zentral
Development & Professional Services

# Useful techniques for a successful Santa deployment

Henry Stamerjohann, June 11 2021

https://zentral.pro

# Whats ahead

**Fleet-wide use of binary authorization and control**

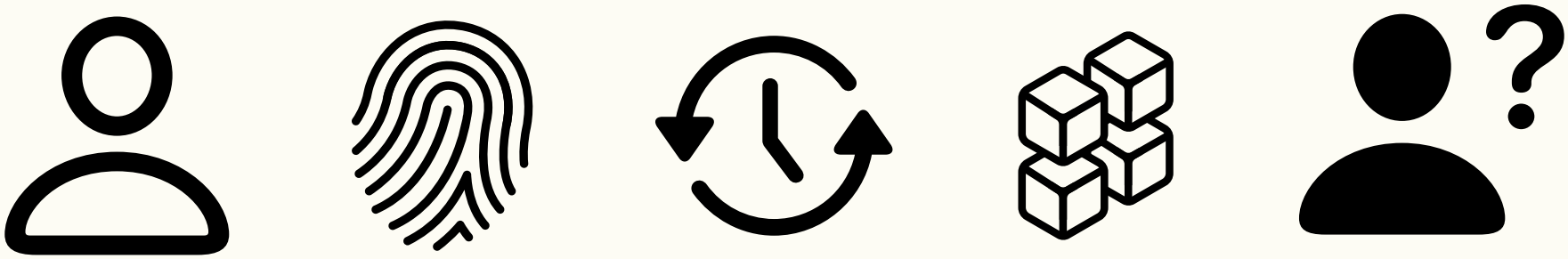
Deploying Google Santa for binary control under macOS

Collecting information about the executables

Organize rules and policies for provisioning to the endpoints

# When you begin with a binary control

**There are a number of questions that need to be clarified**



Who What When Where Why

# Look at Google Santa

## A leading binary authorization system for macOS

- Userland daemon makes execution decisions
- Based on signing certificate or binary hash (SHA-256)
- Endpoint Security Extension for macOS 10.15 and higher*
- Rules and events could be synced with a server


*Kernel Extension available for older macOS versions

# Rules and policies

## Declare and control based on sha-256 information

Santa-Rules.md

### Santa Rules

- Target type: `CERTIFICATE | BINARY | BUNDLE`
- Target sha256: `<hash to add/remove/check>`
- Policy: `ALLOWLIST | BLOCKLIST | SILENT BLOCKLIST | ALLOWLIST COMPILER`
- Custom message: `custom message to display`

example

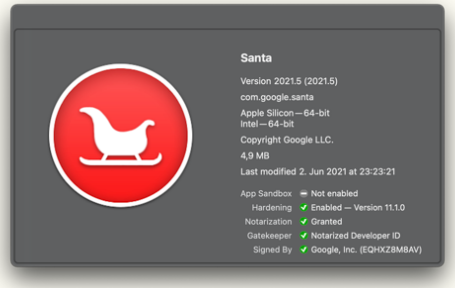
```
# Add rule, allow based on certificate sha256
sudo santactl rule --allow --certificate --sha256 c0fb0030f381b2794b4be8722616b806787a0
```

# What ist required to deploy Santa

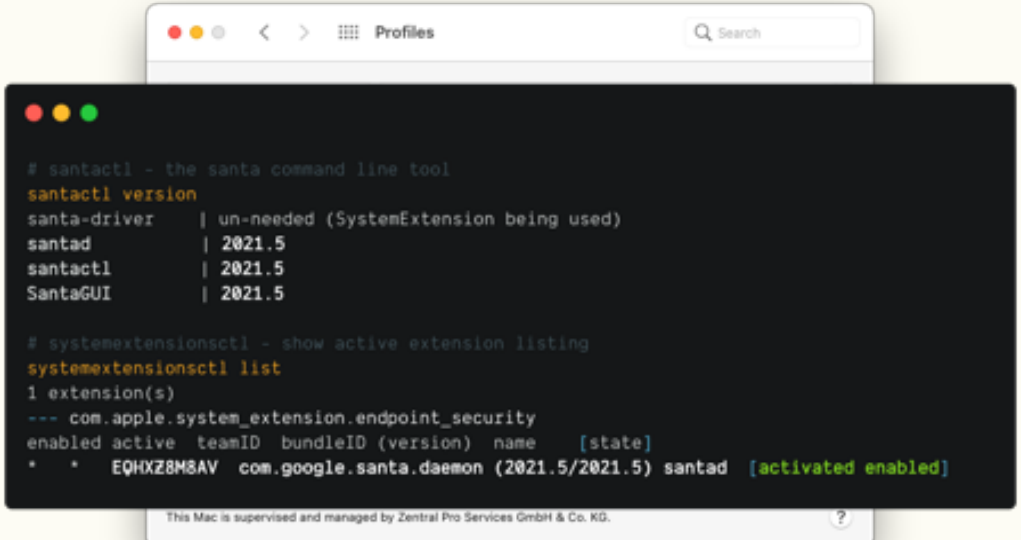
## Deploy required settings via MDM

- Configuration
- Installation package
- System Extension policy payload
- PPPC payload (allow full disk access)
- Notification payload

santa-2021.5.pkg



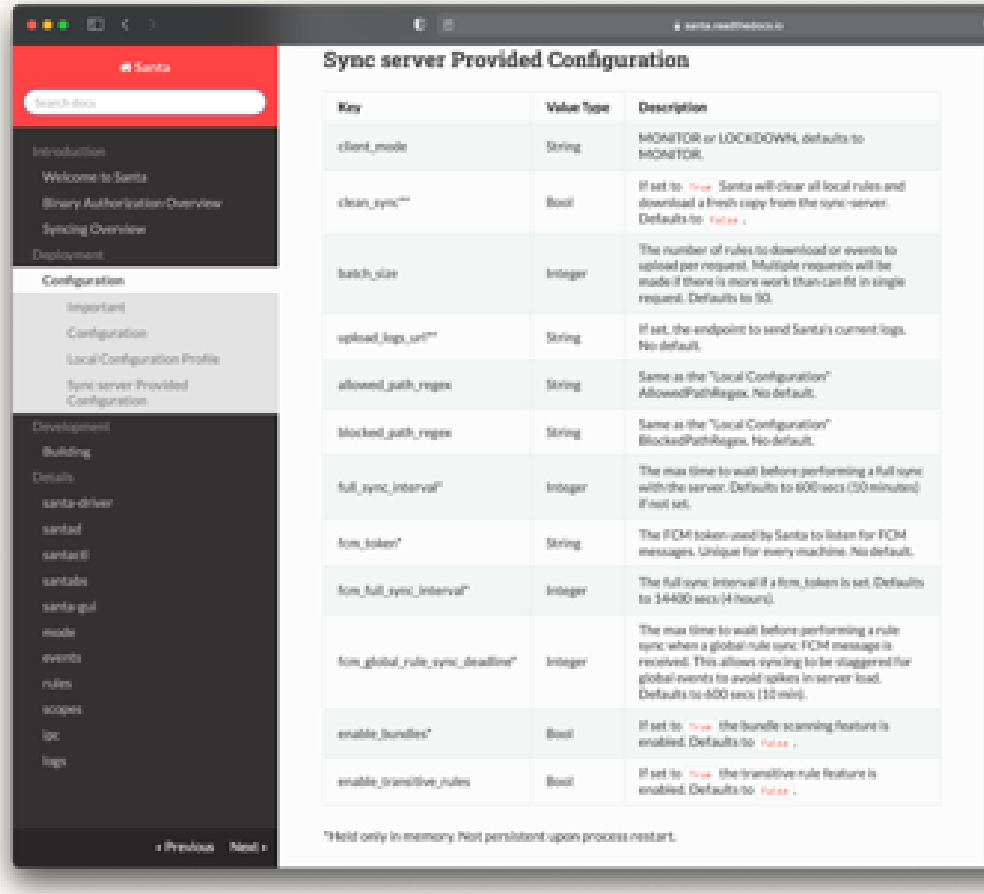




# Sync server config

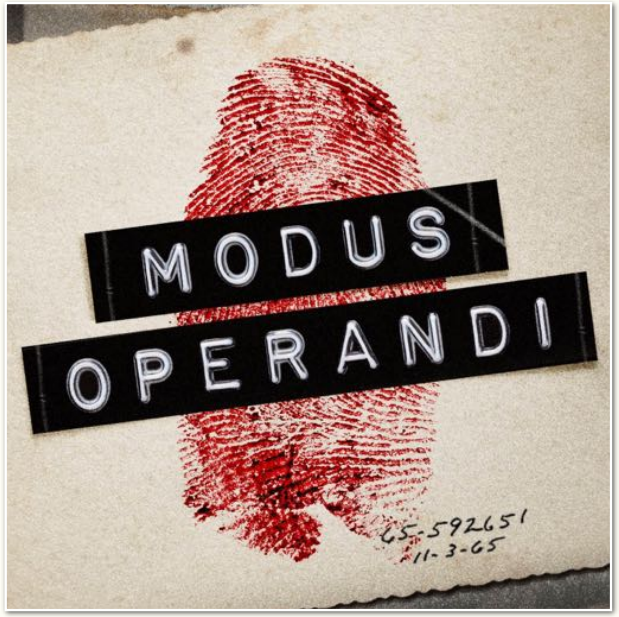
## MDM distributed setting

- Client mode (LOCKDOWN, MONITORING)
- Mutual TLS option (device certificate)
- Sync interval, batch size
- Allowed/blocked path regex
- Info URL for blocked executions



# Operational mode

## Deny or monitor binary execution




MONITORING / LOCKDOWN

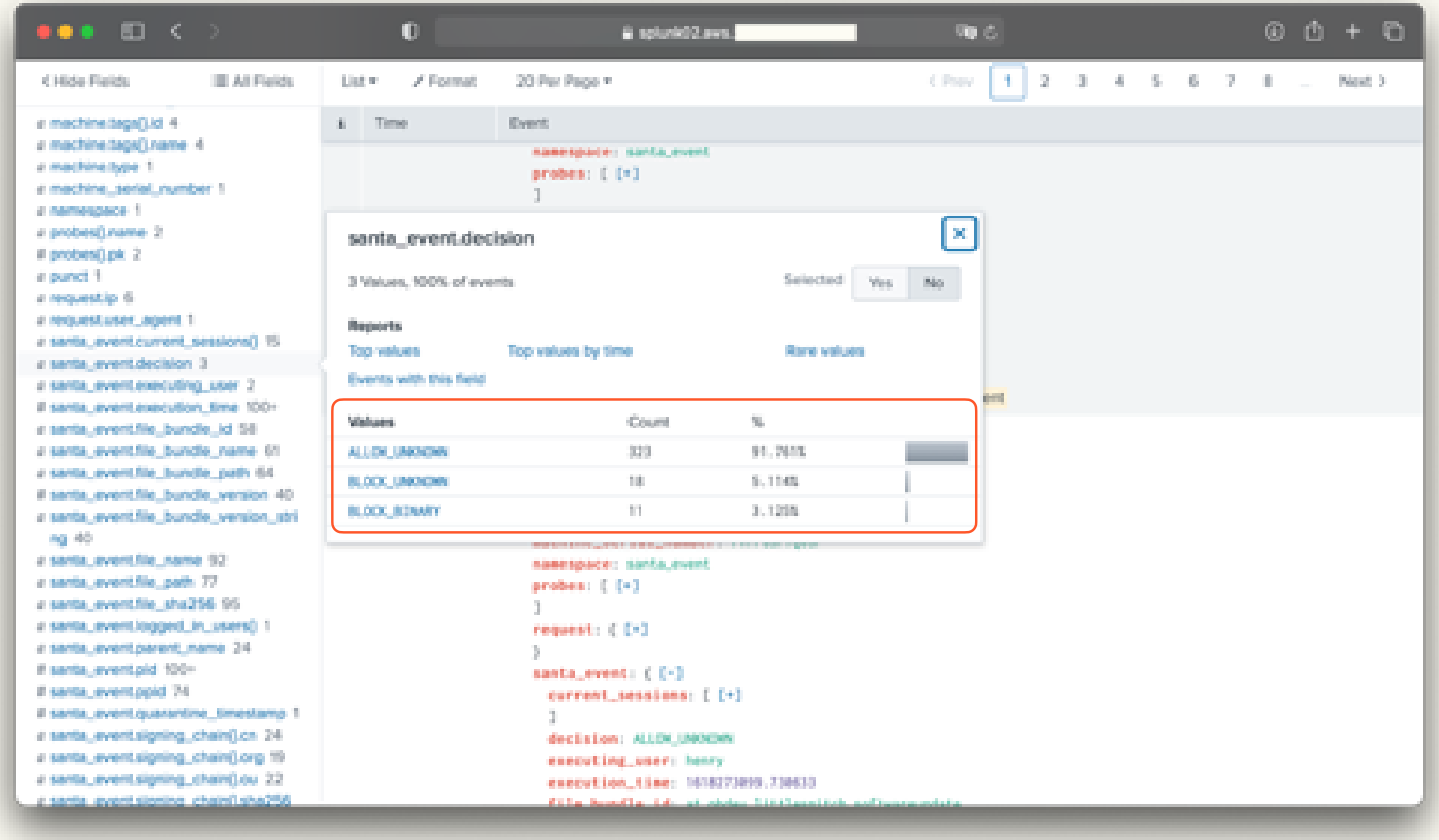
# Know what to control

## Gathering sha256 hash information

- Vendor code signed and binary details
- Use **`santactl`** to scan a local system
- Search in logs or data store (Splunk, et-al.)
- Fine tune collected information
- Build set of rules

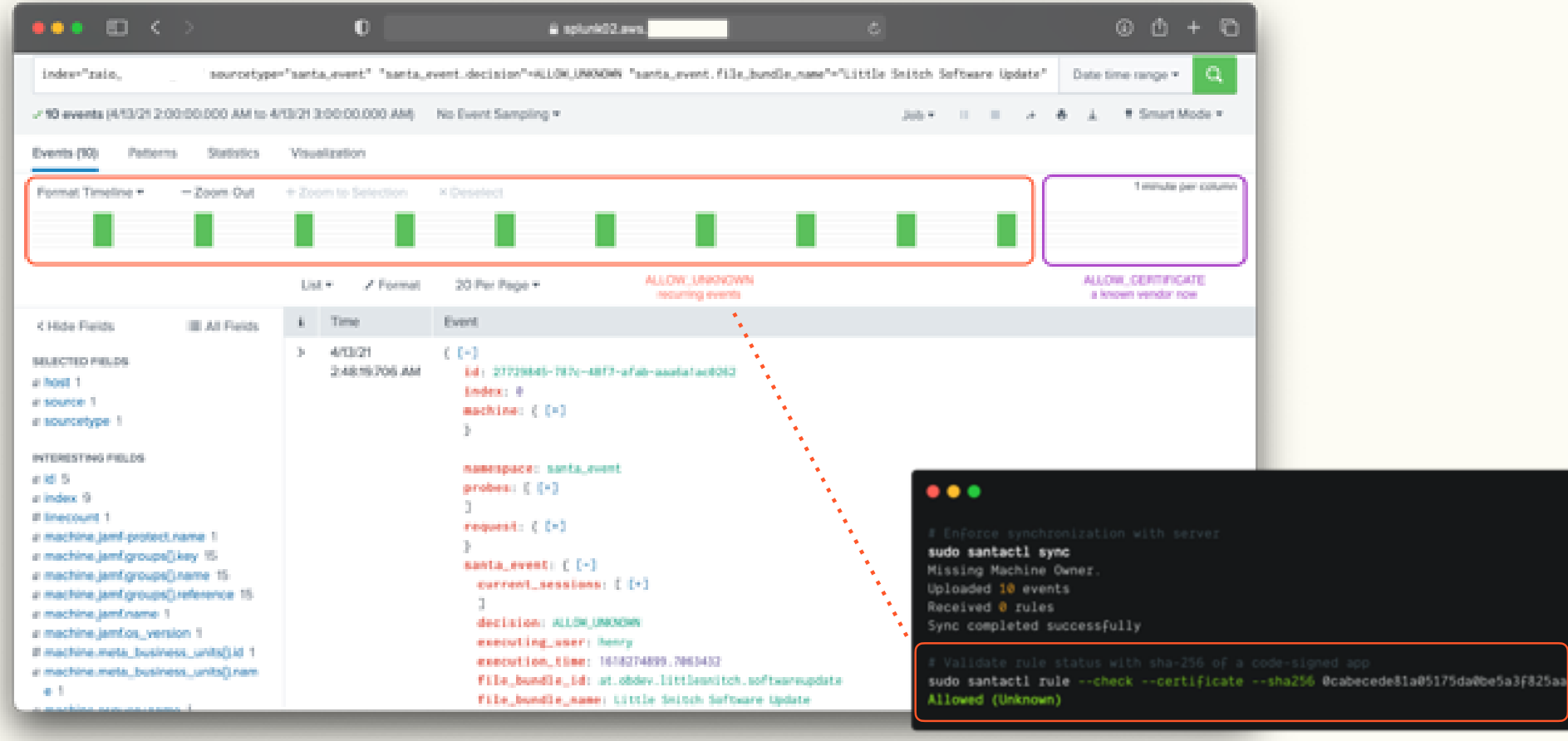
# Collecting event data

## Perform inspection over time



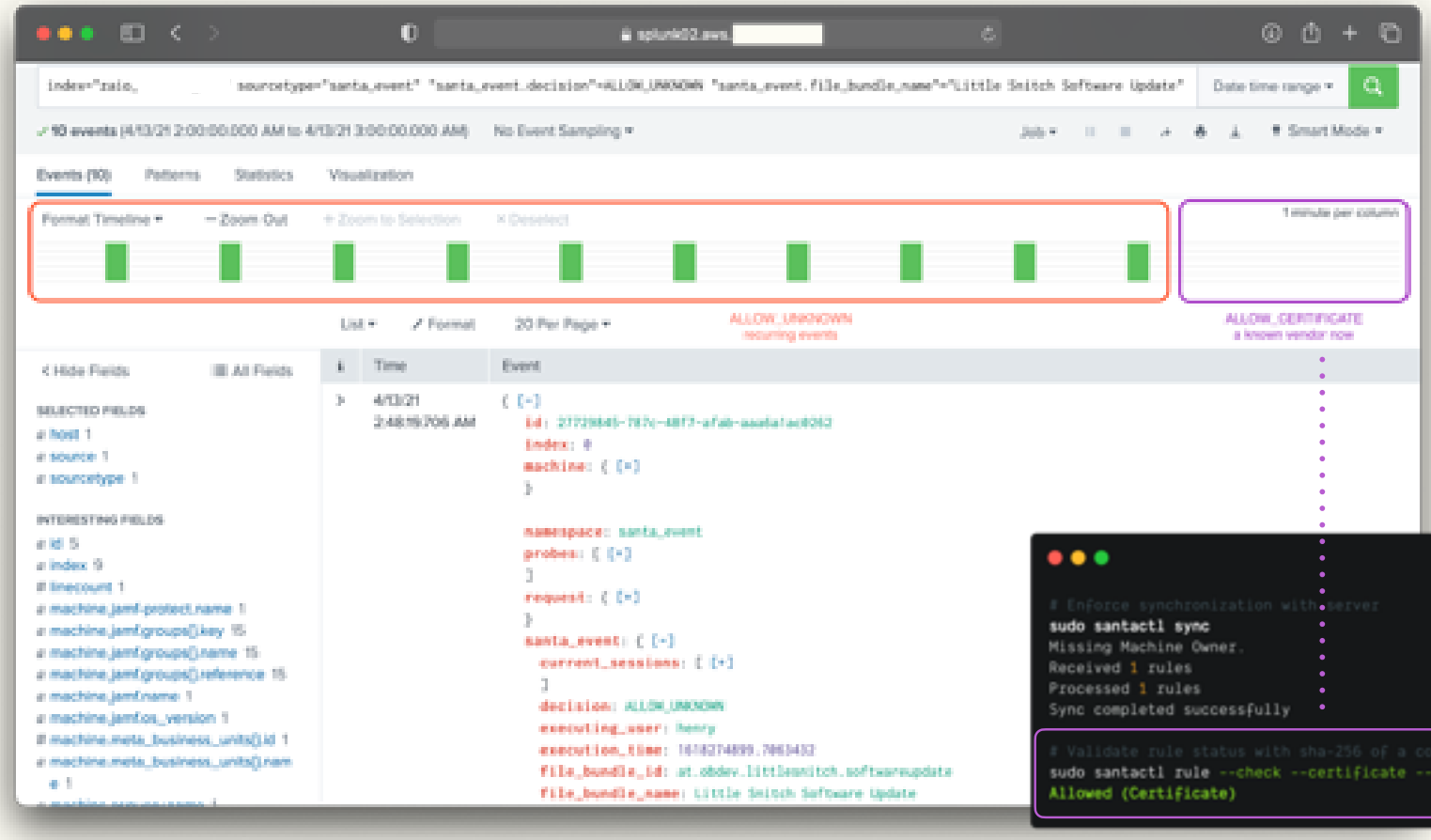
# Collecting event data

## Known apps/binaries no longer return ALLOW_UNKNOWN



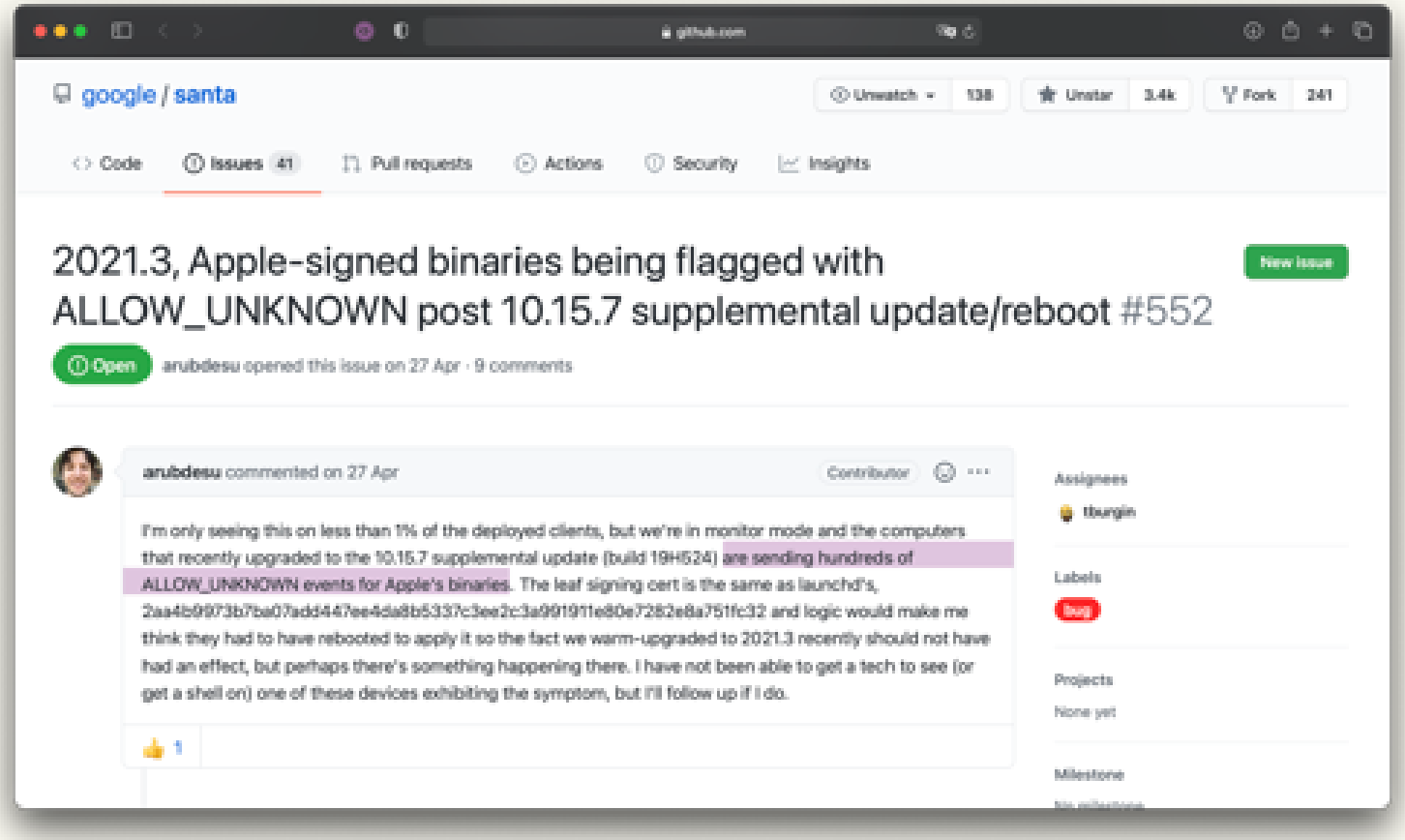
# Collecting event data

## Known apps/binaries no longer return ALLOW_UNKNOWN



# Collecting event data

## Watch out for the spill of ALLOW_UNKNOWN events

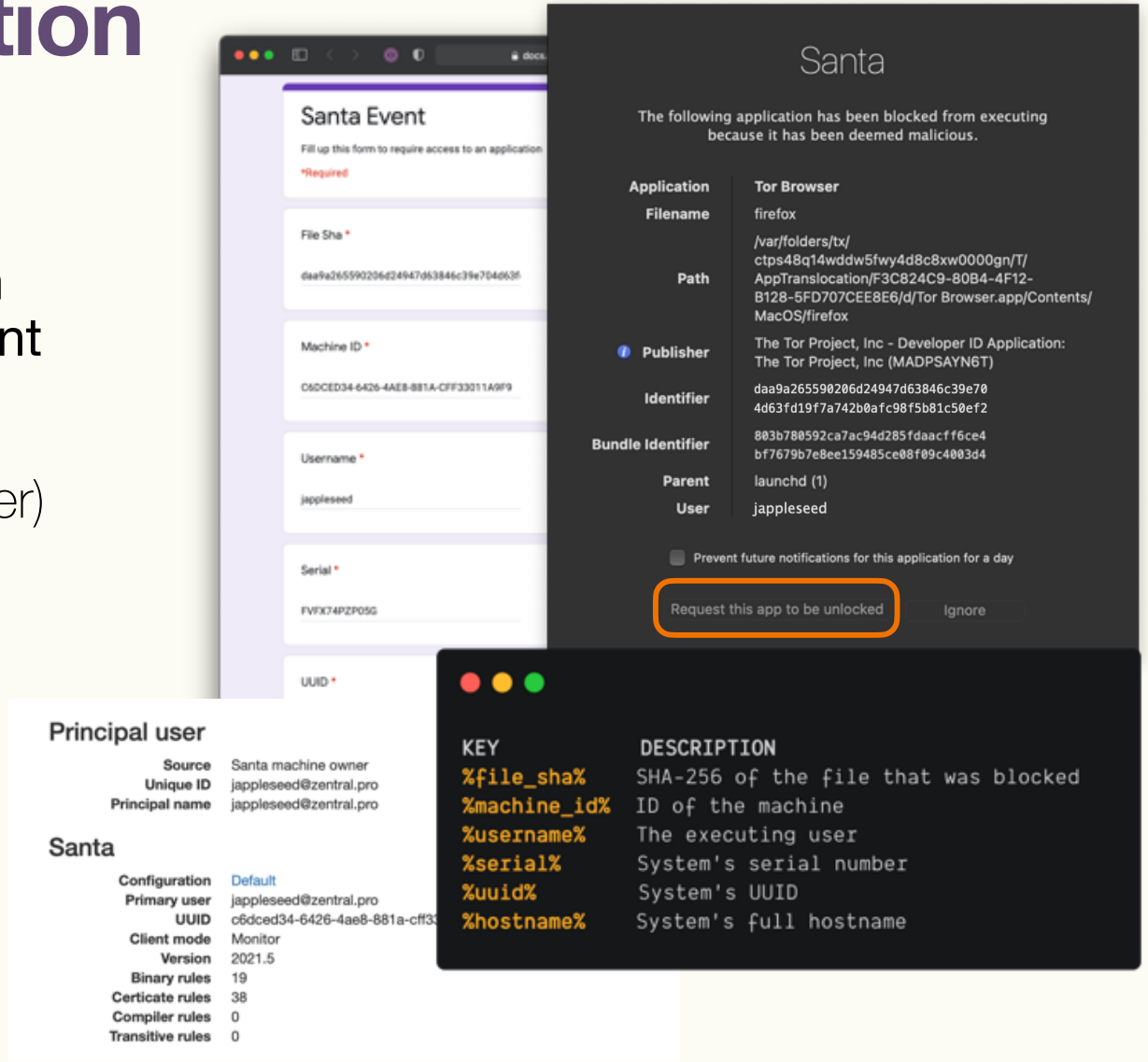



https://github.com/google/santa/issues/552

# Gathering information

## Exception workflow

- Direct users to a web page with more information about the event
- Limit approved exception to specific criteria (e.g. principal user)



# Gathering information

## Know in advance what is commonly used

# Gathering information

## Know in advance what is commonly used

**RAW - collected sha256 hash info**

- Vendor - codesigned hashes
- Binary exec - hashes
- devtools exec - hashes

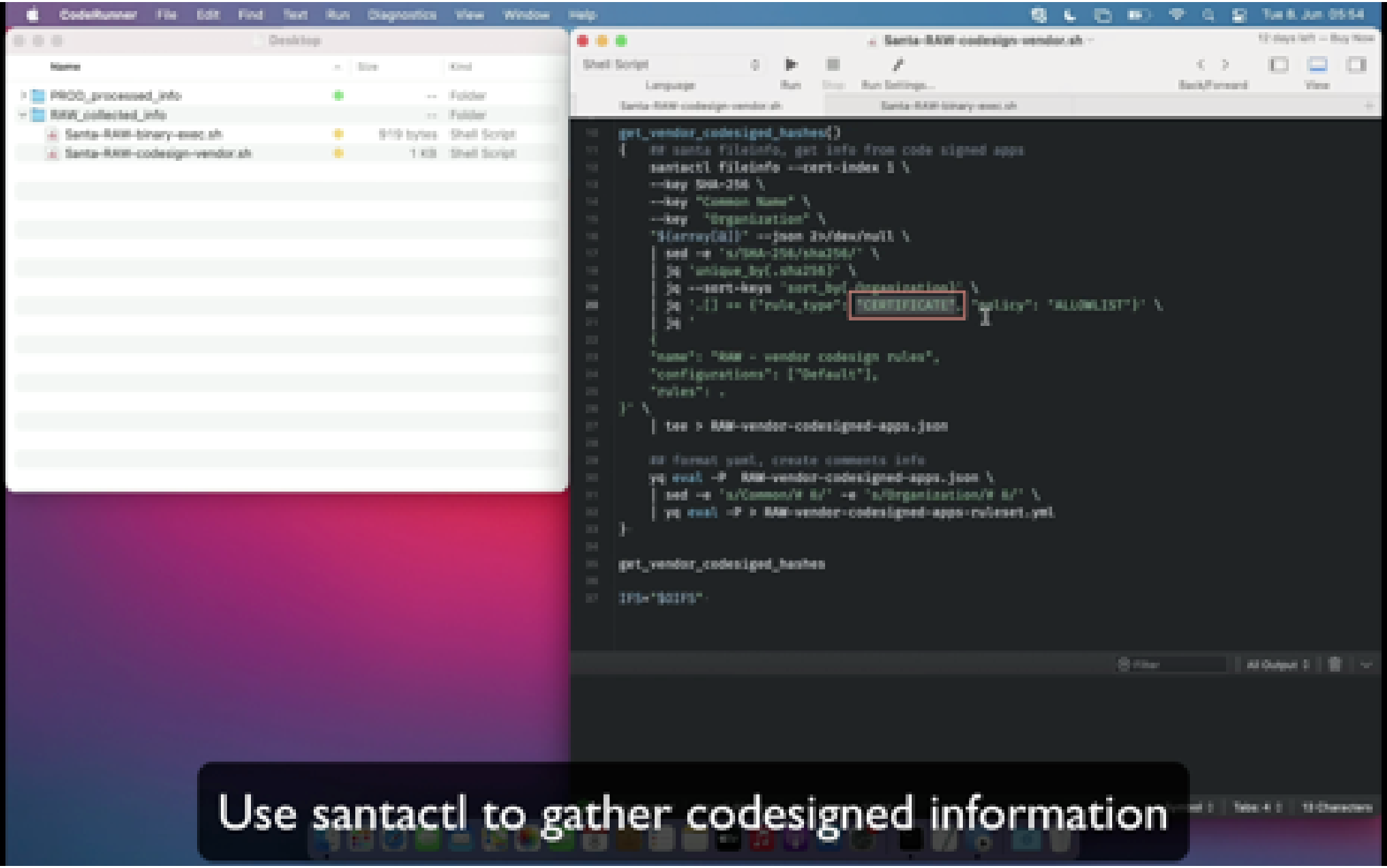
**PROD Rules - processed sha256 hash info**

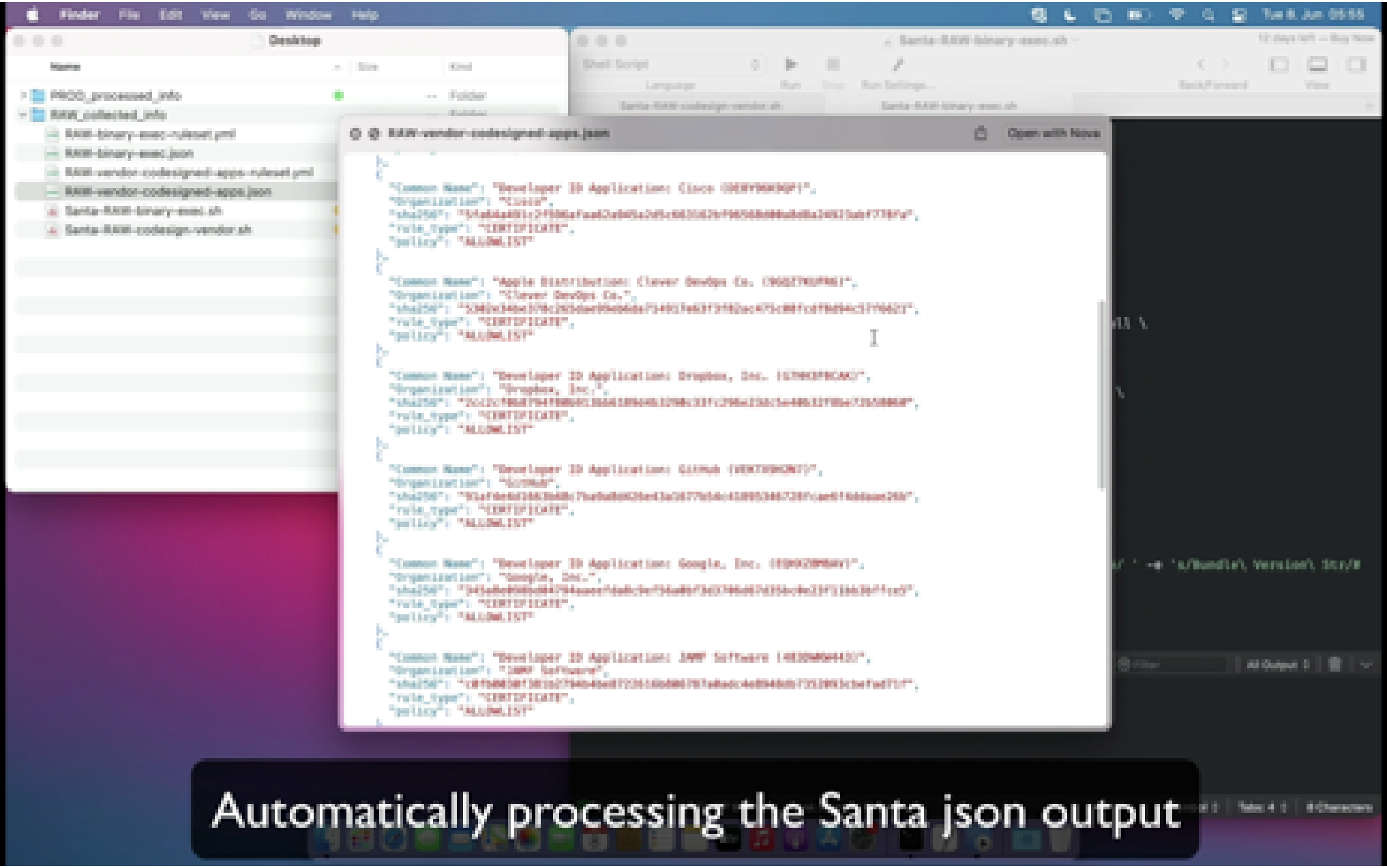
- Core operating rules
- Containment mode rules
- Common app / vendor rules
- Devtools rules
- Denylist rules
- Exceptions requested by users

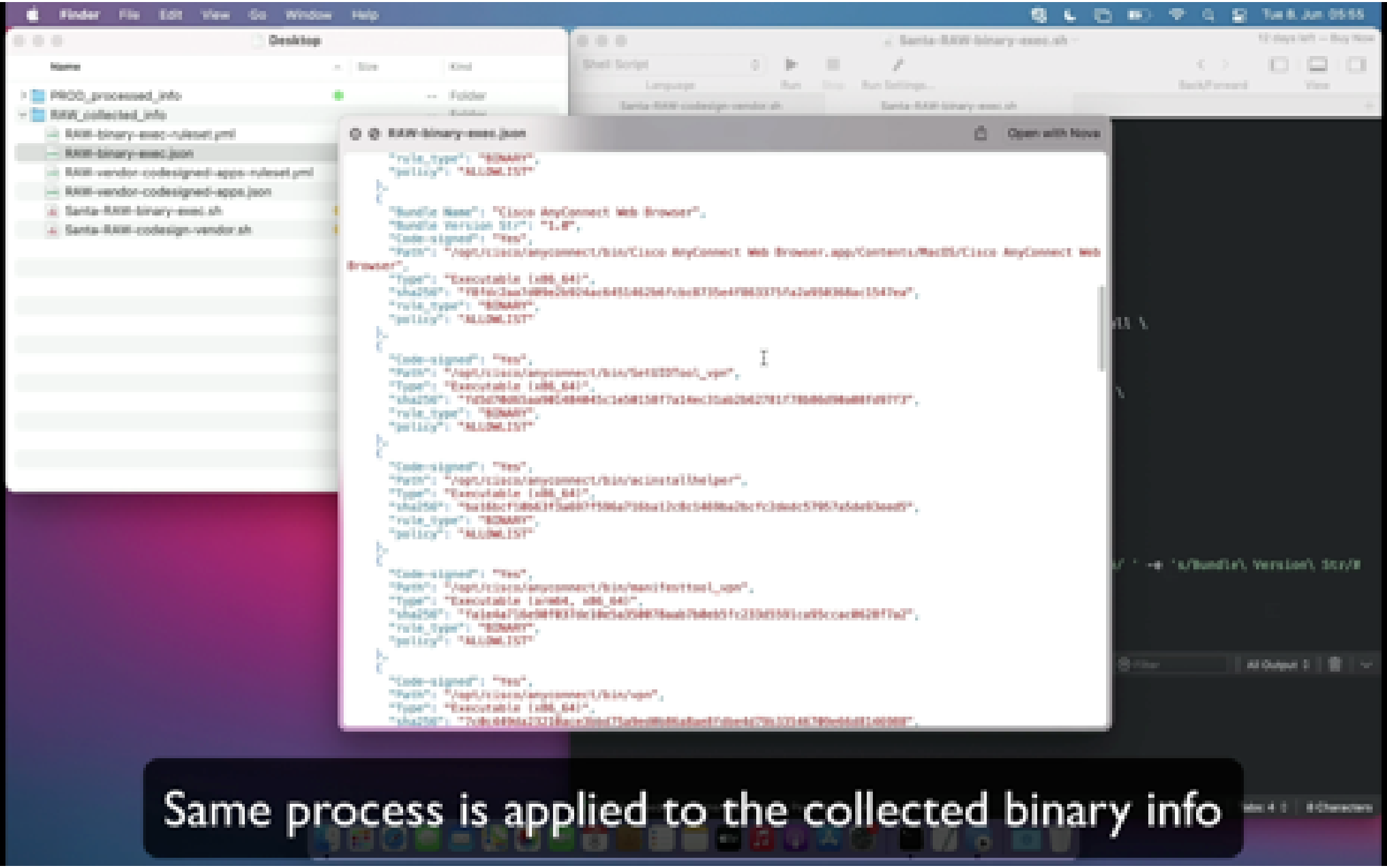
# Plan of action - Demo #1

## Acquiring data on a sample or canary system

- Get "raw" information with **`santactl`**
- Process JSON output into set of rules
- Post-processing to preserve the data in JSON or YAML
- Use **jq / yq** tools for processing


Use santactl to gather codesigned information


Automatically processing the Santa json output


Same process is applied to the collected binary info

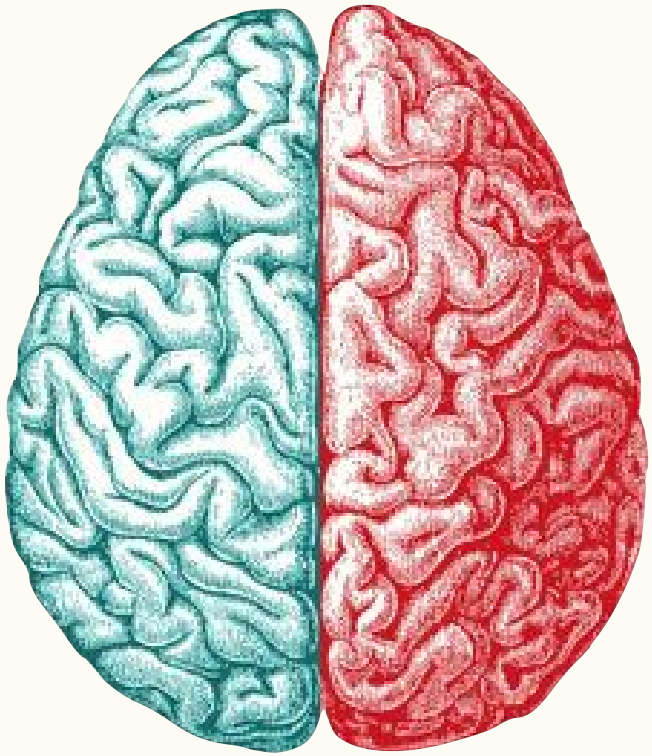
# 80/20

## Lockdown vs. Monitoring

# Split Brain

## Lockdown vs. Monitoring

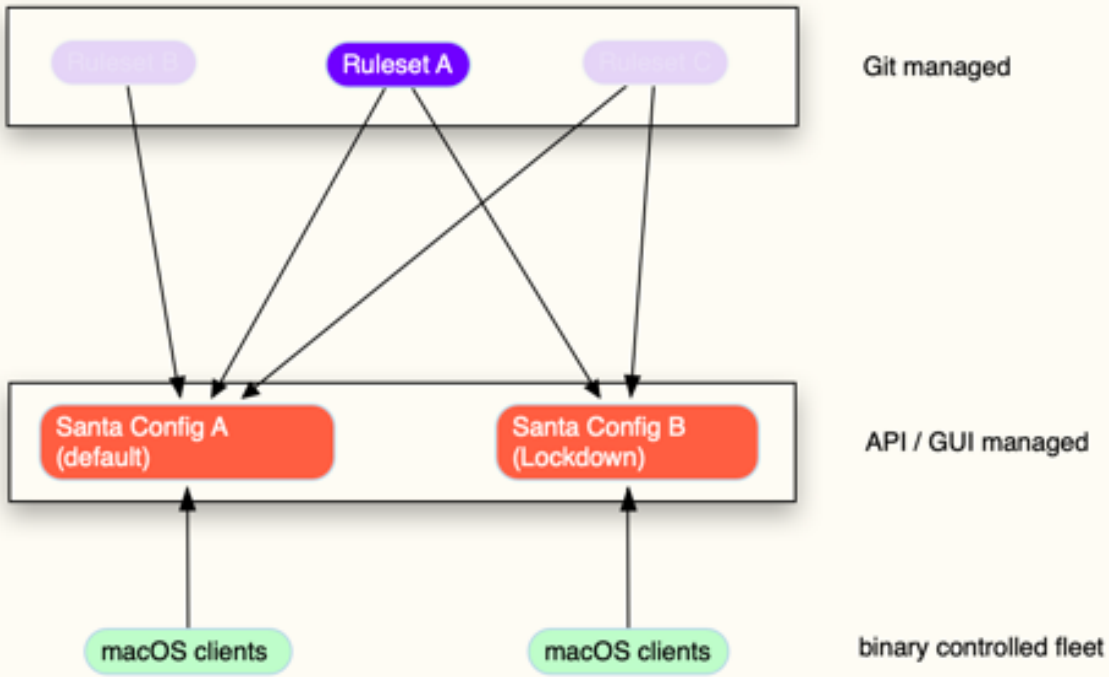

Santa Default
(Config - A)




Santa within bounds
(Config - B)

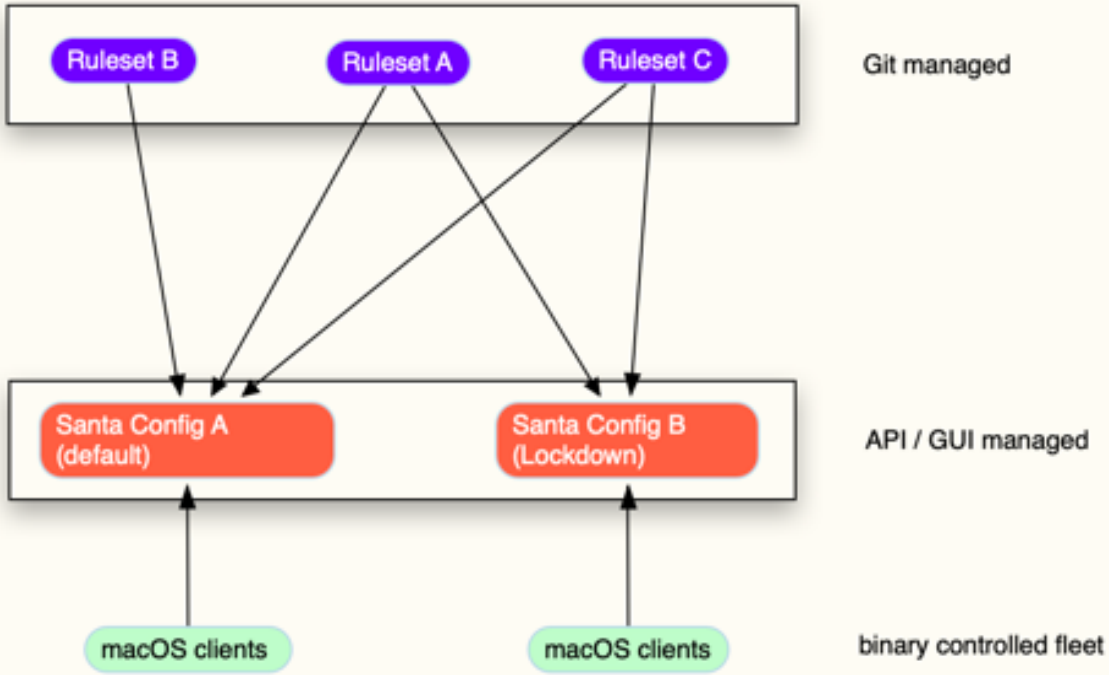
# Building Rulesets

## Git based workflows



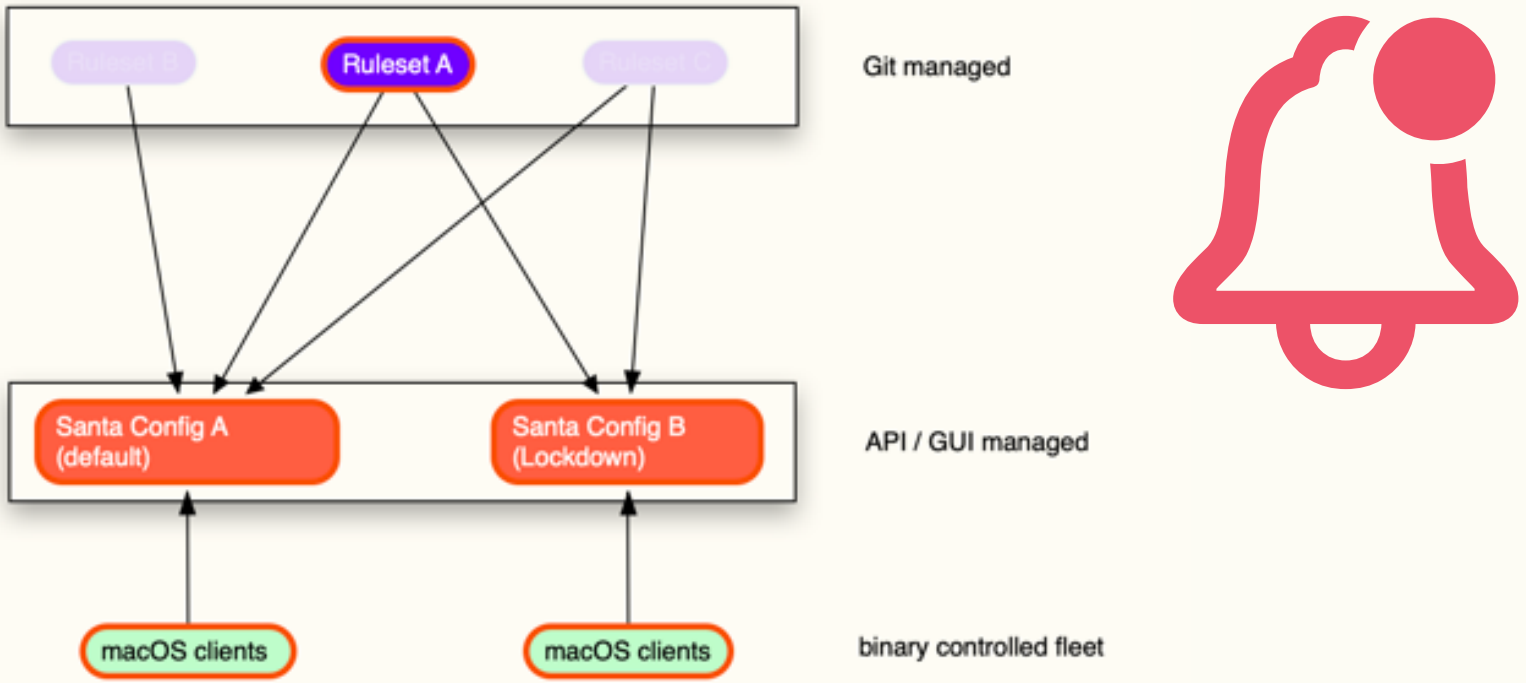
# Building Rulesets

## Git based workflows



# Containment mode

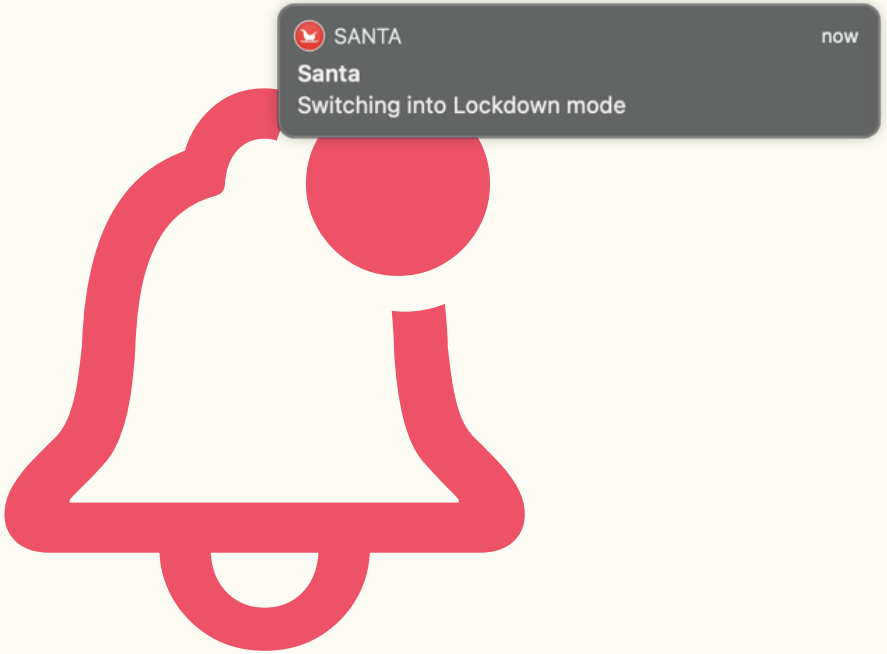
## Allow only the most important tools



# Panic switch

## Be organized on your playbook (when the shit hits the fan)

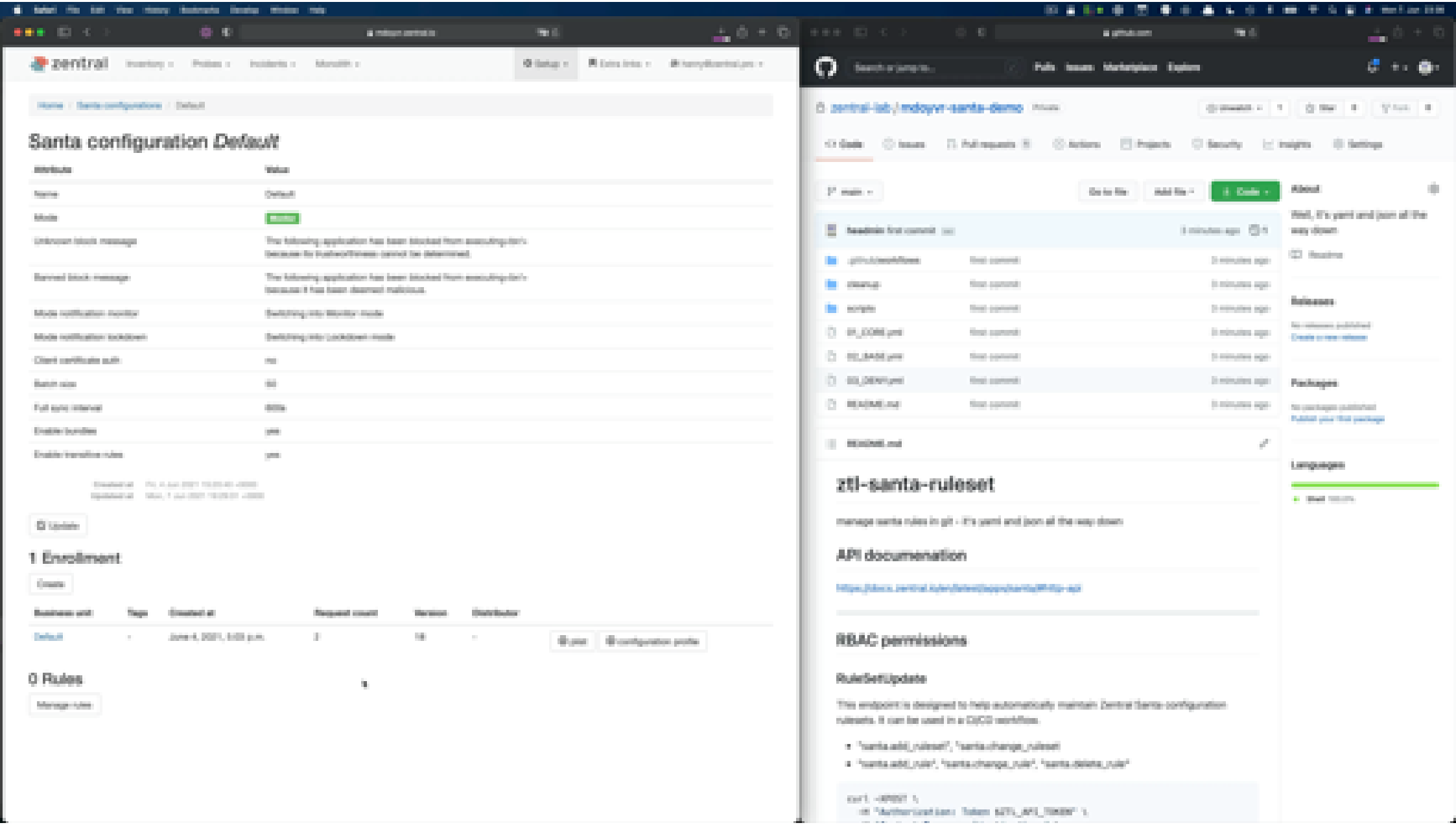
- Allow only the minimum
- Run in Lockdown mode
- Control events in data store / SIEM
- Revert on a granular basis

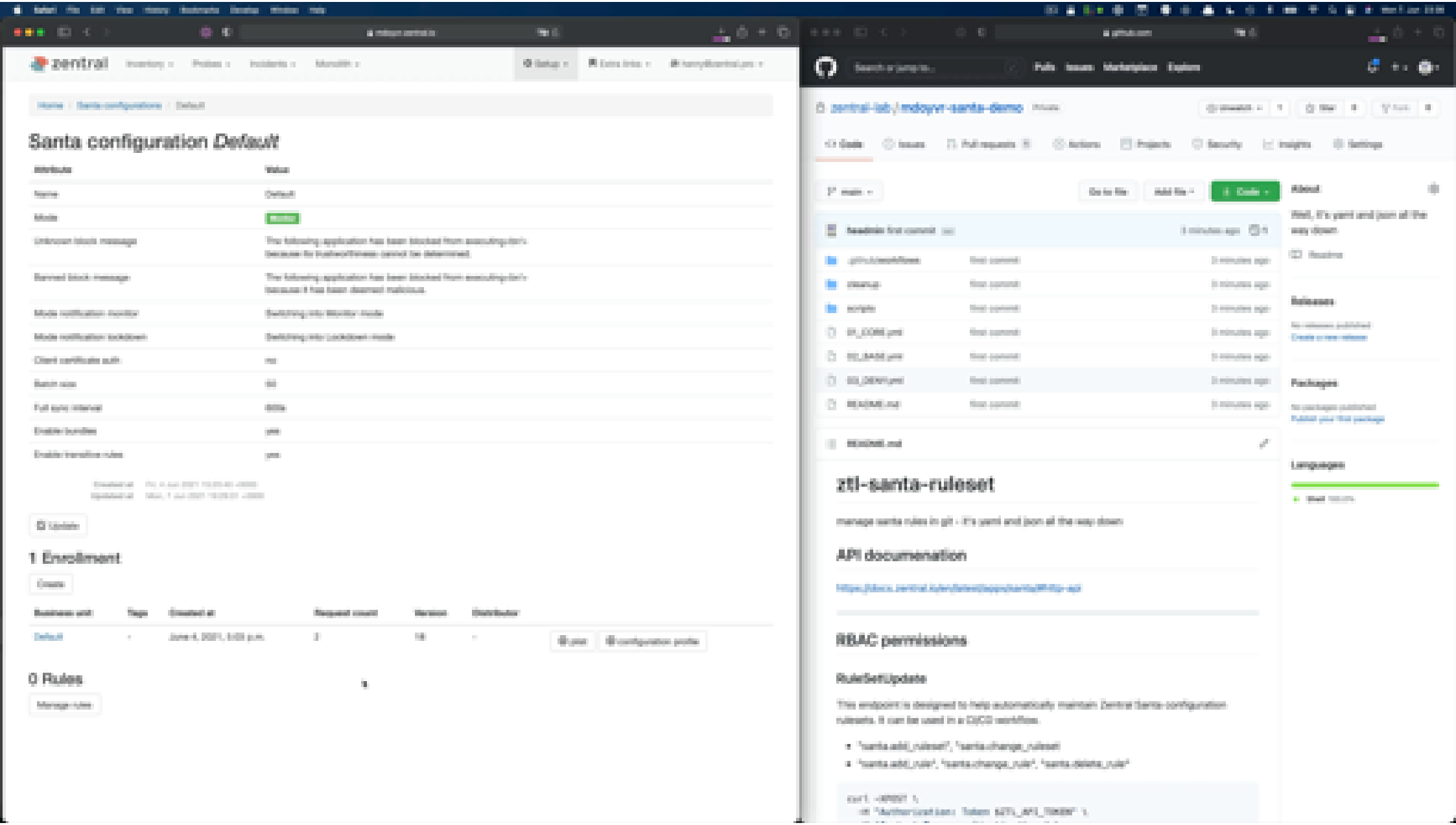


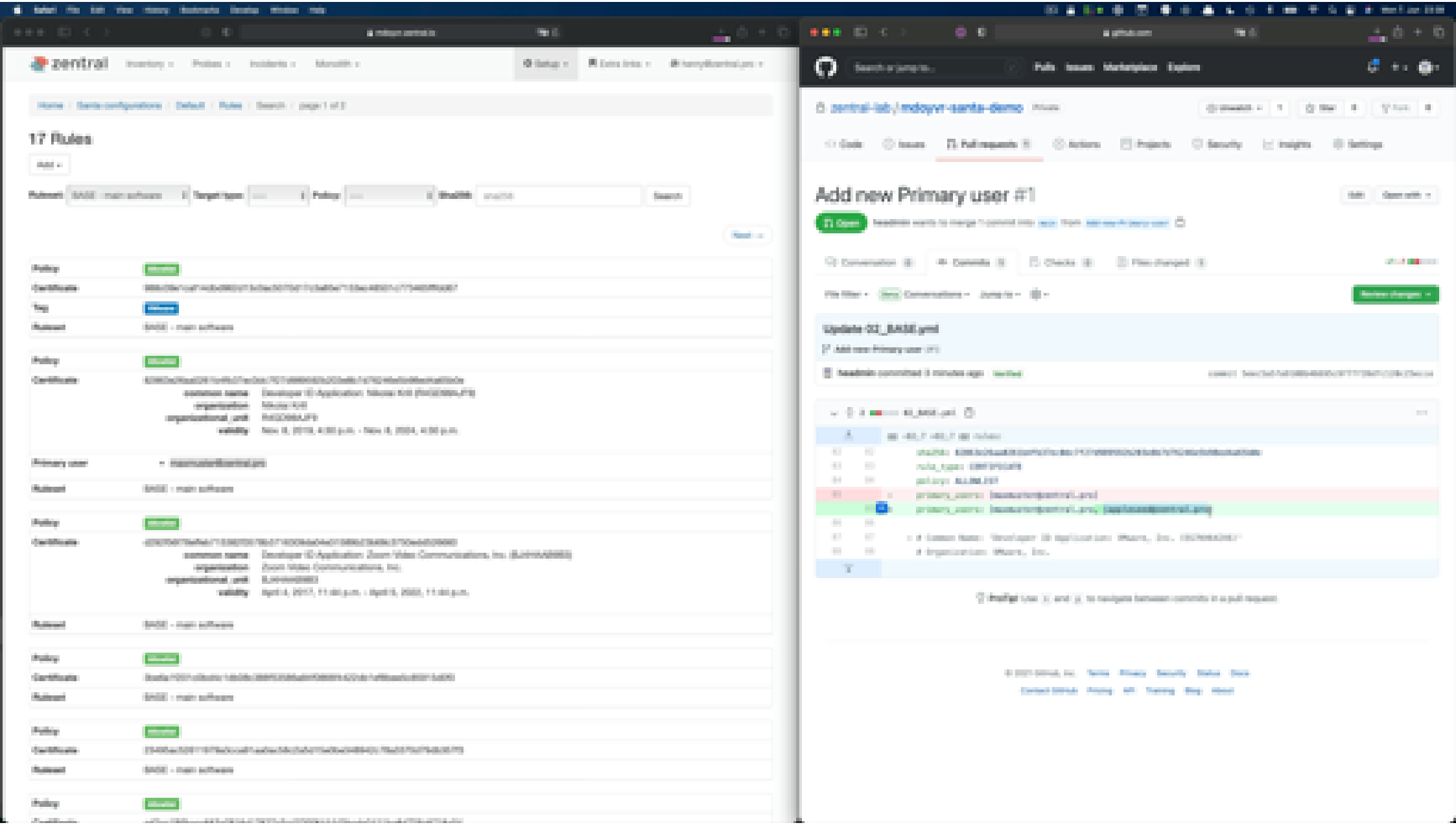
# Plan of action - Demo #2

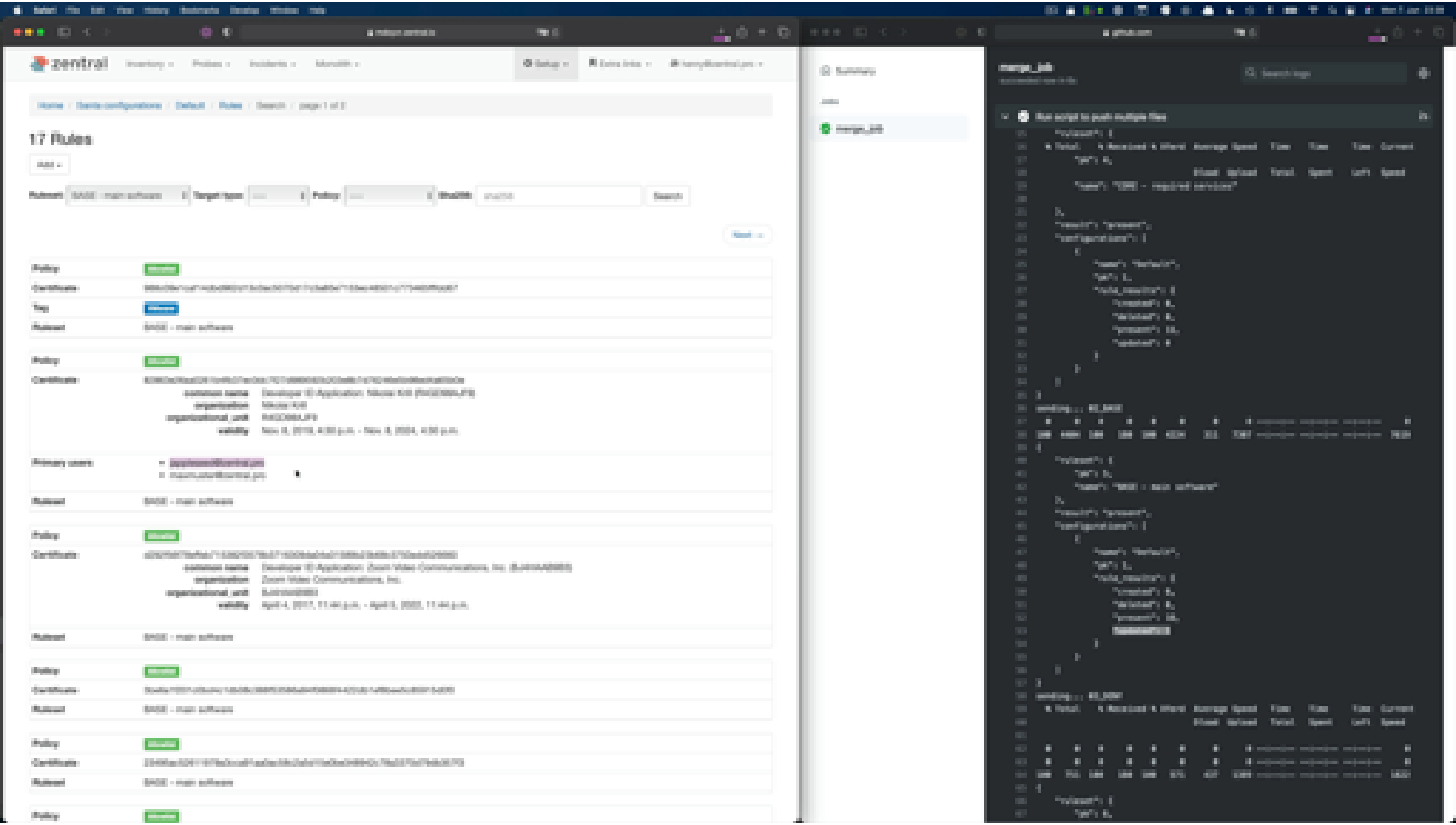
**Run git based workflow**

- GitHub Actions
- Zentral HTTP API
- Santa Sync server is a Zentral instance running in the cloud


zentral
Home / Santa configurations / Default
Santa configuration Default
Attribute
Value
Name
Default
Mode
MONITOR
Unknown block message
The following application has been blocked from executing (bin's because its trustworthiness cannot be determined.
Banned block message
The following application has been blocked from executing (bin's because it has been deemed malicious.
Mode notification monitor
Switching into Monitor mode
Mode notification lockdown
Switching into Lockdown mode
Client certificate auth
no
Batch size
50
Full sync interval
600s
Enable bundles
yes
Enable transitive rules
yes
Update
1 Enrollment
Create
Business unit
Tags
Created at
Request count
Version
Distributor
Default
June 4, 2021, 5:03 p.m.
2
18
yaml
configuration profile
0 Rules
Manage rules
zentral-lab / mdoyvr-santa-demo
Private
Code
Issues
Pull requests
Actions
Projects
Security
Insights
Settings
main
Go to file
Add file
Code
headmin first commit
1 minute ago
.github/workflows
first commit
1 minute ago
cleanup
first commit
1 minute ago
scripts
first commit
1 minute ago
01_CORE.yml
first commit
1 minute ago
02_BASE.yml
first commit
1 minute ago
03_DEMO.yml
first commit
1 minute ago
README.md
first commit
1 minute ago
README.md
ztl-santa-ruleset
manage santa rules in git - it's yaml and json all the way down
API documenation
https://docs.zentral.io/en/latest/apps/santa/#http-api
RBAC permissions
RuleSetUpdate
This endpoint is designed to help automatically maintain Zentral Santa configuration rulesets. It can be used in a CI/CD workflow.
"santa.add_ruleset", "santa.change_ruleset"
"santa.add_rule", "santa.change_rule", "santa.delete_rule"
curl -<HTTP/2
-H "Authorization: Token $ZTL_API_TOKEN" \
About
Well, it's yaml and json all the way down
Readme
Releases
No releases published
Create a new release
Packages
No packages published
Publish your first package
Languages
Shell 100.0%


zentral
Home / Santa configurations / Default
Santa configuration Default
Attribute
Value
Name
Default
Mode
MONITOR
Unknown block message
The following application has been blocked from executing (bin's because its trustworthiness cannot be determined.
Banned block message
The following application has been blocked from executing (bin's because it has been deemed malicious.
Mode notification monitor
Switching into Monitor mode
Mode notification lockdown
Switching into Lockdown mode
Client certificate auth
no
Batch size
50
Full sync interval
600s
Enable bundles
yes
Enable transitive rules
yes
Update
1 Enrollment
Create
Business unit
Tags
Created at
Request count
Version
Distributor
Default
June 4, 2021, 5:03 p.m.
2
18
yaml
configuration profile
0 Rules
Manage rules
zentral-lab / mdoyvr-santa-demo
Private
Code
Issues
Pull requests
Actions
Projects
Security
Insights
Settings
main
Go to file
Add file
Code
headmin first commit
1 minute ago
.github/workflows
first commit
1 minute ago
cleanup
first commit
1 minute ago
scripts
first commit
1 minute ago
01_CORE.yml
first commit
1 minute ago
02_BASE.yml
first commit
1 minute ago
03_DEMO.yml
first commit
1 minute ago
README.md
first commit
1 minute ago
README.md
ztl-santa-ruleset
manage santa rules in git - it's yaml and json all the way down
API documenation
https://docs.zentral.io/en/latest/apps/santa/#http-api
RBAC permissions
RuleSetUpdate
This endpoint is designed to help automatically maintain Zentral Santa configuration rulesets. It can be used in a CI/CD workflow.
"santa.add_ruleset", "santa.change_ruleset"
"santa.add_rule", "santa.change_rule", "santa.delete_rule"
curl -<HTTP/2
-H "Authorization: Token $ZTL_API_TOKEN" \
About
Well, it's yaml and json all the way down
Readme
Releases
No releases published
Create a new release
Packages
No packages published
Publish your first package
Languages
Shell 100.0%


zentral
17 Rules
Add new Primary user #1
Update 02_BASE.yml

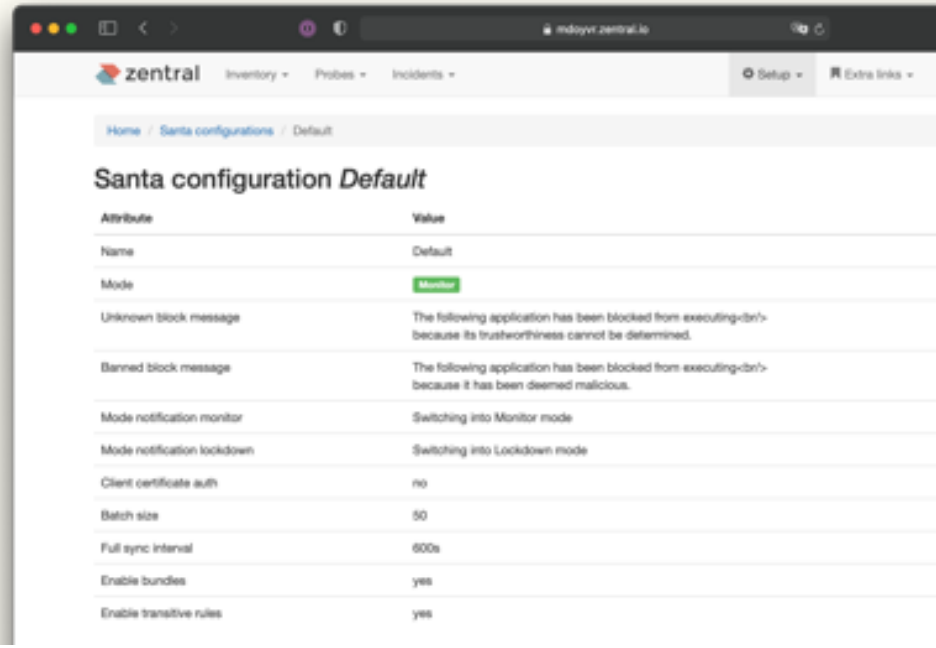

zentral
17 Rules
merge_job
Run script to push multiple files

zentral

# Up-to-date Santa sync server

(It's yaml and json all the way down)

**Zentral open source:**
**https://github.com/zentralopensource/zentral**



# The Zentral project

## Typically runs in a cloud-based deployment


- Complete Santa and Osquery configuration and event management
- Connecting multiple inventories (Jamf, PuppetDB, et-al.)
- Comprehensive event sources (Munki, Jamf Protect, et-al.)
- Manage dynamic Munki manifests (effectively replaces Simian)
- Scalable operation in a full cloud-native setup (GCP, AWS, Azure)*
- SSO and Role Base Access Control (RBAC)
- Multiple primary event data stores





*Support plan for cloud provider deployment (w/Terraform) or use of the free appliance in smaller setups.

# Summary

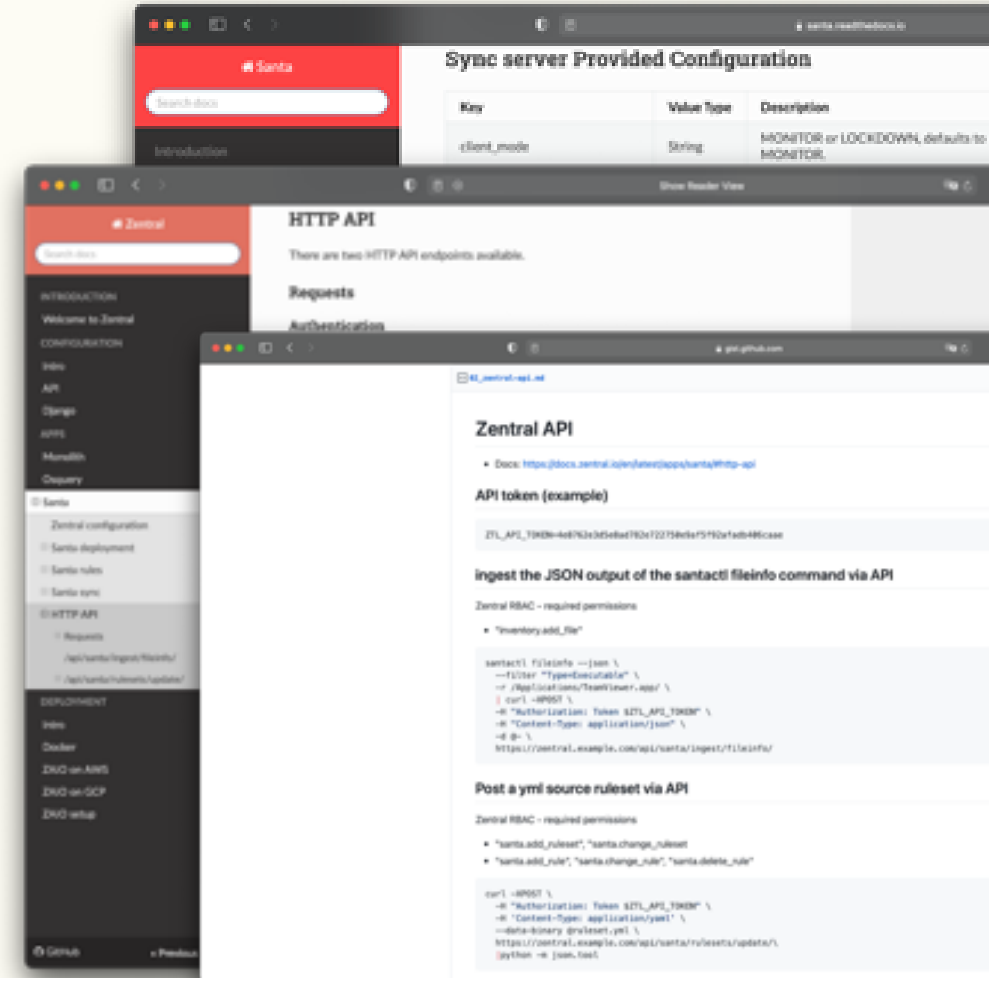
## Effective binary control for macOS

- Know what to approve for whom
- Update rules and policies in a effective time frame
- Consider more than one possible configuration
- Keep control with Git based workflows
- Embrace lockdown mode for a substantial share of the fleet

# Learn more resources

## Manage an effective binary control for macOS

- Santa Documentation
  https://santa.readthedocs.io
- Zentral Documentation
  https://docs.zentral.io
- Santa project
  https://github.com/google/santa
- Zentral open source project
  https://github.com/zentralopensource/zentral
- Moroz open source project
  https://github.com/groob/moroz



zentral
Development & Professional Services

# Thank you

## Say hello / contact us

Twitter: @head_min
Slack: @headmin

Zentral Pro Services
https://zentral.pro