

á apfelwerk



Henry Stamerjohann

Apfelwerk GmbH & Co. KG

 @head_min

 #macadmins

Combine the power of osquery + Santa



Zentral

Security

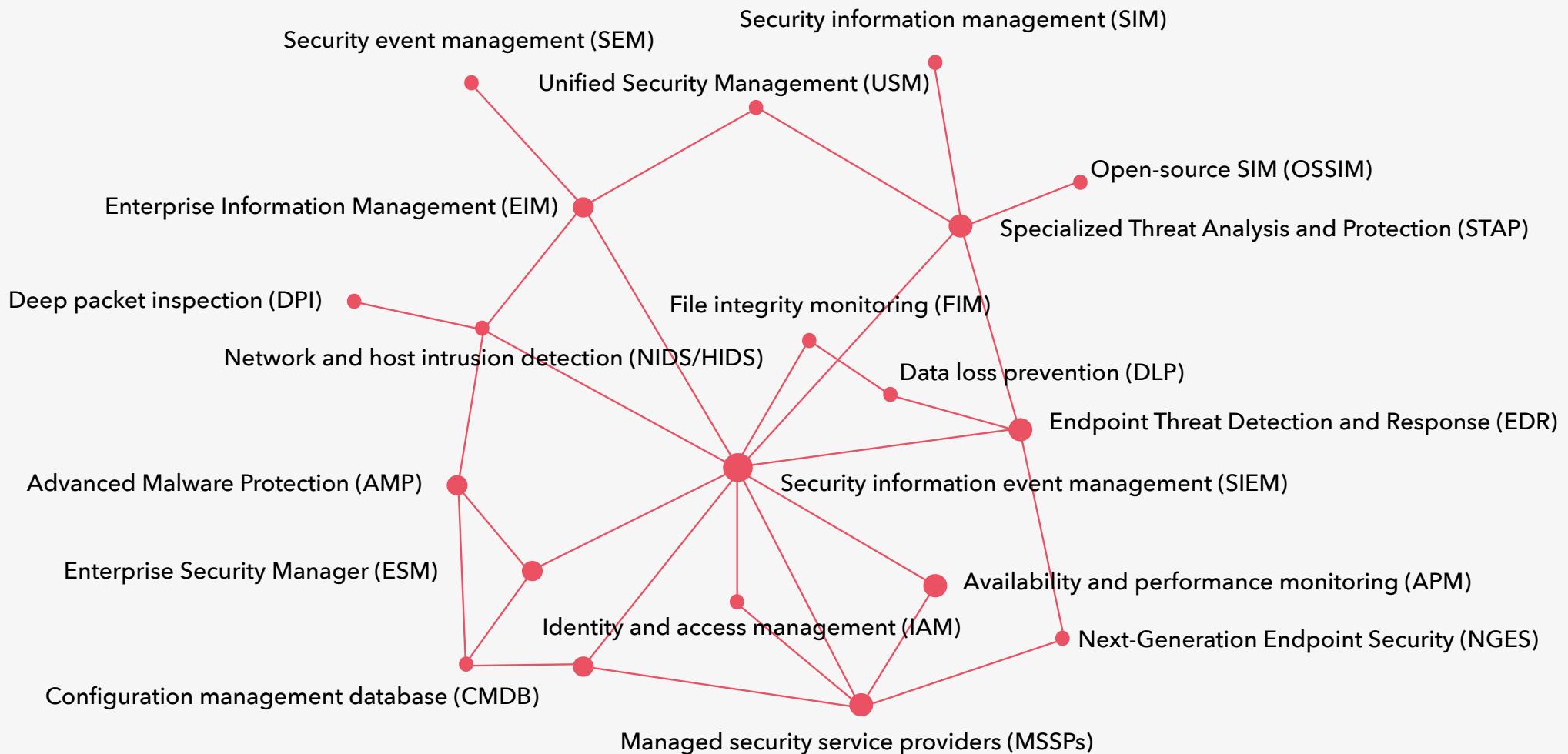
Monitoring

Security

IT Security Market



Security Acronyms and Abbreviations



Management

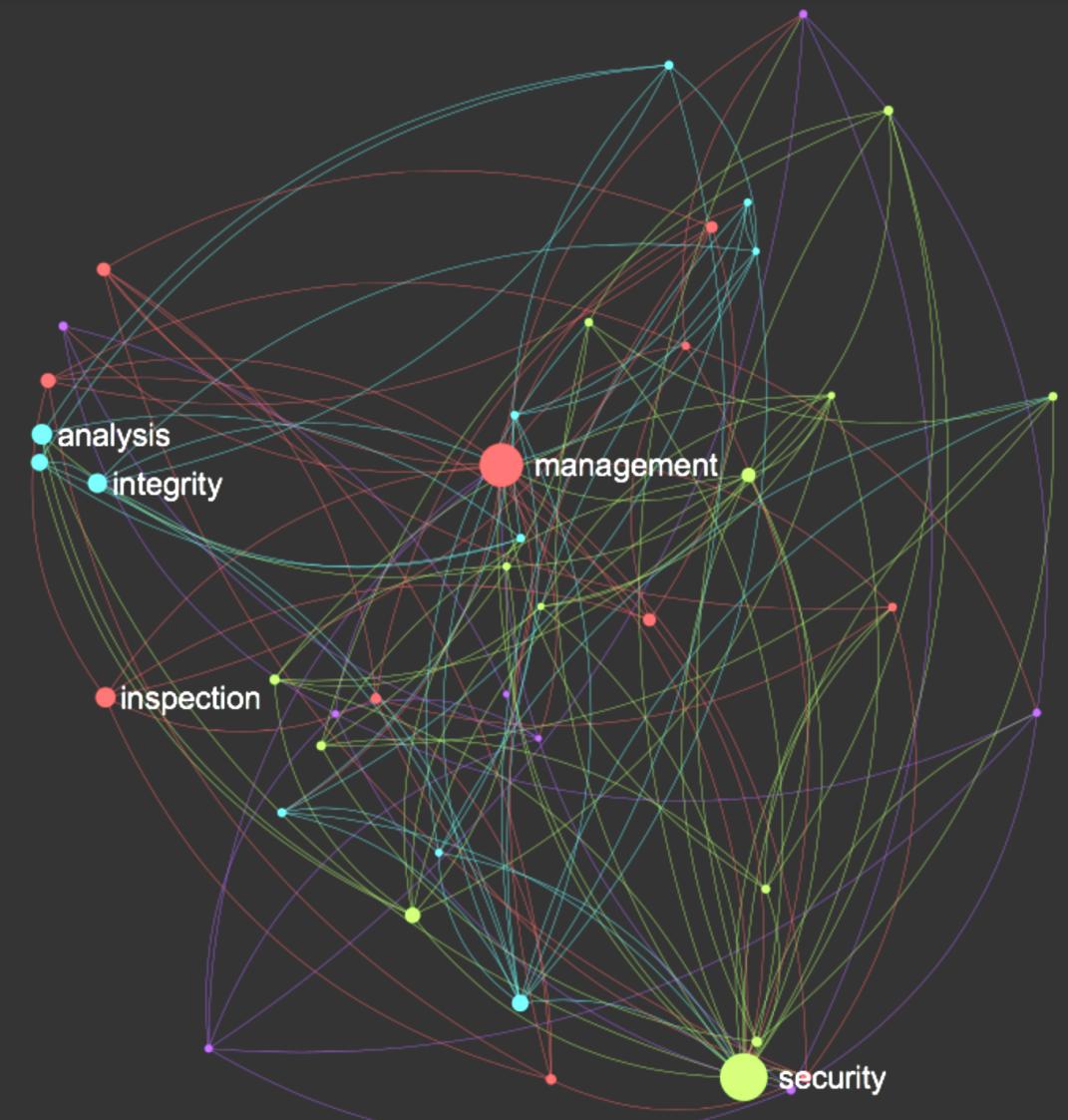
Inspection

Analysis

+

Integrity

Security



Monitoring

Stability

Management
Inspection
Analysis

Integrity
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

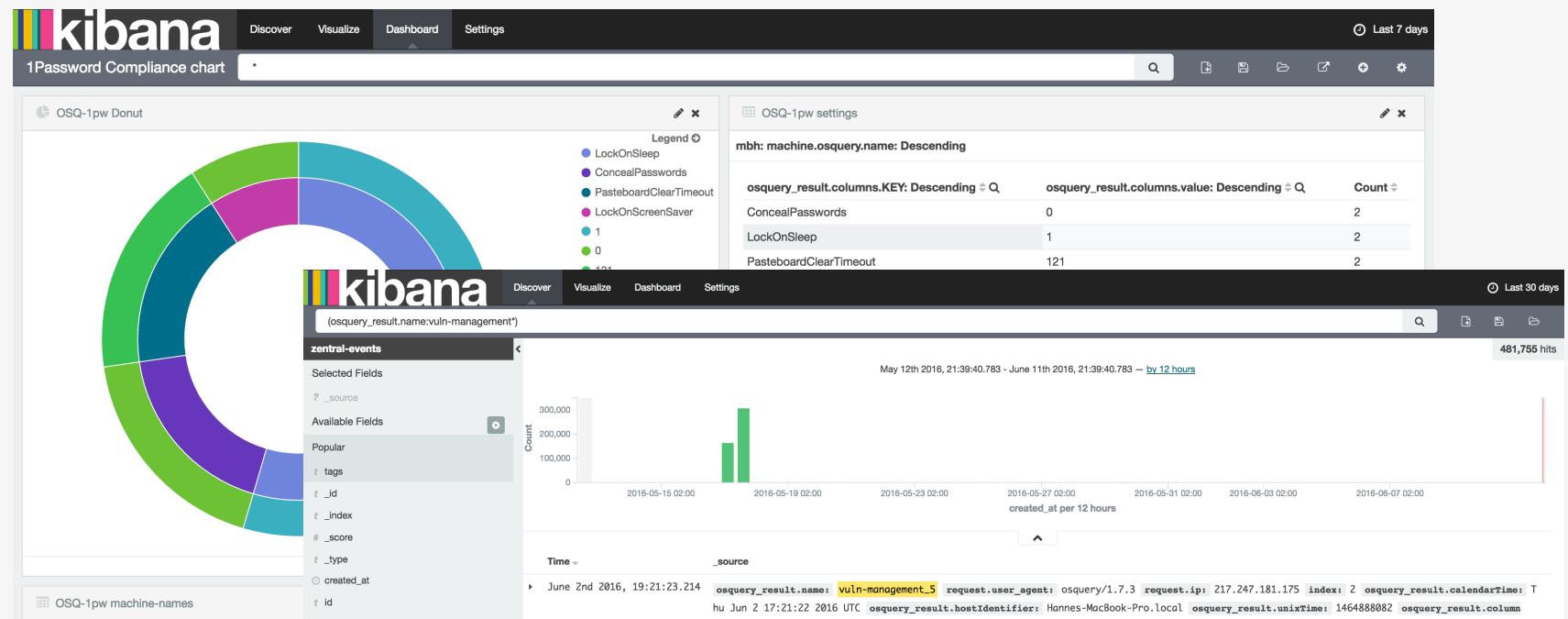
Open Source:
ELK Stack, Prometheus,
Graphite / Grafana

Commercial:
DataDog, Splunk

Metrics Visualization

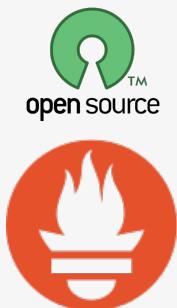
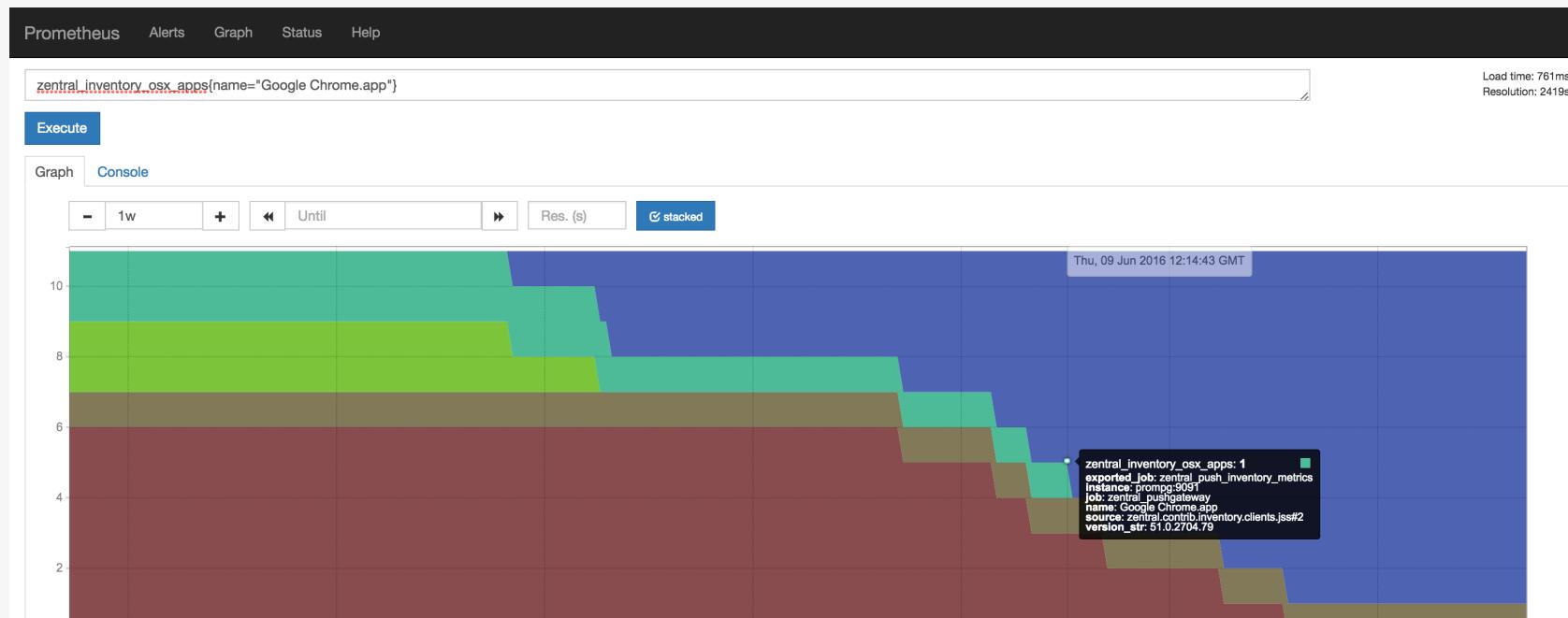
ElasticSearch / Kibana (ELK)

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





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.	<pre>{"request_type": "config"}</pre>
santa_event	June 8, 2016, 6:18 p.m.	<pre>{"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": "efa39e542620418fbf2d96da4f95e41e8a2a3cd6861cff45a59cebc1ffaedfb", "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": "483DWK443", "sha256": "0caf42ad5cf856f4125a1e174692fce7d49a8f6acb70568f3bb53b69acdc979c", "subject": "CN=Developer ID Application, O=JAMF Software, OU=483DWK443"}]}</pre>

Zentral - Probe / osquery compliance

Kibana Discover Visualize Dashboard Settings Last 15 minutes

1Password Compliance chart *

OSQ-1pw Donut

Legend

- ConcealPasswords
- LockOnSleep
- PasteboardClearTimeout
- 0
- 1
- 121

OSQ-1pw settings

mbh: machine.osquery.name: Descending

osquery_result.columns.KEY: Descending	osquery_result.columns.value: Descending	Count
ConcealPasswords	0	1
LockOnSleep	1	1
PasteboardClearTimeout	121	1

Export: Raw Formatted

OSQ-1pw machine-names

machine.osquery.name: Descending	Count
mbh	3

machine.munki.name: Descending

Count	
mbh	3

Zentral - Probe / Santa Blacklist

Screenshot of the Zentral web interface showing the configuration of a Probe for Santa TestApp Unsigned.

The navigation bar includes: zentral, Inventory, Probes, Munki, Osquery, Santa, and Extra links.

The breadcrumb navigation shows: Home / Probes / Santa TestApp Unsigned.

Probe Santa TestApp Unsigned

Active

Update | Delete | Elasticsearch

Filters

Metadata

1. `{'type': 'santa_event'}`

Policies

2. `{'custom_msg': 'Unsigned TestApp launched - this is a Santa blacklist test', 'policy': 'BLACKLIST', 'rule_type': 'BINARY', 'sha256': '3b671540133c9d7618dcebf1c3d4134409dd460c0b17bbad04de4fb99c0271f'}`

Elasticsearch

Actions

3. Name: machine_tag | Configuration: `{'action': 'add', 'tag_id': 12}`



Zentral - Probe / Santa Blacklist

The screenshot shows the Zentral interface for managing probes. A modal window is open, displaying information about a detected application:

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

12 Malware Detected

Probe Santa Test

Active

Update **Delete** **elasticsearc**

Filters

Metadata

1 `{'type': 'santa_event'}`

Policies

2 `{'custom_msg': 'Unsigned', 'policy': 'BLACKLIST', 'rule_type': 'BINARY', 'sha256': '3b671540133c9d7618dcebfc1c3d4134'}`

Actions

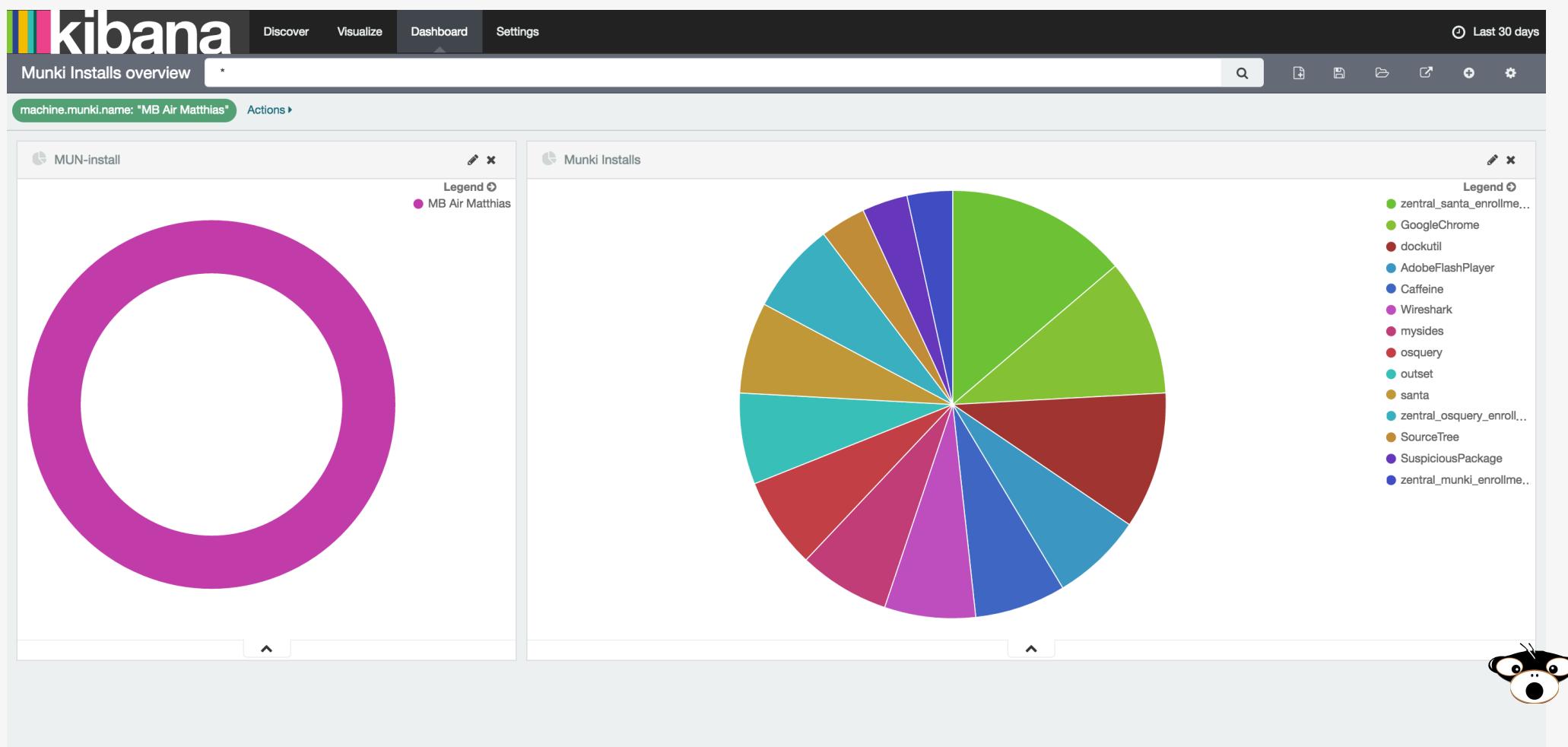
3 **Name** **Configuration**

machine_tag `{"action": "add", "tag_id": 12}`

Extra links ▾



Zentral - Inventory / Munki installs



Zentral - Inventory / Watchman

Kibana Dashboard - Last 24 hours

Watchman - Issues overview

machine.watchman.groups.reference: "report-failed-logins" Actions ▾

INV-watchman-add

Legend

- gkmailserver
- server
- AS_server
- Administrators iMac (6)
- Christophs MacBook P...
- MB_Butterstein
- MacBook Peter
- MacBook brech alt
- Münster-C02MJ1
- PNT-Client-685b35d06...

INV-watchman-reference

Legend

- carbon-copy-cloner
- crashplan-app
- root-capacity
- disk-io-errors
- time-machine
- specified-volumes
- last-reboot
- smart-status
- filemaker-server
- kernel-panics

INV-watchman-Names

Count	machine.watchman.business_unit.name: Descending	machine.watchman.name: Descending	machine_serial_number: Descending	machine.watchman.os_version: Descending
1	Administrators iMac (6)	C02P48LEFY0T	C02MJ141F8J2	OS X 10.11.5 (15F34)
1	Münster-C02MJ1	C02MJ11CF8J2	C07MN1Q1DWYL	OS X 10.10.5 (14F1605)
1	PNT-Client-685b35d06571			OS X 10.11.3 (15D21)
1	gkmailserver			OS X 10.8.5 (12F45)

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



Endpoint Security Tools



osquery



Google Santa

Endpoint Managed Software Solutions



JAMF
software

Munki

Casper Suite

Input

Inventory, Events, Metrics



WATCHMAN
MONITORING



casper
SUITE

REST API

Sal



Endpoint Security Tools



osquery



Google Santa

Endpoint Managed Software Solutions



Munki



Casper Suite

Inventory, Events, Metrics



WATCHMAN
MONITORING



casper
SUITE

REST API

Sal

MDM



REST API

Notifications



Email

GitHub

slack



Sub-Systems



ElasticSearch

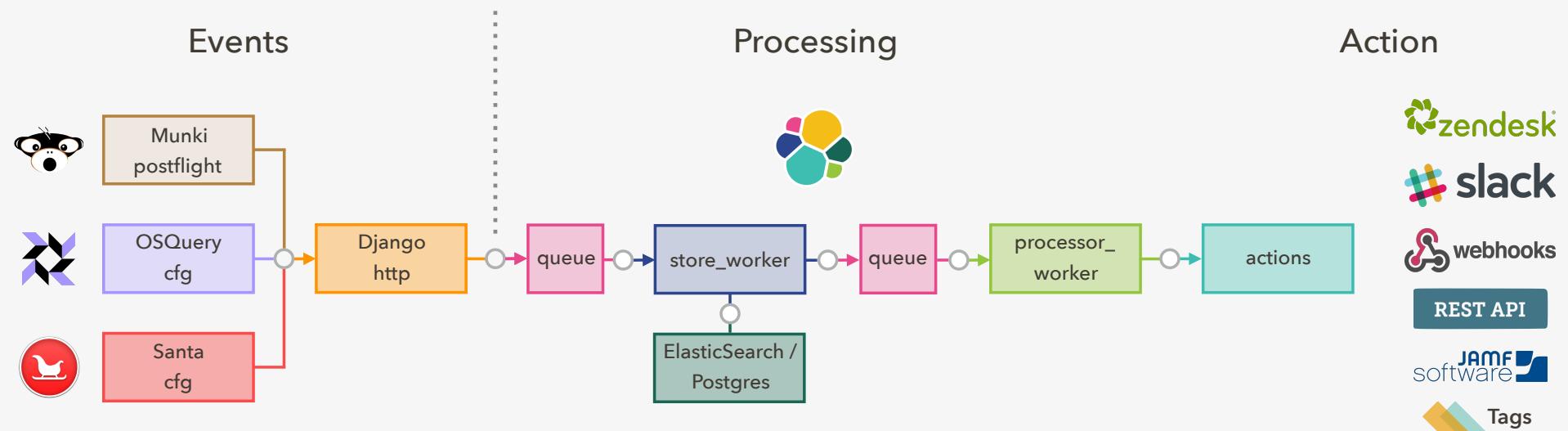


Input

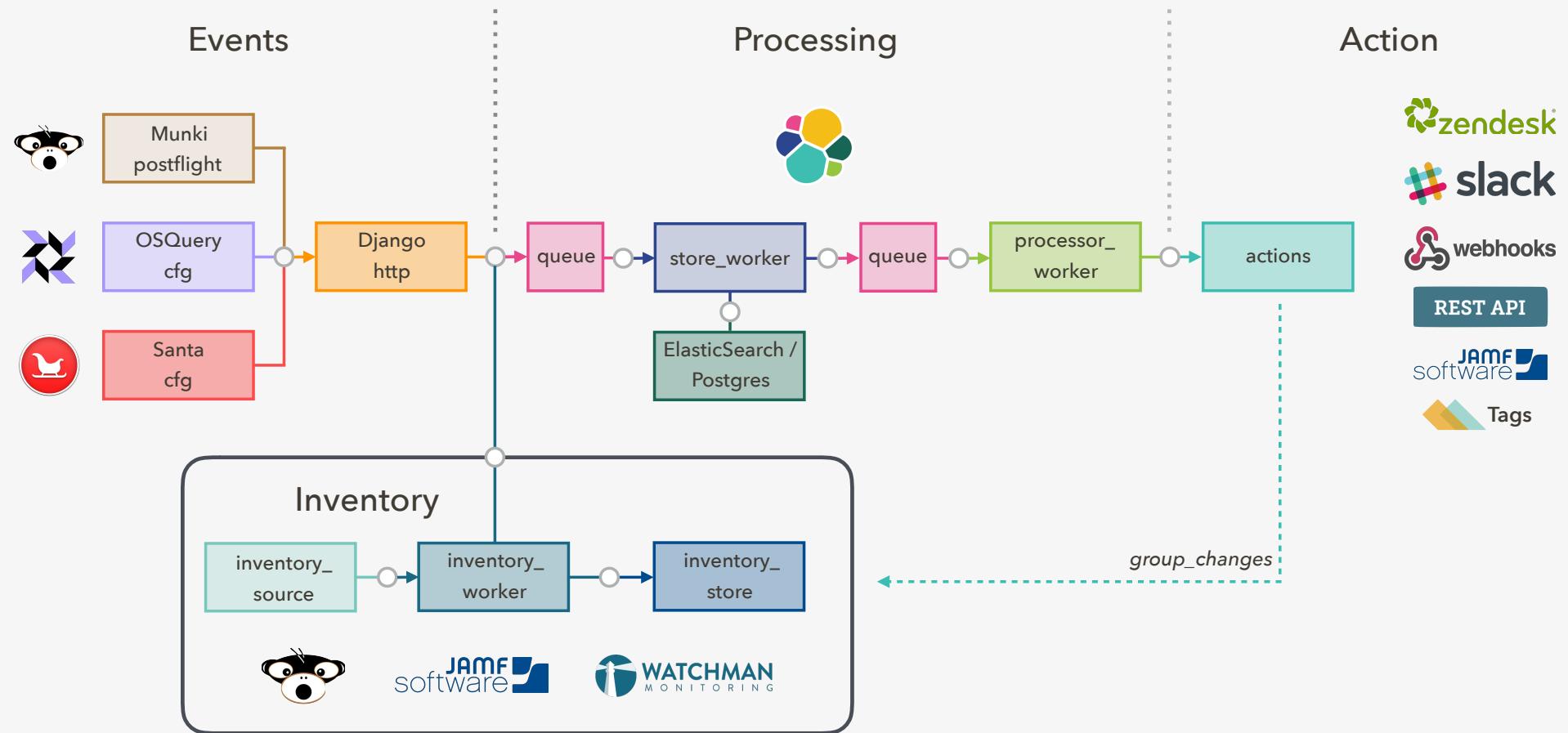
Output

Processing Workflow

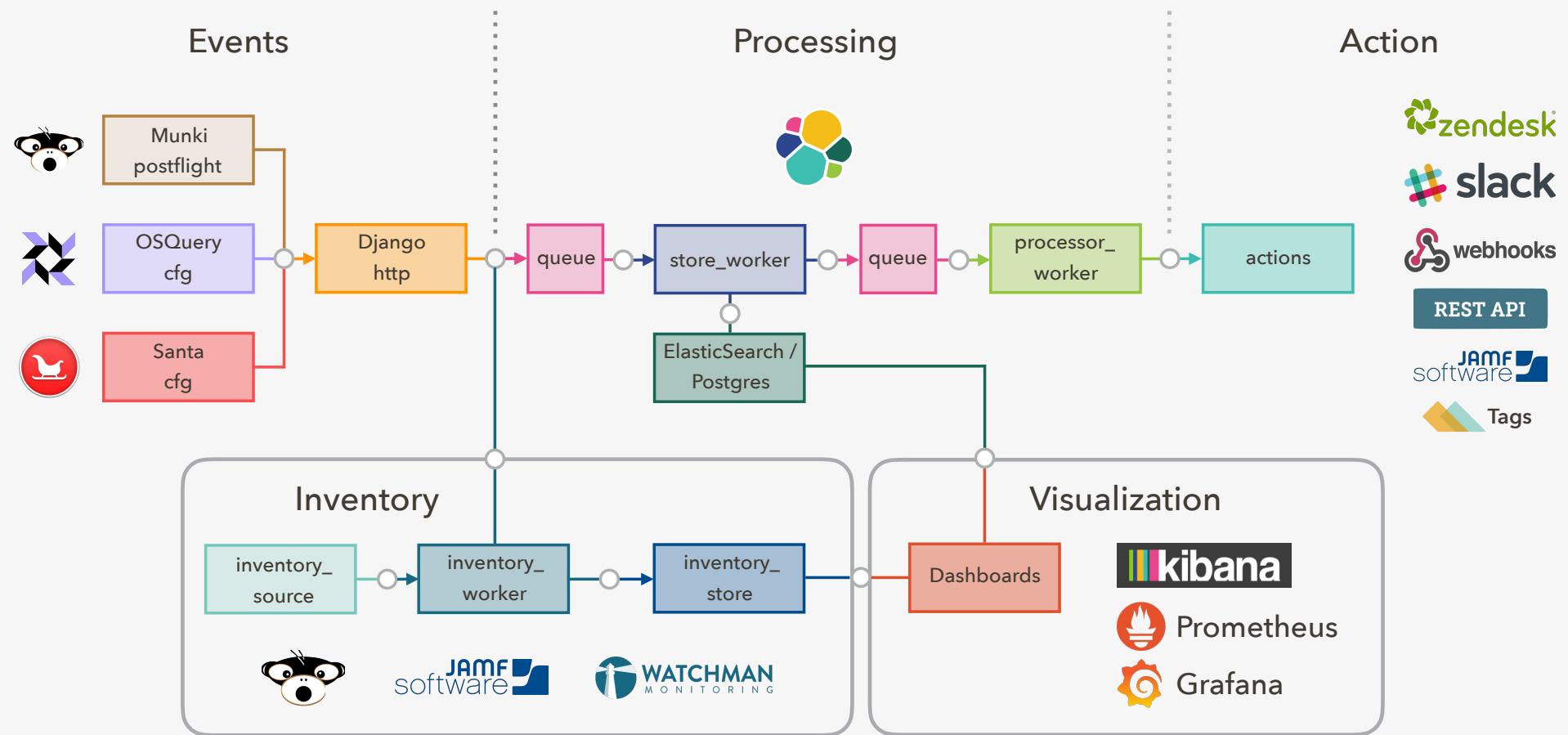
Zentral - Event Processing



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
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

Business Unit
support for
multiple inventory

* osquery only

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

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	<pre>{"action": "add", "tags": 7}</pre>

Demo

Chrome File Edit View History Bookmarks People Window Help

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

Zentral Zentral

henry

https://zentral.apfelwerk.de/inventory/?serial_number=&name=mbh&source=&tag=

Inventory Probes Munki Osquery Santa

Extra links

Home / Inventory machines / Machine search

1 Machine

Serial Number C02QM01AGCN2 Name mbh Apfelwerk

Santa

Unsigned TestApp launched – this is a Santa blacklist test

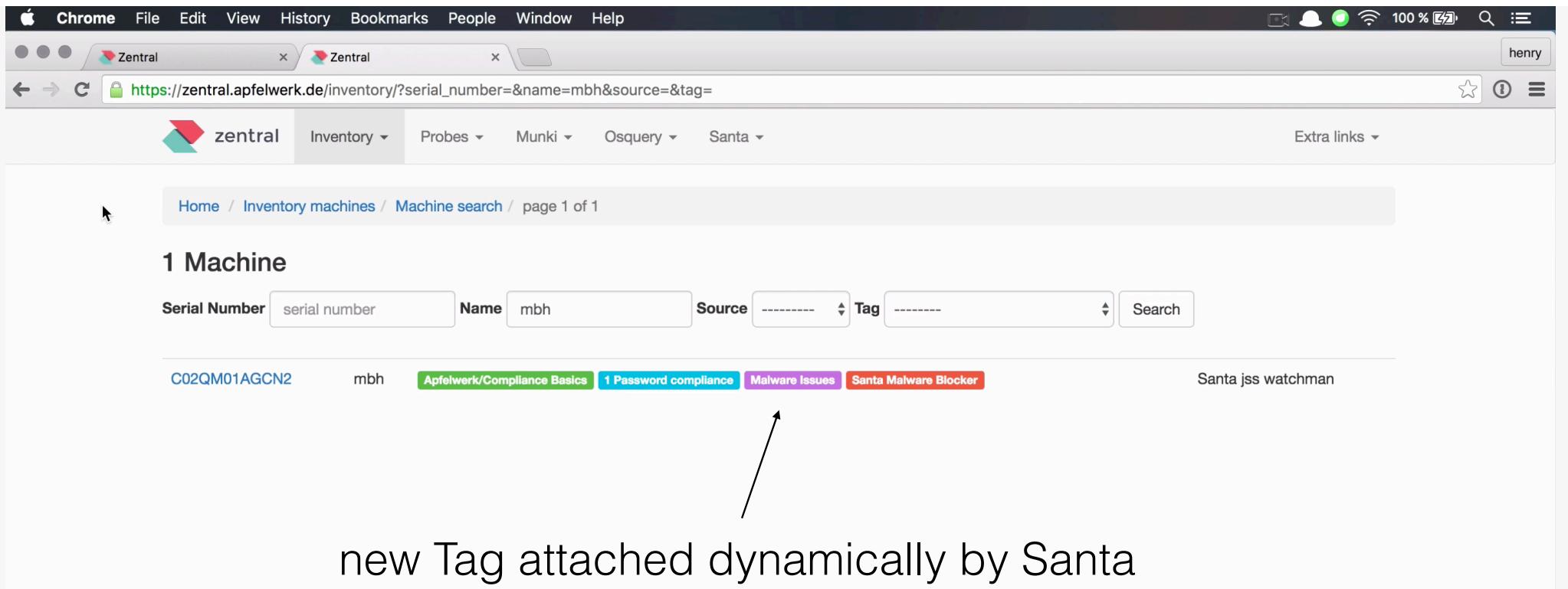
Application	SantaTest Unsigned
Filename	SantaTest Unsigned
Path	/Applications/SantaTest Unsigned.app/Contents/MacOS/SantaTest Unsigned
Publisher	Not code-signed
Identifier	3b671540133c9d7618dcebfc1c3d4134 409dd460c0b17bbad04de4fb99c0271f
Parent	launchd (1)
User	head

Prevent future notifications for this application for a day

Dismiss

Demo

A screenshot of a Chrome browser window showing the Zentral inventory management interface. The URL is https://zentral.apfelwerk.de/inventory/?serial_number=&name=mbh&source=&tag=. The page displays a single machine named 'mbh' with serial number 'C02QM01AGCN2'. The machine is associated with several tags: 'Apfelwerk/Compliance Basics' (green), '1 Password compliance' (cyan), 'Malware Issues' (purple), and 'Santa Malware Blocker' (red). A hand-drawn arrow points from the text 'new Tag attached dynamically by Santa' to the 'Santa Malware Blocker' tag. The top right corner of the slide features a teal triangle containing the word 'Demo'.



new Tag attached dynamically by Santa

Enhanced Search

893 Machines

Serial Number Name Source -----Tag

- jss
- watchman
- Munki
- OSQuery
- Santa

YM84 6CMYL1	18_MM_Besprechungsraum ALT	watchman
C02L4BEHFBJ2	Administrator iMac	watchman
C02L4MEYFBJ2	Administrator iMac (2)	watchman
C02L43H4F8J2	Administrator iMac (3)	watchman
C02L4CRLF8J2	Administrator iMac (4)	watchman
C02L4973F8J2	Administrator iMac (5)	watchman
C02K4PNTDNCR	Administrators iMac	watchman
VM834E5QZE2	Administrators iMac	watchman
C02P4BQWFY0T	Administrators iMac	watchman
C02J2P6JDHUF	Administrators iMac	watchman
C02J4WWXDNCR	Administrators iMac	watchman
C02N4V389FY0T	Administrators iMac	watchman
YM8441N0ZE2	Administrators iMac	watchman
W88C71S1X89	Administrators iMac	watchman
C17JR2PWDNCR	Administrators iMac	watchman
C02N4Q3XNFY0T	Administrators iMac (14)	watchman
C02L3AUXF8J2	Administrators iMac (2)	watchman

Demo



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
--------------	---------	-----------------------------	-----------------------	-------------------	----------------------------------

DGKQV0G5GG7V	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)





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



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: {}
```

CancelSave

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}

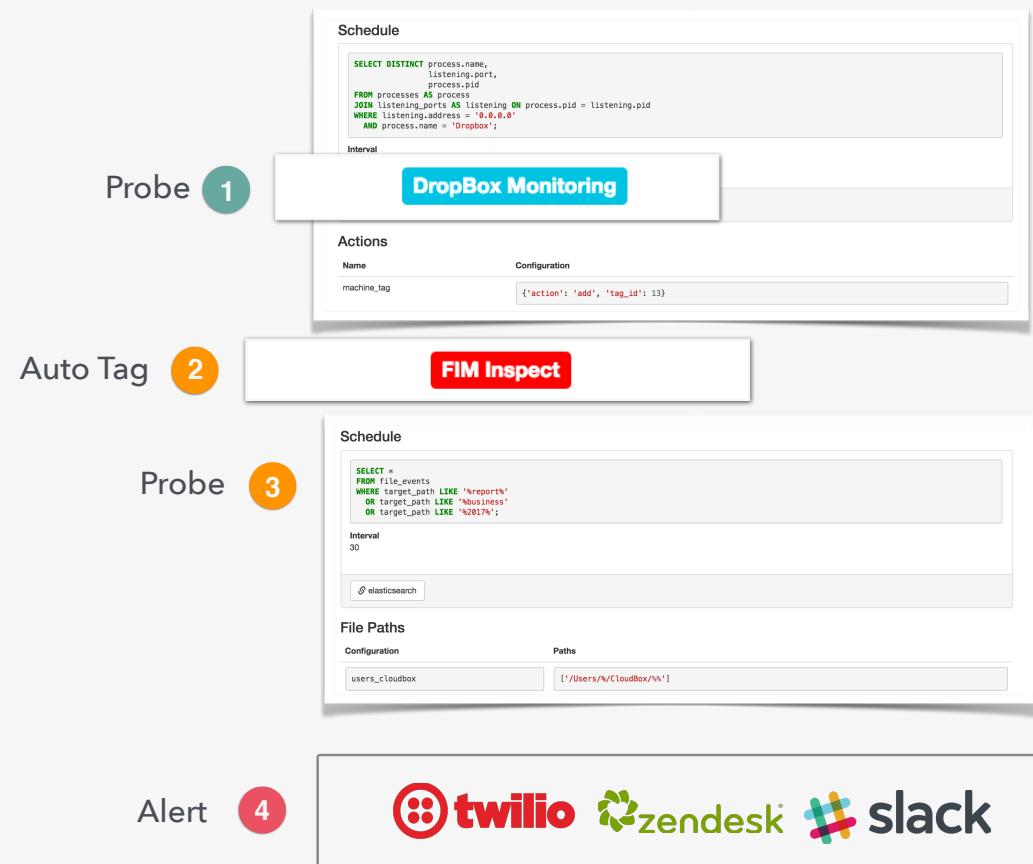
Demo

Examples

Automated FileIntegrityMonitoring (FIM)

Automated Probes (Example)

Broad Scale



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

The collage includes:

- A Prometheus alert dashboard titled "zentral_investor_osx_apfelwerk" showing a graph with values 14, 12, and 10.
- A Kipana dashboard showing a scatter plot of data points.
- A central inventory screen displaying "121 Business units".
- A central probes screen showing "25 Probes" and a list of probe names including "spassword_compliance", "AW Watchman: reference_disk-io-errors", and "AW Watchman: reference_report_failed_logins".
- A central osquery distributed queries screen showing "33 Osquery distributed queries".
- A central business unit screen showing "121 Business units" with a table of units and their details.
- A central dashboard screen showing various metrics and links.

Zentral in Prod (specs)

VM (hosted in German DataCenter)

4 core, 16 GB Ram, Debian based

ElasticSearch, Kibana4

Prometheus, Grafana

Deployment: Ansible & docker-compose

The collage of screenshots illustrates the various components of the Zentral system:

- Top Left:** A Prometheus dashboard showing a stacked area chart with metrics labeled "zcentral_investor_oss_apache2name".
- Top Middle:** A Kibana visualization showing a scatter plot of log data.
- Top Right:** A "Probes" page showing 25 probes, with sections for "Create", "Name", and "Logs".
- Middle Left:** A "Business units" page listing 121 entries, such as "1.1.1.1 (watchman-1)", "2box-architected", and "Academie Sozialre".
- Middle Right:** A "Logs" page titled "33 Ossquery distributed queries" showing log entries for "watchman" and "osqueryd".
- Bottom Left:** A "Metrics" page showing a table of metrics grouped by source, including "watchman", "osqueryd", and "osqueryi".
- Bottom Right:** A "Metrics" page showing a table of metrics grouped by source, including "watchman", "osqueryd", and "osqueryi".

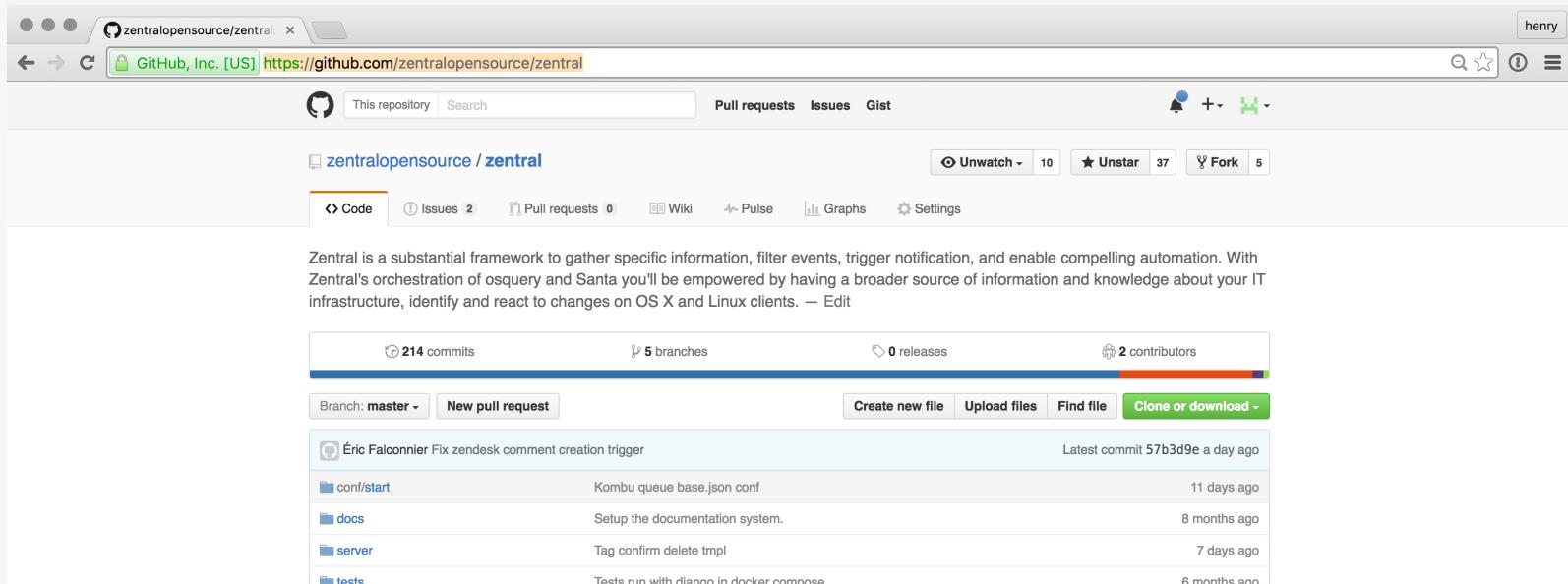


How to get started ?

Project on Github

<https://github.com/zentralopensource/zentral>

<https://github.com/zentralopensource/docs>



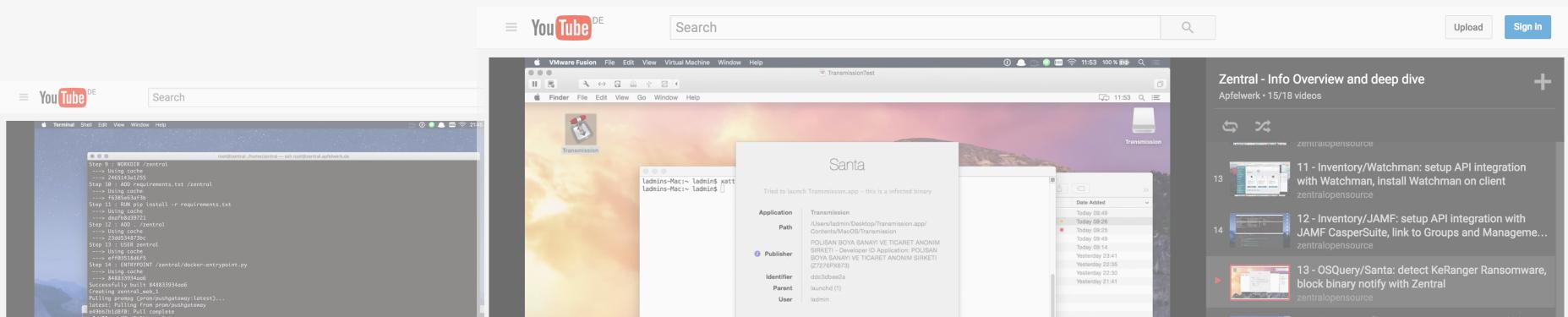
A screenshot of a GitHub repository page for 'zentralopensource / zentral'. The page shows basic repository statistics: 214 commits, 5 branches, 0 releases, and 2 contributors. It also displays a recent commit from Éric Falconnier. The GitHub interface includes standard navigation bars like 'Code', 'Issues', and 'Pull requests'.

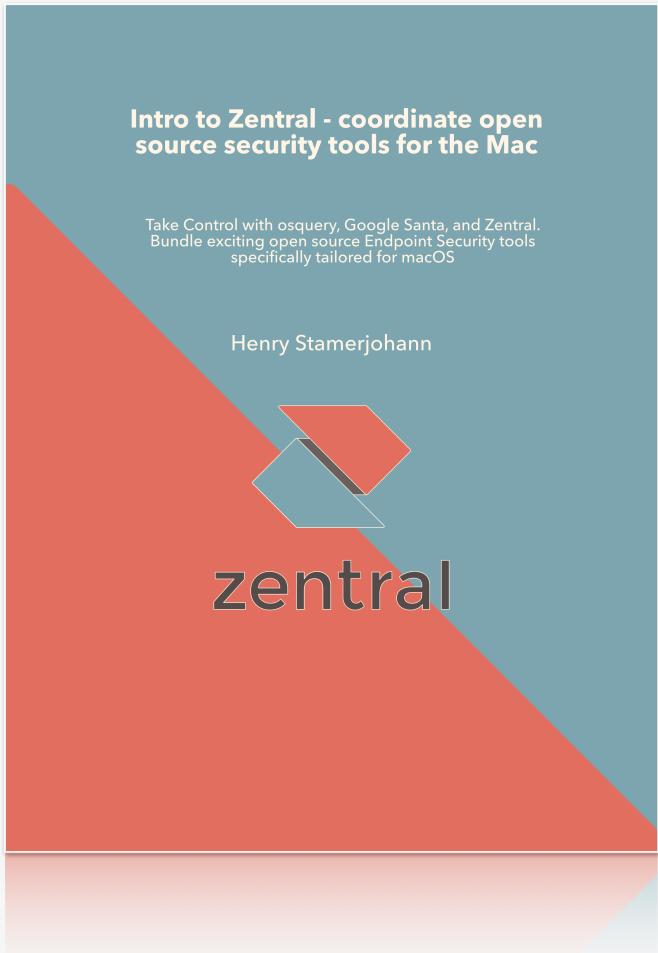
Commit	Message	Date
conf/start	Kombu queue base.json conf	11 days ago
docs	Setup the documentation system.	8 months ago
server	Tag confirm delete tmpl	7 days ago
tests	Tests run with django in docker compose	6 months ago

Video Tutorials

<https://goo.gl/qslVkl>

- 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)

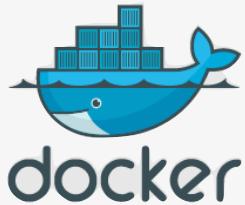
publishing in-progress



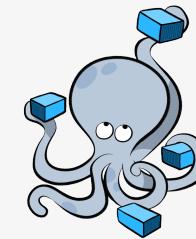
Leanpub

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/qslVkl>

Django Deployment

Deploy like any other Django app
Extend like any Django app (LDAP, AUTH)

requirements.txt

gunicorn

wheel



Thank You !