Logging

About Needles in the Modern Haystack

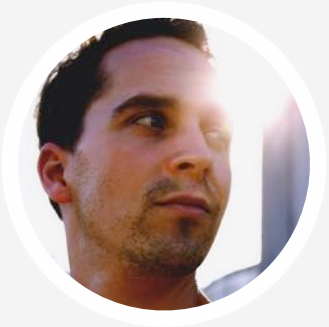
Who are we ?

zentral.pro

zentral.pro

- Founded in Q1 2019
- Based in Germany
- Small, skilled team
- Professional Services
  Research and Development
- Business & Enterprises customers
- B2B Partners

Who am I



Henry Stamerjohann

zentral.pro

- Based in Hamburg, Germany
- Zentral Pro Services *(co-founder)*
- Started the Zentral open source Event Hub Project with Éric Falconnier *(co-founder)*
- Zentral was first shown in public at MacSysAdmin 2015

Landscape

Landscape

Logs & Events

- Computing / Technology

“A lot more events, from many more sources…”

Landscape

Logs & Events

- Computing / Technology

- Cloud Computing Platforms and SaaS
- Linux *(incl. ChromeOS)*
- Microsoft:
  - Azure, Intune, Windows 10
    (new norm, great integrations)
- Apple:
  - macOS, iOS, iPadOS, tvOS
  - Client Management & MDM Provider
    (well known challenge w/ integrations)

Landscape

Logs & Events

- Computing / Technology

“Where, when and what ? “

Landscape

Logs & Events

- Computing / Technology

“Where, when and what ? “

- Created by apps, systems, network and user activity
- Event flow, time stamps, and Frequency
- Common use:
  - Check-based fault detection
  - Log-based monitoring
  - Metrics-based monitoring
  - Collect telemetry data

Event sources and types

Event sources and types

On the endpoints

- Sources

OS

- Installer
- MDMclient
- LaunchServices

Software

- Business apps
- Other apps
- Security Agents
  - Osquery
  - Santa
  - Xnumon

Event sources and types

On the endpoints

- Sources
  - Security Agents: Osquery

Osquery

- Cloud Native Foundation Project
- Powerful Change Detection
- SQL like view of the system

Based on

- OS
- Multi Platform *(Mac, Linux, Windows)*

Event sources and types

On the endpoints

- Sources
  - Security Agents: Google Santa

Santa

- Binary Whitelisting / Blacklisting
- TLS Server *(Backend)*
- Dynamic Config
- Local Log file

Based on

- Kernel extension
- *(soon)* Security Extention

Event sources and types

On the endpoints

- Sources
  - Security Agents: Xnumon

Xnumon

- Log Information on
  - pid
  - path
  - ancestory
  - arguments
  - code-signing information
- Trace activity *(good/bad)*

Based on

- Open BSM
- Kernel extension

Event sources and types

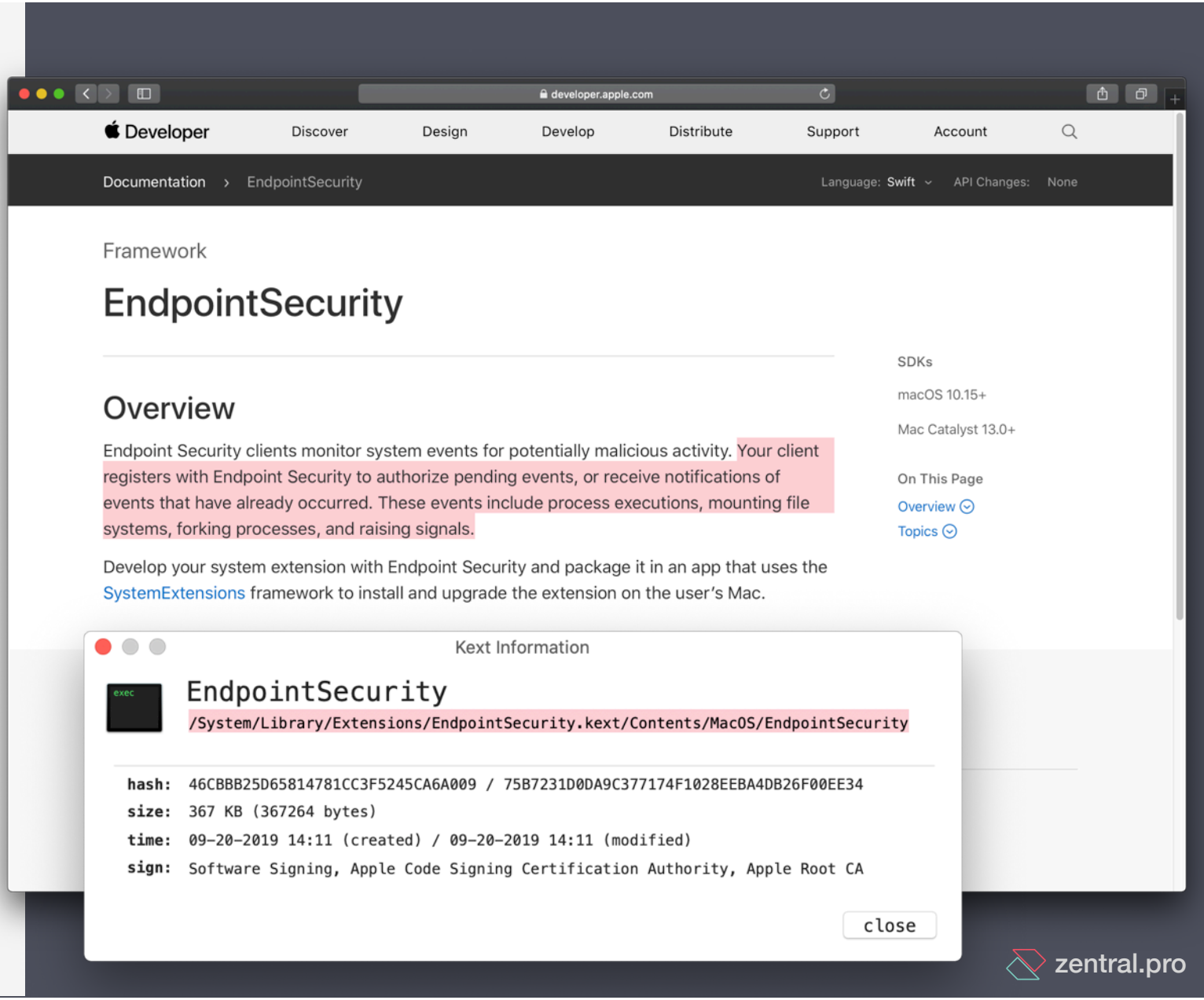
On the endpoints

- Sources
  - Security Agents: System Extensions

Event sources and types

On the endpoints

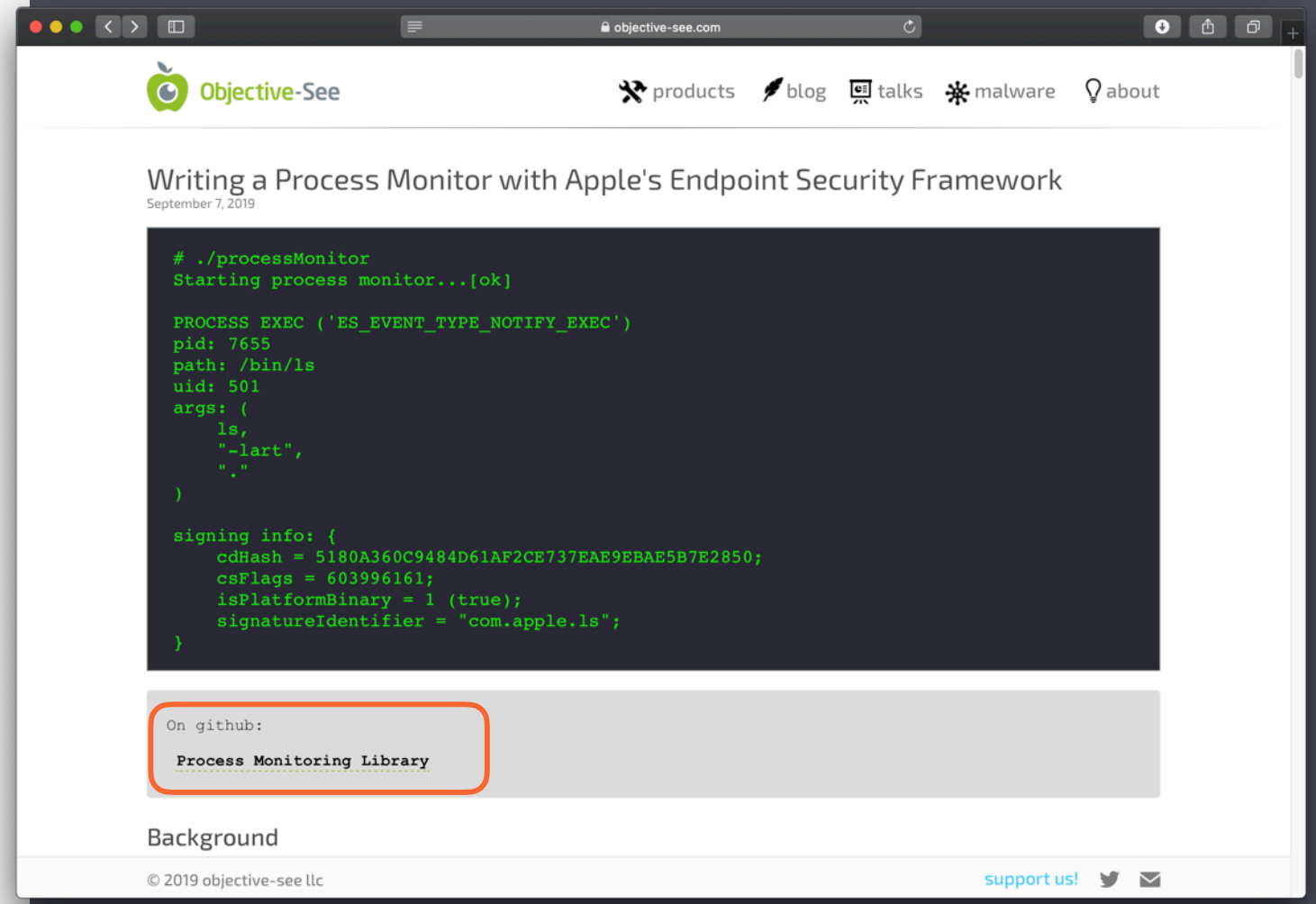
- Sources
  - Security Agents: System Extensions



Event sources and types

On the endpoints

- Sources
  - Security Agents: System Extensions



Event sources and types

On the endpoints

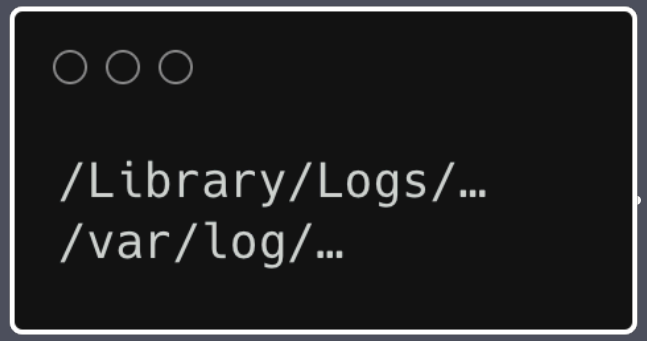
- Outputs

- Written to File
- Written to local Database
- Written to a Backend
- Transferred by an Agent

Event sources and types

On the endpoints

- Outputs
  - File based



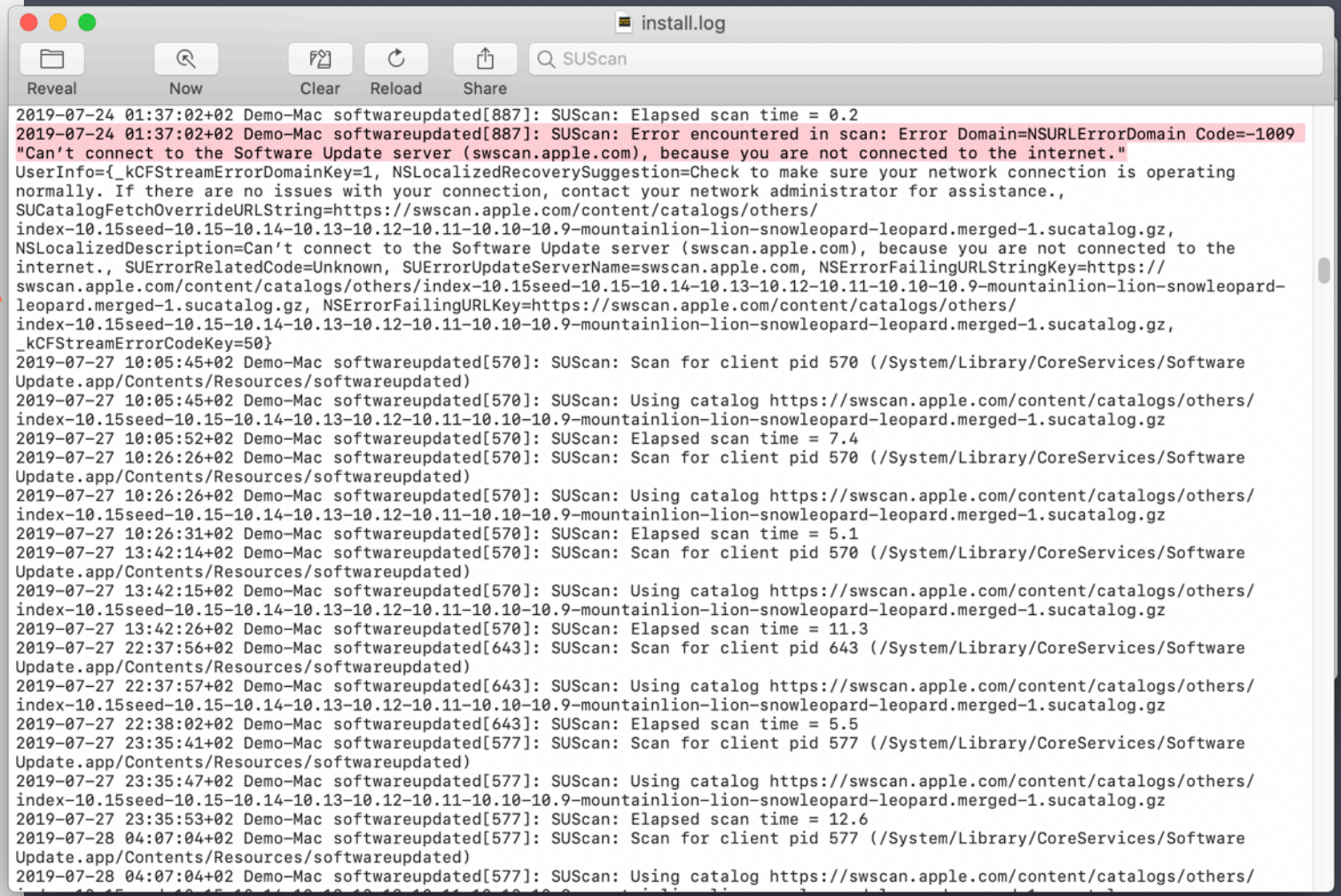
File based - the “classic” use case

- mostly with not so well integrated apps
- Text data in files *(rotated)*
- Sometimes JSON *(1 object per line)*

Event sources and types

On the endpoints

- Outputs
  - File based



Event sources and types

On the endpoints

- Outputs
  - OS log facility

OS log facilities -

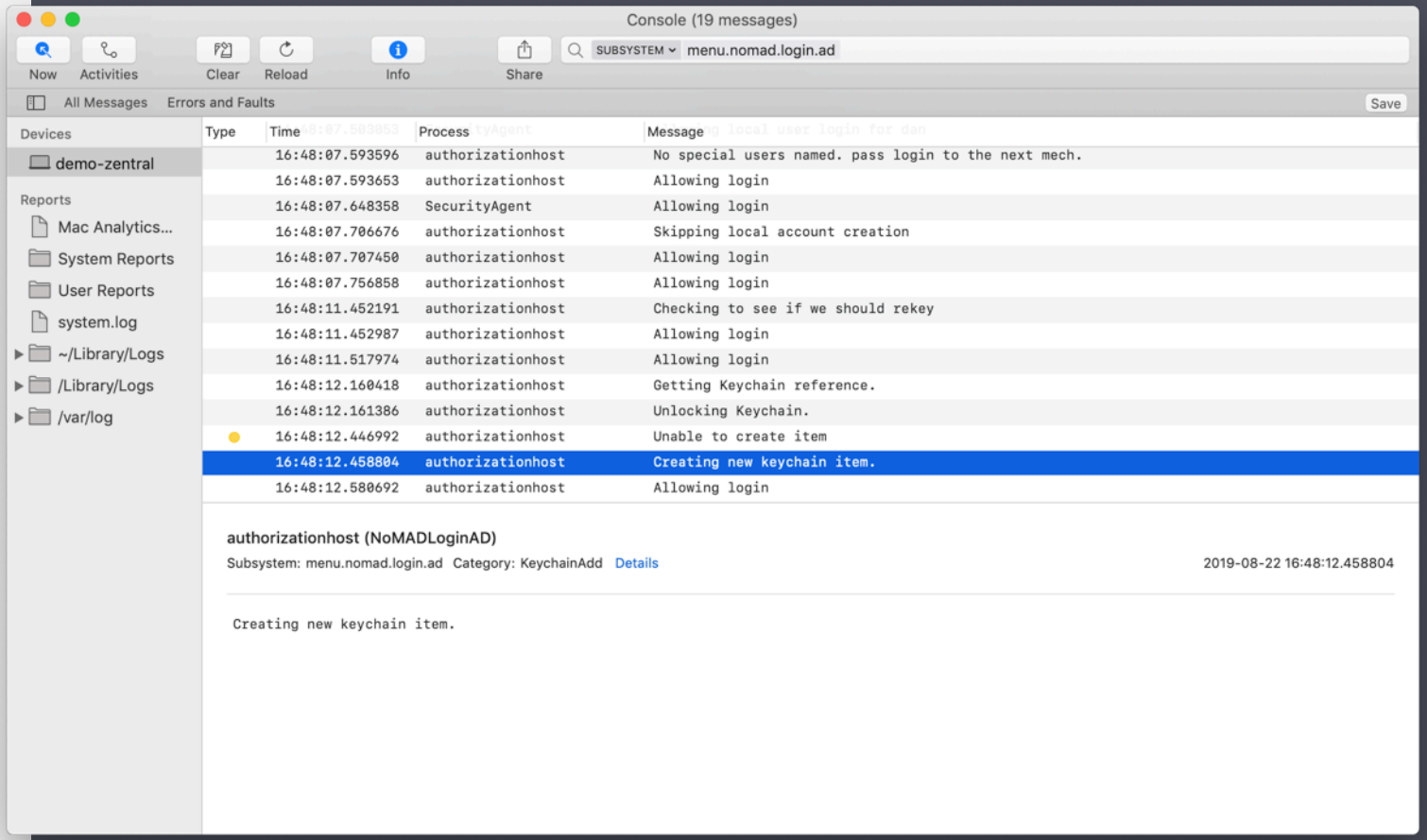
for OS and well behaved / integrated apps

- Apple Unified Logging
  - More structure
  - JSON output possible
  - Configurable persistence
- Syslog *(old in macOS)*

Event sources and types

On the endpoints

- Outputs
  - Unified Logging

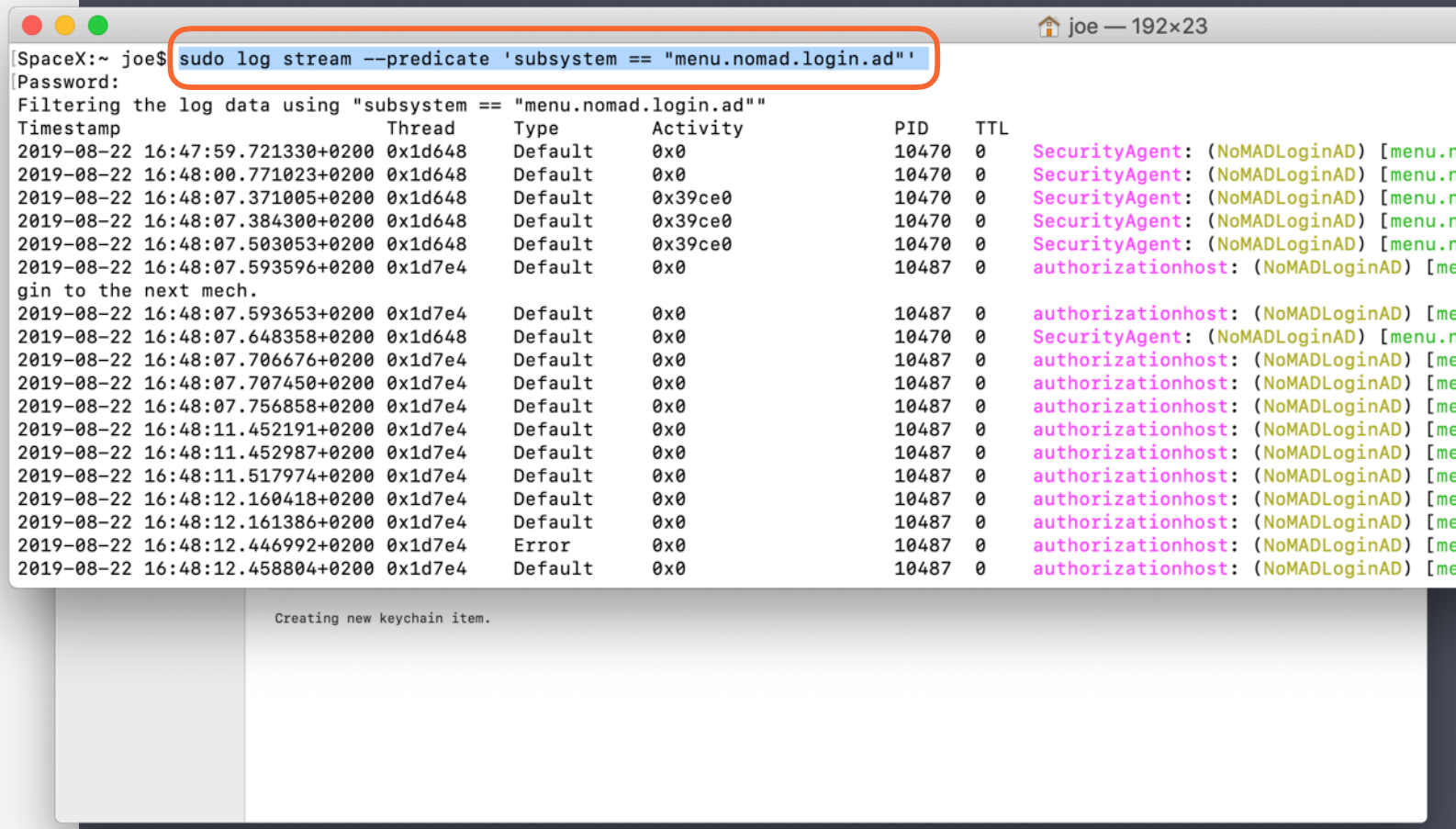


In-memory or persist into **.tracev3** files

Event sources and types

On the endpoints

- Outputs
  - Unified Logging



In-memory or persist into **.tracev3** files

Event sources and types

On the endpoints

- Outputs
  - Unified Logging

```
# Jamf Connect debug

log stream --predicate 'subsystem == "com.jamf.connect.login"' --debug --info
```

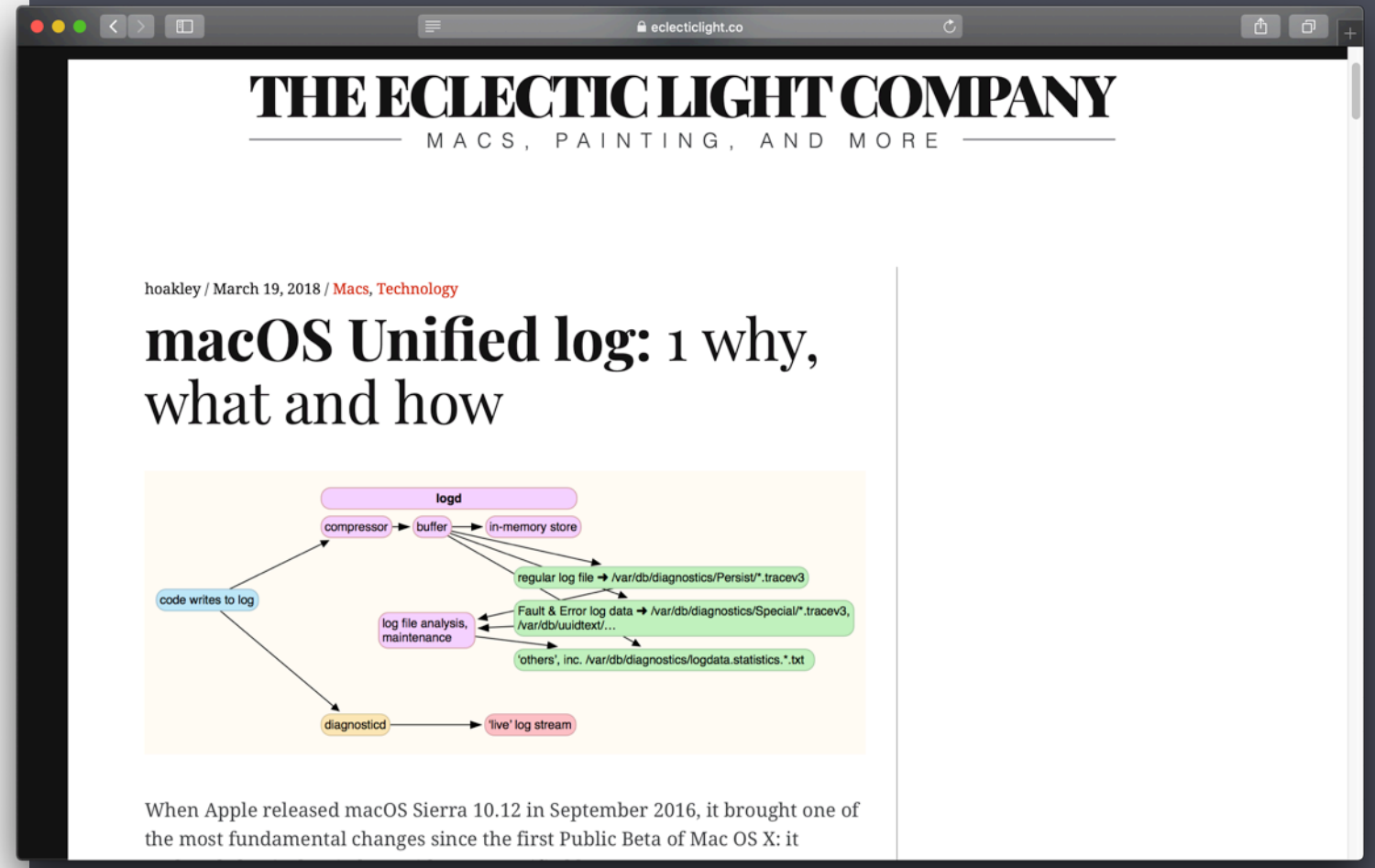
`--predicate`	Filter element *(subsystem type)*
`--debug`	Details depth
`--style`	Formatting *(json)*

Event sources and types

On the endpoints

- Outputs
  - Unified Logging

https://eclecticlight.co/2018/03/19/macos-unified-log-1-why-what-and-how/



Howard Oakley @ Electriclight Company

Event sources and types

On the endpoints

- Outputs
  - Custom

- JSON payload posted on a HTTPS endpoint *(Osquery, Santa,…)*
- Publish to Kafka *(Osquery)*
- Other custom variants…

Event sources and types

Server / Cloud

- Sources

Identity Provider

- Sign-ins / Sign-in errors *(AzureAD, Okta, …)*

Inventory

- Computer check-in *(Jamf Pro, WorkspaceOne, …)*
- Group changes *(SimpleMDM, Jamf Pro, …)*

MDM *(SaaS, open source MDM)*

- Configuration profile pushed
- Device Enrollments

Security providers

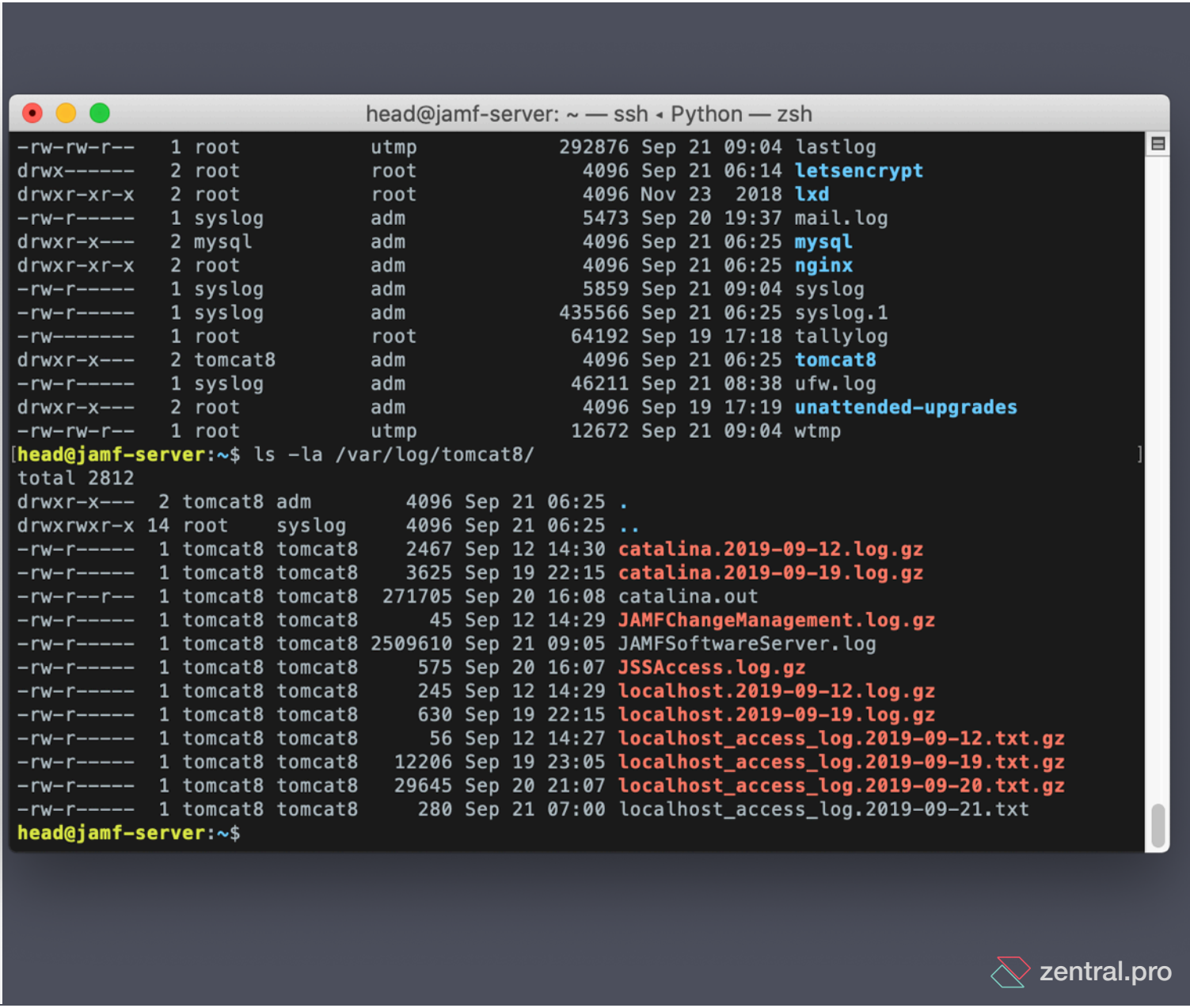
- Malware detected/removed

  (Microsoft Defender ATP, Malwarebytes)

Event sources and types

Server / Cloud

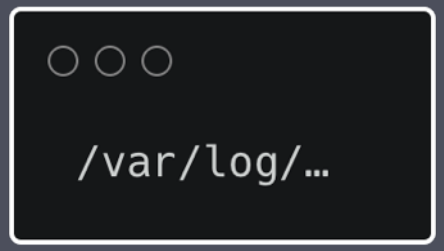
- Outputs



Event sources and types

Server / Cloud

- Outputs



- File based - for most of the logs
  - Text data in files *(rotated)*
  - Log archives
- Service logs *(systemd / journalctl)*

Event sources and types

Server / Cloud

- Outputs

- API *(Jamf Pro, Microsoft Graph SecurityAPI)*
- Webhooks *(Jamf Pro, Okta, …)*
- Files on a server

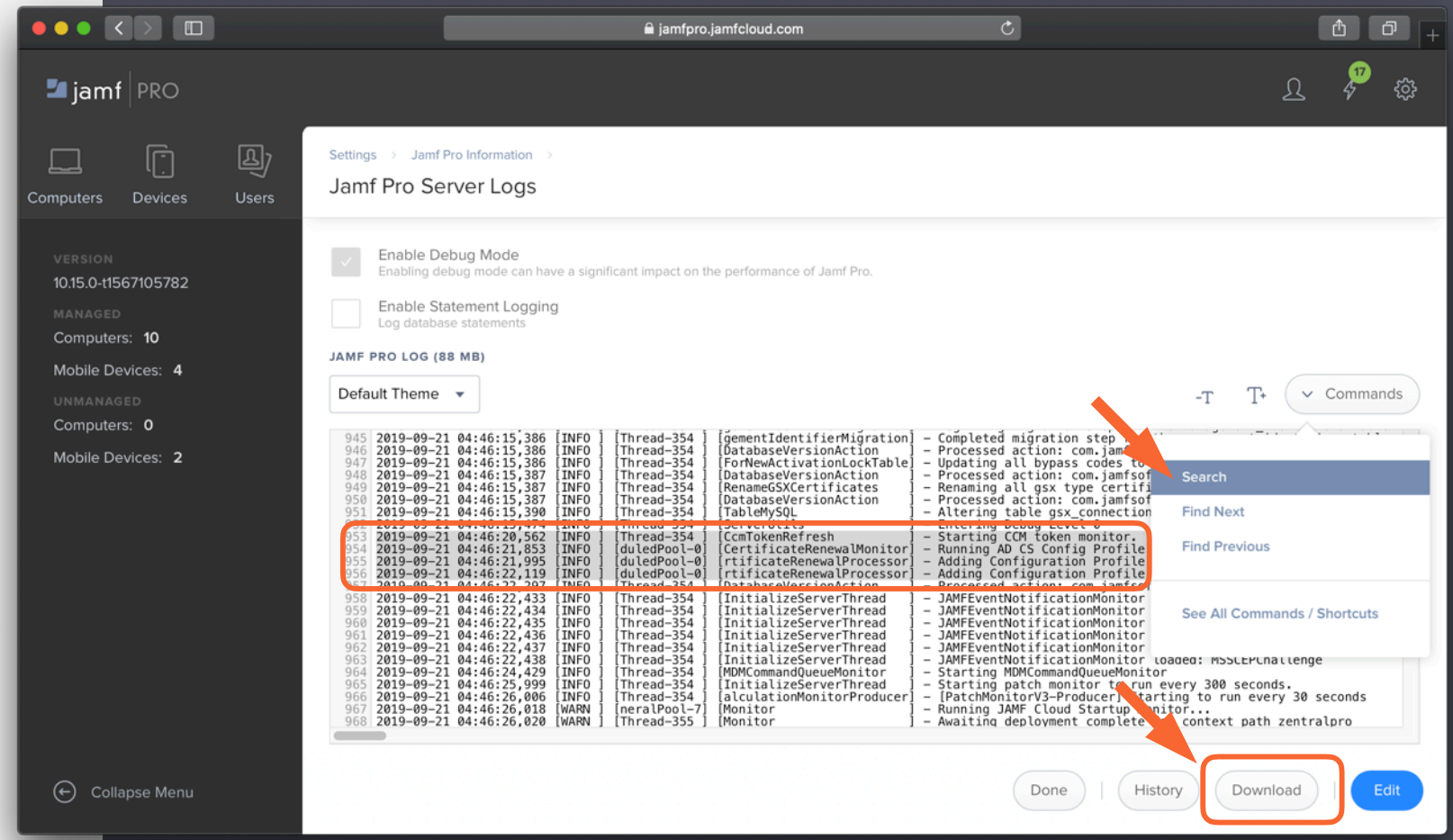
  (i.e.Jamf Pro in custom deployment)
- Blobs on a storage service
- GUI + manual download
- Events in a Message Broker

  (Azure Event Hubs)

Event sources and types

Server / Cloud

- Outputs
  - Jamf Pro



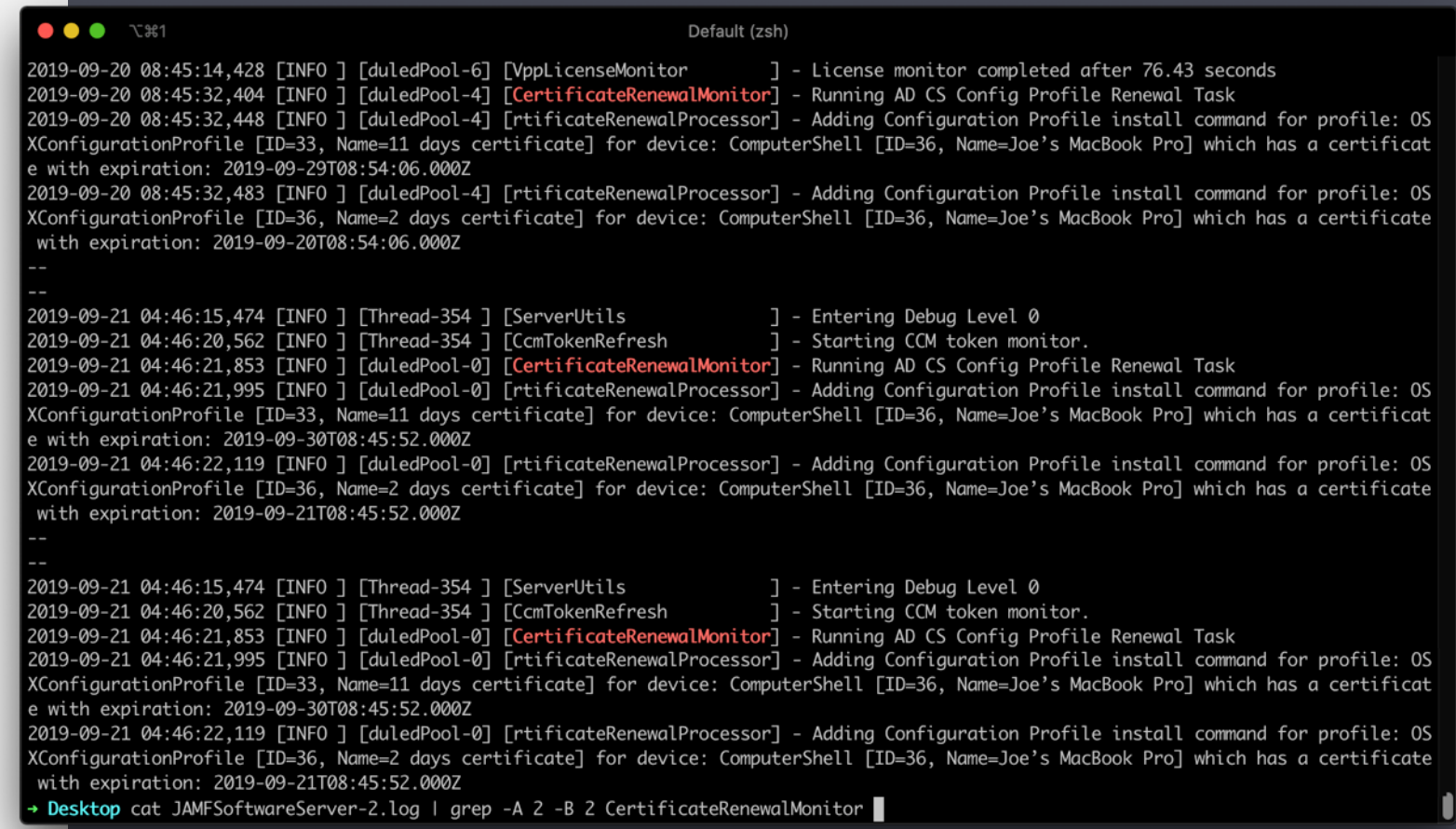
Search in browser or download

zentral.pro

Event sources and types

Server / Cloud

- Outputs
  - Jamf Pro

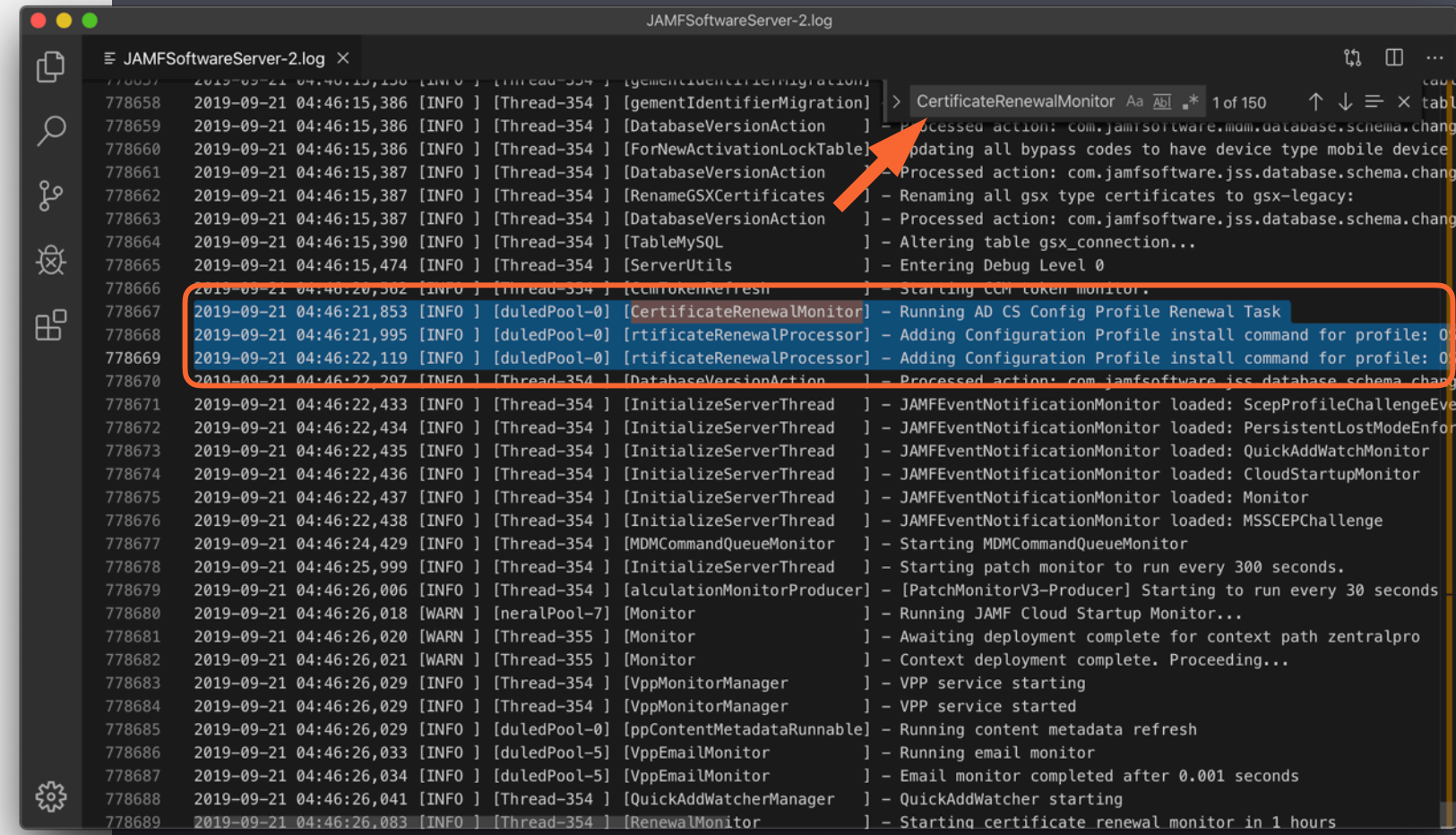


Search and grep *(keywords, errors, …)*

Event sources and types

Server / Cloud

- Outputs
  - Jamf Pro



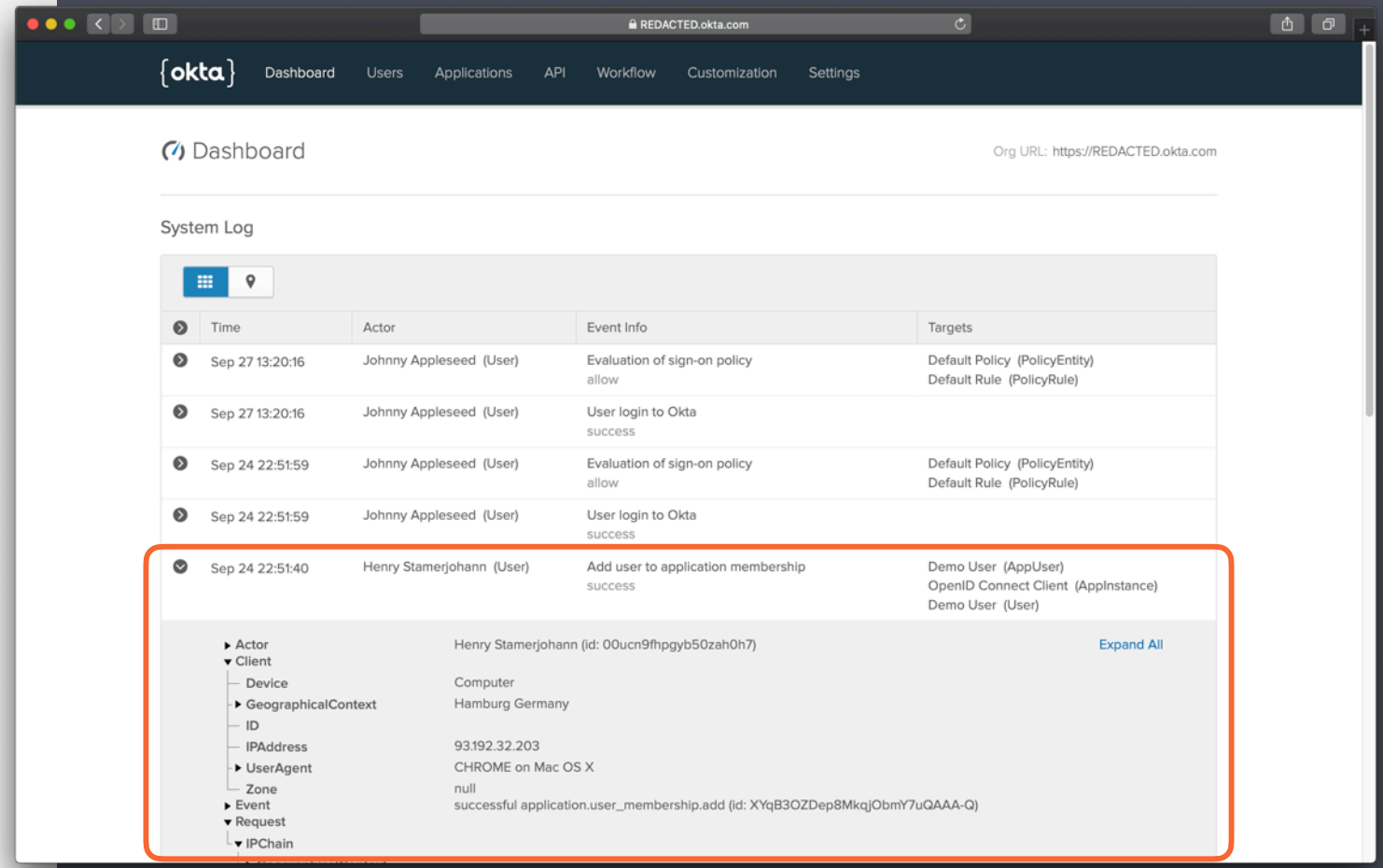
Search and grep *(keywords, errors, …)*

zentral.pro

Event sources and types

Server / Cloud

- Outputs
  - IDP - Okta



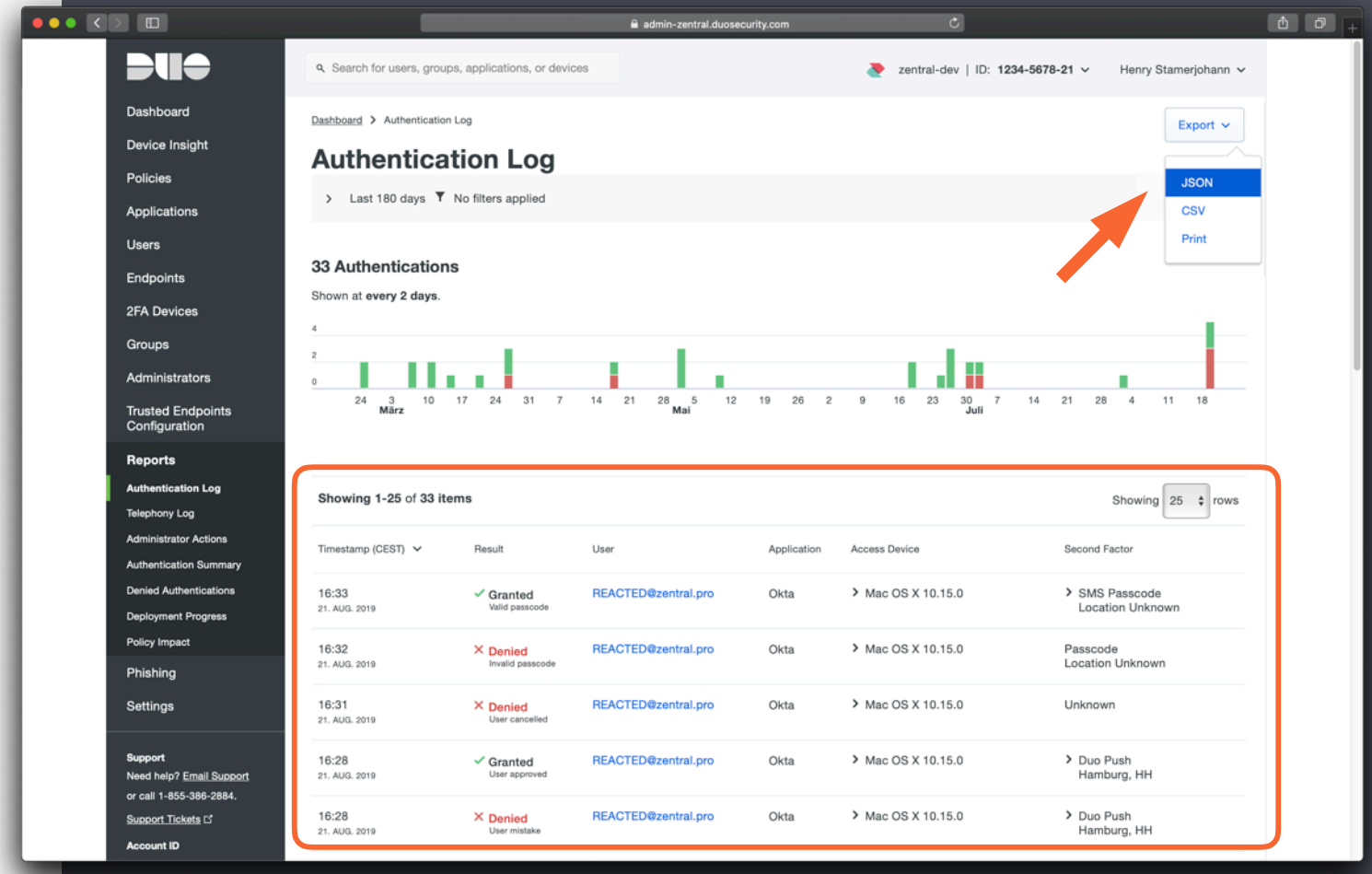
Event audit trail *(sign-ins, edits or changes)*

zentral.pro

Event sources and types

Server / Cloud

- Outputs
  - IDP - Duo



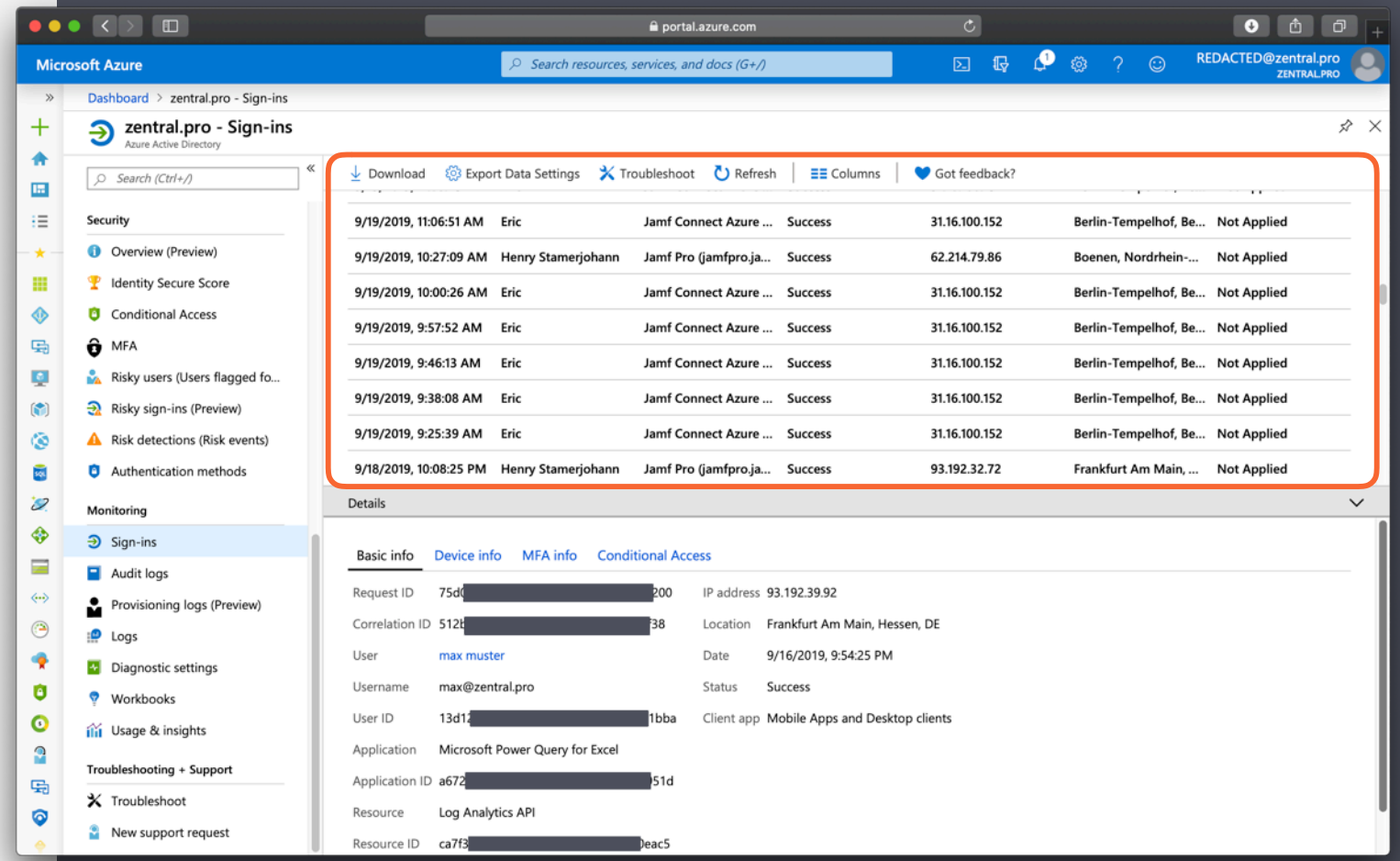
Authentications *(export json, csv)*

zentral.pro

Event sources and types

Server / Cloud

- Outputs
  - IDP - Azure AD



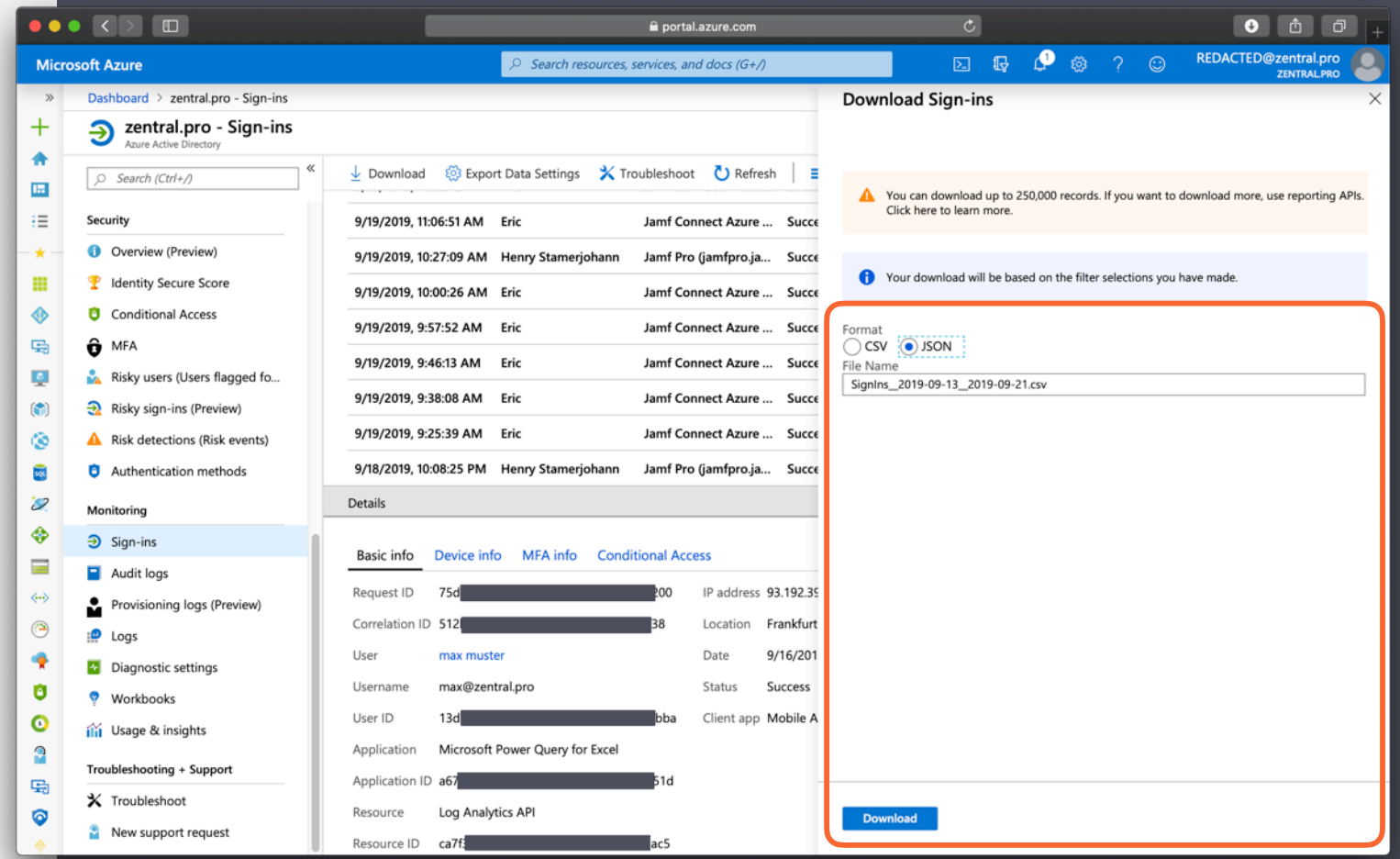
Sign-in Logs *(export json, csv)*

zentral.pro

Event sources and types

Server / Cloud

- Outputs
  - IDP - Azure AD



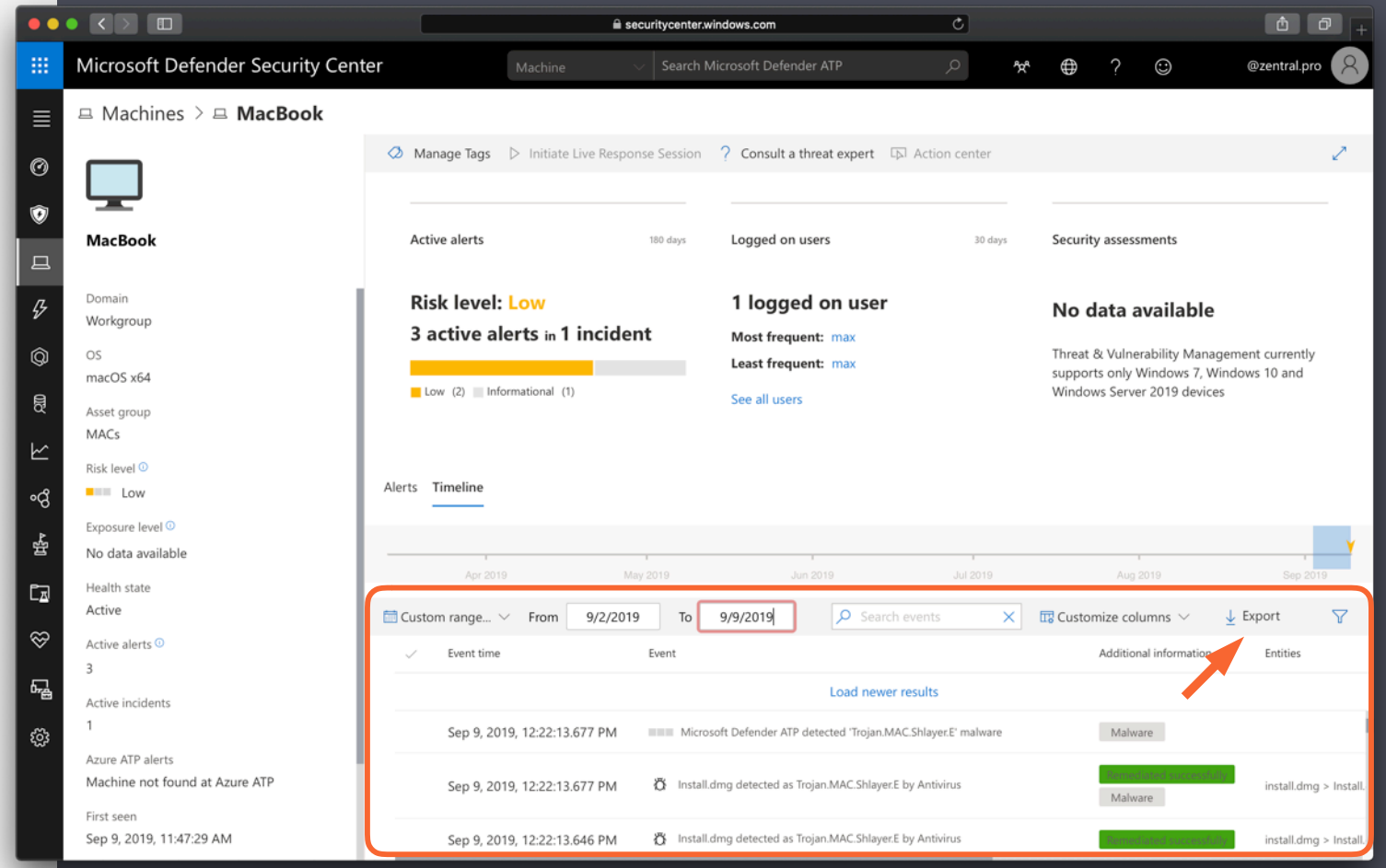
Sign-in Logs *(export json, csv)*

zentral.pro

Event sources and types

Server / Cloud

- Outputs
  - ATP Defender



AV Activity / Remediation *(export csv)*

zentral.pro

Event sources and types

Server / Cloud

- Outputs
  - Post processing

- Build reports from CSV
- Analyze/process JSON
- Upload and repurpose event data
- Share with other Teams
- Store for Compliance *(Backups)*
- Use to get support from a Vendor

Ship and collect the events

Ship and collect the events

Problems / Issues

- Reality

- Many different sources
- Many different formats
- No single place where to look at events / search for events
- Too many events

Ship and collect the events

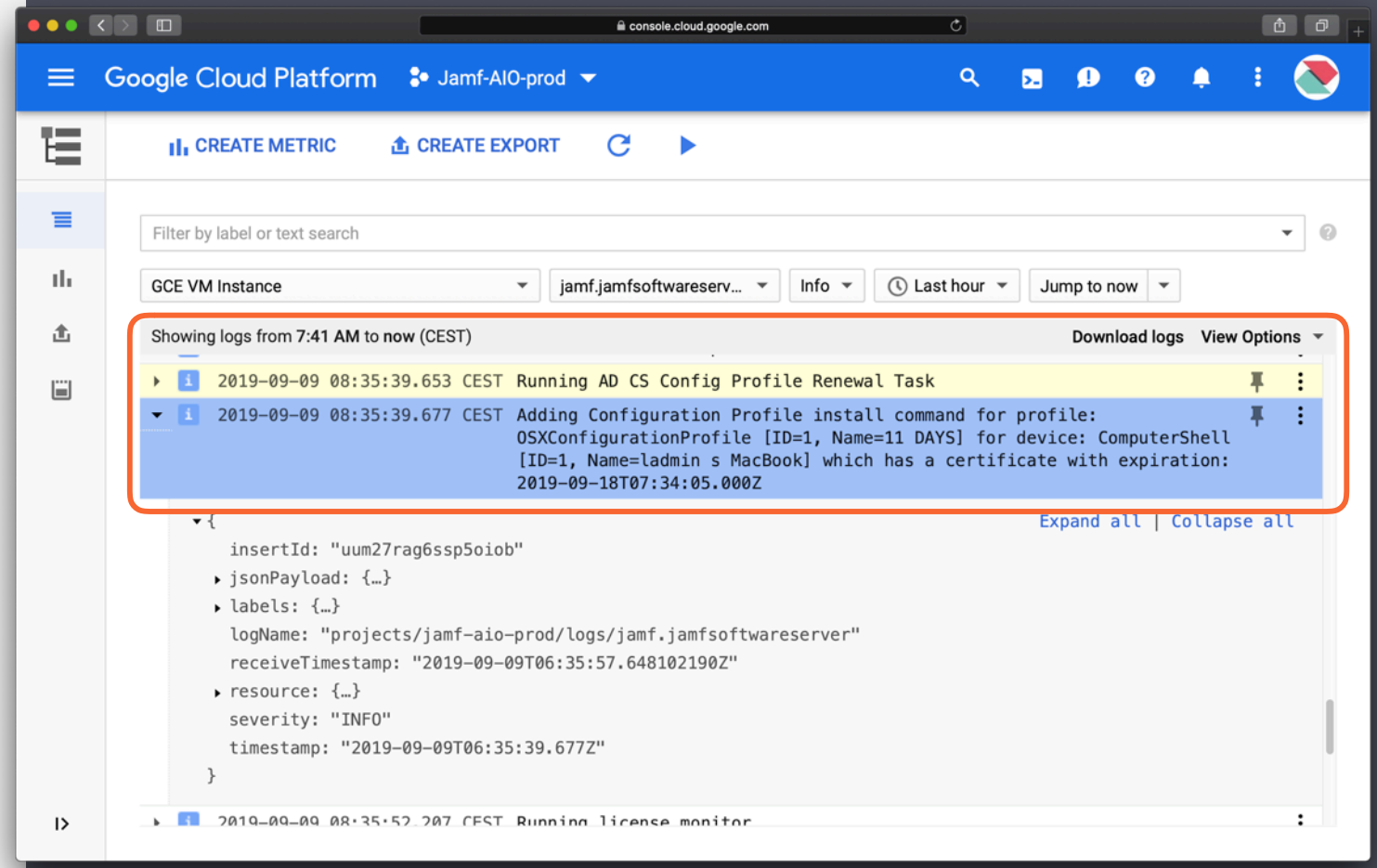
Existing Solutions

- Elastic Stack *(formerly ELK Stack)*
- Splunk
- Sumo Logic
- Stackdriver
- Zentral
- et.al

Ship and collect the events

Existing Solutions

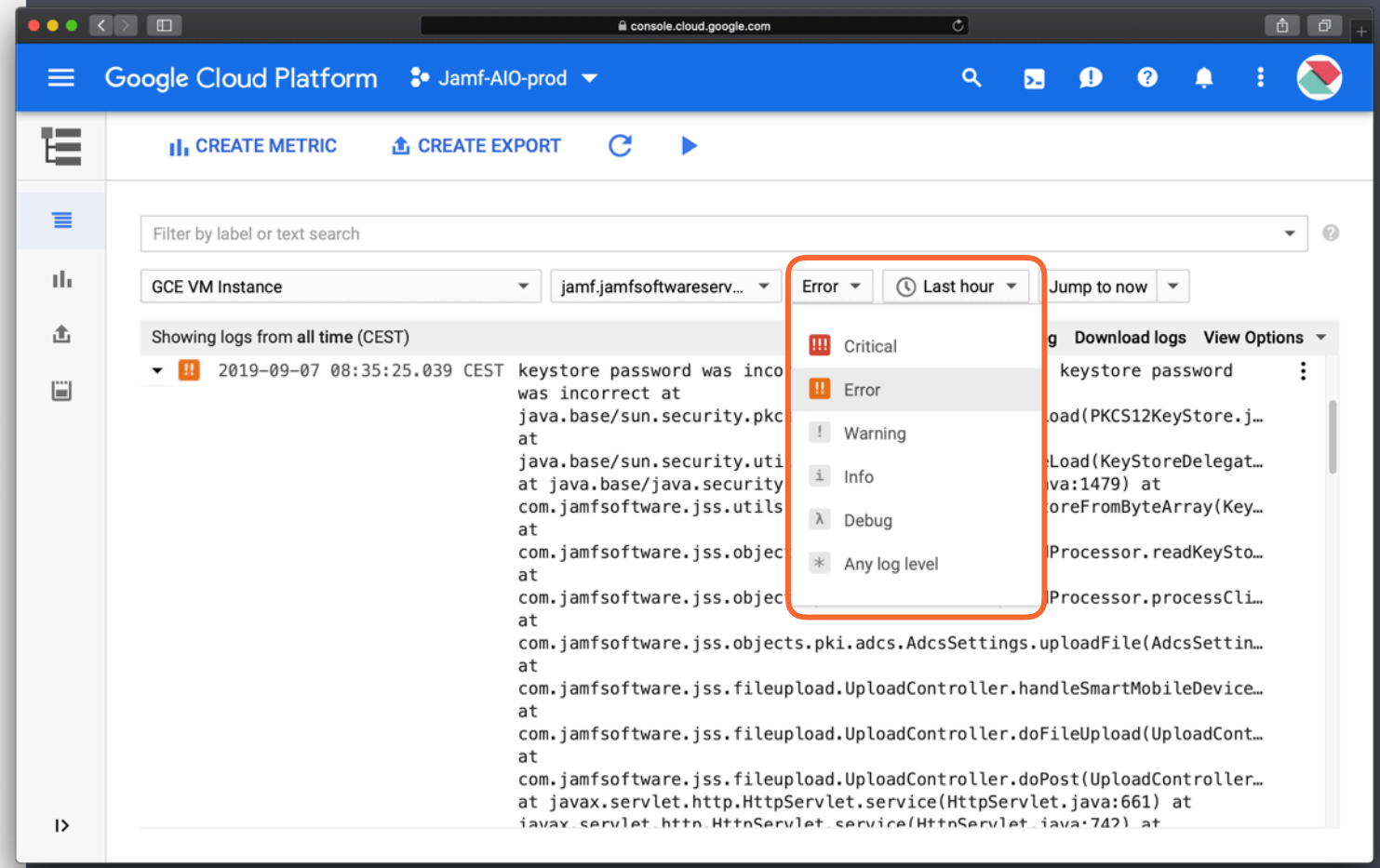
- Log Facilities
  - Stackdriver Logging



Ship and collect the events

Existing Solutions

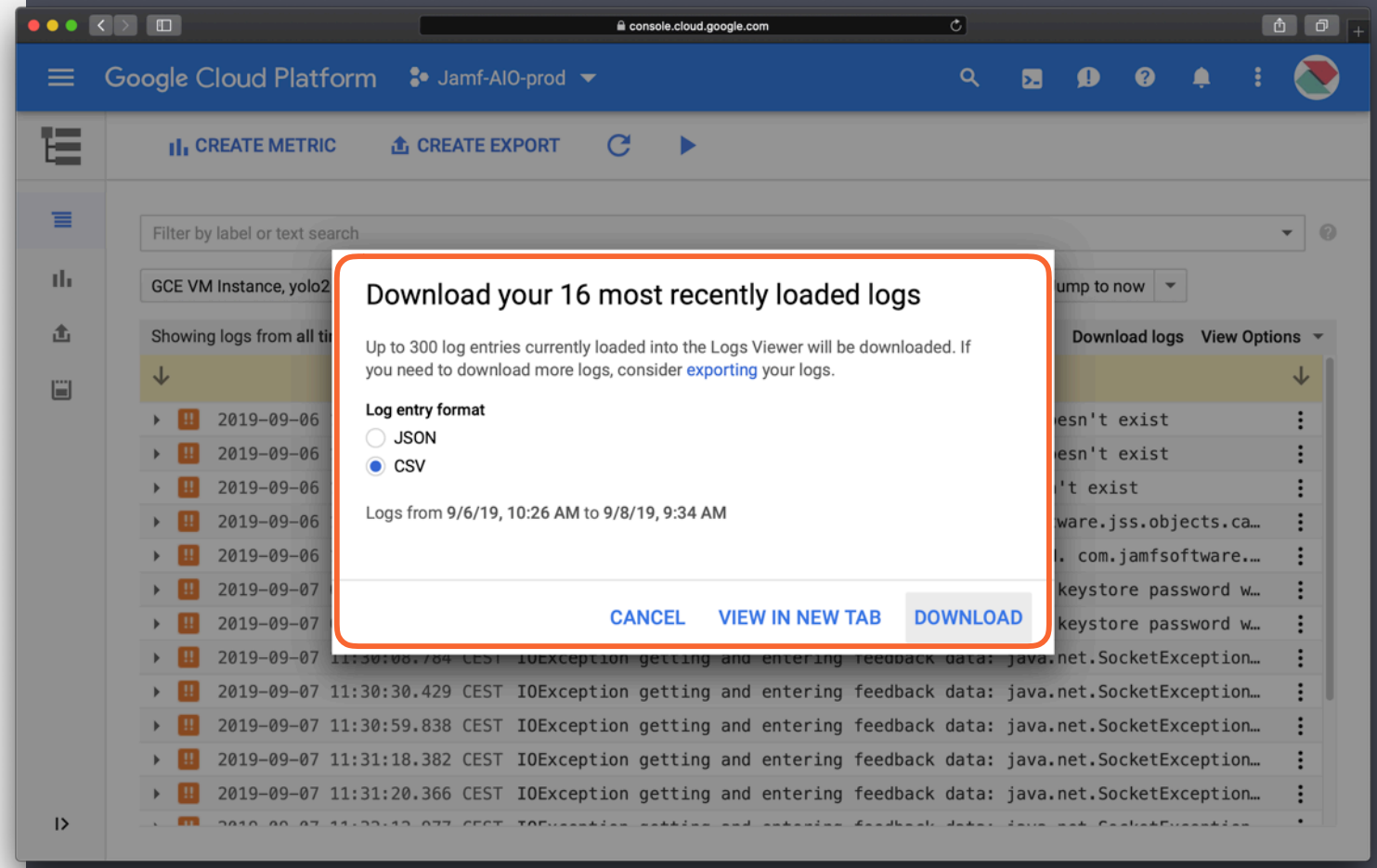
- Log Facilities
  - Stackdriver Logging



Ship and collect the events

Existing Solutions

- Log Facilities
  - Stackdriver Logging



Ship and collect the events

How to connect the sources

- Endpoints

- Collect file based logs *(by agents)*
- Run agents directly
- RPC / HTTPS Osquery events to Kolide or similar services
- Unified logging to Elastic Stack on Mac endpoints *(i.e. Filebeat)*

Ship and collect the events

How to connect the sources

- Endpoints
  - Agents

    FileBeat

FileBeat (by Elastic)

- Read local file based logs
  - Build-in Modules
- Pre-filter, Normalize events
- Ship to Elastic Stack *(Kibana, Logstash)*

Based on

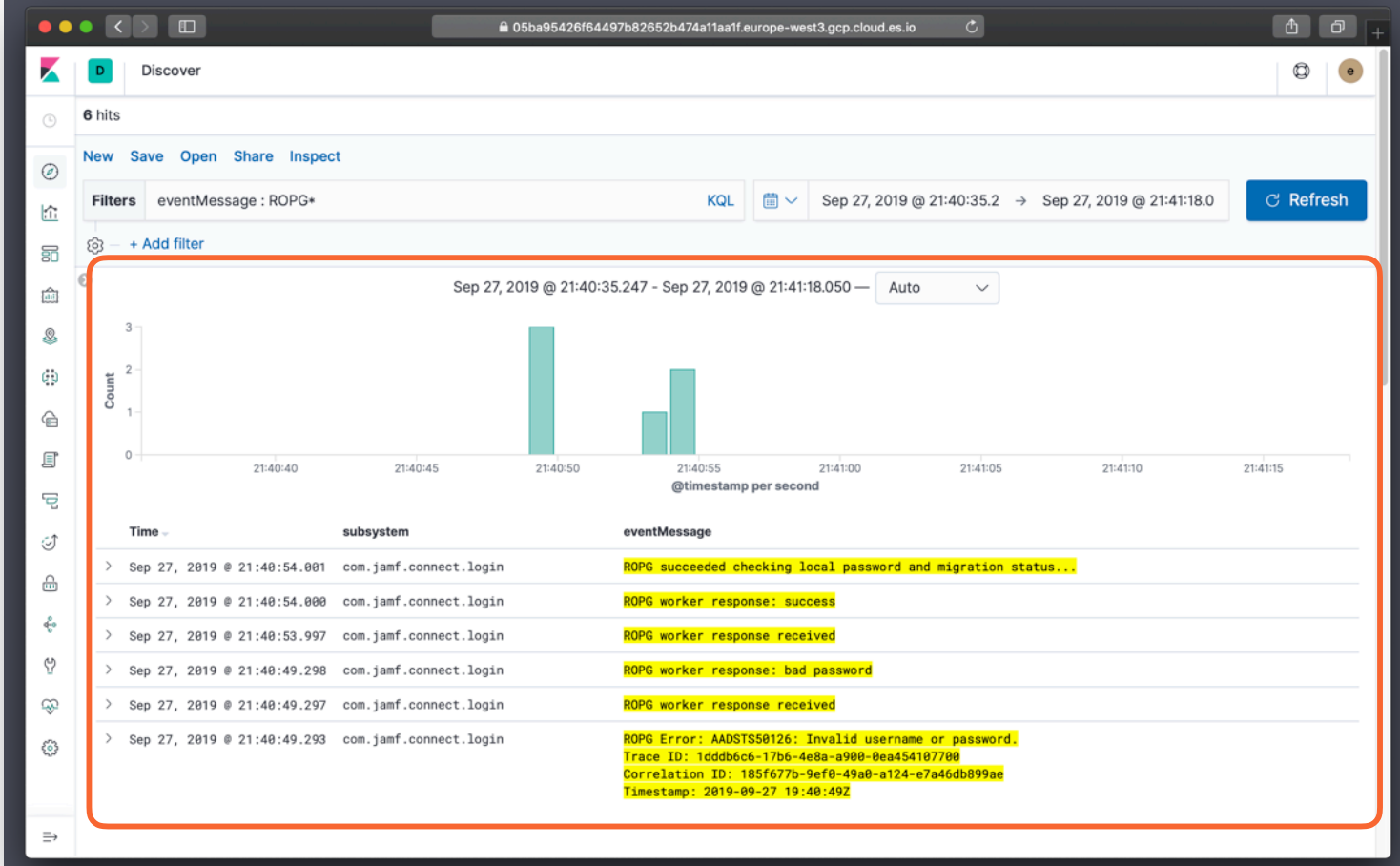
- Open source code - Beats family
- Elastic core component
- `filebeat.yml` config file

Ship and collect the events

How to connect the sources

- Endpoints
  - Agents

    Endpoint logs to ElasticStack



Subsystem shipped to Elastic Stack

Ship and collect the events

How to connect the sources

- Server / Cloud

- Internal routing
  (Azure AD monitoring to Azure Sentinel)
- Interconnect Services with Message Brokers *(Azure Event Hubs connect to Sumo Logic)*
- Webhooks to push event data
  (Jamf, SimpleMDM)
- API pulling data
  (Custom Apps for Reporting, Dashboards)

Ship and collect the events

How to connect the sources

- Dedicated Event Hub
  Zentral
  (Open Source)

zentral

- Productive and Research Platform
- Collect Events in parallel
  - Inventory *(Jamf, Intune, Munki, et.all…)*
  - Identity Providers *(Okta, AzureAD)*
  - Endpoint Agents *(Santa, Osquery, Filebeat)*
- Normalize and attribute Event Data
- Historic Data stored in Elastic Search
- Connect with other Event Hubs
  (Azure Event Hub, SIEM Systems)

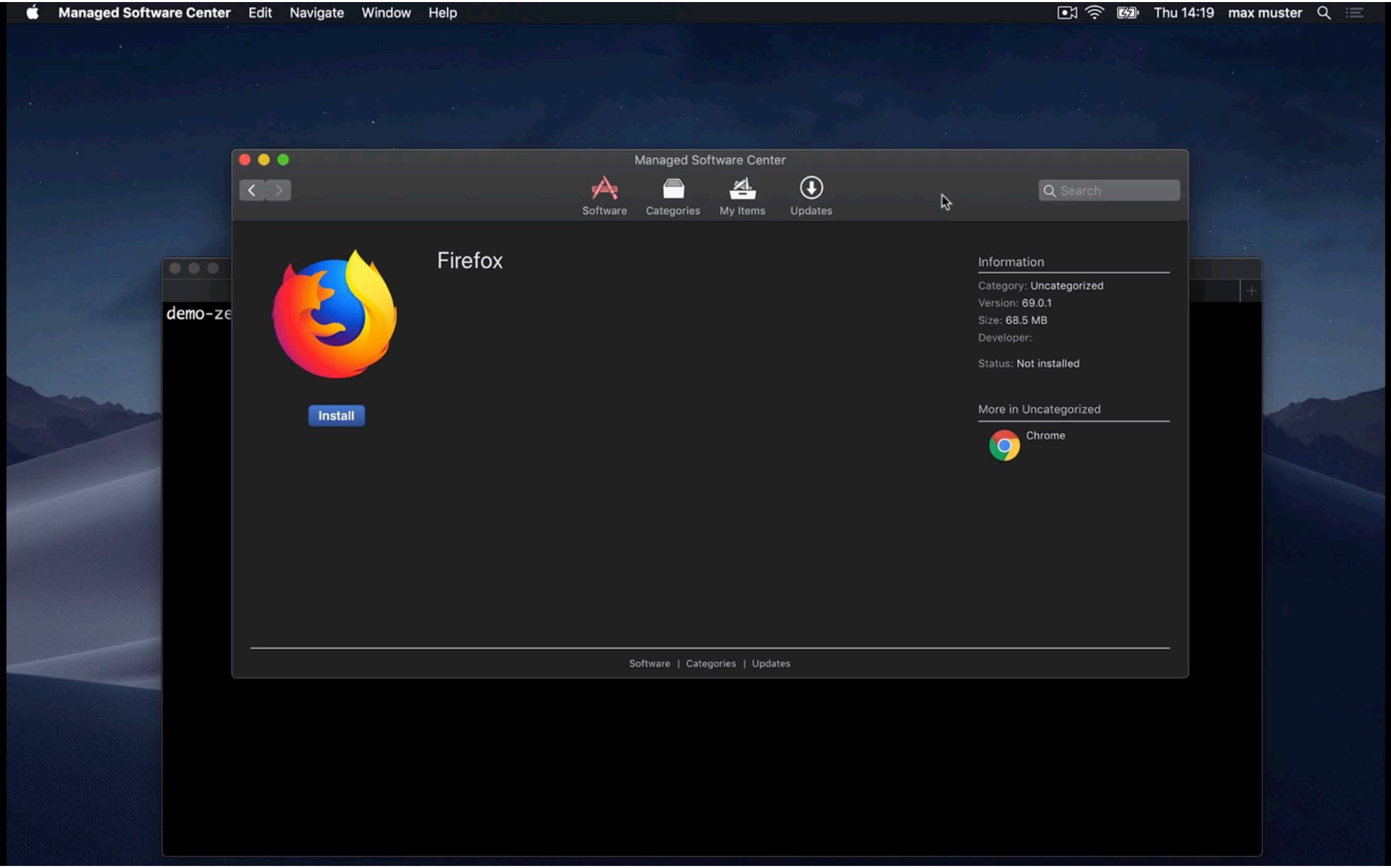
Ship and collect the events

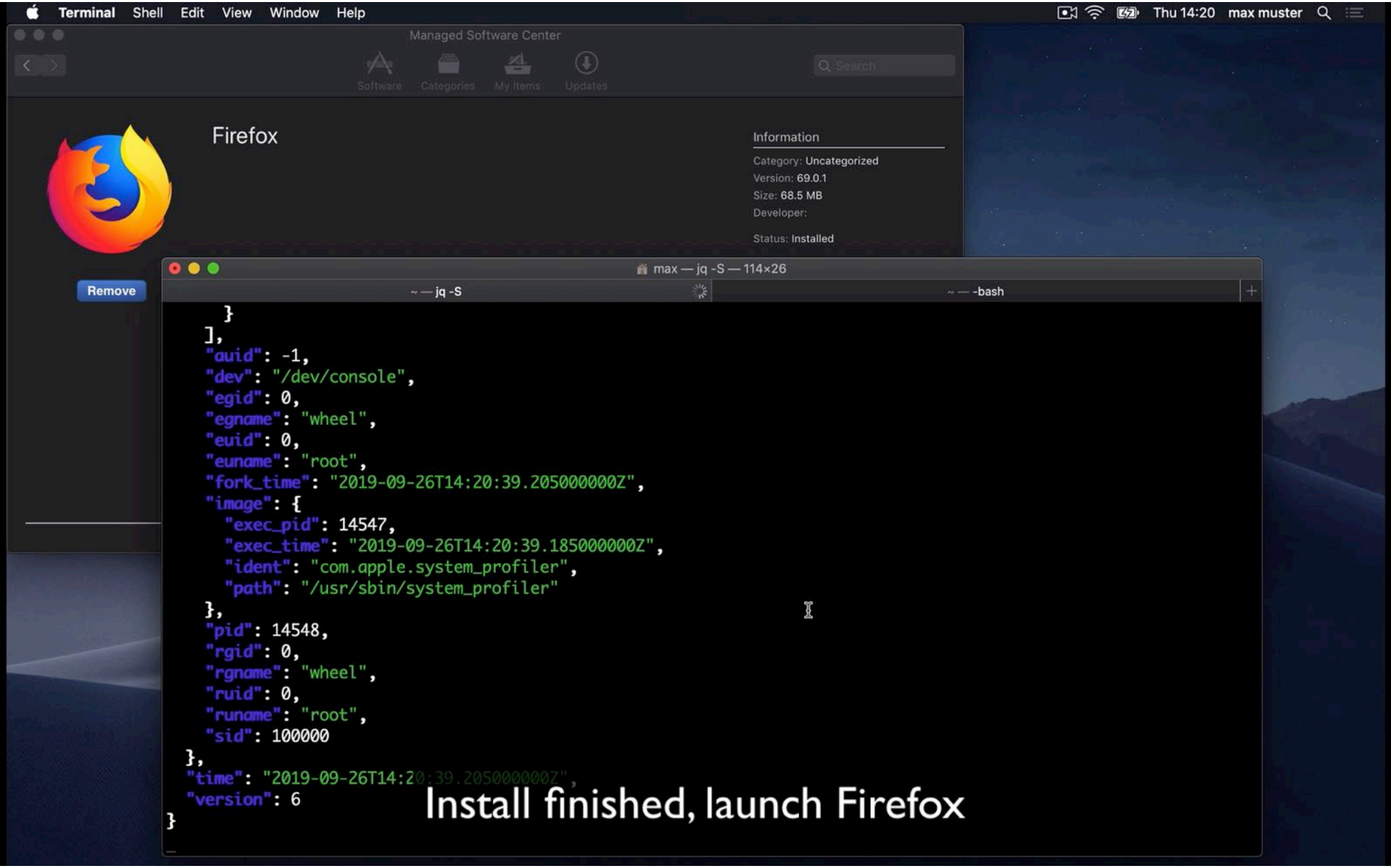
How to connect the sources

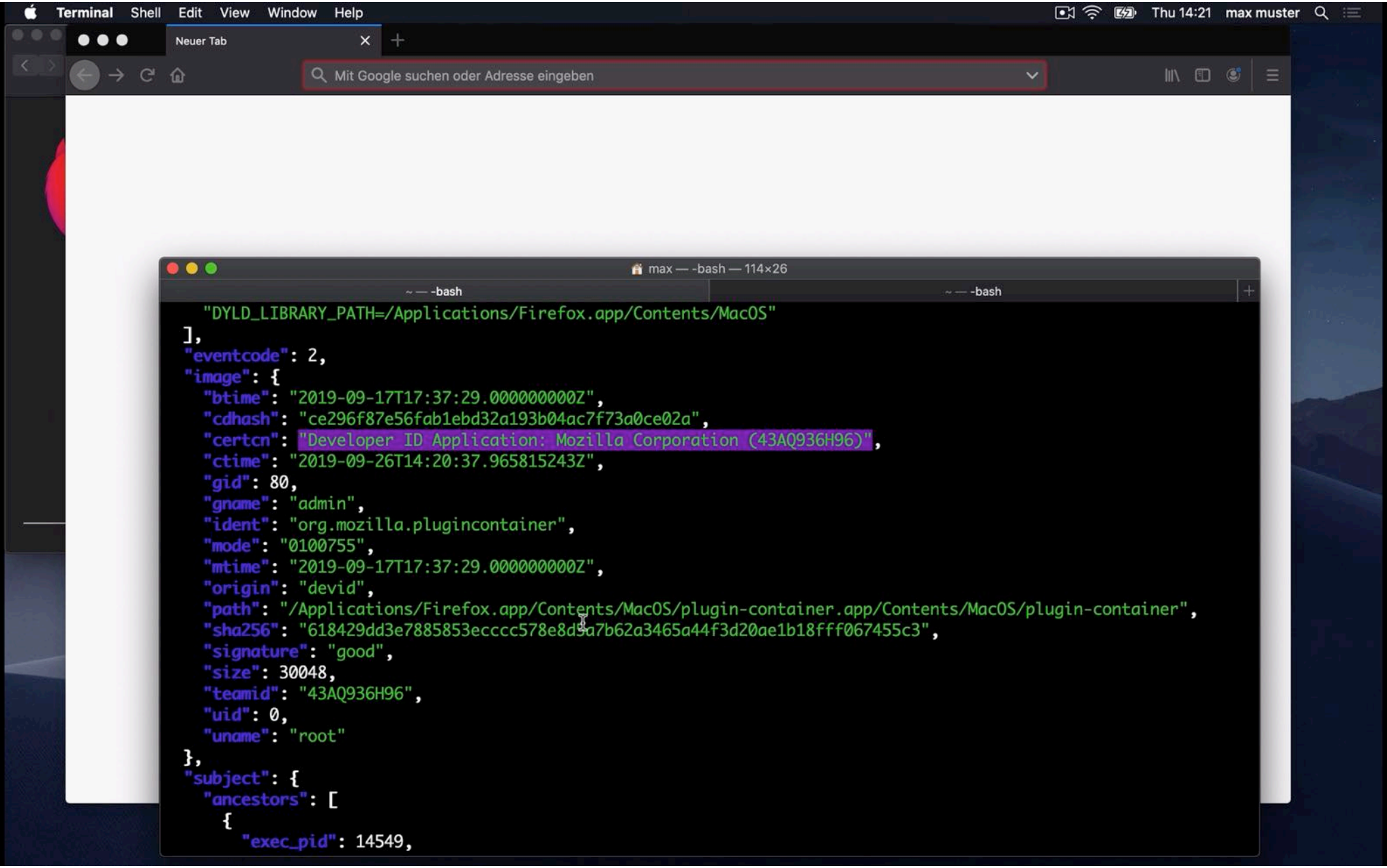
- Demo 1
  Binary Auditing

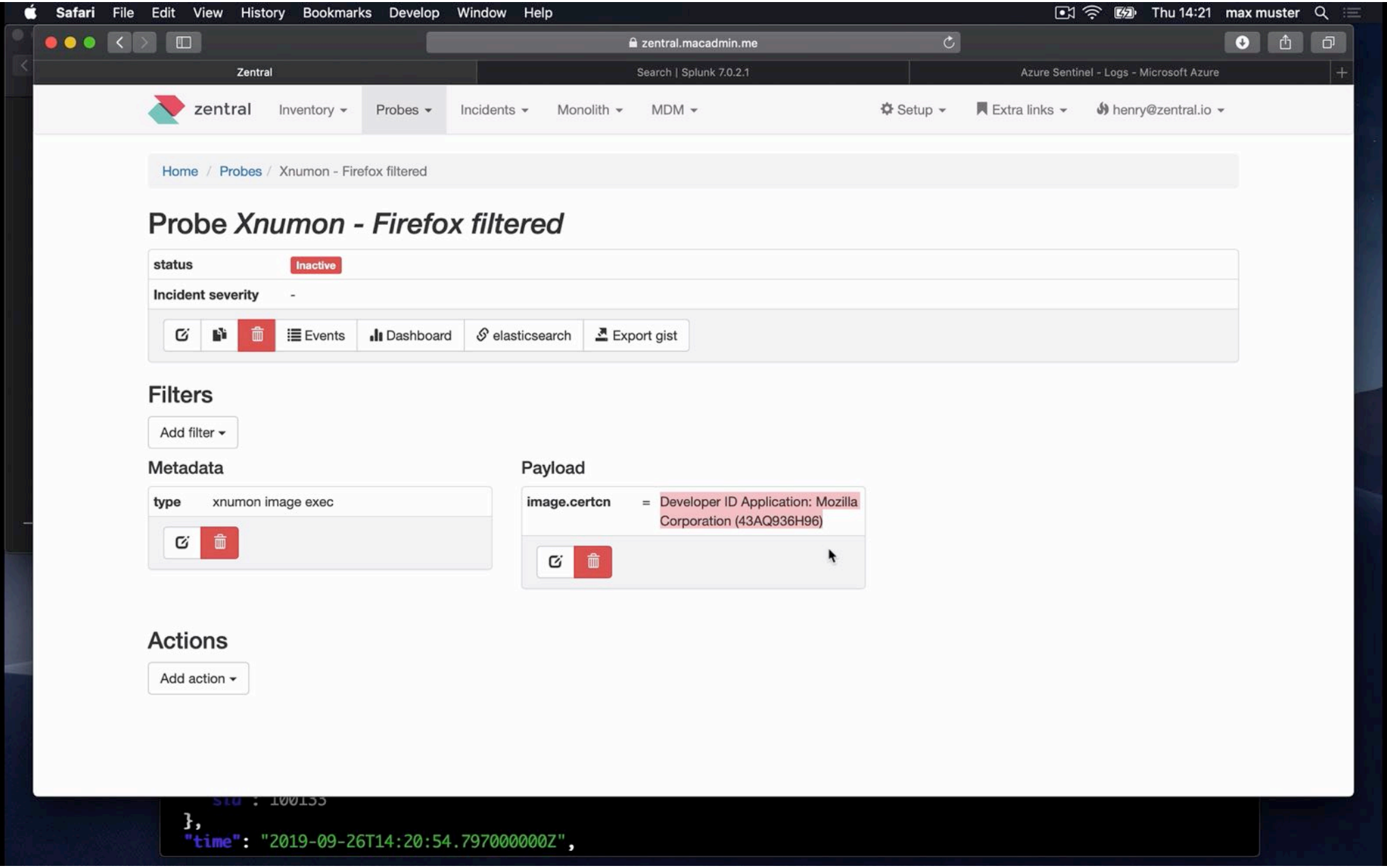
DEMO #1

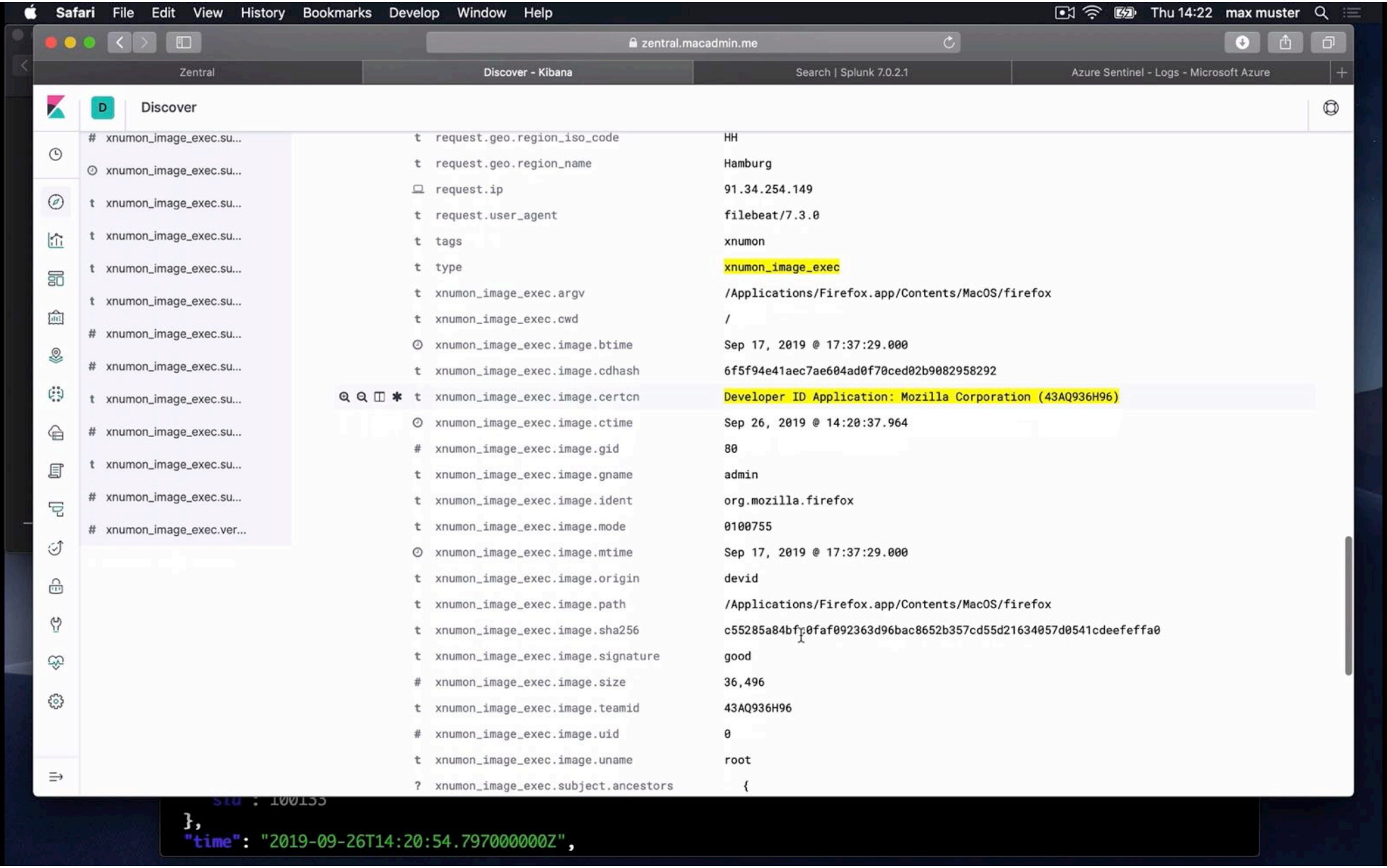
- Binary Auditing with Xnumon
- Inspect a Software install and launch
- Look into the local log file *(JSON)*
  - See process logs, with SHA-256 and code sigining informtation
- Ship the logs to Elastic Stack *(w/ FileBeat)*
- Run a quick filtering in Zentral
- See filtered Events in Kibana UI

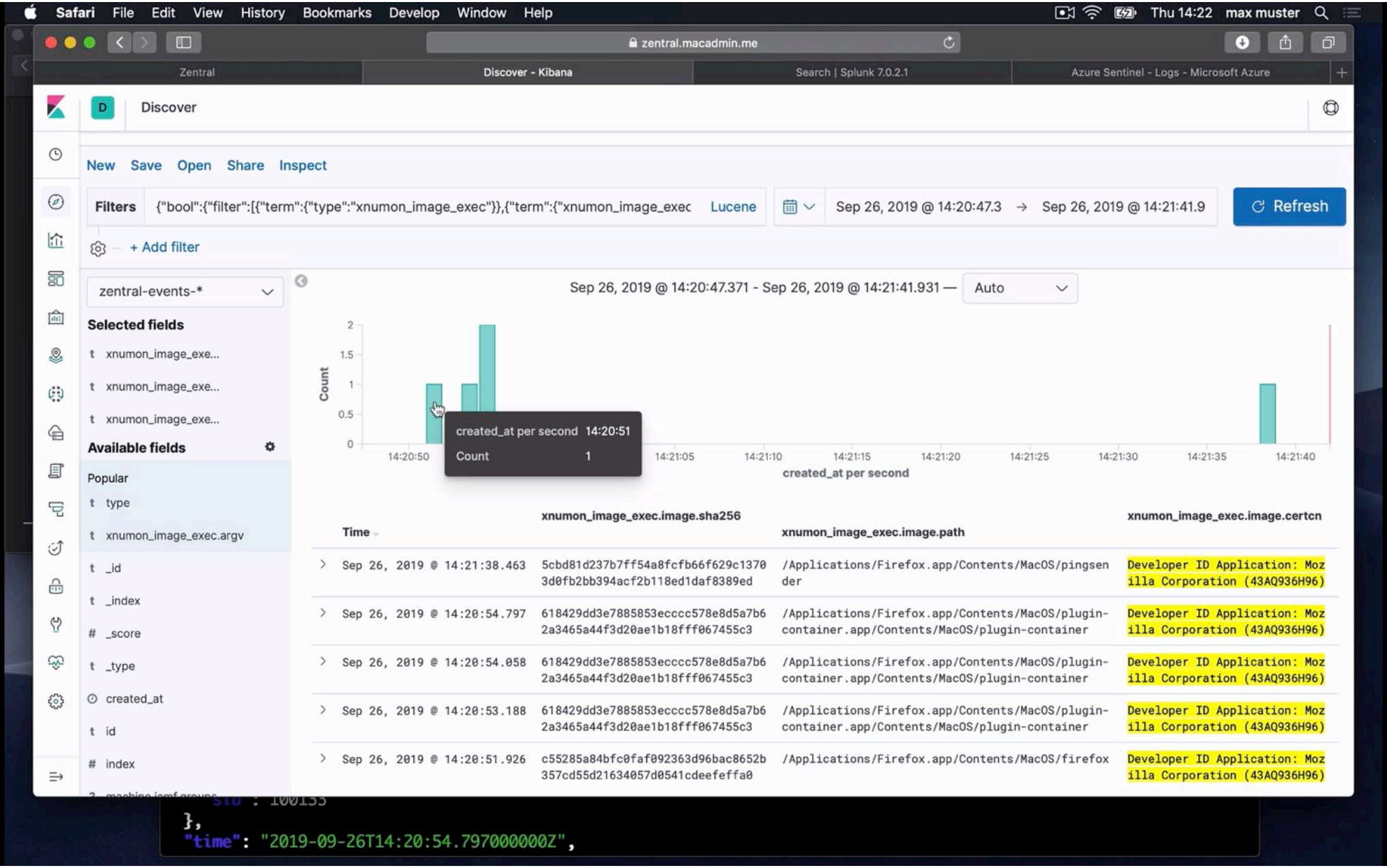

Managed Software Center Edit Navigate Window Help
Thu 14:19 max muster
Managed Software Center
Software
Categories
My Items
Updates
Search
Firefox
Install
Information
Category: Uncategorized
Version: 69.0.1
Size: 68.5 MB
Developer:
Status: Not installed
More in Uncategorized
Chrome
Software | Categories | Updates


Terminal Shell Edit View Window Help
Thu 14:20 max muster
Managed Software Center
Software Categories My Items Updates
Search
Firefox
Information
Category: Uncategorized
Version: 69.0.1
Size: 68.5 MB
Developer:
Status: Installed
Remove
max — jq -S — 114×26
~ — jq -S
~ — -bash
}
],
"auid": -1,
"dev": "/dev/console",
"egid": 0,
"egname": "wheel",
"euid": 0,
"euname": "root",
"fork_time": "2019-09-26T14:20:39.205000000Z",
"image": {
"exec_pid": 14547,
"exec_time": "2019-09-26T14:20:39.185000000Z",
"ident": "com.apple.system_profiler",
"path": "/usr/sbin/system_profiler"
},
"pid": 14548,
"rgid": 0,
"rgname": "wheel",
"ruid": 0,
"runame": "root",
"sid": 100000
},
"time": "2019-09-26T14:20:39.205000000Z",
"version": 6
}
Install finished, launch Firefox


Terminal Shell Edit View Window Help
Thu 14:21 max muster
Neuer Tab
Mit Google suchen oder Adresse eingeben
max — -bash — 114×26
~ — -bash
~ — -bash
"DYLD_LIBRARY_PATH=/Applications/Firefox.app/Contents/MacOS"
],
"eventcode": 2,
"image": {
"btime": "2019-09-17T17:37:29.000000000Z",
"cdhash": "ce296f87e56fab1ebd32a193b04ac7f73a0ce02a",
"certcn": "Developer ID Application: Mozilla Corporation (43AQ936H96)",
"ctime": "2019-09-26T14:20:37.965815243Z",
"gid": 80,
"gname": "admin",
"ident": "org.mozilla.plugincontainer",
"mode": "0100755",
"mtime": "2019-09-17T17:37:29.000000000Z",
"origin": "devid",
"path": "/Applications/Firefox.app/Contents/MacOS/plugin-container.app/Contents/MacOS/plugin-container",
"sha256": "618429dd3e7885853ecccc578e8d3a7b62a3465a44f3d20ae1b18fff067455c3",
"signature": "good",
"size": 30048,
"teamid": "43AQ936H96",
"uid": 0,
"uname": "root"
},
"subject": {
"ancestors": [
{
"exec_pid": 14549,


Safari File Edit View History Bookmarks Develop Window Help
Thu 14:21 max muster
zentral.macadmin.me
Zentral
Search | Splunk 7.0.2.1
Azure Sentinel - Logs - Microsoft Azure
zentral
Inventory
Probes
Incidents
Monolith
MDM
Setup
Extra links
henry@zentral.io
Home / Probes / Xnumon - Firefox filtered
Probe Xnumon - Firefox filtered
status
Inactive
Incident severity
-
Events
Dashboard
elasticsearch
Export gist
Filters
Add filter
Metadata
type
xnumon image exec
Payload
image.certcn
=
Developer ID Application: Mozilla Corporation (43AQ936H96)
Actions
Add action
"time": "2019-09-26T14:20:54.797000000Z",


Safari File Edit View History Bookmarks Develop Window Help
Thu 14:22 max muster
zentral.macadmin.me
Zentral
Discover - Kibana
Search | Splunk 7.0.2.1
Azure Sentinel - Logs - Microsoft Azure
Discover
request.geo.region_iso_code HH
request.geo.region_name Hamburg
request.ip 91.34.254.149
request.user_agent filebeat/7.3.0
tags xnumon
type xnumon_image_exec
xnumon_image_exec.argv /Applications/Firefox.app/Contents/MacOS/firefox
xnumon_image_exec.cwd /
xnumon_image_exec.image.btime Sep 17, 2019 @ 17:37:29.000
xnumon_image_exec.image.cdhash 6f5f94e41aec7ae604ad0f70ced02b9082958292
xnumon_image_exec.image.certcn Developer ID Application: Mozilla Corporation (43AQ936H96)
xnumon_image_exec.image.ctime Sep 26, 2019 @ 14:20:37.964
xnumon_image_exec.image.gid 80
xnumon_image_exec.image.gname admin
xnumon_image_exec.image.ident org.mozilla.firefox
xnumon_image_exec.image.mode 0100755
xnumon_image_exec.image.mtime Sep 17, 2019 @ 17:37:29.000
xnumon_image_exec.image.origin devid
xnumon_image_exec.image.path /Applications/Firefox.app/Contents/MacOS/firefox
xnumon_image_exec.image.sha256 c55285a84bf0faf092363d96bac8652b357cd55d21634057d0541cdeefeffa0
xnumon_image_exec.image.signature good
xnumon_image_exec.image.size 36,496
xnumon_image_exec.image.teamid 43AQ936H96
xnumon_image_exec.image.uid 0
xnumon_image_exec.image.uname root
xnumon_image_exec.subject.ancestors
"time": "2019-09-26T14:20:54.797000000Z",


Safari File Edit View History Bookmarks Develop Window Help
Thu 14:22 max muster
zentral.macadmin.me
Zentral
Discover - Kibana
Search | Splunk 7.0.2.1
Azure Sentinel - Logs - Microsoft Azure
Discover
New Save Open Share Inspect
Filters
{"bool":{"filter":[{"term":{"type":"xnumon_image_exec"}},{"term":{"xnumon_image_exec
Lucene
Sep 26, 2019 @ 14:20:47.3 → Sep 26, 2019 @ 14:21:41.9
Refresh
+ Add filter
zentral-events-*
Selected fields
t xnumon_image_exe...
t xnumon_image_exe...
t xnumon_image_exe...
Available fields
Popular
t type
t xnumon_image_exec.argv
t _id
t _index
_score
t _type
created_at
t id
index
Sep 26, 2019 @ 14:20:47.371 - Sep 26, 2019 @ 14:21:41.931 — Auto
Count
created_at per second 14:20:51
Count 1
created_at per second
Time
xnumon_image_exec.image.sha256
xnumon_image_exec.image.path
xnumon_image_exec.image.certcn
Sep 26, 2019 @ 14:21:38.463 5cbd81d237b7ff54a8fcfb66f629c13703d0fb2bb394acf2b118ed1daf8389ed /Applications/Firefox.app/Contents/MacOS/pingsender Developer ID Application: Mozilla Corporation (43AQ936H96)
Sep 26, 2019 @ 14:20:54.797 618429dd3e7885853ecccc578e8d5a7b62a3465a44f3d20ae1b18fff067455c3 /Applications/Firefox.app/Contents/MacOS/plugin-container.app/Contents/MacOS/plugin-container Developer ID Application: Mozilla Corporation (43AQ936H96)
Sep 26, 2019 @ 14:20:54.058 618429dd3e7885853ecccc578e8d5a7b62a3465a44f3d20ae1b18fff067455c3 /Applications/Firefox.app/Contents/MacOS/plugin-container.app/Contents/MacOS/plugin-container Developer ID Application: Mozilla Corporation (43AQ936H96)
Sep 26, 2019 @ 14:20:53.188 618429dd3e7885853ecccc578e8d5a7b62a3465a44f3d20ae1b18fff067455c3 /Applications/Firefox.app/Contents/MacOS/plugin-container.app/Contents/MacOS/plugin-container Developer ID Application: Mozilla Corporation (43AQ936H96)
Sep 26, 2019 @ 14:20:51.926 c55285a84bfc0faf092363d96bac8652b357cd55d21634057d0541cdeefeffa0 /Applications/Firefox.app/Contents/MacOS/firefox Developer ID Application: Mozilla Corporation (43AQ936H96)
},
"time": "2019-09-26T14:20:54.797000000Z",

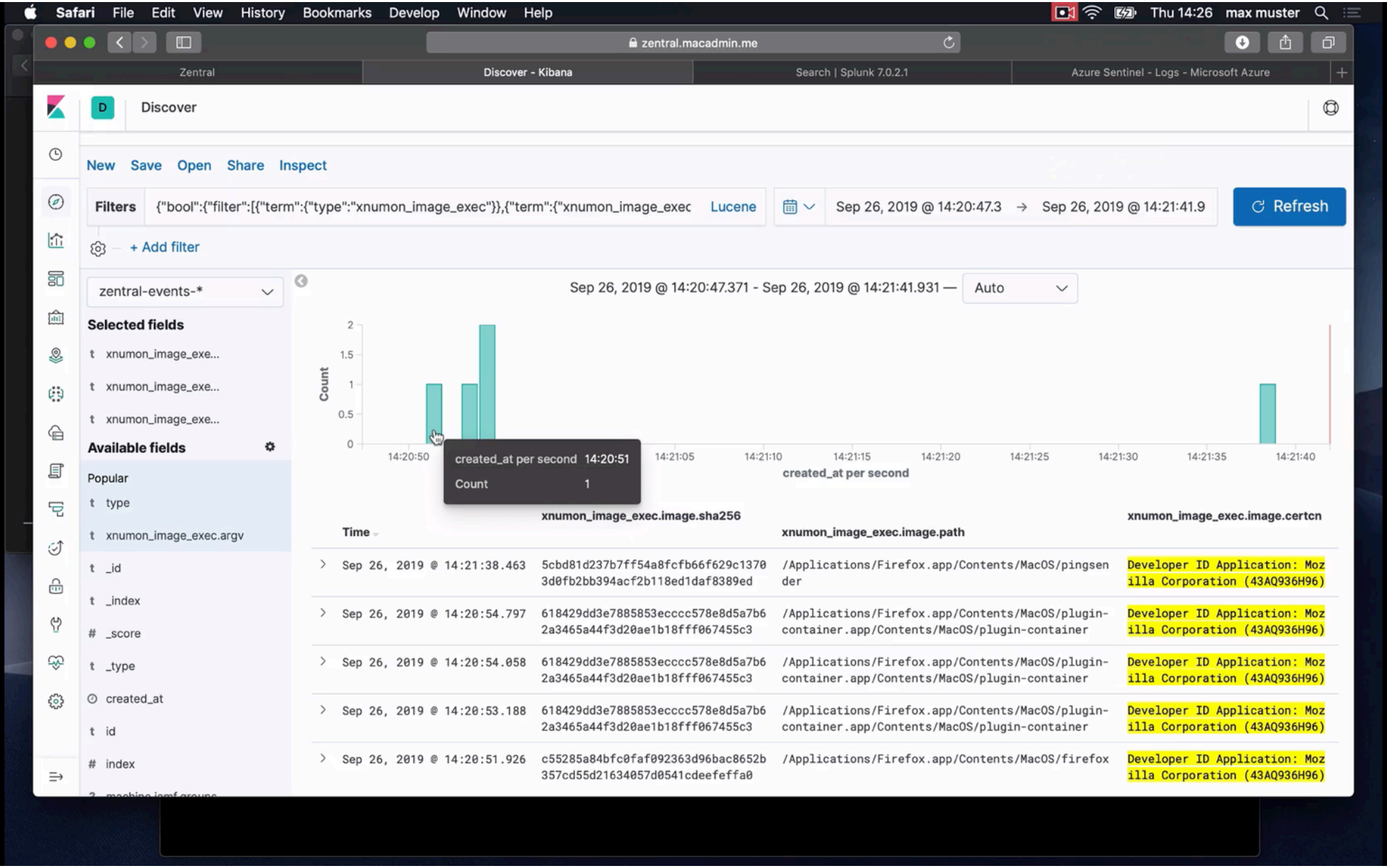
Ship and collect the events

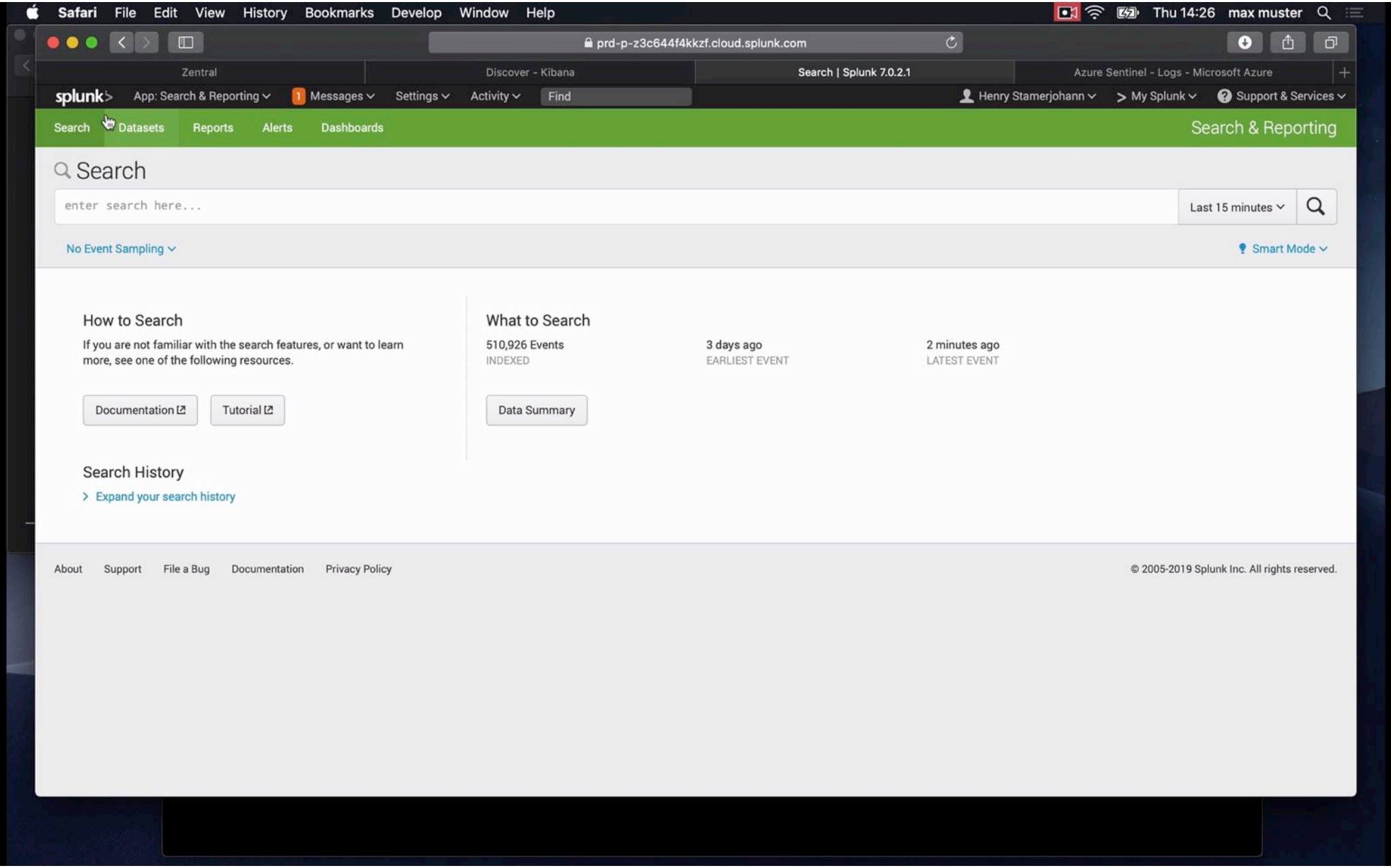
How to connect the sources

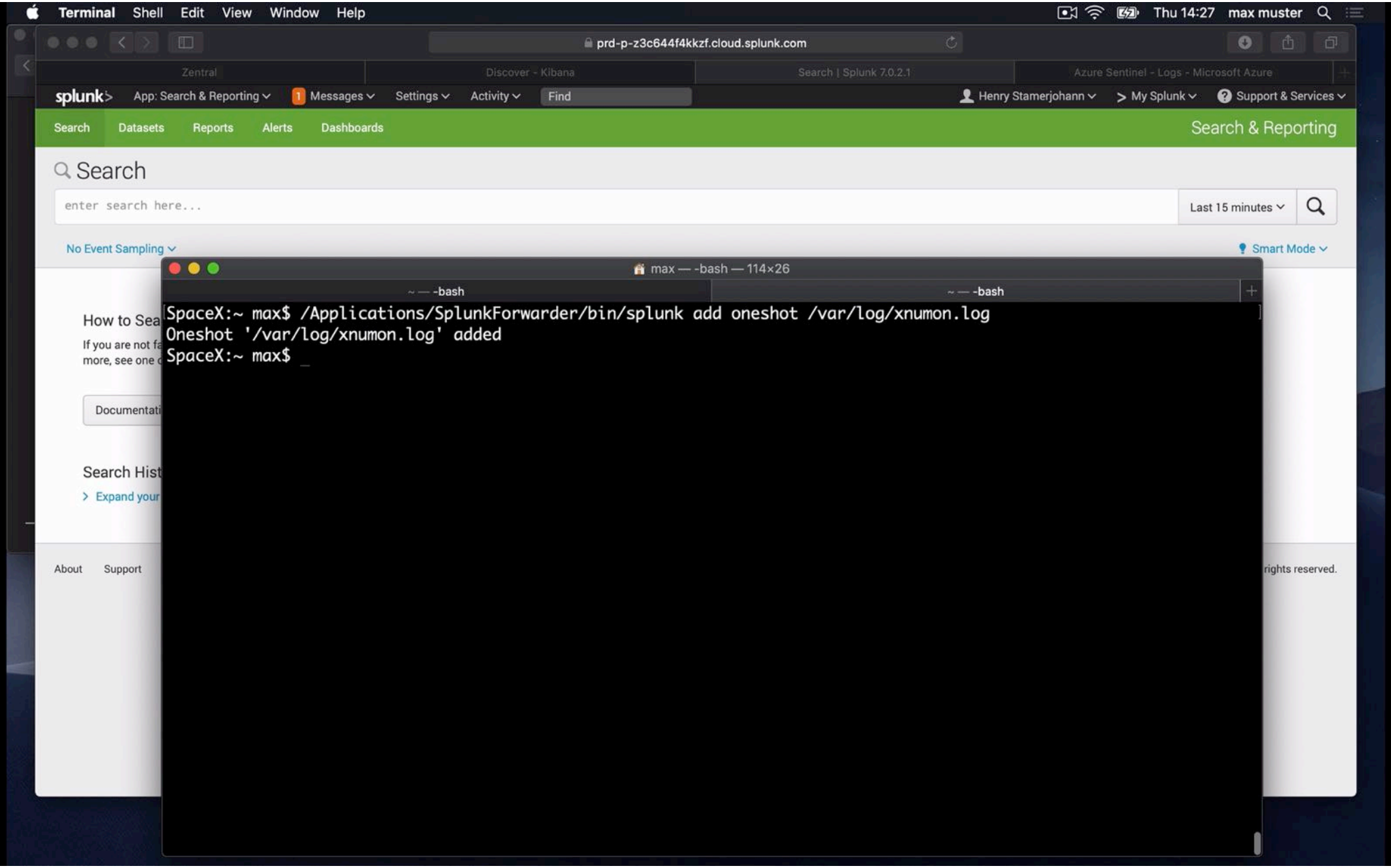
- Demo 2
  Binary Auditing

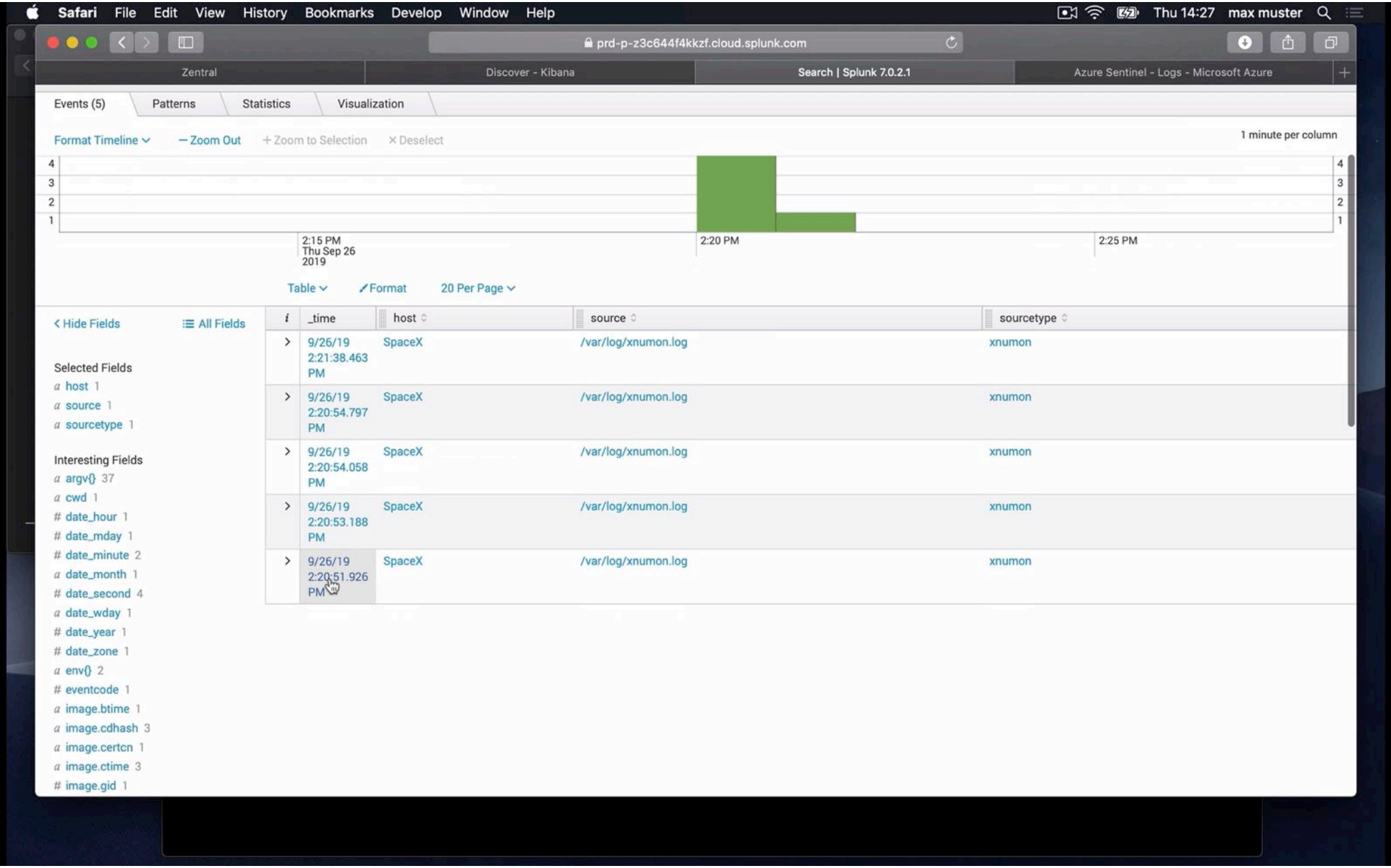
DEMO #2

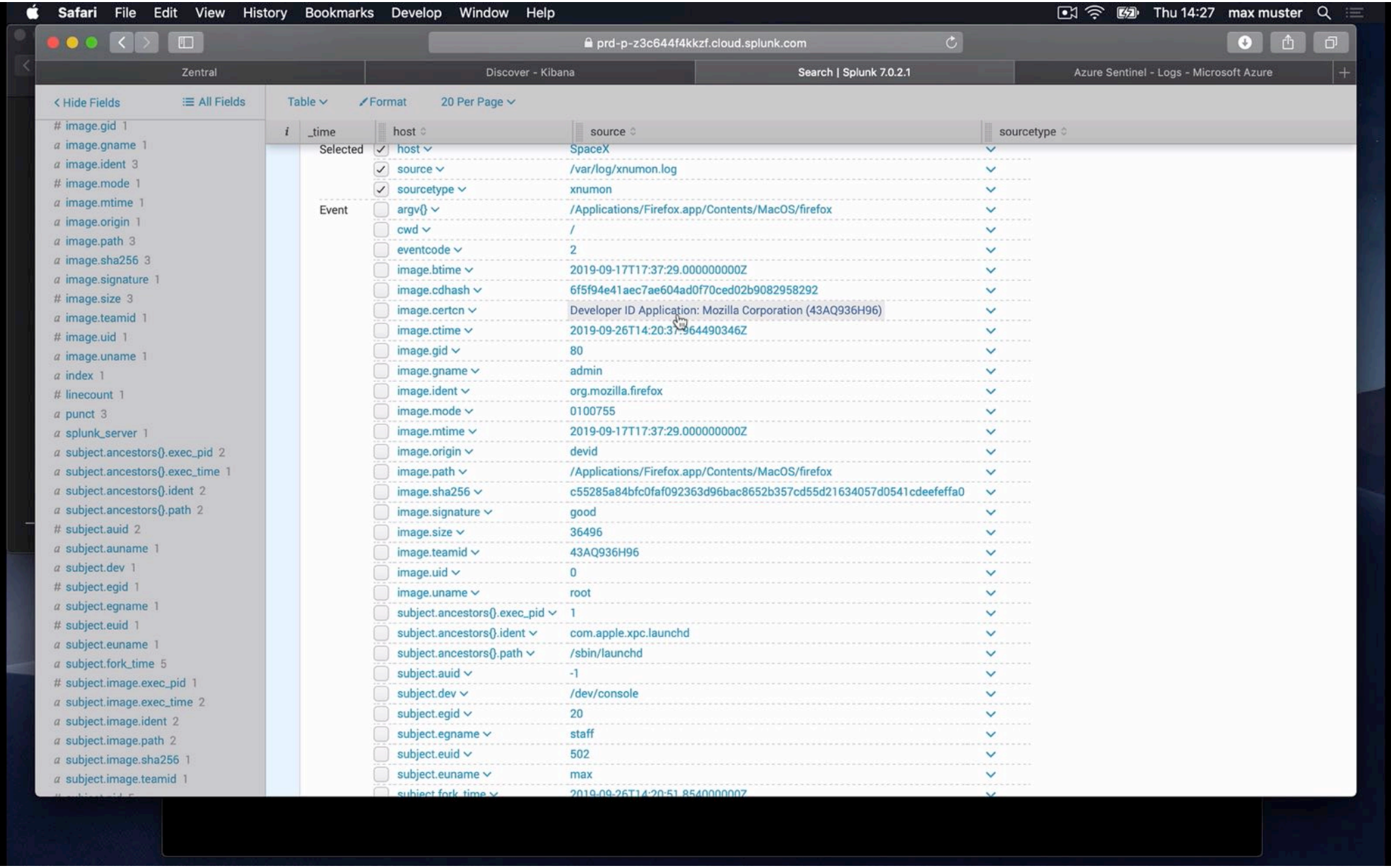
- Ship same log to a commercial SaaS
- Look into events in the SaaS
- Next level - interconnecting
  Event Hubs and normalized event stream
- See Events filtered in a SIEM
  (Security Incident Event Management)

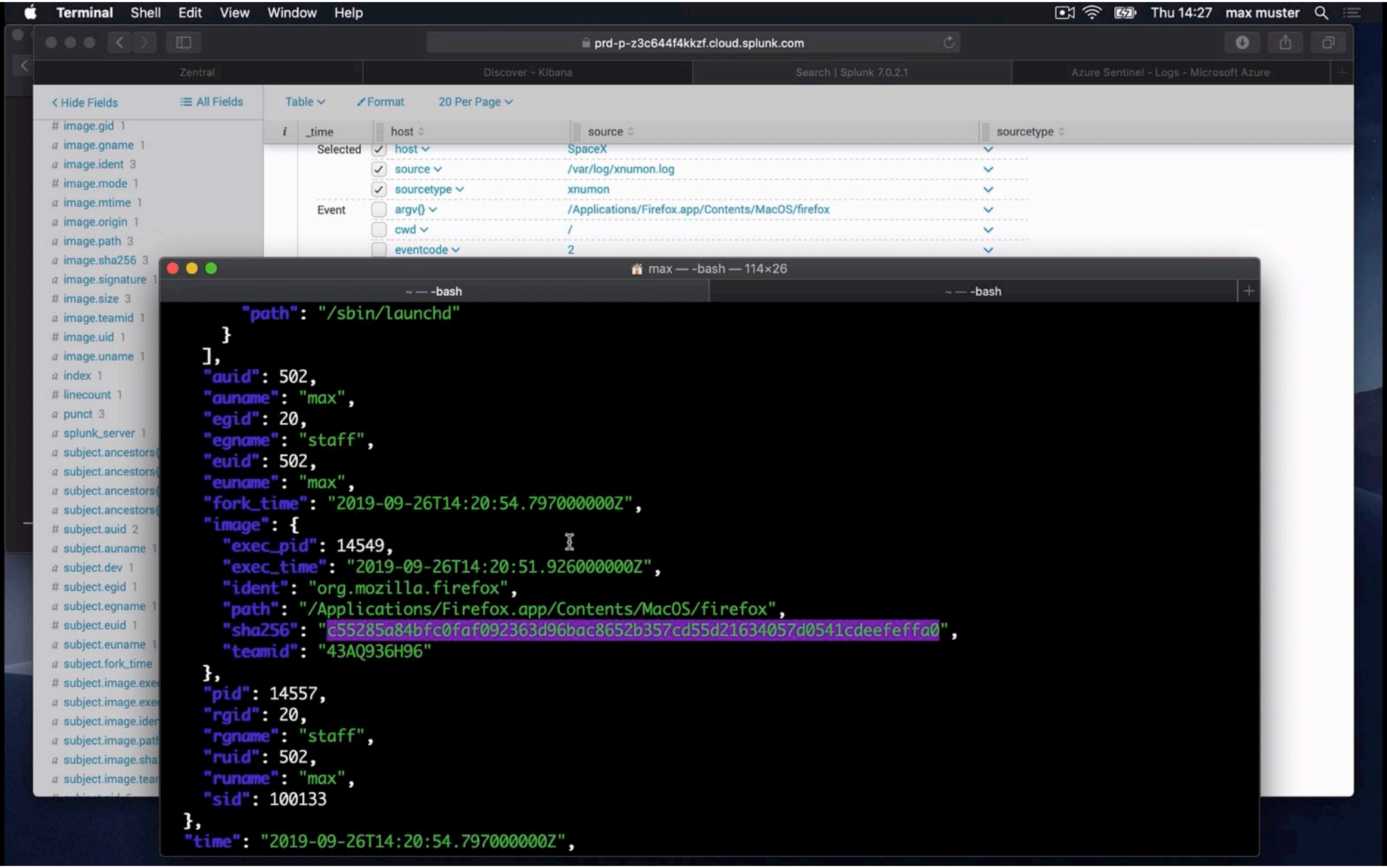

Safari File Edit View History Bookmarks Develop Window Help
Thu 14:26 max muster
zentral.macadmin.me
Zentral
Discover - Kibana
Search | Splunk 7.0.2.1
Azure Sentinel - Logs - Microsoft Azure
Discover
New Save Open Share Inspect
Filters
{"bool":{"filter":[{"term":{"type":"xnumon_image_exec"}},{"term":{"xnumon_image_exec
Lucene
Sep 26, 2019 @ 14:20:47.3 → Sep 26, 2019 @ 14:21:41.9
Refresh
+ Add filter
zentral-events-*
Selected fields
t xnumon_image_exe...
t xnumon_image_exe...
t xnumon_image_exe...
Available fields
Popular
t type
t xnumon_image_exec.argv
t _id
t _index
_score
t _type
created_at
t id
index
Sep 26, 2019 @ 14:20:47.371 - Sep 26, 2019 @ 14:21:41.931 —
Auto
Count
created_at per second
created_at per second 14:20:51
Count 1
Time
xnumon_image_exec.image.sha256
xnumon_image_exec.image.path
xnumon_image_exec.image.certcn
Sep 26, 2019 @ 14:21:38.463 5cbd81d237b7ff54a8fcfb66f629c13703d0fb2bb394acf2b118ed1daf8389ed /Applications/Firefox.app/Contents/MacOS/pingsender Developer ID Application: Mozilla Corporation (43AQ936H96)
Sep 26, 2019 @ 14:20:54.797 618429dd3e7885853ecccc578e8d5a7b62a3465a44f3d20ae1b18fff067455c3 /Applications/Firefox.app/Contents/MacOS/plugin-container.app/Contents/MacOS/plugin-container Developer ID Application: Mozilla Corporation (43AQ936H96)
Sep 26, 2019 @ 14:20:54.058 618429dd3e7885853ecccc578e8d5a7b62a3465a44f3d20ae1b18fff067455c3 /Applications/Firefox.app/Contents/MacOS/plugin-container.app/Contents/MacOS/plugin-container Developer ID Application: Mozilla Corporation (43AQ936H96)
Sep 26, 2019 @ 14:20:53.188 618429dd3e7885853ecccc578e8d5a7b62a3465a44f3d20ae1b18fff067455c3 /Applications/Firefox.app/Contents/MacOS/plugin-container.app/Contents/MacOS/plugin-container Developer ID Application: Mozilla Corporation (43AQ936H96)
Sep 26, 2019 @ 14:20:51.926 c55285a84bfc0faf092363d96bac8652b357cd55d21634057d0541cdeefeffa0 /Applications/Firefox.app/Contents/MacOS/firefox Developer ID Application: Mozilla Corporation (43AQ936H96)

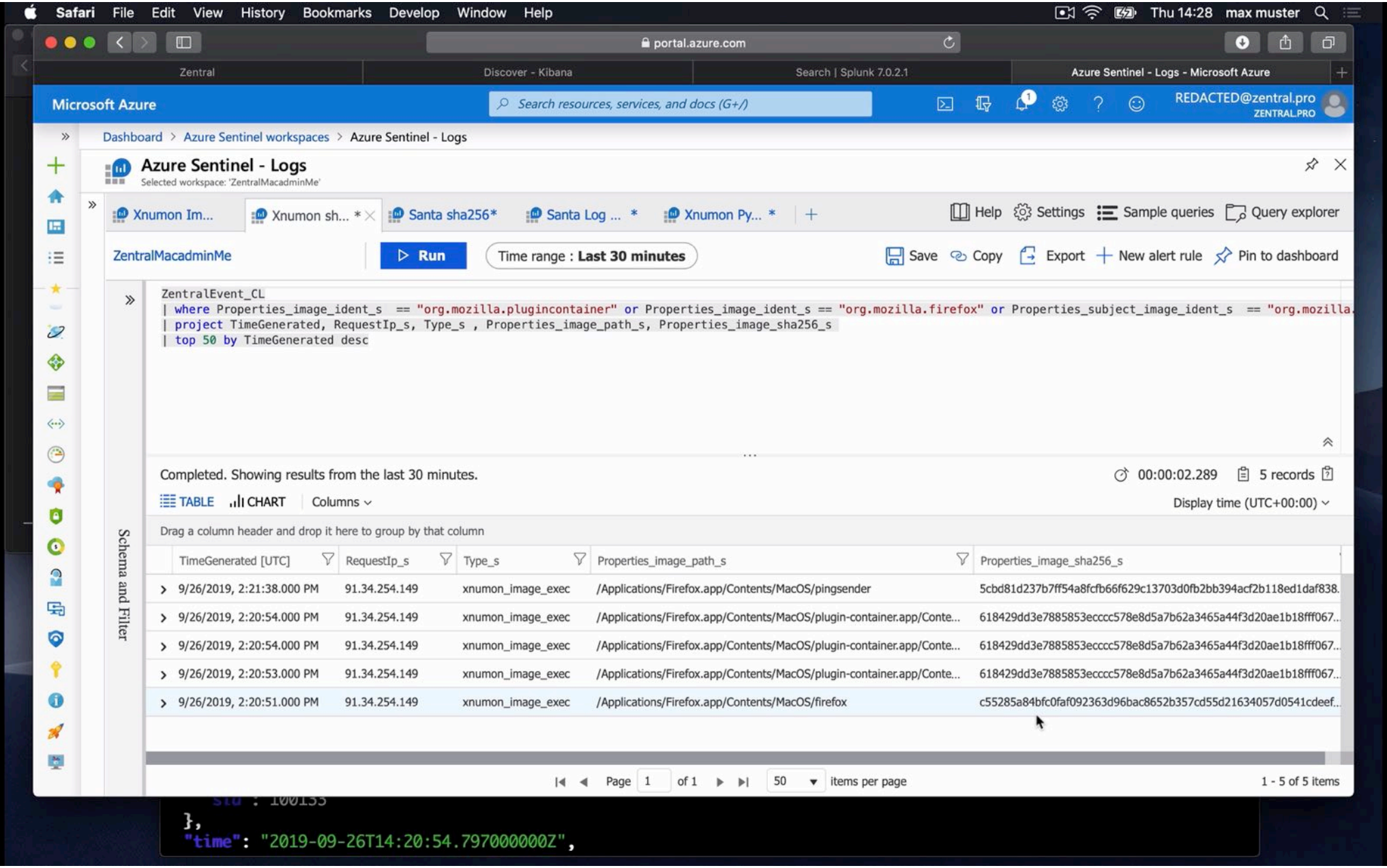

Safari File Edit View History Bookmarks Develop Window Help
Thu 14:26 max muster
prd-p-z3c644f4kkzf.cloud.splunk.com
Zentral
Discover - Kibana
Search | Splunk 7.0.2.1
Azure Sentinel - Logs - Microsoft Azure
splunk>
App: Search & Reporting
1 Messages
Settings
Activity
Find
Henry Stamerjohann
My Splunk
Support & Services
Search
Datasets
Reports
Alerts
Dashboards
Search & Reporting
Search
enter search here...
Last 15 minutes
No Event Sampling
Smart Mode
How to Search
If you are not familiar with the search features, or want to learn more, see one of the following resources.
Documentation
Tutorial
What to Search
510,926 Events
INDEXED
3 days ago
EARLIEST EVENT
2 minutes ago
LATEST EVENT
Data Summary
Search History
Expand your search history
About
Support
File a Bug
Documentation
Privacy Policy
© 2005-2019 Splunk Inc. All rights reserved.

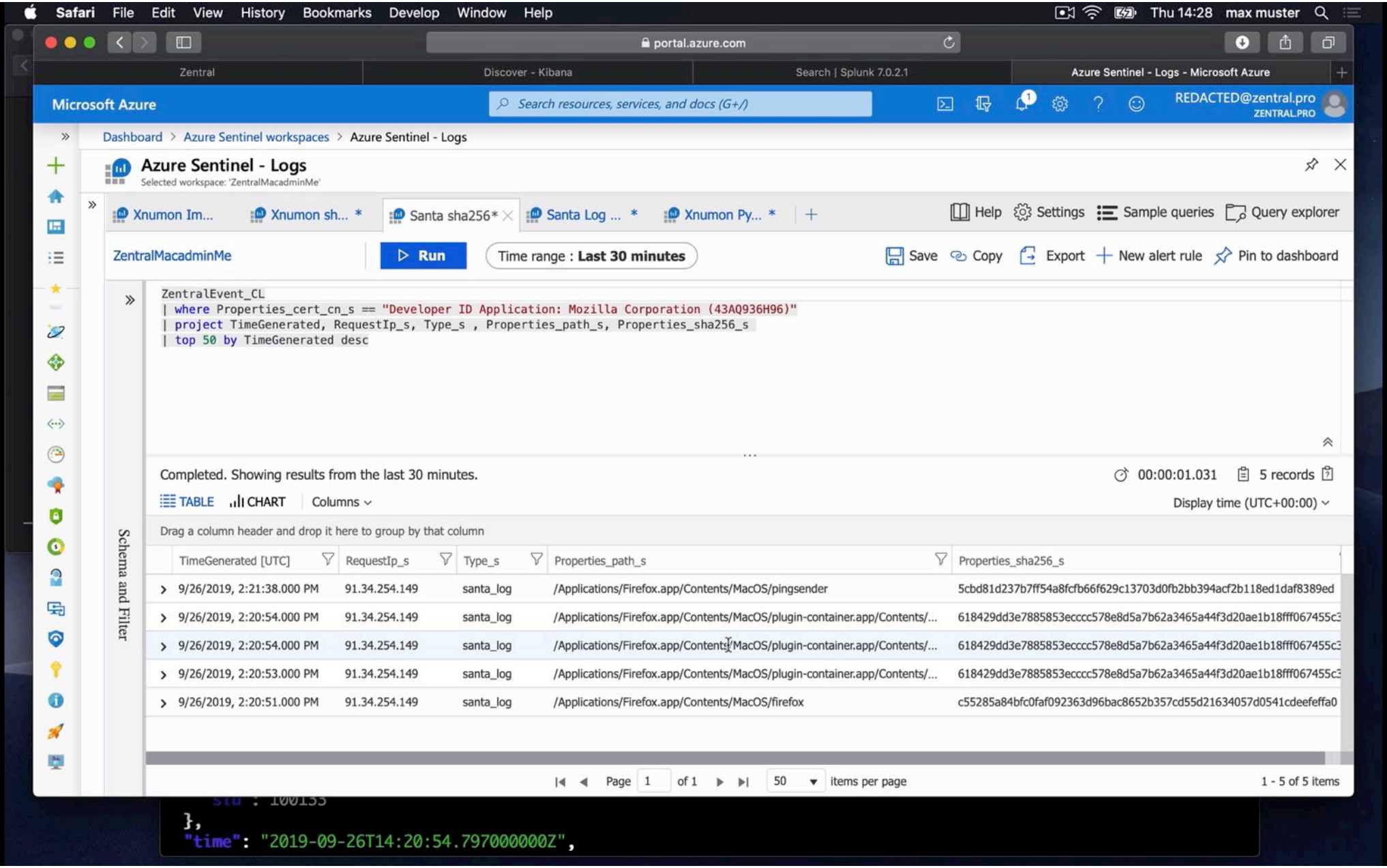

Terminal Shell Edit View Window Help
Thu 14:27 max muster
prd-p-z3c644f4kkzf.cloud.splunk.com
Zentral
Discover - Kibana
Search | Splunk 7.0.2.1
Azure Sentinel - Logs - Microsoft Azure
splunk> App: Search & Reporting Messages Settings Activity Find
Henry Stamerjohann My Splunk Support & Services
Search Datasets Reports Alerts Dashboards
Search & Reporting
Search
enter search here...
Last 15 minutes
No Event Sampling
Smart Mode
How to Sea
If you are not fa
more, see one
Documentati
Search Hist
Expand your
About Support
rights reserved.
max — -bash — 114×26
~ — -bash
~ — -bash
SpaceX:~ max$ /Applications/SplunkForwarder/bin/splunk add oneshot /var/log/xnumon.log
Oneshot '/var/log/xnumon.log' added
SpaceX:~ max$

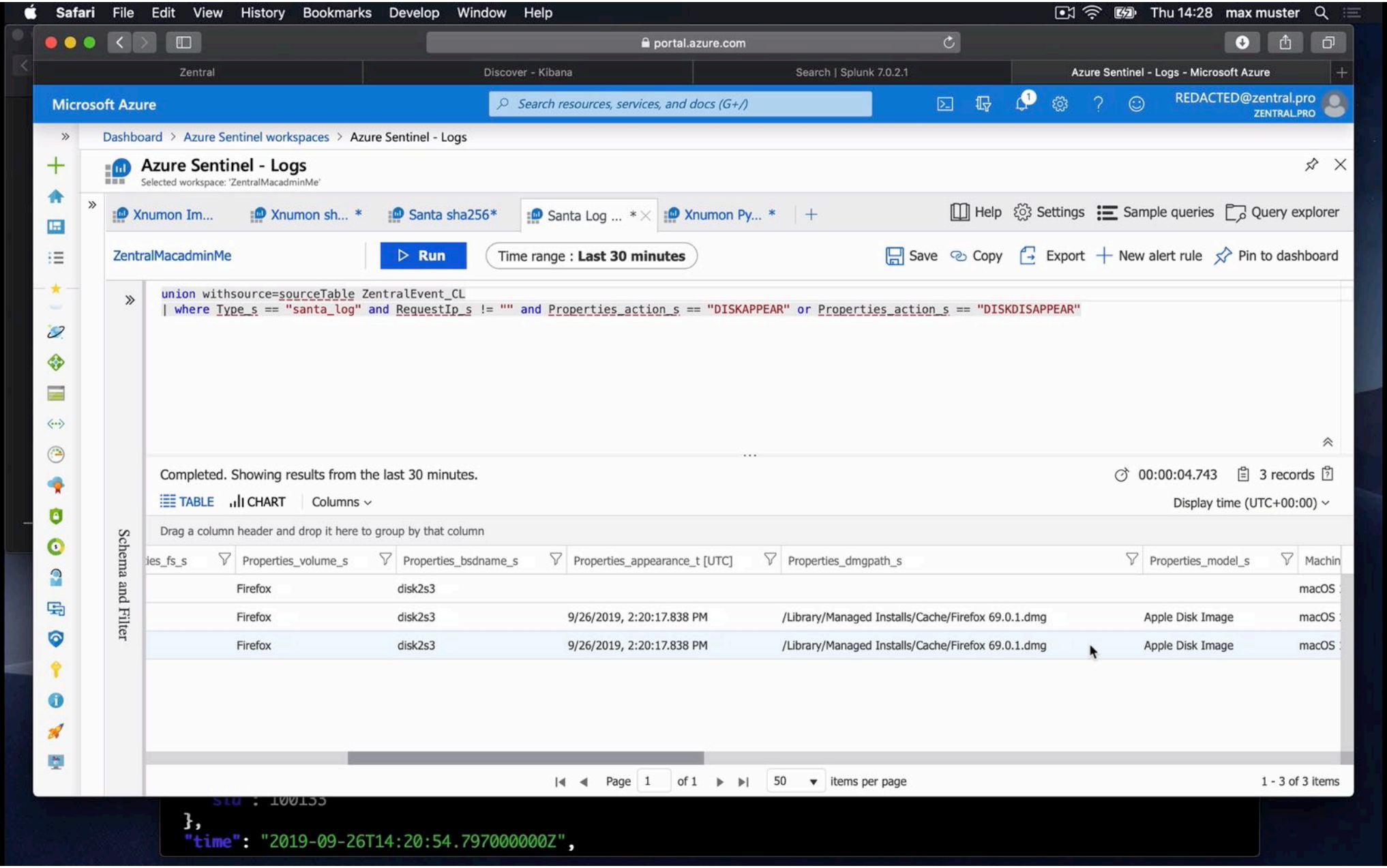

Safari File Edit View History Bookmarks Develop Window Help
Thu 14:27 max muster
prd-p-z3c644f4kkzf.cloud.splunk.com
Zentral
Discover - Kibana
Search | Splunk 7.0.2.1
Azure Sentinel - Logs - Microsoft Azure
Events (5)
Patterns
Statistics
Visualization
Format Timeline
Zoom Out
Zoom to Selection
Deselect
1 minute per column
2:15 PM Thu Sep 26 2019
2:20 PM
2:25 PM
Table
Format
20 Per Page
Hide Fields
All Fields
Selected Fields
host 1
source 1
sourcetype 1
Interesting Fields
argv{} 37
cwd 1
date_hour 1
date_mday 1
date_minute 2
date_month 1
date_second 4
date_wday 1
date_year 1
date_zone 1
env{} 2
eventcode 1
image.btime 1
image.cdhash 3
image.certcn 1
image.ctime 3
image.gid 1
i
_time
host
source
sourcetype
9/26/19 2:21:38.463 PM SpaceX /var/log/xnumon.log xnumon
9/26/19 2:20:54.797 PM SpaceX /var/log/xnumon.log xnumon
9/26/19 2:20:54.058 PM SpaceX /var/log/xnumon.log xnumon
9/26/19 2:20:53.188 PM SpaceX /var/log/xnumon.log xnumon
9/26/19 2:20:51.926 PM SpaceX /var/log/xnumon.log xnumon

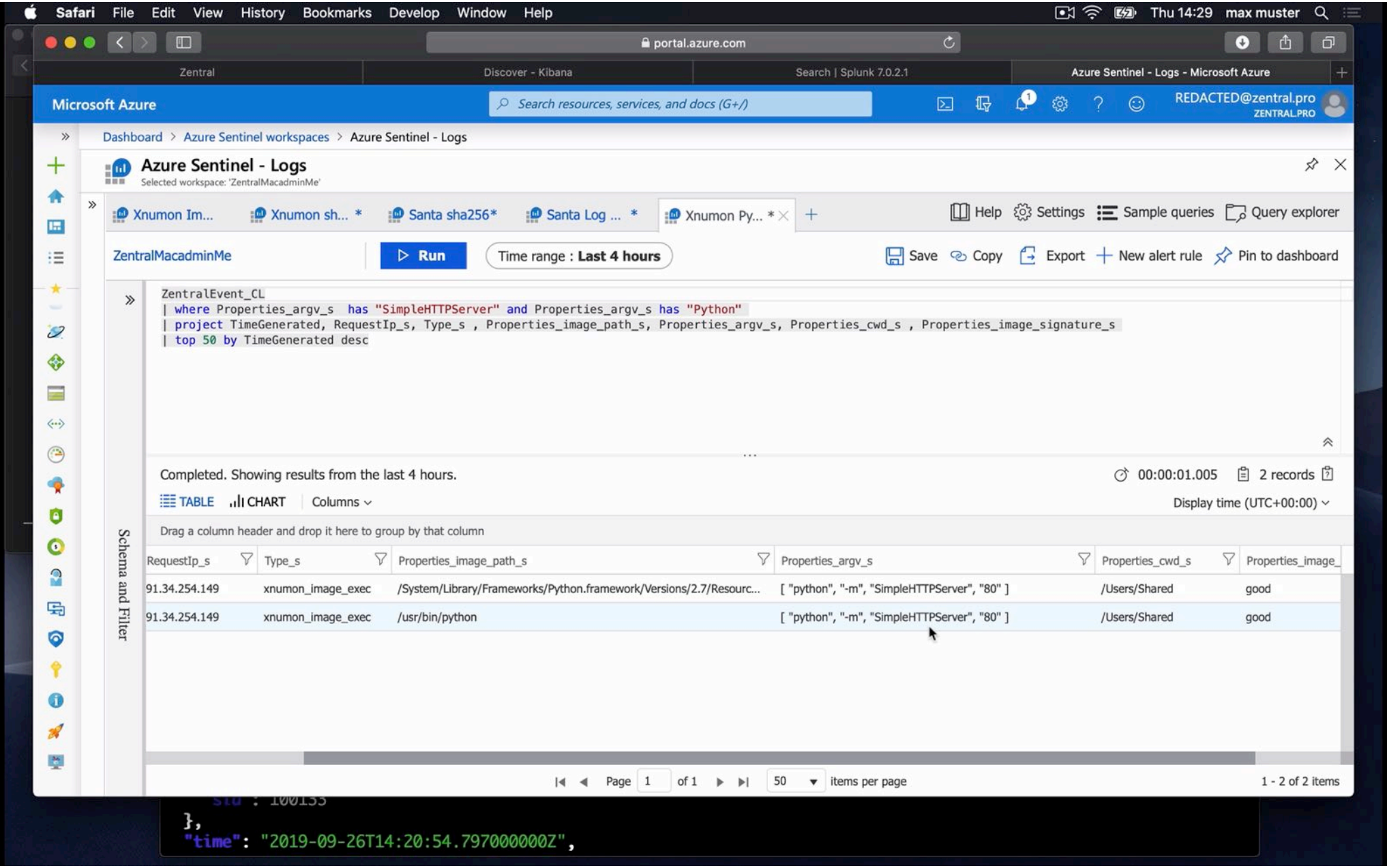

Safari File Edit View History Bookmarks Develop Window Help
Thu 14:27 max muster
prd-p-z3c644f4kkzf.cloud.splunk.com
Zentral
Discover - Kibana
Search | Splunk 7.0.2.1
Azure Sentinel - Logs - Microsoft Azure
Hide Fields
All Fields
Table
Format
20 Per Page
i
_time
host
source
sourcetype
Selected
host
SpaceX
source
/var/log/xnumon.log
sourcetype
xnumon
Event
argv{}
/Applications/Firefox.app/Contents/MacOS/firefox
cwd
/
eventcode
2
image.btime
2019-09-17T17:37:29.000000000Z
image.cdhash
6f5f94e41aec7ae604ad0f70ced02b9082958292
image.certcn
Developer ID Application: Mozilla Corporation (43AQ936H96)
image.ctime
2019-09-26T14:20:37.964490346Z
image.gid
80
image.gname
admin
image.ident
org.mozilla.firefox
image.mode
0100755
image.mtime
2019-09-17T17:37:29.000000000Z
image.origin
devid
image.path
/Applications/Firefox.app/Contents/MacOS/firefox
image.sha256
c55285a84bfc0faf092363d96bac8652b357cd55d21634057d0541cdeefeffa0
image.signature
good
image.size
36496
image.teamid
43AQ936H96
image.uid
0
image.uname
root
subject.ancestors{}.exec_pid
1
subject.ancestors{}.ident
com.apple.xpc.launchd
subject.ancestors{}.path
/sbin/launchd
subject.auid
-1
subject.dev
/dev/console
subject.egid
20
subject.egname
staff
subject.euid
502
subject.euname
max
subject.fork_time
2019-09-26T14:20:51.854000000Z
image.gid 1
a image.gname 1
a image.ident 3
image.mode 1
a image.mtime 1
a image.origin 1
a image.path 3
a image.sha256 3
a image.signature 1
image.size 3
a image.teamid 1
image.uid 1
a image.uname 1
a index 1
linecount 1
a punct 3
a splunk_server 1
a subject.ancestors{}.exec_pid 2
a subject.ancestors{}.exec_time 1
a subject.ancestors{}.ident 2
a subject.ancestors{}.path 2
subject.auid 2
a subject.auname 1
a subject.dev 1
subject.egid 1
a subject.egname 1
subject.euid 1
a subject.euname 1
a subject.fork_time 5
subject.image.exec_pid 1
a subject.image.exec_time 2
a subject.image.ident 2
a subject.image.path 2
a subject.image.sha256 1
a subject.image.teamid 1


Terminal Shell Edit View Window Help
Thu 14:27 max muster
prd-p-z3c644f4kkzf.cloud.splunk.com
Zentral
Discover - Kibana
Search | Splunk 7.0.2.1
Azure Sentinel - Logs - Microsoft Azure
Hide Fields
All Fields
Table
Format
20 Per Page
_time
host
source
sourcetype
Selected
host
SpaceX
source
/var/log/xnumon.log
sourcetype
xnumon
Event
argv{}
/Applications/Firefox.app/Contents/MacOS/firefox
cwd
/
eventcode
2
max — -bash — 114×26
~ — -bash
~ — -bash
"path": "/sbin/launchd"
}
],
"auid": 502,
"auname": "max",
"egid": 20,
"egname": "staff",
"euid": 502,
"euname": "max",
"fork_time": "2019-09-26T14:20:54.797000000Z",
"image": {
"exec_pid": 14549,
"exec_time": "2019-09-26T14:20:51.926000000Z",
"ident": "org.mozilla.firefox",
"path": "/Applications/Firefox.app/Contents/MacOS/firefox",
"sha256": "c55285a84bfc0faf092363d96bac8652b357cd55d21634057d0541cdeefeffa0",
"teamid": "43AQ936H96"
},
"pid": 14557,
"rgid": 20,
"rgname": "staff",
"ruid": 502,
"runame": "max",
"sid": 100133
},
"time": "2019-09-26T14:20:54.797000000Z",


Safari File Edit View History Bookmarks Develop Window Help
Thu 14:28 max muster
portal.azure.com
Zentral
Discover - Kibana
Search | Splunk 7.0.2.1
Azure Sentinel - Logs - Microsoft Azure
Microsoft Azure
Search resources, services, and docs (G+/)
REDACTED@zentral.pro
ZENTRAL.PRO
Dashboard > Azure Sentinel workspaces > Azure Sentinel - Logs
Azure Sentinel - Logs
Selected workspace: 'ZentralMacadminMe'
Xnumon Im...
Xnumon sh... *
Santa sha256*
Santa Log ... *
Xnumon Py... *
Help
Settings
Sample queries
Query explorer
ZentralMacadminMe
Run
Time range : Last 30 minutes
Save
Copy
Export
New alert rule
Pin to dashboard
ZentralEvent_CL
| where Properties_image_ident_s == "org.mozilla.plugincontainer" or Properties_image_ident_s == "org.mozilla.firefox" or Properties_subject_image_ident_s == "org.mozilla
| project TimeGenerated, RequestIp_s, Type_s , Properties_image_path_s, Properties_image_sha256_s
| top 50 by TimeGenerated desc
Completed. Showing results from the last 30 minutes.
00:00:02.289
5 records
TABLE
CHART
Columns
Display time (UTC+00:00)
Drag a column header and drop it here to group by that column
Schema and Filter
TimeGenerated [UTC]
RequestIp_s
Type_s
Properties_image_path_s
Properties_image_sha256_s
9/26/2019, 2:21:38.000 PM 91.34.254.149 xnumon_image_exec /Applications/Firefox.app/Contents/MacOS/pingsender 5cbd81d237b7ff54a8fcfb66f629c13703d0fb2bb394acf2b118ed1daf838...
9/26/2019, 2:20:54.000 PM 91.34.254.149 xnumon_image_exec /Applications/Firefox.app/Contents/MacOS/plugin-container.app/Conte... 618429dd3e7885853ecccc578e8d5a7b62a3465a44f3d20ae1b18fff067...
9/26/2019, 2:20:54.000 PM 91.34.254.149 xnumon_image_exec /Applications/Firefox.app/Contents/MacOS/plugin-container.app/Conte... 618429dd3e7885853ecccc578e8d5a7b62a3465a44f3d20ae1b18fff067...
9/26/2019, 2:20:53.000 PM 91.34.254.149 xnumon_image_exec /Applications/Firefox.app/Contents/MacOS/plugin-container.app/Conte... 618429dd3e7885853ecccc578e8d5a7b62a3465a44f3d20ae1b18fff067...
9/26/2019, 2:20:51.000 PM 91.34.254.149 xnumon_image_exec /Applications/Firefox.app/Contents/MacOS/firefox c55285a84bfc0faf092363d96bac8652b357cd55d21634057d0541cdeef...
Page 1 of 1
50 items per page
1 - 5 of 5 items
},
"time": "2019-09-26T14:20:54.797000000Z",


Safari File Edit View History Bookmarks Develop Window Help
Thu 14:28 max muster
portal.azure.com
Zentral
Discover - Kibana
Search | Splunk 7.0.2.1
Azure Sentinel - Logs - Microsoft Azure
Microsoft Azure
Search resources, services, and docs (G+/)
REDACTED@zentral.pro
ZENTRAL.PRO
Dashboard > Azure Sentinel workspaces > Azure Sentinel - Logs
Azure Sentinel - Logs
Selected workspace: 'ZentralMacadminMe'
Xnumon Im...
Xnumon sh... *
Santa sha256*
Santa Log ... *
Xnumon Py... *
Help
Settings
Sample queries
Query explorer
ZentralMacadminMe
Run
Time range : Last 30 minutes
Save
Copy
Export
New alert rule
Pin to dashboard
ZentralEvent_CL
| where Properties_cert_cn_s == "Developer ID Application: Mozilla Corporation (43AQ936H96)"
| project TimeGenerated, RequestIp_s, Type_s , Properties_path_s, Properties_sha256_s
| top 50 by TimeGenerated desc
Completed. Showing results from the last 30 minutes.
00:00:01.031
5 records
TABLE
CHART
Columns
Display time (UTC+00:00)
Drag a column header and drop it here to group by that column
Schema and Filter
TimeGenerated [UTC]
RequestIp_s
Type_s
Properties_path_s
Properties_sha256_s
9/26/2019, 2:21:38.000 PM 91.34.254.149 santa_log /Applications/Firefox.app/Contents/MacOS/pingsender 5cbd81d237b7ff54a8fcfb66f629c13703d0fb2bb394acf2b118ed1daf8389ed
9/26/2019, 2:20:54.000 PM 91.34.254.149 santa_log /Applications/Firefox.app/Contents/MacOS/plugin-container.app/Contents/... 618429dd3e7885853ecccc578e8d5a7b62a3465a44f3d20ae1b18fff067455c3
9/26/2019, 2:20:54.000 PM 91.34.254.149 santa_log /Applications/Firefox.app/Contents/MacOS/plugin-container.app/Contents/... 618429dd3e7885853ecccc578e8d5a7b62a3465a44f3d20ae1b18fff067455c3
9/26/2019, 2:20:53.000 PM 91.34.254.149 santa_log /Applications/Firefox.app/Contents/MacOS/plugin-container.app/Contents/... 618429dd3e7885853ecccc578e8d5a7b62a3465a44f3d20ae1b18fff067455c3
9/26/2019, 2:20:51.000 PM 91.34.254.149 santa_log /Applications/Firefox.app/Contents/MacOS/firefox c55285a84bfc0faf092363d96bac8652b357cd55d21634057d0541cdeefeffa0
Page 1 of 1
50 items per page
1 - 5 of 5 items
},
"time": "2019-09-26T14:20:54.797000000Z",


Safari File Edit View History Bookmarks Develop Window Help
Thu 14:28 max muster
portal.azure.com
Zentral
Discover - Kibana
Search | Splunk 7.0.2.1
Azure Sentinel - Logs - Microsoft Azure
Microsoft Azure
Search resources, services, and docs (G+/)
REDACTED@zentral.pro
ZENTRAL.PRO
Dashboard > Azure Sentinel workspaces > Azure Sentinel - Logs
Azure Sentinel - Logs
Selected workspace: 'ZentralMacadminMe'
Xnumon Im...
Xnumon sh... *
Santa sha256*
Santa Log ... *
Xnumon Py... *
Help
Settings
Sample queries
Query explorer
ZentralMacadminMe
Run
Time range : Last 30 minutes
Save
Copy
Export
New alert rule
Pin to dashboard
union withsource=sourceTable ZentralEvent_CL
| where Type_s == "santa_log" and RequestIp_s != "" and Properties_action_s == "DISKAPPEAR" or Properties_action_s == "DISKDISAPPEAR"
Completed. Showing results from the last 30 minutes.
00:00:04.743
3 records
TABLE
CHART
Columns
Display time (UTC+00:00)
Drag a column header and drop it here to group by that column
Schema and Filter
Properties_volume_s
Properties_bsdname_s
Properties_appearance_t [UTC]
Properties_dmgpath_s
Properties_model_s
Machin
Firefox disk2s3 macOS
Firefox disk2s3 9/26/2019, 2:20:17.838 PM /Library/Managed Installs/Cache/Firefox 69.0.1.dmg Apple Disk Image macOS
Firefox disk2s3 9/26/2019, 2:20:17.838 PM /Library/Managed Installs/Cache/Firefox 69.0.1.dmg Apple Disk Image macOS
Page 1 of 1
50
items per page
1 - 3 of 3 items
},
"time": "2019-09-26T14:20:54.797000000Z",


Safari File Edit View History Bookmarks Develop Window Help
Thu 14:29 max muster
portal.azure.com
Zentral
Discover - Kibana
Search | Splunk 7.0.2.1
Azure Sentinel - Logs - Microsoft Azure
Microsoft Azure
Search resources, services, and docs (G+/)
REDACTED@zentral.pro
ZENTRAL.PRO
Dashboard > Azure Sentinel workspaces > Azure Sentinel - Logs
Azure Sentinel - Logs
Selected workspace: 'ZentralMacadminMe'
Xnumon Im...
Xnumon sh... *
Santa sha256*
Santa Log ... *
Xnumon Py... *
Help
Settings
Sample queries
Query explorer
ZentralMacadminMe
Run
Time range : Last 4 hours
Save
Copy
Export
New alert rule
Pin to dashboard
ZentralEvent_CL
| where Properties_argv_s has "SimpleHTTPServer" and Properties_argv_s has "Python"
| project TimeGenerated, RequestIp_s, Type_s , Properties_image_path_s, Properties_argv_s, Properties_cwd_s , Properties_image_signature_s
| top 50 by TimeGenerated desc
Completed. Showing results from the last 4 hours.
00:00:01.005
2 records
TABLE
CHART
Columns
Display time (UTC+00:00)
Drag a column header and drop it here to group by that column
RequestIp_s
Type_s
Properties_image_path_s
Properties_argv_s
Properties_cwd_s
Properties_image_
91.34.254.149
xnumon_image_exec
/System/Library/Frameworks/Python.framework/Versions/2.7/Resourc...
["python", "-m", "SimpleHTTPServer", "80"]
/Users/Shared
good
91.34.254.149
xnumon_image_exec
/usr/bin/python
["python", "-m", "SimpleHTTPServer", "80"]
/Users/Shared
good
Schema and Filter
Page 1 of 1
50 items per page
1 - 2 of 2 items
},
"time": "2019-09-26T14:20:54.797000000Z",

Ship and collect the events

How to connect the sources

- Server / Cloud
  - Log analytics

Commercial Log Analytics

- SumoLogic
- Splunk
- DataDog
- Elastic Cloud

et.al

Benefits

- Managed Platform
- High volume capability
- Cost based on volume

Ship and collect the events

How to connect the sources

- Server / Cloud
  - EDR / SIEM Solutions

Commercial SIEM

- ArcSite
- Azure Sentinel
- Chronicle Security
- PaloAlto Cortex XDR
- Q-Radar (IBM)

et.al

Benefits

- Managed Platform
- High volume capability

Conclusion

Conclusion

What can be improved

- Benefits / Next Level

- Better organize event aggregation
- Consolidate data in Event Hubs
- SIEM alerting, Machine Learning
  (too many sign-in errors, …)
- Bring together the admins and the security engineers

Conclusion

What can be improved

- Benefits / Next Level

“Bring together the admins and the security engineers“

https://github.com/zentralopensource/MacSysAdmin-Conference-2019

Thank you !

Q & A

https://int.zentral.pro

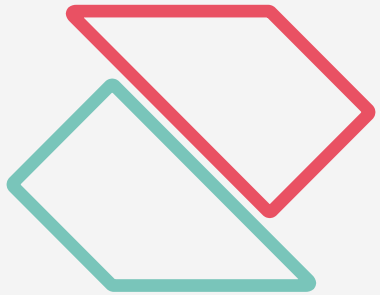
Support our open source development

https://www.patreon.com/zentral

hi@zentral.pro

https://int.zentral.pro

zentral_io



zentral.pro

MacSysAdmin 2019