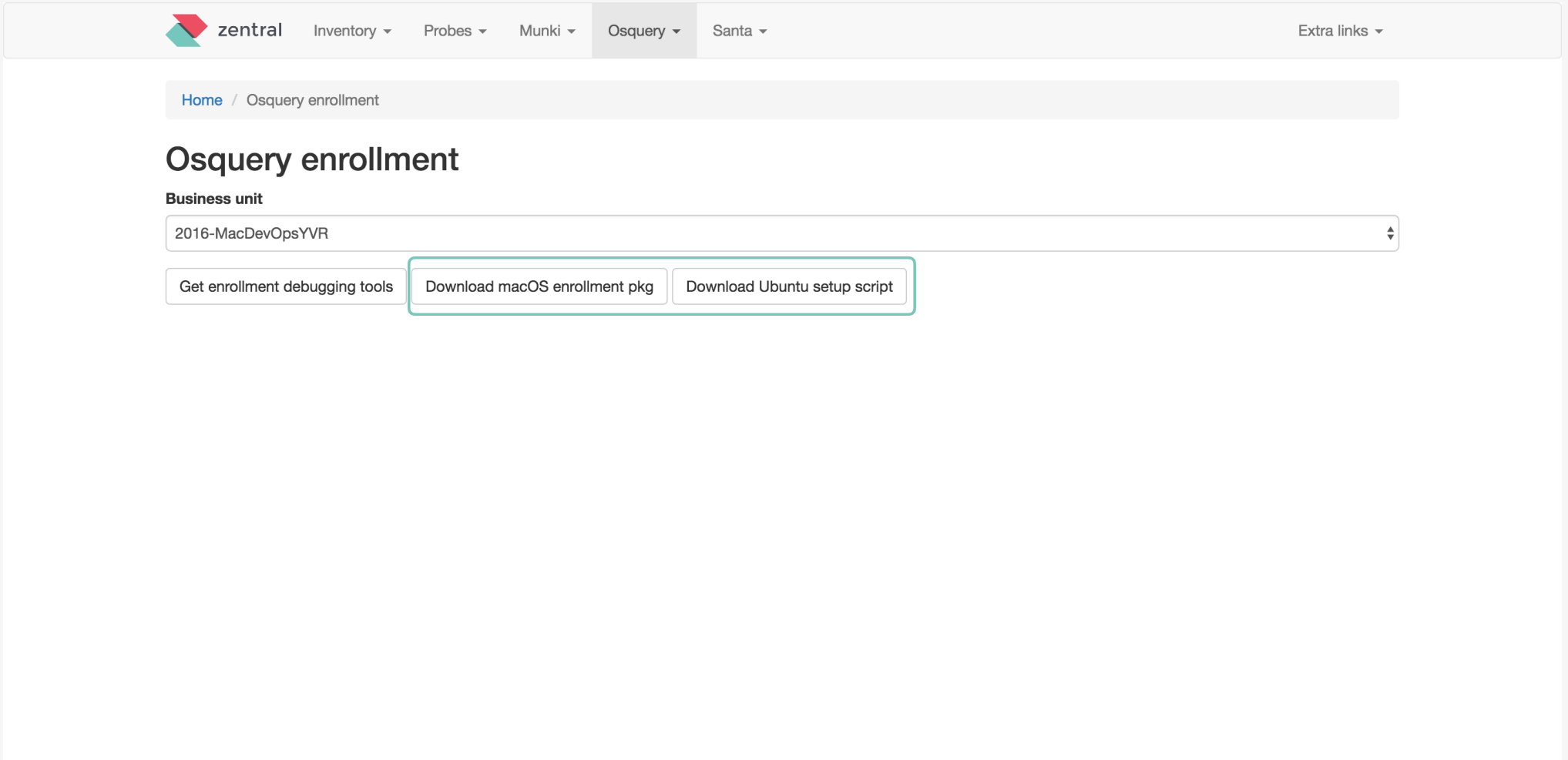
Inventory	osquery	santa	munki	ubuntu *
install path	/usr/local/zentral/osquery	/var/db/santa	postflight.d	/etc/zentral/osquery

* osquery only

Business Unit support for multiple inventory

Inventory	JSS	SAL	Watchman	Zentral
BU	Site	BU	Groups	BU
Group	Group / Smart Group	Group	Plugin-Results	Group
devices	macOS	macOS	macOS / Linux	macOS / Linux

Enrollment


zentral
Inventory
Probes
Munki
Osquery
Santa
Extra links
Home / Osquery enrollment
Osquery enrollment
Business unit
2016-MacDevOpsYVR
Get enrollment debugging tools
Download macOS enrollment pkg
Download Ubuntu setup script

Tags

Tags / Dynamic Scope

Tags **create** Groups / Smart Groups

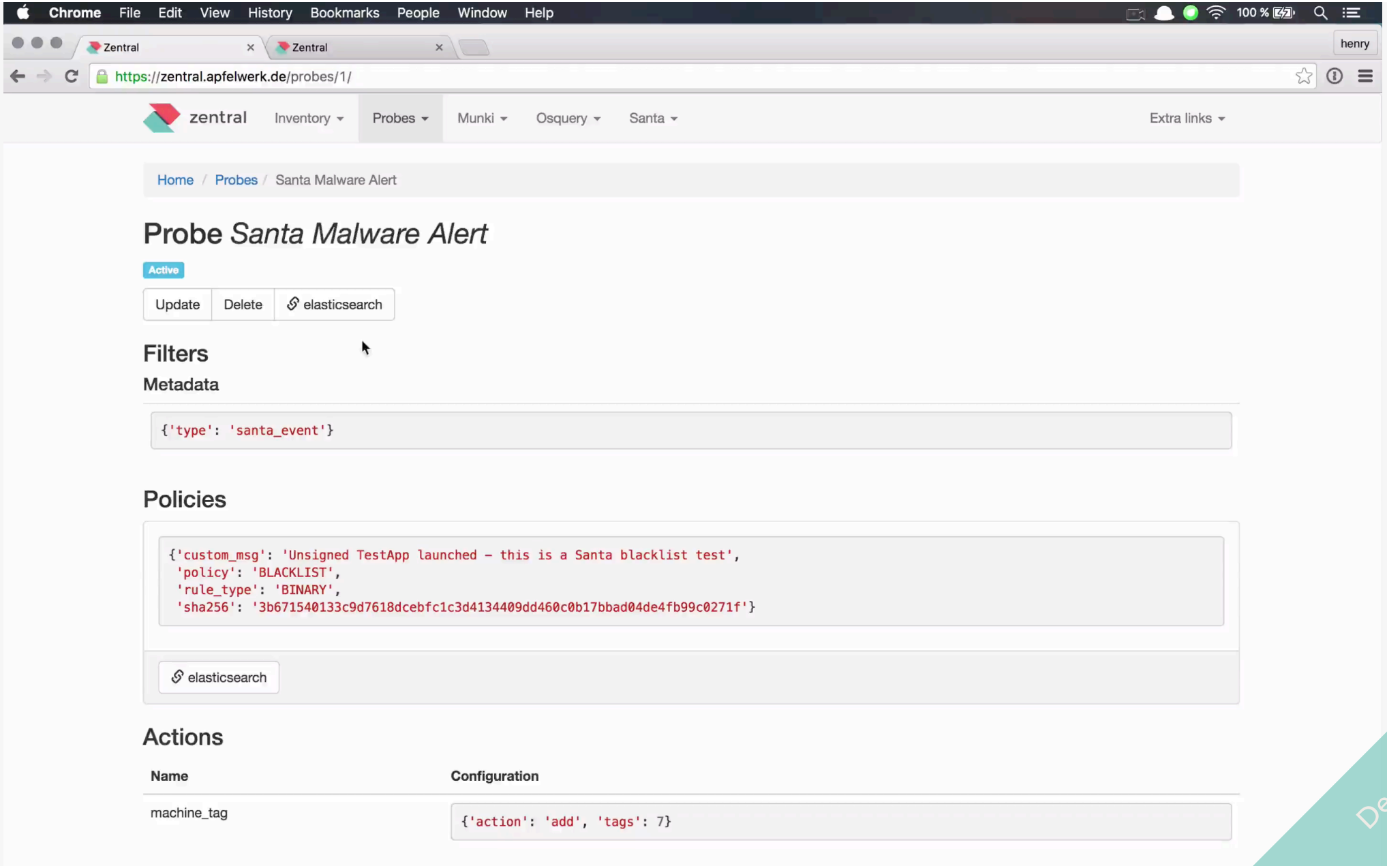
Actions can **add/remove** Tags on **dynamic criteria**

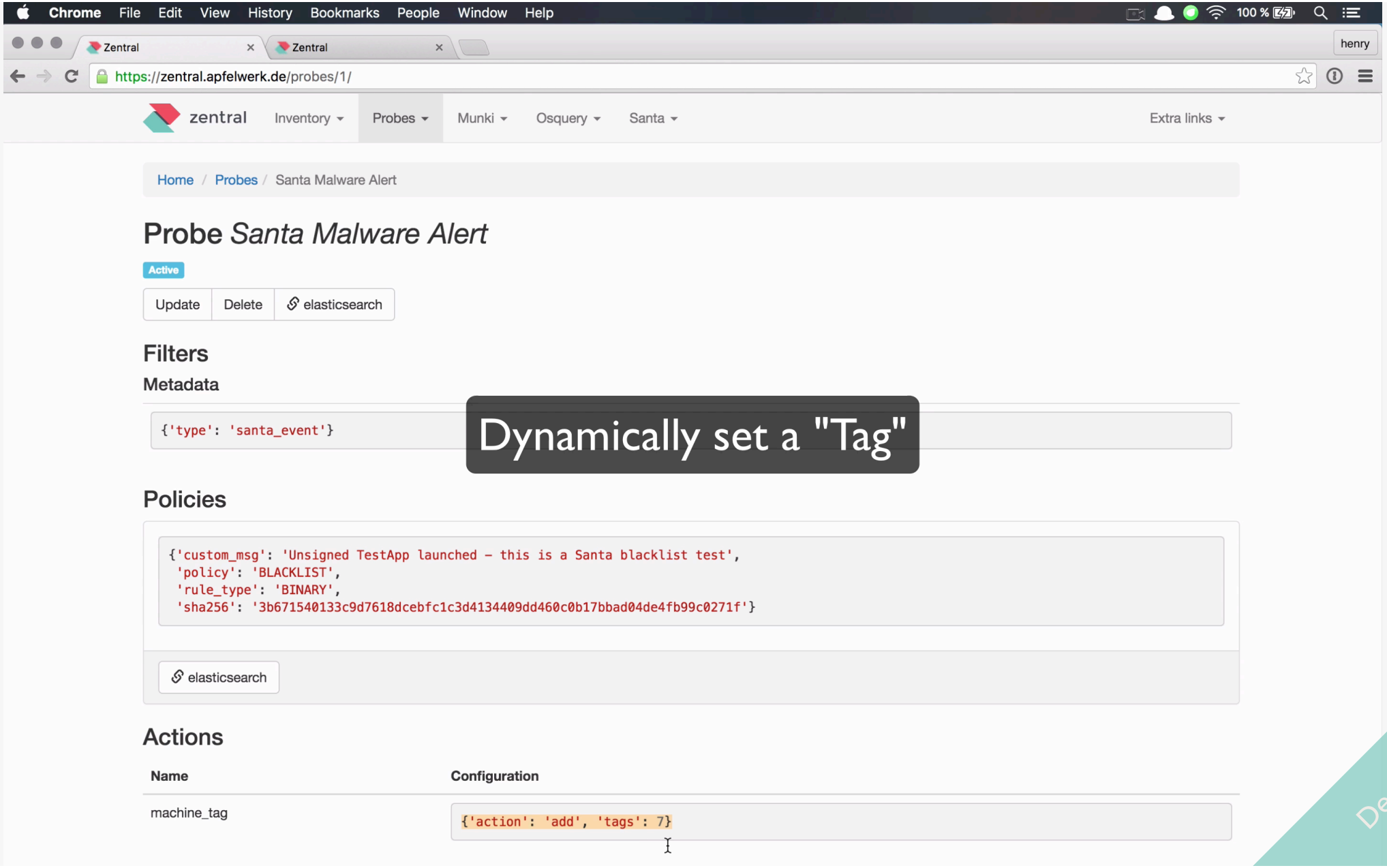
Tags work **across** BusinessUnits

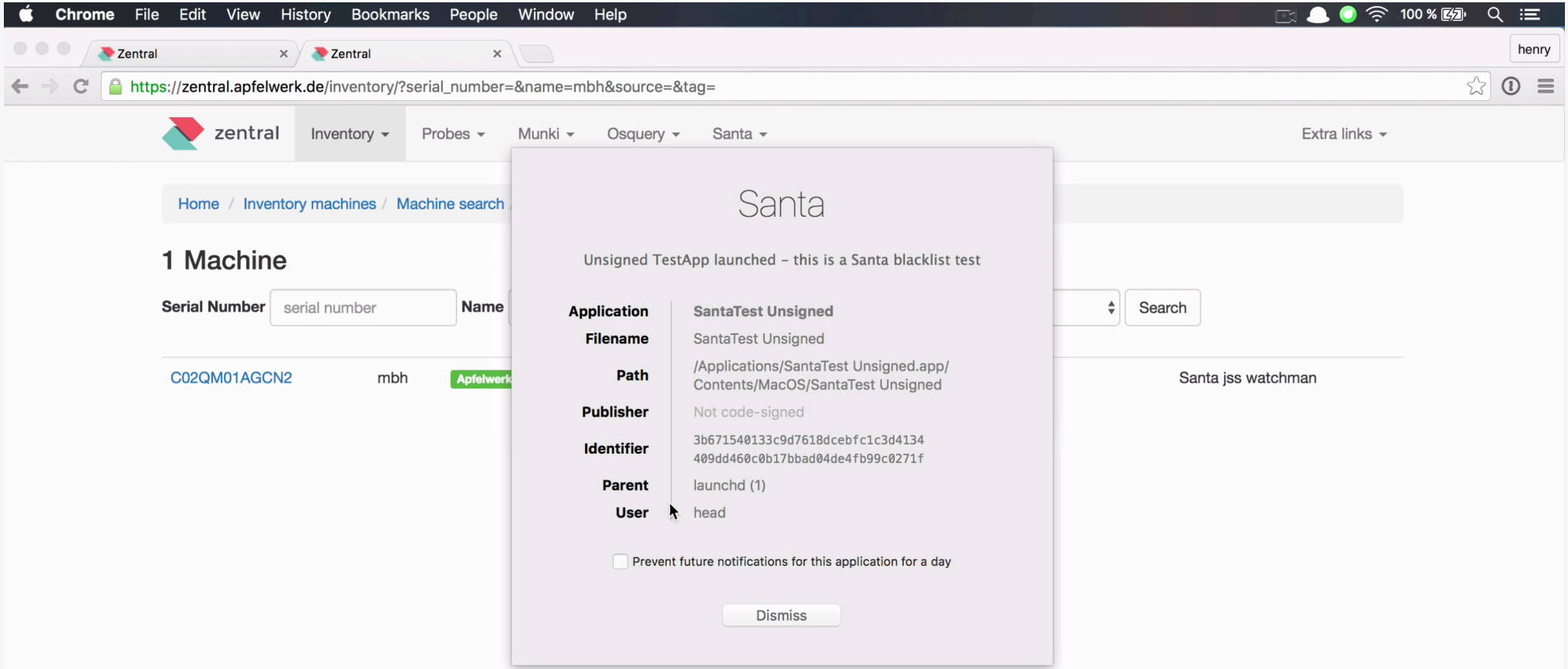
Can be **restricted** to specific BusinessUnits

Tags will **set scope** for distributed queries (osquery)

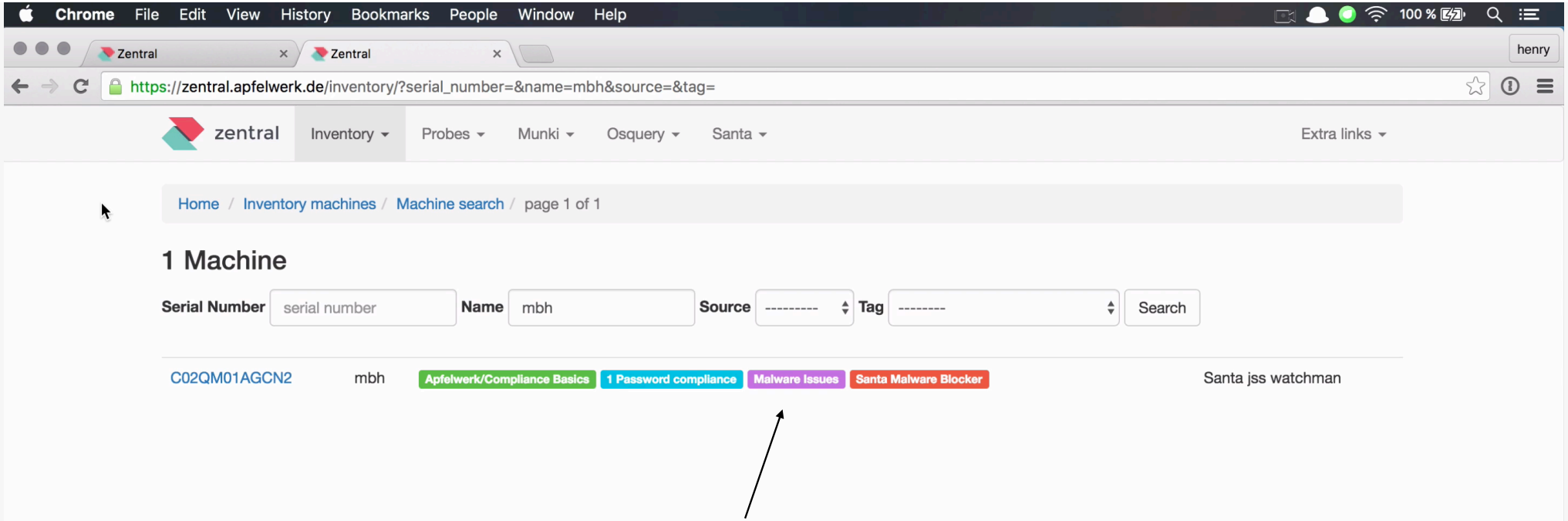
Scope **Probes** using **filter on Tags**


Chrome File Edit View History Bookmarks People Window Help
100 %
Zentral
Zentral
henry
https://zentral.apfelwerk.de/probes/1/
zentral
Inventory
Probes
Munki
Osquery
Santa
Extra links
Home / Probes / Santa Malware Alert
Probe Santa Malware Alert
Active
Update
Delete
elasticsearch
Filters
Metadata
{'type': 'santa_event'}
Policies
{'custom_msg': 'Unsigned TestApp launched - this is a Santa blacklist test',
'policy': 'BLACKLIST',
'rule_type': 'BINARY',
'sha256': '3b671540133c9d7618dcebfc1c3d4134409dd460c0b17bbad04de4fb99c0271f'}
elasticsearch
Actions
Name
Configuration
machine_tag
{'action': 'add', 'tags': 7}
Demo


Chrome File Edit View History Bookmarks People Window Help
100 %
Zentral
Zentral
henry
https://zentral.apfelwerk.de/probes/1/
zentral
Inventory
Probes
Munki
Osquery
Santa
Extra links
Home / Probes / Santa Malware Alert
Probe Santa Malware Alert
Active
Update
Delete
elasticsearch
Filters
Metadata
{'type': 'santa_event'}
Dynamically set a "Tag"
Policies
{'custom_msg': 'Unsigned TestApp launched - this is a Santa blacklist test',
'policy': 'BLACKLIST',
'rule_type': 'BINARY',
'sha256': '3b671540133c9d7618dcebfc1c3d4134409dd460c0b17bbad04de4fb99c0271f'}
elasticsearch
Actions
Name
Configuration
machine_tag
{'action': 'add', 'tags': 7}
Demo


Chrome File Edit View History Bookmarks People Window Help
100 %
Zentral
Zentral
henry
https://zentral.apfelwerk.de/inventory/?serial_number=&name=mbh&source=&tag=
zentral
Inventory
Probes
Munki
Osquery
Santa
Extra links
Home / Inventory machines / Machine search
1 Machine
Serial Number
serial number
Name
Search
C02QM01AGCN2
mbh
Apfelwerk
Santa jss watchman
Santa
Unsigned TestApp launched – this is a Santa blacklist test
Application
SantaTest Unsigned
Filename
SantaTest Unsigned
Path
/Applications/SantaTest Unsigned.app/
Contents/MacOS/SantaTest Unsigned
Publisher
Not code-signed
Identifier
3b671540133c9d7618dcebfc1c3d4134
409dd460c0b17bbad04de4fb99c0271f
Parent
launchd (1)
User
head
Prevent future notifications for this application for a day
Dismiss

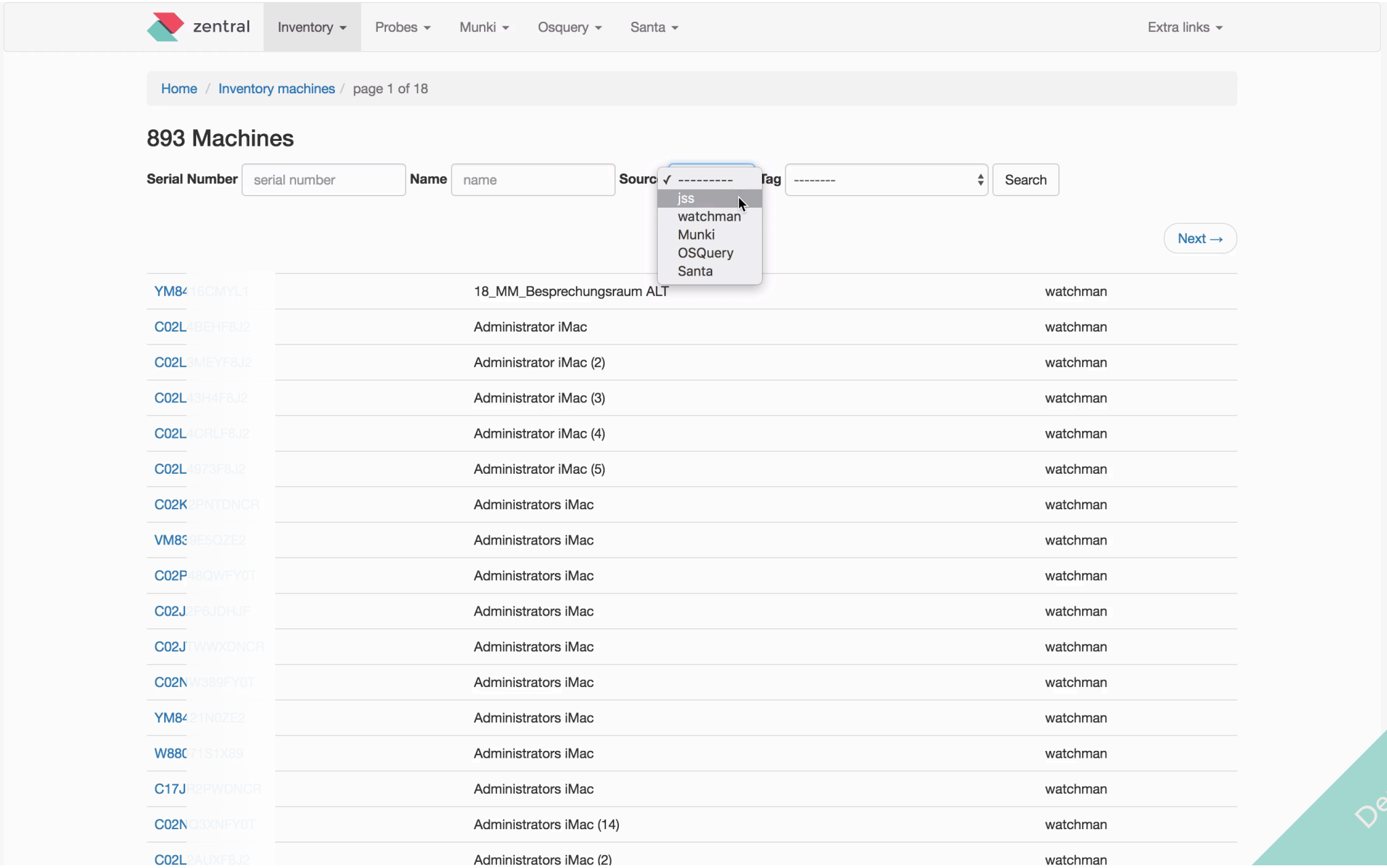
Demo

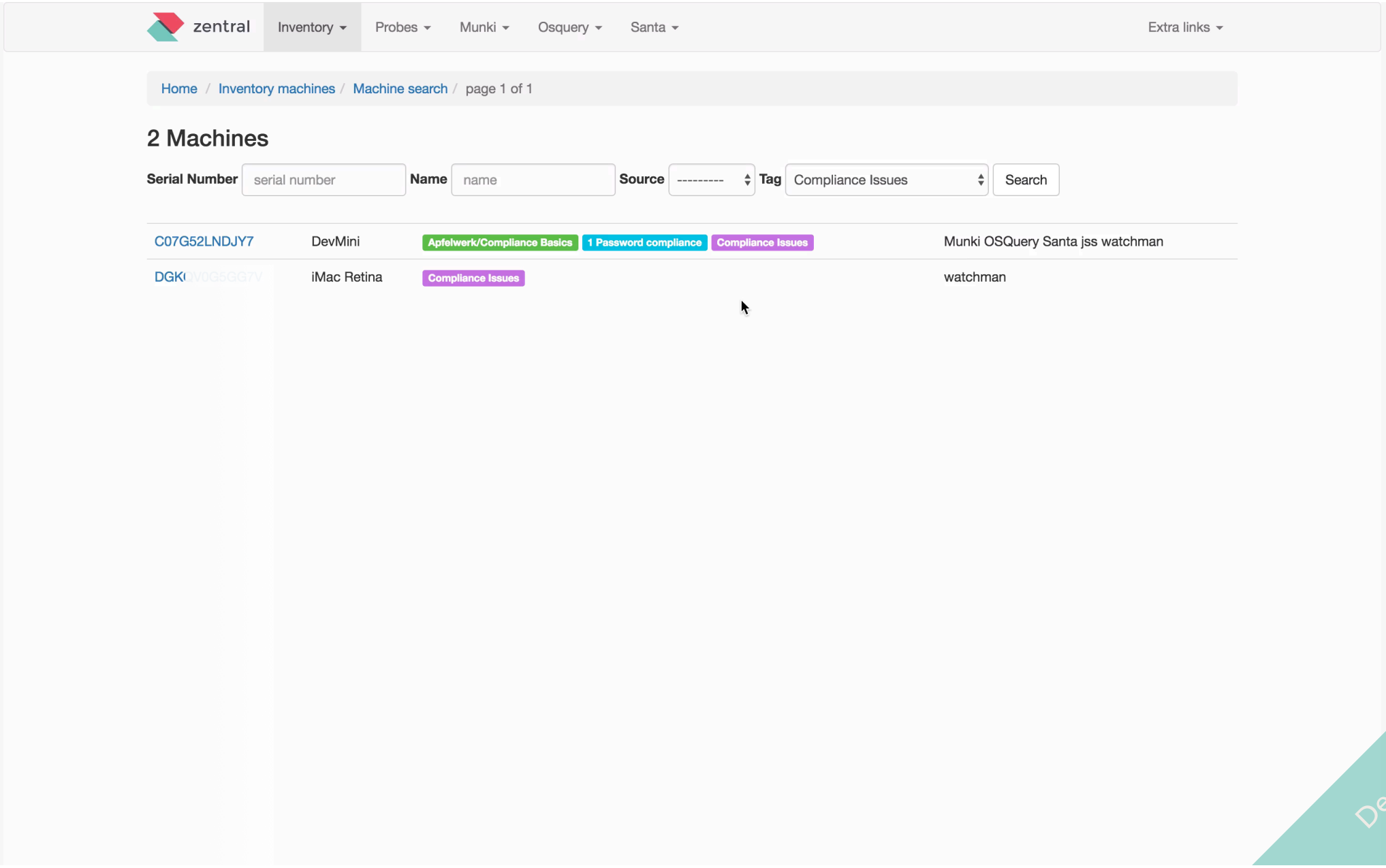


new Tag attached dynamically by Santa

Demo

Enhanced Search


zentral
Inventory
Probes
Munki
Osquery
Santa
Extra links
Home / Inventory machines / page 1 of 18
893 Machines
Serial Number
serial number
Name
name
Sourc
Tag
Search
jss
watchman
Munki
OSQuery
Santa
Next →
18_MM_Besprechungsraum ALT
Administrator iMac
Administrator iMac (2)
Administrator iMac (3)
Administrator iMac (4)
Administrator iMac (5)
Administrators iMac
watchman
Demo


zentral
Inventory
Probes
Munki
Osquery
Santa
Extra links
Home / Inventory machines / Machine search / page 1 of 1
2 Machines
Serial Number
serial number
Name
name
Source

Tag
Compliance Issues
Search
C07G52LNDJY7
DevMini
Apfelwerk/Compliance Basics
1 Password compliance
Compliance Issues
Munki OSQuery Santa jss watchman
DGK
iMac Retina
Compliance Issues
watchman
Demo

Probe Editor

Probe Editor

Create **new** Probes in **browser**

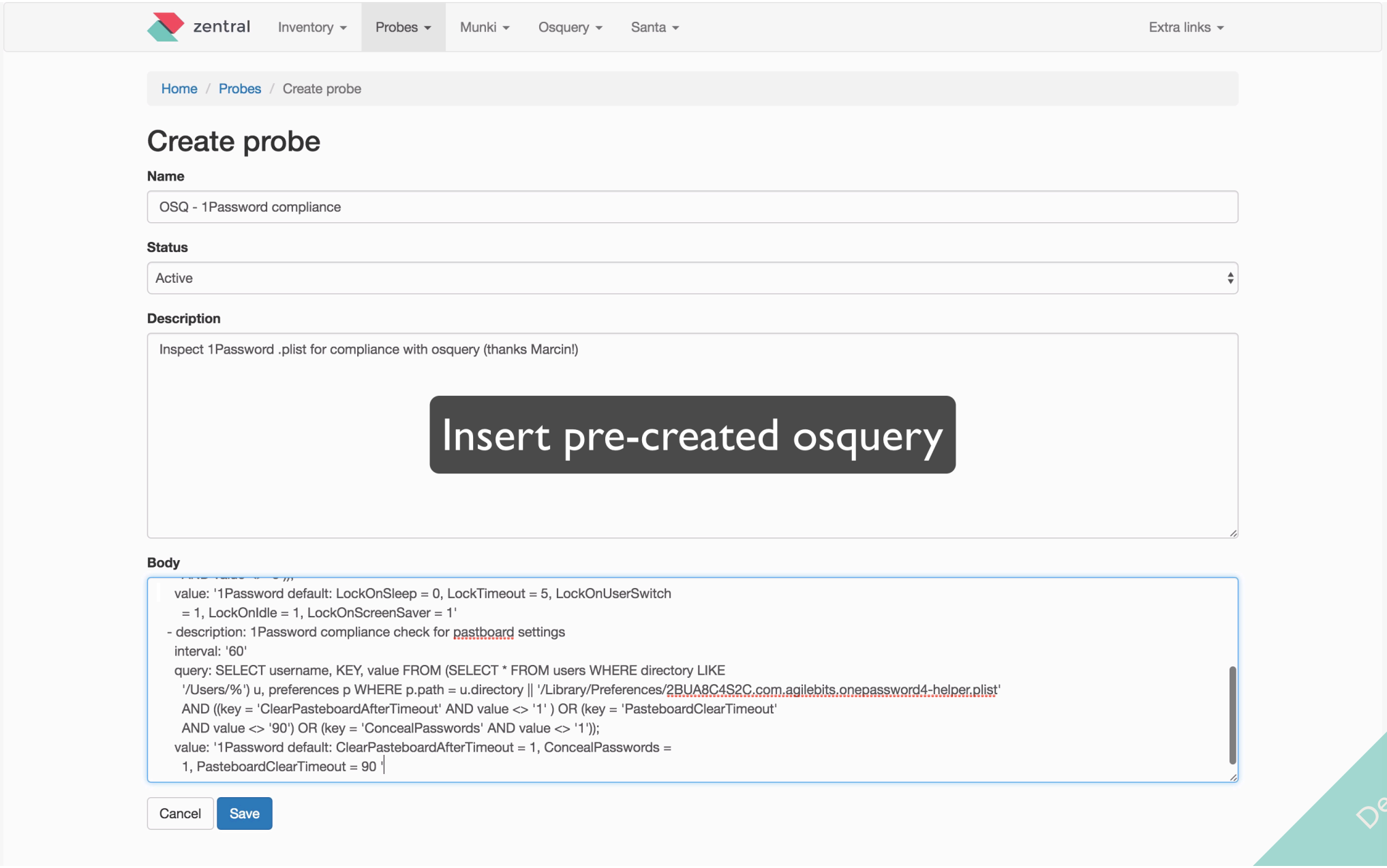
Automatically assigned to devices

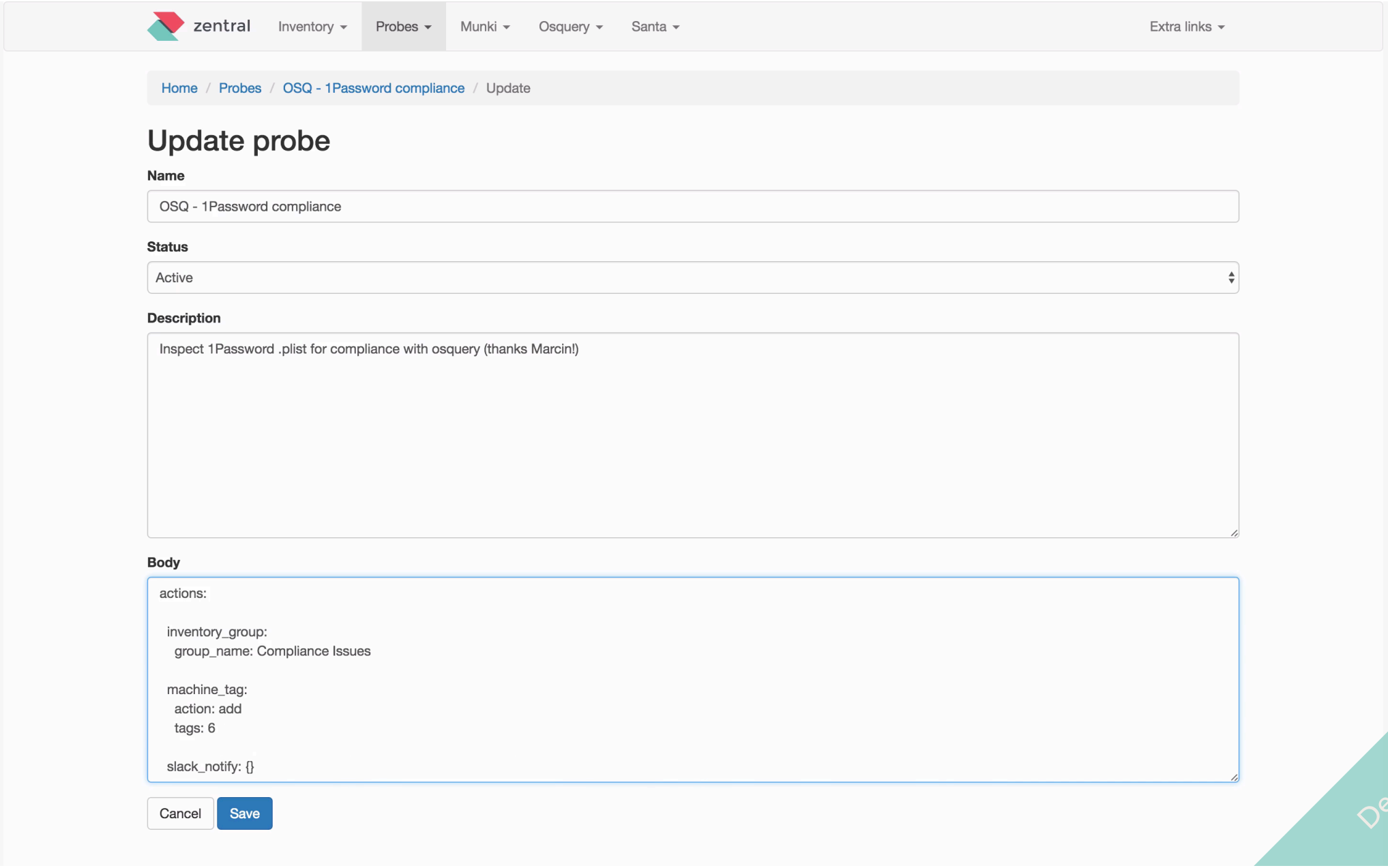
Filter on Tags will **set scope**

Basic **linting** for YAML/JSON

Auto-reload processor_worker in background

Import script for probes (file based)


zentral
Inventory
Probes
Munki
Osquery
Santa
Extra links
Home / Probes / Create probe
Create probe
Name
OSQ - 1Password compliance
Status
Active
Description
Inspect 1Password .plist for compliance with osquery (thanks Marcin!)
Insert pre-created osquery
Body
value: '1Password default: LockOnSleep = 0, LockTimeout = 5, LockOnUserSwitch
= 1, LockOnIdle = 1, LockOnScreenSaver = 1'
- description: 1Password compliance check for pastboard settings
interval: '60'
query: SELECT username, KEY, value FROM (SELECT * FROM users WHERE directory LIKE
'/Users/%') u, preferences p WHERE p.path = u.directory || '/Library/Preferences/2BUA8C4S2C.com.agilebits.onepassword4-helper.plist'
AND ((key = 'ClearPasteboardAfterTimeout' AND value <> '1') OR (key = 'PasteboardClearTimeout'
AND value <> '90') OR (key = 'ConcealPasswords' AND value <> '1'));
value: '1Password default: ClearPasteboardAfterTimeout = 1, ConcealPasswords =
1, PasteboardClearTimeout = 90 '
Cancel
Save
Demo


zentral
Inventory
Probes
Munki
Osquery
Santa
Extra links
Home / Probes / OSQ - 1Password compliance / Update
Update probe
Name
OSQ - 1Password compliance
Status
Active
Description
Inspect 1Password .plist for compliance with osquery (thanks Marcin!)
Body
actions:
inventory_group:
group_name: Compliance Issues
machine_tag:
action: add
tags: 6
slack_notify: {}
Cancel
Save
Demo

elasticsearch

```
SELECT username,
       KEY,
       value
FROM
  (SELECT *
   FROM users
   WHERE directory LIKE '/Users/%') u,
     preferences p
WHERE p.path = u.directory || '/Library/Preferences/2BUA8C4S2C.com.agilebits.onepassword4-helper.plist'
  AND ((KEY = 'ClearPasteboardAfterTimeout'
        AND value <> '1')
       OR (KEY = 'PasteboardClearTimeout'
           AND value <> '90')
       OR (KEY = 'ConcealPasswords'
           AND value <> '1'));
```

Interval
60
Value
1Password default: ClearPasteboardAfterTimeout = 1, ConcealPasswords = 1, PasteboardClearTimeout = 90
Description
1Password compliance check for pastboard settings

elasticsearch

Actions

Name	Configuration
inventory_group	`{'group_name': 'Compliance Issues'}`
slack_notify	`{}`
machine_tag	`{'action': 'add', 'tags': 6}`

Examples

Automated FileIntegrityMonitoring (FIM)

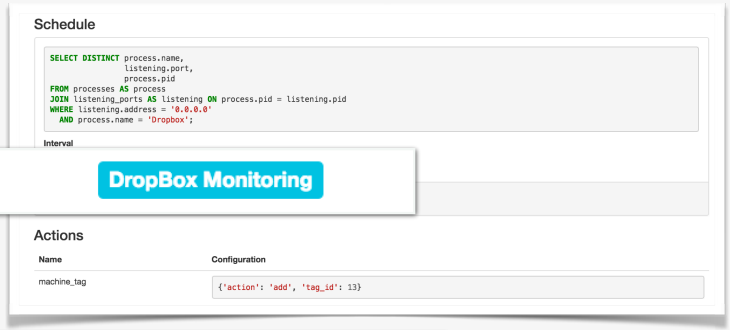
Automated Probes (Example)

Broad Scale

In Depth

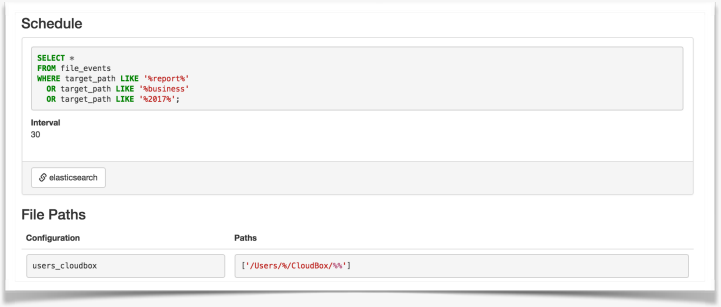
1. Tag "monitoring" > osquery: listen for process
2. osquery > Action: set Tag "FIM inspect"
3. Probe: osquery FIM inspect system events in path
4. Action: Alert a Team > breach reported

Probe 1



Auto Tag 2

Probe 3



Alert 4

Case study:
Zentral in Production

Apfelwerk MSP

933 devices

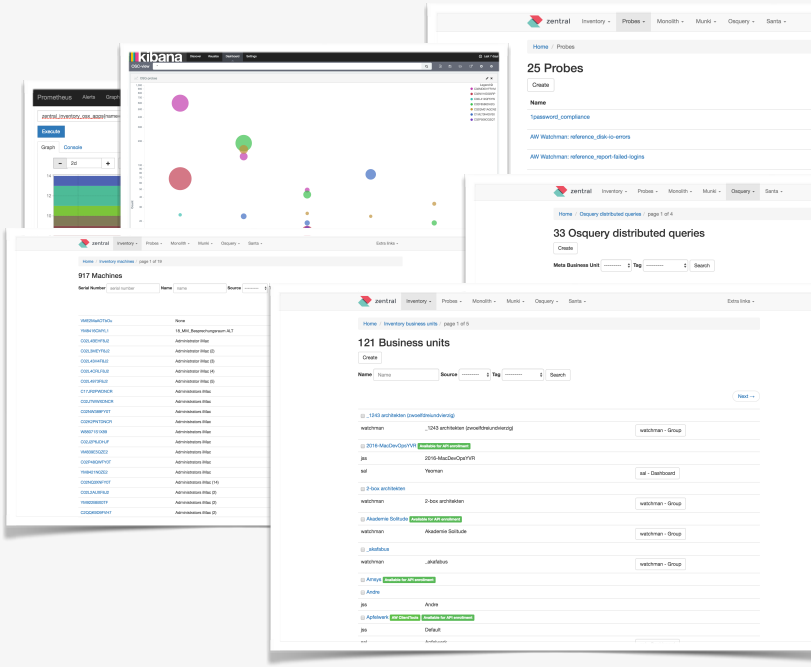
121 BusinessUnits (~ 90 clients)

3% Linux Servers

Watchman, Munki, JSS

Managed munki (rollout in progress)

osquery and Santa on < 10% of devices



apfelwerk

Zentral in Prod (specs)

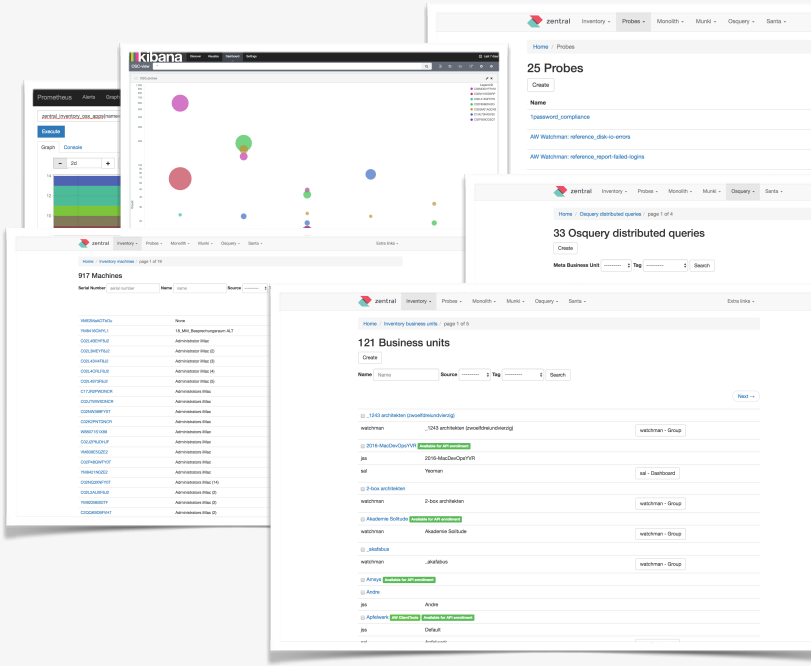
VM (hosted in German DataCenter)

4 core, 16 GB Ram, Debian based

ElasticSearch, Kibana4

Prometheus, Grafana

Deployment: Ansible & docker-compose



apfelwerk

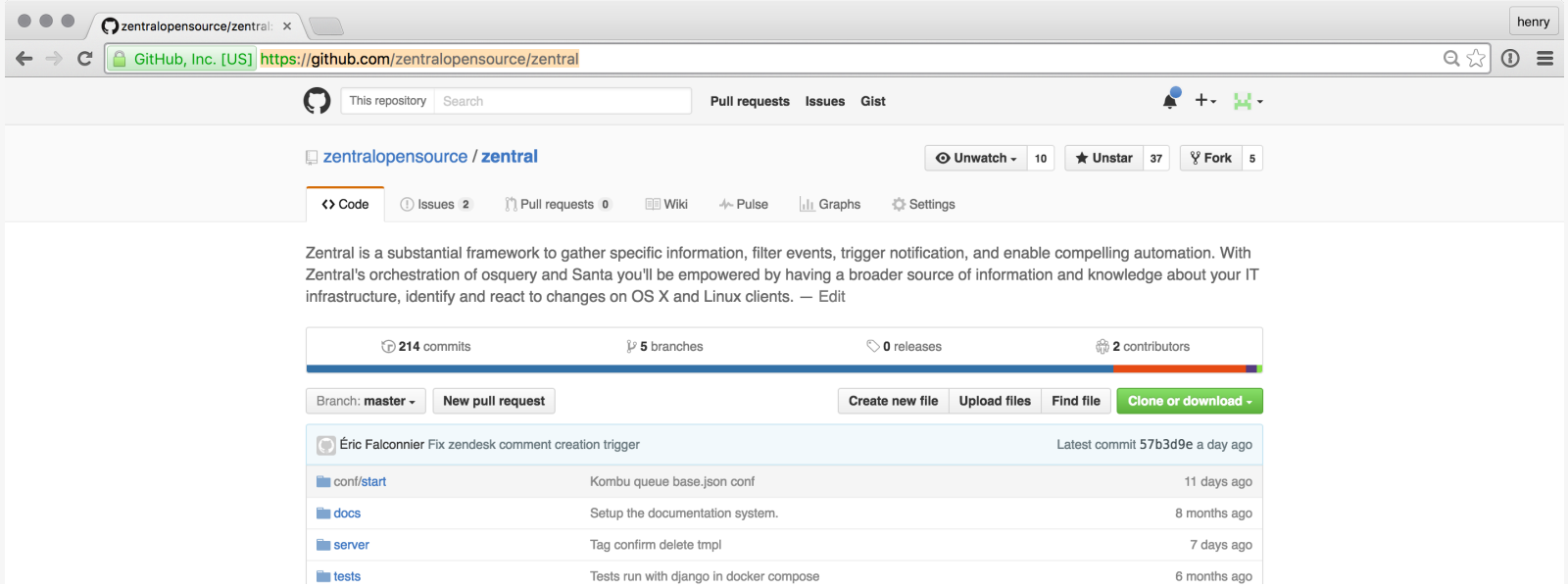
How to get started ?

Project on Github

https://github.com/zentralopensource/zentral

https://github.com/zentralopensource/docs

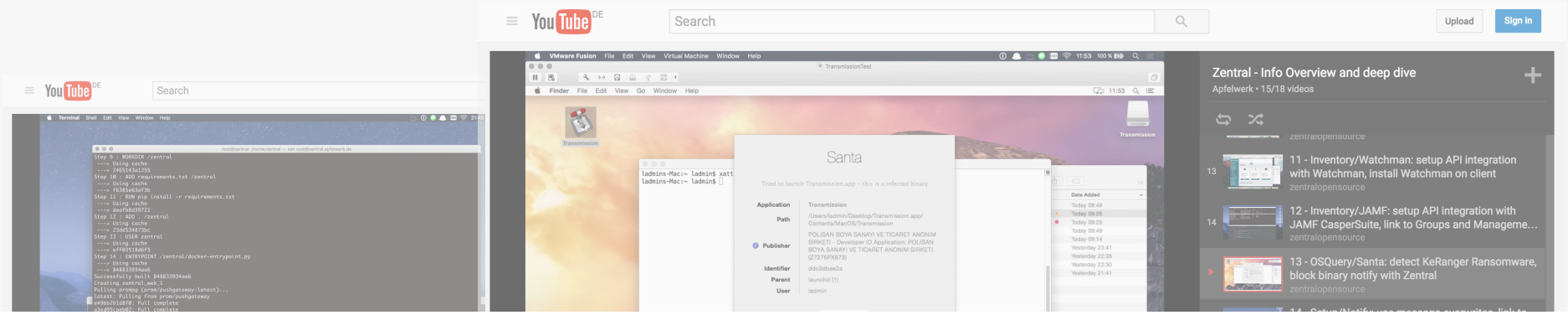
@zentral_io



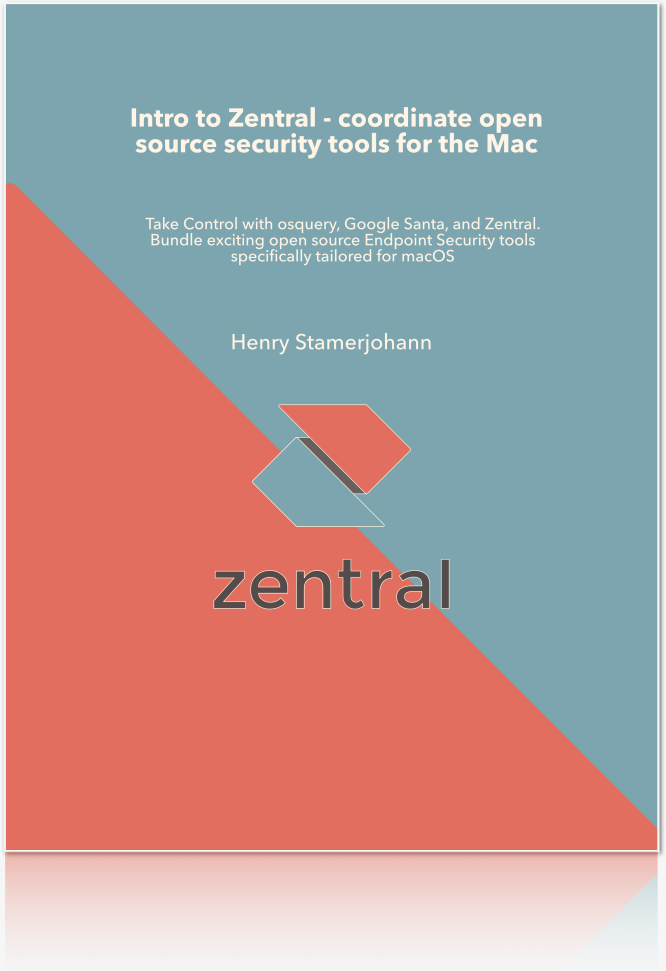
Video Tutorials

https://goo.gl/qsIVkl

- **17 Episodes** - how to setup Zentral with **osquery**, **Santa**, **Munki**
- Simple start with **docker-compose**, details to integrate with **JAMF JSS** & **Watchman**,
- Connecting with Sal, MunkireportPHP, MonkeyBox



E-book



Intro to Zentral *(free ebook)*

https://leanpub.com/zentral

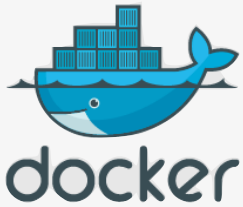
PDF (for your computer)
EPUB (for iPad and other ebook readers)
MOBI (for Kindle)

publishing in-progress

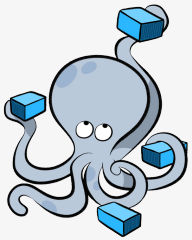
Leanpub

Deployment

Ready, Get, Set - Docker!



Docker multicontainer setup
with **docker-compose**



```
git clone https://github.com/zentralopensource/zentral.git
```

```
docker-compose up -d
```

hint: Tutorials https://goo.gl/qsIVkl

Quick Start

Django Deployment

Deploy like any other Django app

Extend like any Django app (LDAP, AUTH)

```
requirements.txt
gunicorn
wheel
```

Thank You !