

# Logging

# About Needles in the Modern Haystack

## Who are we ?

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



- 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
  - ancestry
  - 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

The screenshot shows a web browser window on developer.apple.com. The URL is developer.apple.com. The page title is "EndpointSecurity". The navigation bar includes links for Apple Developer, Discover, Design, Develop, Distribute, Support, Account, and a search icon. Below the navigation bar, the breadcrumb trail shows "Documentation > EndpointSecurity". On the right side of the header, there are dropdown menus for "Language: Swift" and "API Changes: None". The main content area has a heading "Framework" and the title "EndpointSecurity". A horizontal line separates this from the "Overview" section. The "Overview" text states: "Endpoint Security clients monitor system events for potentially malicious activity. Your client registers with Endpoint Security to authorize pending events, or receive notifications of events that have already occurred. These events include process executions, mounting file systems, forking processes, and raising signals." To the right of this text, there is a sidebar with "SDKs" (macOS 10.15+, Mac Catalyst 13.0+), and "On This Page" links for "Overview" and "Topics". At the bottom of the page, a modal dialog titled "Kext Information" displays details for the "EndpointSecurity" kext. The dialog shows the path "/System/Library/Extensions/EndpointSecurity.kext/Contents/MacOS/EndpointSecurity". It lists the following information: hash: 46CBBB25D65814781CC3F5245CA6A009 / 75B7231D0DA9C377174F1028EEBA4DB26F00EE34, size: 367 KB (367264 bytes), time: 09-20-2019 14:11 (created) / 09-20-2019 14:11 (modified), sign: Software Signing, Apple Code Signing Certification Authority, Apple Root CA. A "close" button is at the bottom right of the dialog.

Framework

## EndpointSecurity

---

### Overview

Endpoint Security clients monitor system events for potentially malicious activity. Your client registers with Endpoint Security to authorize pending events, or receive notifications of events that have already occurred. These events include process executions, mounting file systems, forking processes, and raising signals.

Develop your system extension with Endpoint Security and package it in an app that uses the [SystemExtensions](#) framework to install and upgrade the extension on the user's Mac.

SDKs

macOS 10.15+  
Mac Catalyst 13.0+

On This Page

[Overview](#) [Topics](#)

Kext Information

**EndpointSecurity**  
/System/Library/Extensions/EndpointSecurity.kext/Contents/MacOS/EndpointSecurity

hash: 46CBBB25D65814781CC3F5245CA6A009 / 75B7231D0DA9C377174F1028EEBA4DB26F00EE34  
size: 367 KB (367264 bytes)  
time: 09-20-2019 14:11 (created) / 09-20-2019 14:11 (modified)  
sign: Software Signing, Apple Code Signing Certification Authority, Apple Root CA

close

 zentral.pro

# Event sources and types

On the endpoints

- ▶ Sources
- ▶ Security Agents:  
System Extensions

The screenshot shows a web browser window displaying a blog post on the Objective-See website. The title of the post is "Writing a Process Monitor with Apple's Endpoint Security Framework", dated September 7, 2019. The post contains a code snippet demonstrating the use of the Endpoint Security Framework to monitor processes. A callout box highlights a link to the "Process Monitoring Library" on GitHub, which is circled in red. The footer of the page includes copyright information, support links, and social media icons.

Writing a Process Monitor with Apple's Endpoint Security Framework

September 7, 2019

```
# ./processMonitor
Starting process monitor...[ok]

PROCESS EXEC ('ES_EVENT_TYPE_NOTIFY_EXEC')
pid: 7655
path: /bin/ls
uid: 501
args: (
    ls,
    "-lart",
    "."
)

signing info: {
    cdHash = 5180A360C9484D61AF2CE737EAE9EBAE5B7E2850;
    csFlags = 603996161;
    isPlatformBinary = 1 (true);
    signatureIdentifier = "com.apple.ls";
}
```

On github:  
[Process Monitoring Library](#)

Background

© 2019 objective-see llc

support us! [Twitter](#) [Email](#)

 zentral.pro

# Event sources and types

On the endpoints

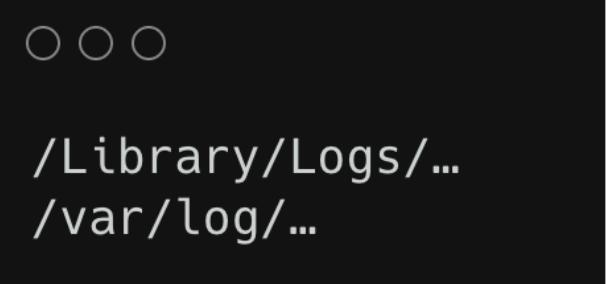
► Outputs

- 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

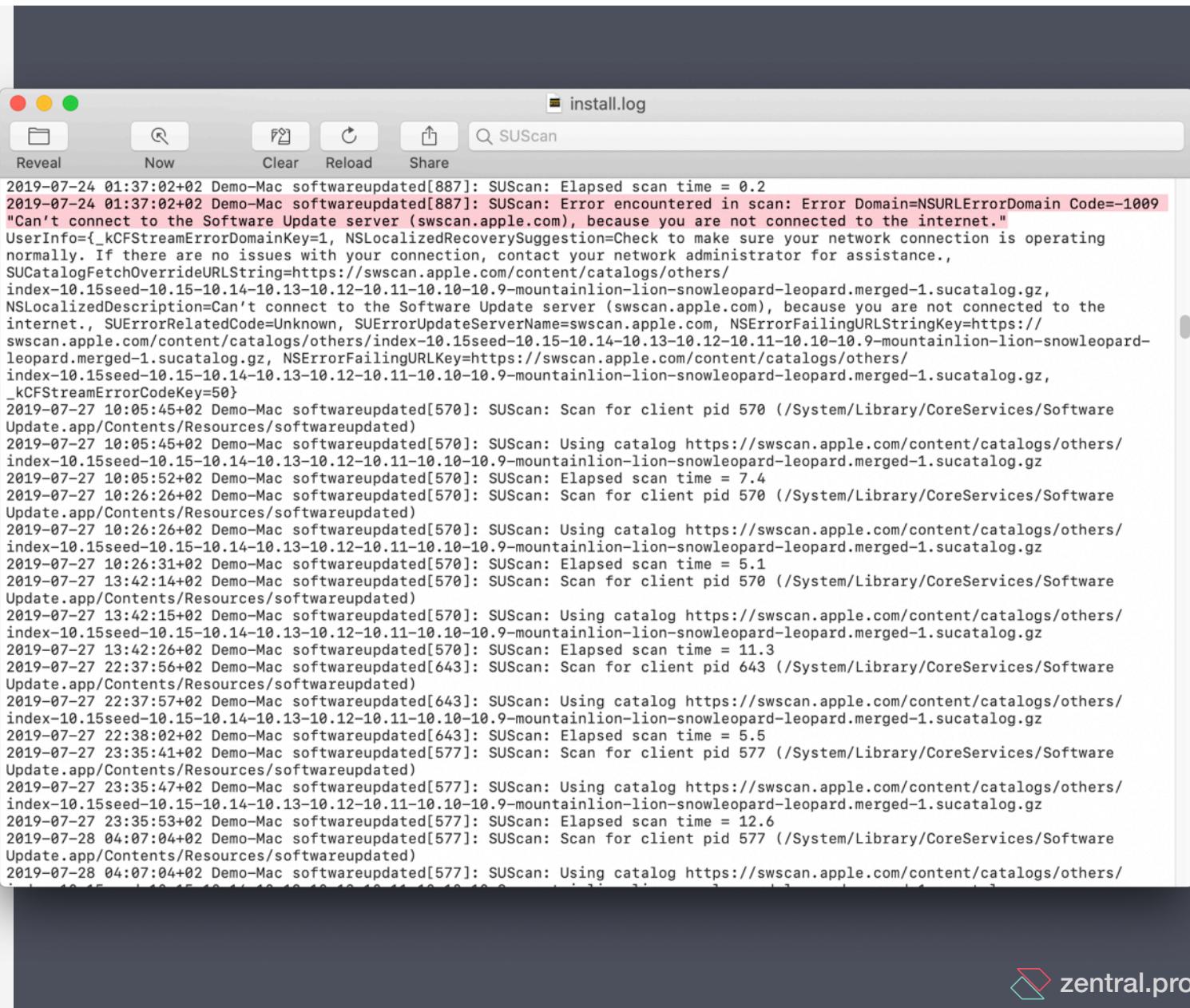
- mostly with not so well integrated apps
- Text data in files (*rotated*)
- Sometimes JSON (1 object per line)

# Event sources and types

On the endpoints

▶ Outputs

▶ File based



```
2019-07-24 01:37:02+02 Demo-Mac softwareupdated[887]: SUScan: Elapsed scan time = 0.2
2019-07-24 01:37:02+02 Demo-Mac softwareupdated[887]: SUScan: Error encountered in scan: Error Domain=NSURLErrorDomain Code=-1009
"Can't connect to the Software Update server (swscan.apple.com), because you are not connected to the internet."
UserInfo={_kCFStreamErrorDomainKey=1, NSLocalizedRecoverySuggestion=Check to make sure your network connection is operating
normally. If there are no issues with your connection, contact your network administrator for assistance.,
SUCatalogFetchOverrideURLString=https://swscan.apple.com/content/catalogs/others/
index-10.15seed-10.15-10.14-10.13-10.12-10.11-10.10-10.9-mountainlion-lion-snowleopard-leopard.merged-1.sucatalog.gz,
NSLocalizedDescription=Can't connect to the Software Update server (swscan.apple.com), because you are not connected to the
internet., SUErrorRelatedCode=Unknown, SUErrorUpdateServerName=swscan.apple.com, NSErrorFailingURLStringKey=https://
swscan.apple.com/content/catalogs/others/index-10.15seed-10.15-10.14-10.13-10.12-10.11-10.10-10.9-mountainlion-lion-snowleopard-
leopard.merged-1.sucatalog.gz, NSErrorFailingURLKey=https://swscan.apple.com/content/catalogs/others/
index-10.15seed-10.15-10.14-10.13-10.12-10.11-10.10-10.9-mountainlion-lion-snowleopard-leopard.merged-1.sucatalog.gz,
_kCFStreamErrorCodeKey=50}
2019-07-27 10:05:45+02 Demo-Mac softwareupdated[570]: SUScan: Scan for client pid 570 (/System/Library/CoreServices/Software
Update.app/Contents/Resources/softwareupdated)
2019-07-27 10:05:45+02 Demo-Mac softwareupdated[570]: SUScan: Using catalog https://swscan.apple.com/content/catalogs/others/
index-10.15seed-10.15-10.14-10.13-10.12-10.11-10.10-10.9-mountainlion-lion-snowleopard-leopard.merged-1.sucatalog.gz
2019-07-27 10:05:52+02 Demo-Mac softwareupdated[570]: SUScan: Elapsed scan time = 7.4
2019-07-27 10:26:26+02 Demo-Mac softwareupdated[570]: SUScan: Scan for client pid 570 (/System/Library/CoreServices/Software
Update.app/Contents/Resources/softwareupdated)
2019-07-27 10:26:26+02 Demo-Mac softwareupdated[570]: SUScan: Using catalog https://swscan.apple.com/content/catalogs/others/
index-10.15seed-10.15-10.14-10.13-10.12-10.11-10.10-10.9-mountainlion-lion-snowleopard-leopard.merged-1.sucatalog.gz
2019-07-27 10:26:31+02 Demo-Mac softwareupdated[570]: SUScan: Elapsed scan time = 5.1
2019-07-27 13:42:14+02 Demo-Mac softwareupdated[570]: SUScan: Scan for client pid 570 (/System/Library/CoreServices/Software
Update.app/Contents/Resources/softwareupdated)
2019-07-27 13:42:15+02 Demo-Mac softwareupdated[570]: SUScan: Using catalog https://swscan.apple.com/content/catalogs/others/
index-10.15seed-10.15-10.14-10.13-10.12-10.11-10.10-10.9-mountainlion-lion-snowleopard-leopard.merged-1.sucatalog.gz
2019-07-27 13:42:26+02 Demo-Mac softwareupdated[570]: SUScan: Elapsed scan time = 11.3
2019-07-27 22:37:56+02 Demo-Mac softwareupdated[643]: SUScan: Scan for client pid 643 (/System/Library/CoreServices/Software
Update.app/Contents/Resources/softwareupdated)
2019-07-27 22:37:57+02 Demo-Mac softwareupdated[643]: SUScan: Using catalog https://swscan.apple.com/content/catalogs/others/
index-10.15seed-10.15-10.14-10.13-10.12-10.11-10.10-10.9-mountainlion-lion-snowleopard-leopard.merged-1.sucatalog.gz
2019-07-27 22:38:02+02 Demo-Mac softwareupdated[643]: SUScan: Elapsed scan time = 5.5
2019-07-27 23:35:41+02 Demo-Mac softwareupdated[577]: SUScan: Scan for client pid 577 (/System/Library/CoreServices/Software
Update.app/Contents/Resources/softwareupdated)
2019-07-27 23:35:47+02 Demo-Mac softwareupdated[577]: SUScan: Using catalog https://swscan.apple.com/content/catalogs/others/
index-10.15seed-10.15-10.14-10.13-10.12-10.11-10.10-10.9-mountainlion-lion-snowleopard-leopard.merged-1.sucatalog.gz
2019-07-27 23:35:53+02 Demo-Mac softwareupdated[577]: SUScan: Elapsed scan time = 12.6
2019-07-28 04:07:04+02 Demo-Mac softwareupdated[577]: SUScan: Scan for client pid 577 (/System/Library/CoreServices/Software
Update.app/Contents/Resources/softwareupdated)
2019-07-28 04:07:04+02 Demo-Mac softwareupdated[577]: SUScan: Using catalog https://swscan.apple.com/content/catalogs/others/
index-10.15seed-10.15-10.14-10.13-10.12-10.11-10.10-10.9-mountainlion-lion-snowleopard-leopard.merged-1.sucatalog.gz
```

## Event sources and types

On the endpoints

- ▶ Outputs
- ▶ OS log facility

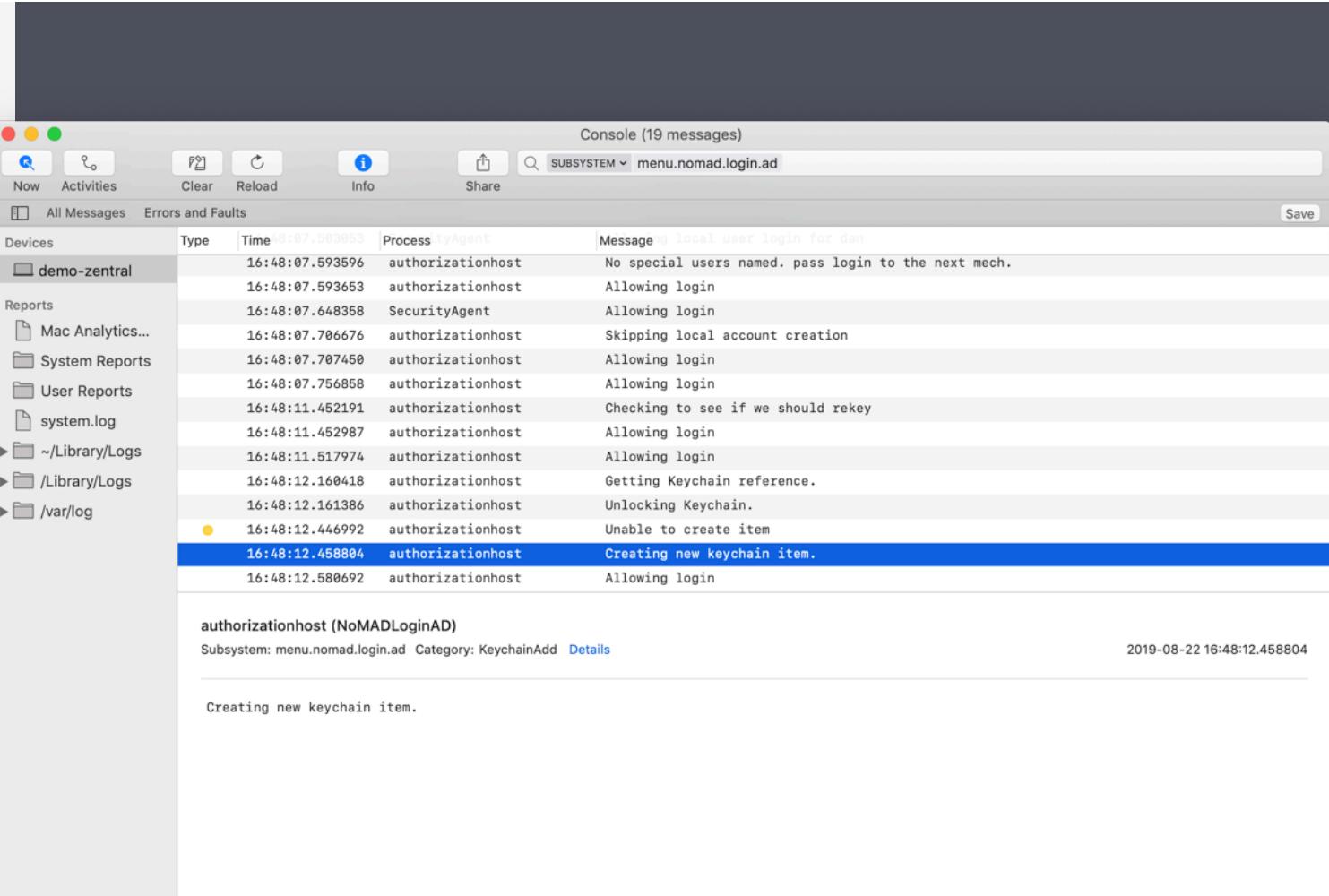
OS log facilities -  
for OS and well behaved / integrated apps

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

# Event sources and types

On the endpoints

- ▶ Outputs
- ▶ Unified Logging



The screenshot shows the macOS Console application window. The title bar reads "Console (19 messages)" and "SUBSYSTEM ▾ menu.nomad.login.ad". The main pane displays a table of log messages. The left sidebar lists "Devices" (demo-zentral) and "Reports" (Mac Analytics..., System Reports, User Reports, system.log, ~/Library/Logs, /Library/Logs, /var/log). The table has columns: Devices, Type, Time, Process, Agent, and Message. One message is highlighted in blue: "16:48:12.458804 authorizationhost Creating new keychain item." Below the table, a detailed view shows "authorizationhost (NoMADLoginAD)" with "Subsystem: menu.nomad.login.ad Category: KeychainAdd Details". The timestamp "2019-08-22 16:48:12.458804" is also present.

Devices	Type	Time	Process	Agent	Message
demo-zentral		16:48:07.593596		authorizationhost	No special users named. pass login to the next mech.
		16:48:07.593653		authorizationhost	Allowing login
		16:48:07.648358		SecurityAgent	Allowing login
		16:48:07.706676		authorizationhost	Skipping local account creation
		16:48:07.707450		authorizationhost	Allowing login
		16:48:07.756858		authorizationhost	Allowing login
		16:48:11.452191		authorizationhost	Checking to see if we should rekey
		16:48:11.452987		authorizationhost	Allowing login
		16:48:11.517974		authorizationhost	Allowing login
		16:48:12.160418		authorizationhost	Getting Keychain reference.
		16:48:12.161386		authorizationhost	Unlocking Keychain.
		16:48:12.446992		authorizationhost	Unable to create item
		16:48:12.458804		authorizationhost	Creating new keychain item.
		16:48:12.580692		authorizationhost	Allowing login

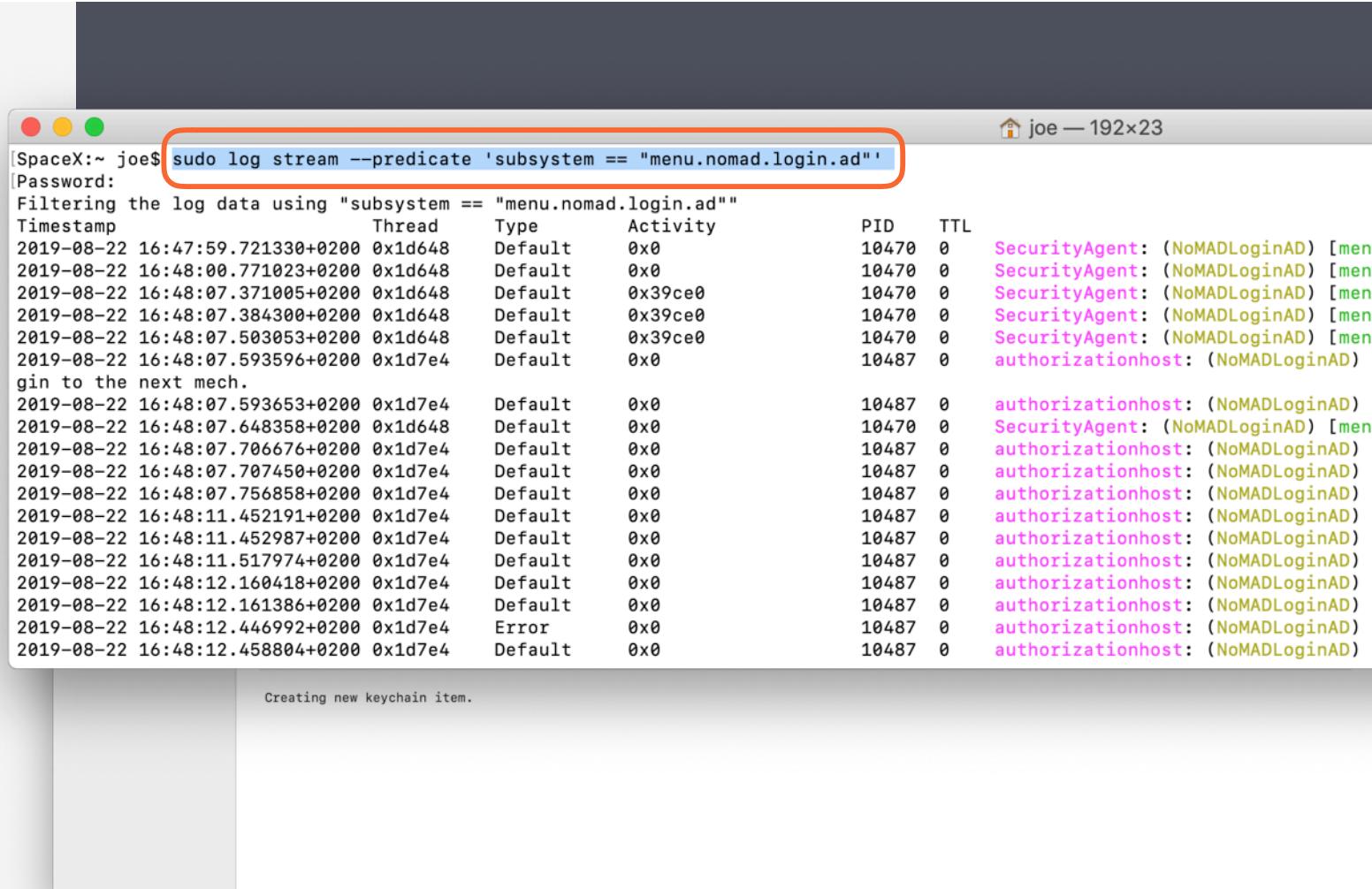
In-memory or persist  
into .tracev3 files

# Event sources and types

On the endpoints

- ▶ Outputs
- ▶ Unified Logging

In-memory or persist  
into .tracev3 files



The screenshot shows a terminal window titled "joe — 192x23" running on a Mac OS X system. The command entered is "sudo log stream --predicate 'subsystem == \"menu.nomad.login.ad\"'". The output is a table of log entries with columns: Timestamp, Thread, Type, Activity, PID, TTL, and Log message. The log messages are mostly "SecurityAgent: (NoMADLoginAD) [menu.r...]" and "authorizationhost: (NoMADLoginAD) [me...". A red box highlights the command line.

Timestamp	Thread	Type	Activity	PID	TTL	Log message
2019-08-22 16:47:59.721330+0200	0x1d648	Default	0x0	10470	0	SecurityAgent: (NoMADLoginAD) [menu.r...
2019-08-22 16:48:00.771023+0200	0x1d648	Default	0x0	10470	0	SecurityAgent: (NoMADLoginAD) [menu.r...
2019-08-22 16:48:07.371005+0200	0x1d648	Default	0x39ce0	10470	0	SecurityAgent: (NoMADLoginAD) [menu.r...
2019-08-22 16:48:07.384300+0200	0x1d648	Default	0x39ce0	10470	0	SecurityAgent: (NoMADLoginAD) [menu.r...
2019-08-22 16:48:07.503053+0200	0x1d648	Default	0x39ce0	10470	0	SecurityAgent: (NoMADLoginAD) [menu.r...
2019-08-22 16:48:07.593596+0200	0x1d7e4	Default	0x0	10487	0	authorizationhost: (NoMADLoginAD) [me...
			gin to the next mech.			
2019-08-22 16:48:07.593653+0200	0x1d7e4	Default	0x0	10487	0	authorizationhost: (NoMADLoginAD) [me...
2019-08-22 16:48:07.648358+0200	0x1d648	Default	0x0	10470	0	SecurityAgent: (NoMADLoginAD) [menu.r...
2019-08-22 16:48:07.706676+0200	0x1d7e4	Default	0x0	10487	0	authorizationhost: (NoMADLoginAD) [me...
2019-08-22 16:48:07.707450+0200	0x1d7e4	Default	0x0	10487	0	authorizationhost: (NoMADLoginAD) [me...
2019-08-22 16:48:07.756858+0200	0x1d7e4	Default	0x0	10487	0	authorizationhost: (NoMADLoginAD) [me...
2019-08-22 16:48:11.452191+0200	0x1d7e4	Default	0x0	10487	0	authorizationhost: (NoMADLoginAD) [me...
2019-08-22 16:48:11.452987+0200	0x1d7e4	Default	0x0	10487	0	authorizationhost: (NoMADLoginAD) [me...
2019-08-22 16:48:11.517974+0200	0x1d7e4	Default	0x0	10487	0	authorizationhost: (NoMADLoginAD) [me...
2019-08-22 16:48:12.160418+0200	0x1d7e4	Default	0x0	10487	0	authorizationhost: (NoMADLoginAD) [me...
2019-08-22 16:48:12.161386+0200	0x1d7e4	Default	0x0	10487	0	authorizationhost: (NoMADLoginAD) [me...
2019-08-22 16:48:12.446992+0200	0x1d7e4	Error	0x0	10487	0	authorizationhost: (NoMADLoginAD) [me...
2019-08-22 16:48:12.458804+0200	0x1d7e4	Default	0x0	10487	0	authorizationhost: (NoMADLoginAD) [me...

# 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 ( <i>subsystem type</i> )
--debug	Details depth
--style	Formatting ( <i>json</i> )

# Event sources and types

On the endpoints

- ▶ Outputs
- ▶ Unified Logging

[https://eclecticlight.co/  
2018/03/19/macoss-unified-log-1-  
why-what-and-how/](https://eclecticlight.co/2018/03/19/macoss-unified-log-1-why-what-and-how/)

THE ECLECTIC LIGHT COMPANY  
MACS, PAINTING, AND MORE

hoakley / March 19, 2018 / Macs, Technology

## macOS Unified log: 1 why, what and how

```
graph TD; A[code writes to log] --> B[logd]; B --> C[compressor]; C --> D[buffer]; D --> E[in-memory store]; E --> F[regular log file: /var/db/diagnostics/Persist/*.tracev3]; E --> G[Fault & Error log data: /var/db/diagnostics/Special/*.tracev3, /var/db/uidtext/*]; E --> H['others', inc. /var/db/diagnostics/logdata.statistics.*.txt]; I[diagnosticd] --> J['live' log stream]
```

When Apple released macOS Sierra 10.12 in September 2016, it brought one of the most fundamental changes since the first Public Beta of Mac OS X: it

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

```
head@jamf-server: ~ — ssh - Python — zsh
-rw-rw-r-- 1 root      utmp          292876 Sep 21 09:04 lastlog
drwx----- 2 root      root          4096 Sep 21 06:14 letsencrypt
drwxr-xr-x 2 root      root          4096 Nov 23 2018 lxd
-rw-r----- 1 syslog    adm           5473 Sep 20 19:37 mail.log
drwxr-x--- 2 mysql     adm           4096 Sep 21 06:25 mysql
drwxr-xr-x 2 root      adm           4096 Sep 21 06:25 nginx
-rw-r----- 1 syslog    adm           5859 Sep 21 09:04 syslog
-rw-r----- 1 syslog    adm           435566 Sep 21 06:25 syslog.1
-rw----- 1 root      root          64192 Sep 19 17:18 tallylog
drwxr-x--- 2 tomcat8   adm           4096 Sep 21 06:25 tomcat8
-rw-r----- 1 syslog    adm           46211 Sep 21 08:38 ufw.log
drwxr-x--- 2 root      adm           4096 Sep 19 17:19 unattended-upgrades
-rw-rw-r-- 1 root      utmp          12672 Sep 21 09:04 wtmp
[head@jamf-server:~$ ls -la /var/log/tomcat8/
total 2812
drwxr-x--- 2 tomcat8 adm      4096 Sep 21 06:25 .
drwxrwxr-x 14 root    syslog  4096 Sep 21 06:25 ..
-rw-r----- 1 tomcat8 tomcat8  2467 Sep 12 14:30 catalina.2019-09-12.log.gz
-rw-r----- 1 tomcat8 tomcat8  3625 Sep 19 22:15 catalina.2019-09-19.log.gz
-rw-r--r-- 1 tomcat8 tomcat8 271705 Sep 20 16:08 catalina.out
-rw-r----- 1 tomcat8 tomcat8   45 Sep 12 14:29 JAMFChangeManagement.log.gz
-rw-r----- 1 tomcat8 tomcat8 2509610 Sep 21 09:05 JAMFSoftwareServer.log
-rw-r----- 1 tomcat8 tomcat8   575 Sep 20 16:07 JSSAccess.log.gz
-rw-r----- 1 tomcat8 tomcat8  245 Sep 12 14:29 localhost.2019-09-12.log.gz
-rw-r----- 1 tomcat8 tomcat8  630 Sep 19 22:15 localhost.2019-09-19.log.gz
-rw-r----- 1 tomcat8 tomcat8   56 Sep 12 14:27 localhost_access_log.2019-09-12.txt.gz
-rw-r----- 1 tomcat8 tomcat8 12206 Sep 19 23:05 localhost_access_log.2019-09-19.txt.gz
-rw-r----- 1 tomcat8 tomcat8 29645 Sep 20 21:07 localhost_access_log.2019-09-20.txt.gz
-rw-r----- 1 tomcat8 tomcat8   280 Sep 21 07:00 localhost_access_log.2019-09-21.txt
head@jamf-server:~$
```

# Event sources and types

Server / Cloud

▶ Outputs

○ ○ ○  
/var/log/...

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

# Event sources and types

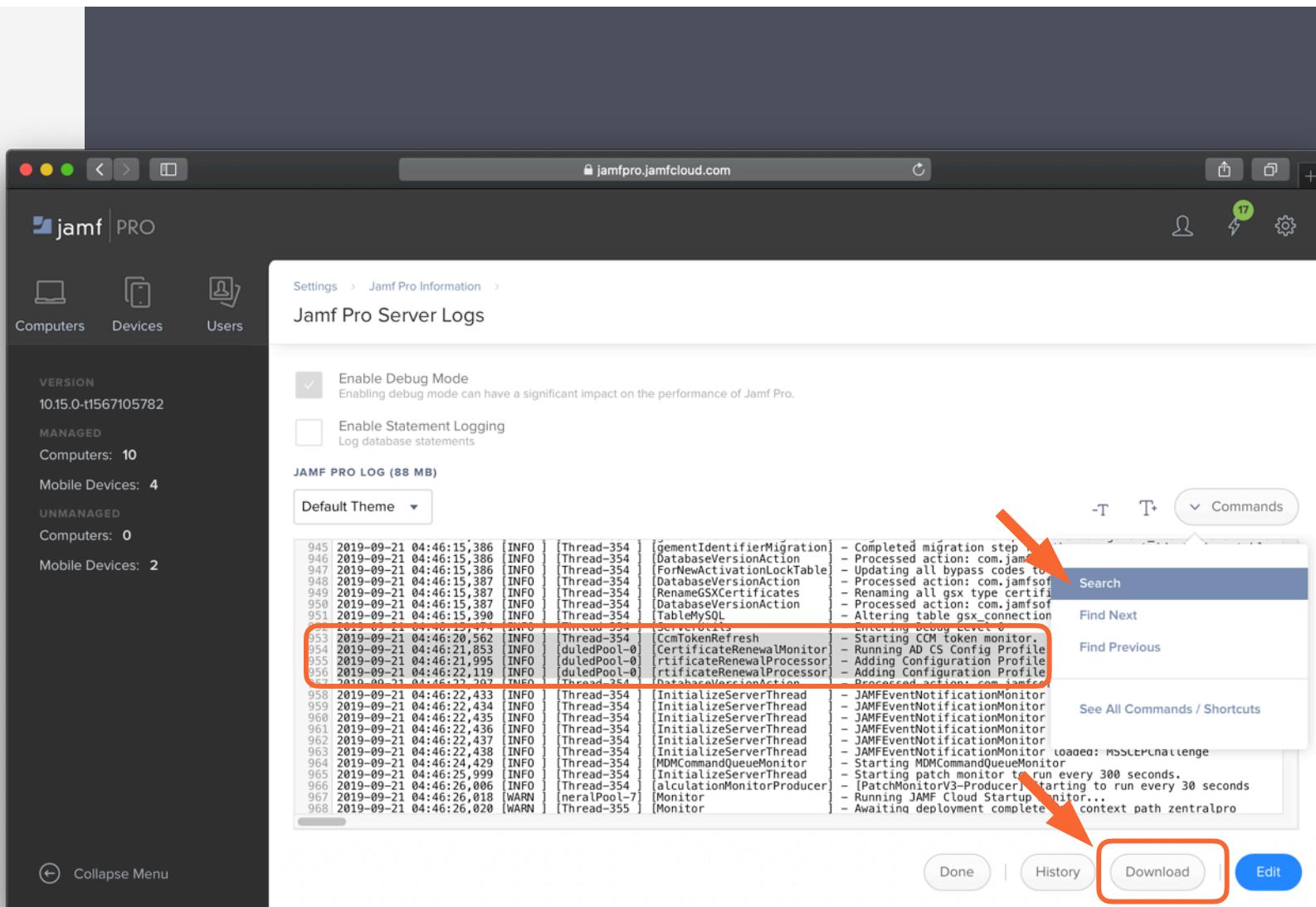
Server / Cloud  
▶ Outputs

- **API** (*Jamf Pro, Microsoft Graph Security API*)
- **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

# Event sources and types

Server / Cloud

► Outputs

► Jamf Pro

```
Default (zsh)

2019-09-20 08:45:14,428 [INFO ] [duledPool-6] [VppLicenseMonitor      ] - License monitor completed after 76.43 seconds
2019-09-20 08:45:32,404 [INFO ] [duledPool-4] [CertificateRenewalMonitor] - Running AD CS Config Profile Renewal Task
2019-09-20 08:45:32,448 [INFO ] [duledPool-4] [rtificateRenewalProcessor] - Adding Configuration Profile install command for profile: OS XConfigurationProfile [ID=33, Name=11 days certificate] for device: ComputerShell [ID=36, Name=Joe's MacBook Pro] which has a certificate with expiration: 2019-09-29T08:54:06.000Z
2019-09-20 08:45:32,483 [INFO ] [duledPool-4] [rtificateRenewalProcessor] - Adding Configuration Profile install command for profile: OS XConfigurationProfile [ID=36, Name=2 days certificate] for device: ComputerShell [ID=36, Name=Joe's MacBook Pro] which has a certificate with expiration: 2019-09-20T08:54:06.000Z
--
--
2019-09-21 04:46:15,474 [INFO ] [Thread-354 ] [ServerUtils           ] - Entering Debug Level 0
2019-09-21 04:46:20,562 [INFO ] [Thread-354 ] [CcmTokenRefresh       ] - Starting CCM token monitor.
2019-09-21 04:46:21,853 [INFO ] [duledPool-0] [CertificateRenewalMonitor] - Running AD CS Config Profile Renewal Task
2019-09-21 04:46:21,995 [INFO ] [duledPool-0] [rtificateRenewalProcessor] - Adding Configuration Profile install command for profile: OS XConfigurationProfile [ID=33, Name=11 days certificate] for device: ComputerShell [ID=36, Name=Joe's MacBook Pro] which has a certificate with expiration: 2019-09-30T08:45:52.000Z
2019-09-21 04:46:22,119 [INFO ] [duledPool-0] [rtificateRenewalProcessor] - Adding Configuration Profile install command for profile: OS XConfigurationProfile [ID=36, Name=2 days certificate] for device: ComputerShell [ID=36, Name=Joe's MacBook Pro] which has a certificate with expiration: 2019-09-21T08:45:52.000Z
--
--
2019-09-21 04:46:15,474 [INFO ] [Thread-354 ] [ServerUtils           ] - Entering Debug Level 0
2019-09-21 04:46:20,562 [INFO ] [Thread-354 ] [CcmTokenRefresh       ] - Starting CCM token monitor.
2019-09-21 04:46:21,853 [INFO ] [duledPool-0] [CertificateRenewalMonitor] - Running AD CS Config Profile Renewal Task
2019-09-21 04:46:21,995 [INFO ] [duledPool-0] [rtificateRenewalProcessor] - Adding Configuration Profile install command for profile: OS XConfigurationProfile [ID=33, Name=11 days certificate] for device: ComputerShell [ID=36, Name=Joe's MacBook Pro] which has a certificate with expiration: 2019-09-30T08:45:52.000Z
2019-09-21 04:46:22,119 [INFO ] [duledPool-0] [rtificateRenewalProcessor] - Adding Configuration Profile install command for profile: OS XConfigurationProfile [ID=36, Name=2 days certificate] for device: ComputerShell [ID=36, Name=Joe's MacBook Pro] which has a certificate with expiration: 2019-09-21T08:45:52.000Z
→ Desktop cat JAMFSwerver-2.log | grep -A 2 -B 2 CertificateRenewalMonitor
```

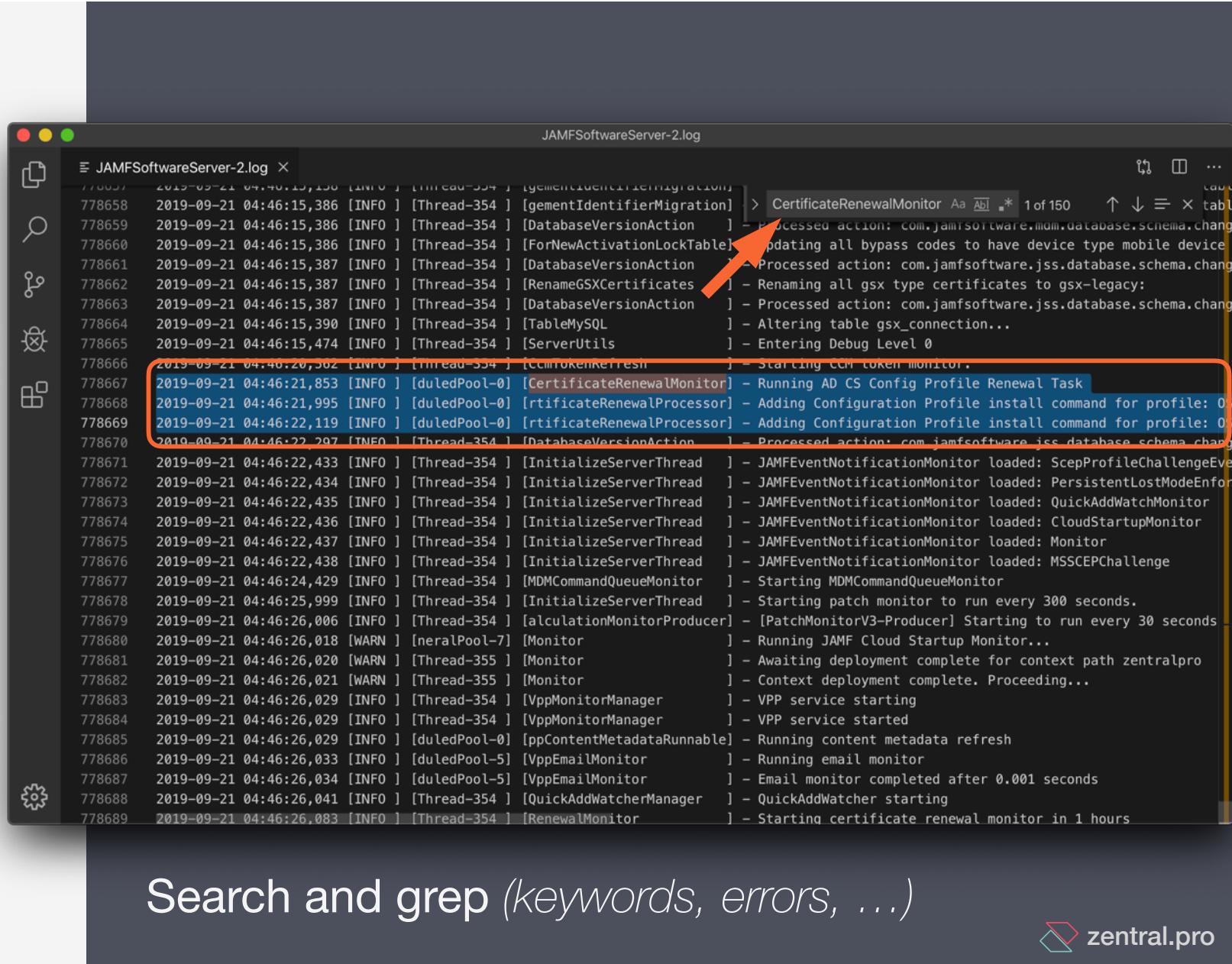
Search and grep (keywords, errors, ...)

# Event sources and types

Server / Cloud

► Outputs

► Jamf Pro



```
JAMFSoftwareServer-2.log
778657 2019-09-21 04:46:15,150 [INFO ] [Thread-354] [gemtIdentifierMigration] > CertificateRenewalMonitor Aa Abi * 1 of 150 ↑ ↓ ≡ X tab
778658 2019-09-21 04:46:15,386 [INFO ] [Thread-354] [gemtIdentifierMigration] > CertificateRenewalMonitor Aa Abi * 1 of 150 ↑ ↓ ≡ X tab
778659 2019-09-21 04:46:15,386 [INFO ] [Thread-354] [DatabaseVersionAction] ] - Processed action: com.jamfsoftware.jss.database.schema.chang
778660 2019-09-21 04:46:15,386 [INFO ] [Thread-354] [ForNewActivationLockTable] ] - Updating all bypass codes to have device type mobile device
778661 2019-09-21 04:46:15,387 [INFO ] [Thread-354] [DatabaseVersionAction] ] - Processed action: com.jamfsoftware.jss.database.schema.chang
778662 2019-09-21 04:46:15,387 [INFO ] [Thread-354] [RenameGSXCertificates] ] - Renaming all gsx type certificates to gsx-legacy:
778663 2019-09-21 04:46:15,387 [INFO ] [Thread-354] [DatabaseVersionAction] ] - Processed action: com.jamfsoftware.jss.database.schema.chang
778664 2019-09-21 04:46:15,390 [INFO ] [Thread-354] [TableMySQL] ] - Altering table gsx_connection...
778665 2019-09-21 04:46:15,474 [INFO ] [Thread-354] [ServerUtils] ] - Entering Debug Level 0
778666 2019-09-21 04:46:20,362 [INFO ] [Thread-354] [ccmTokenRefresh] ] - Starting ccm token monitor.
778667 2019-09-21 04:46:21,853 [INFO ] [duledPool-0] [CertificateRenewalMonitor] - Running AD CS Config Profile Renewal Task
778668 2019-09-21 04:46:21,995 [INFO ] [duledPool-0] [rtificateRenewalProcessor] - Adding Configuration Profile install command for profile: 0
778669 2019-09-21 04:46:22,119 [INFO ] [duledPool-0] [rtificateRenewalProcessor] - Adding Configuration Profile install command for profile: 0
778670 2019-09-21 04:46:22,297 [INFO ] [Thread-354] [DatabaseVersionAction] ] - Processed action: com.jamfsoftware.jss.database.schema.chang
778671 2019-09-21 04:46:22,433 [INFO ] [Thread-354] [InitializeServerThread] ] - JAMFEventNotificationMonitor loaded: ScepProfileChallengeEve
778672 2019-09-21 04:46:22,434 [INFO ] [Thread-354] [InitializeServerThread] ] - JAMFEventNotificationMonitor loaded: PersistentLostModeEnfor
778673 2019-09-21 04:46:22,435 [INFO ] [Thread-354] [InitializeServerThread] ] - JAMFEventNotificationMonitor loaded: QuickAddWatchMonitor
778674 2019-09-21 04:46:22,436 [INFO ] [Thread-354] [InitializeServerThread] ] - JAMFEventNotificationMonitor loaded: CloudStartupMonitor
778675 2019-09-21 04:46:22,437 [INFO ] [Thread-354] [InitializeServerThread] ] - JAMFEventNotificationMonitor loaded: Monitor
778676 2019-09-21 04:46:22,438 [INFO ] [Thread-354] [InitializeServerThread] ] - JAMFEventNotificationMonitor loaded: MSSCEPChallenge
778677 2019-09-21 04:46:24,429 [INFO ] [Thread-354] [MDMCommandQueueMonitor] ] - Starting MDMCommandQueueMonitor
778678 2019-09-21 04:46:25,999 [INFO ] [Thread-354] [InitializeServerThread] ] - Starting patch monitor to run every 300 seconds.
778679 2019-09-21 04:46:26,006 [INFO ] [Thread-354] [alculationMonitorProducer] - [PatchMonitorV3-Producer] Starting to run every 30 seconds
778680 2019-09-21 04:46:26,018 [WARN ] [neralPool-7] [Monitor] ] - Running JAMF Cloud Startup Monitor...
778681 2019-09-21 04:46:26,020 [WARN ] [Thread-355] [Monitor] ] - Awaiting deployment complete for context path zentralpro
778682 2019-09-21 04:46:26,021 [WARN ] [Thread-355] [Monitor] ] - Context deployment complete. Proceeding...
778683 2019-09-21 04:46:26,029 [INFO ] [Thread-354] [VppMonitorManager] ] - VPP service starting
778684 2019-09-21 04:46:26,029 [INFO ] [Thread-354] [VppMonitorManager] ] - VPP service started
778685 2019-09-21 04:46:26,029 [INFO ] [duledPool-0] [ppContentMetadataRunnable] - Running content metadata refresh
778686 2019-09-21 04:46:26,033 [INFO ] [duledPool-5] [VppEmailMonitor] ] - Running email monitor
778687 2019-09-21 04:46:26,034 [INFO ] [duledPool-5] [VppEmailMonitor] ] - Email monitor completed after 0.001 seconds
778688 2019-09-21 04:46:26,041 [INFO ] [Thread-354] [QuickAddWatcherManager] ] - QuickAddWatcher starting
778689 2019-09-21 04:46:26,083 [INFO ] [Thread-354] [RenewalMonitor] ] - Starting certificate renewal monitor in 1 hours
```

Search and grep (keywords, errors, ...)

 zentral.pro

# Event sources and types

## Server / Cloud

- ▶ Outputs
- ▶ IDP - Okta

The screenshot shows the Okta Dashboard with the System Log tab selected. The log table displays several events, with one specific event from Sep 24 22:51:40 highlighted by a red box. This event details the addition of a user to application membership. The expanded view shows the following context:

Actor	Client	Device	GeographicalContext	ID	IPAddress	UserAgent	Zone	Event	Request	IPChain
Henry Stamerjohann (User)		Computer	Hamburg Germany		93.192.32.203	CHROME on Mac OS X	null			successful application.user_membership.add (id: XYqB3OZDep8MkqjObmY7uQAAA-Q)

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

# Event sources and types

Server / Cloud

► Outputs

► IDP - Duo

The screenshot shows the Duo Authentication Log page. On the left is a sidebar with navigation links: Dashboard, Device Insight, Policies, Applications, Users, Endpoints, 2FA Devices, Groups, Administrators, Trusted Endpoints Configuration, Reports (which is selected), Authentication Log, Telephony Log, Administrator Actions, Authentication Summary, Denied Authentications, Deployment Progress, Policy Impact, Phishing, Settings, Support (with a link to Email Support), and Account ID.

The main content area has a search bar at the top. Below it is a breadcrumb trail: Dashboard > Authentication Log. A histogram titled "33 Authentications" shows the count of authentications per day from March 24 to July 18. An orange arrow points to the "Export" button in the top right corner of the histogram area, which includes options for JSON, CSV, and Print.

A table below the histogram displays 25 of 33 items, each row representing an authentication event. The columns are: Timestamp (CEST), Result, User, Application, Access Device, and Second Factor. The table rows are:

Timestamp (CEST)	Result	User	Application	Access Device	Second Factor
16:33 21. AUG. 2019	✓ Granted Valid passcode	REACTED@zentral.pro	Okta	Mac OS X 10.15.0	SMS Passcode Location Unknown
16:32 21. AUG. 2019	✗ Denied Invalid passcode	REACTED@zentral.pro	Okta	Mac OS X 10.15.0	Passcode Location Unknown
16:31 21. AUG. 2019	✗ Denied User cancelled	REACTED@zentral.pro	Okta	Mac OS X 10.15.0	Unknown
16:28 21. AUG. 2019	✓ Granted User approved	REACTED@zentral.pro	Okta	Mac OS X 10.15.0	Duo Push Hamburg, HH
16:28 21. AUG. 2019	✗ Denied User mistake	REACTED@zentral.pro	Okta	Mac OS X 10.15.0	Duo Push Hamburg, HH

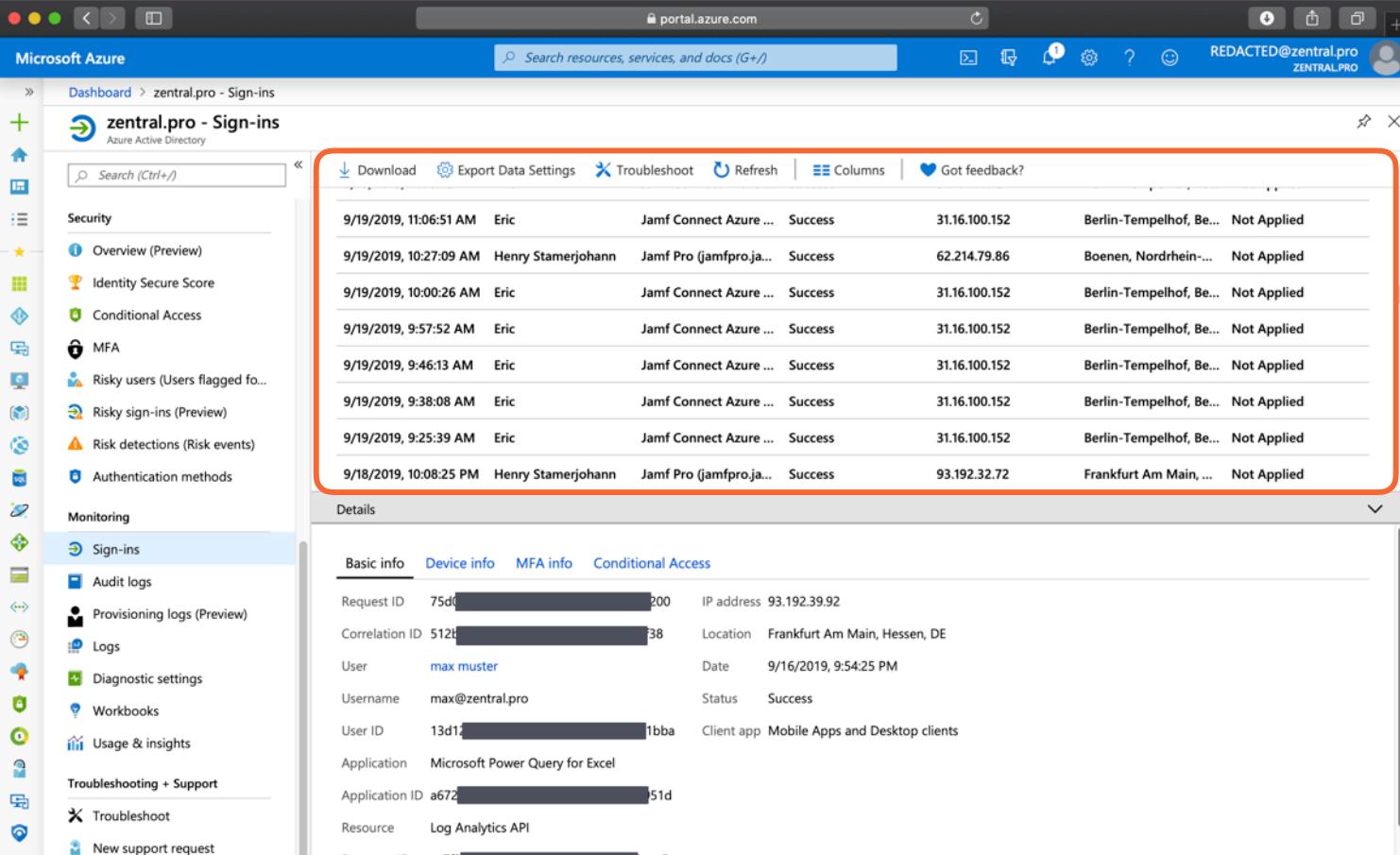
Authentications (*export json, csv*)

# Event sources and types

Server / Cloud

► Outputs

► IDP - Azure AD



The screenshot shows the Microsoft Azure portal interface for the 'zentral.pro - Sign-ins' service. The left sidebar lists various monitoring and troubleshooting options. The main area displays a table of sign-in logs. The table has a red border around its header and first few rows. The columns include Date, User, Application, Status, IP Address, Location, and Action. The data shows several successful sign-ins from different users and devices.

Date	User	Application	Status	IP Address	Location	Action
9/19/2019, 11:06:51 AM	Eric	Jamf Connect Azure ...	Success	31.16.100.152	Berlin-Tempelhof, Be...	Not Applied
9/19/2019, 10:27:09 AM	Henry Stamerjohann	Jamf Pro (jamfpro.ja...	Success	62.214.79.86	Boenen, Nordrhein...	Not Applied
9/19/2019, 10:00:26 AM	Eric	Jamf Connect Azure ...	Success	31.16.100.152	Berlin-Tempelhof, Be...	Not Applied
9/19/2019, 9:57:52 AM	Eric	Jamf Connect Azure ...	Success	31.16.100.152	Berlin-Tempelhof, Be...	Not Applied
9/19/2019, 9:46:13 AM	Eric	Jamf Connect Azure ...	Success	31.16.100.152	Berlin-Tempelhof, Be...	Not Applied
9/19/2019, 9:38:08 AM	Eric	Jamf Connect Azure ...	Success	31.16.100.152	Berlin-Tempelhof, Be...	Not Applied
9/19/2019, 9:25:39 AM	Eric	Jamf Connect Azure ...	Success	31.16.100.152	Berlin-Tempelhof, Be...	Not Applied
9/18/2019, 10:08:25 PM	Henry Stamerjohann	Jamf Pro (jamfpro.ja...	Success	93.192.32.72	Frankfurt Am Main, ...	Not Applied

Details

Basic info	Device info	MFA info	Conditional Access
Request ID: 75d0[REDACTED]200	IP address: 93.192.39.92		
Correlation ID: 512b[REDACTED]38	Location: Frankfurt Am Main, Hessen, DE		
User: max muster	Date: 9/16/2019, 9:54:25 PM		
Username: max@zentral.pro	Status: Success		
User ID: 13d1[REDACTED]1bba	Client app: Mobile Apps and Desktop clients		
Application: Microsoft Power Query for Excel			
Application ID: a672[REDACTED]51d			
Resource: Log Analytics API			
Resource ID: ca7f3[REDACTED]0eac5			

Sign-in Logs (export json, csv)



# Event sources and types

Server / Cloud

► Outputs

► IDP - Azure AD

The screenshot shows the Microsoft Azure portal interface for the 'zentral.pro - Sign-ins' section. On the left, a sidebar lists various monitoring and troubleshooting options. The main area displays a table of sign-in logs with columns for Date, User, Application, and Result. Below the table, a 'Details' section provides a breakdown of the most recent sign-in. At the bottom right, there is a 'Download Sign-ins' panel with options to choose between CSV or JSON formats and a file name input field. A red box highlights this panel.

Date	User	Application	Result
9/19/2019, 11:06:51 AM	Eric	Jamf Connect Azure ...	Success
9/19/2019, 10:27:09 AM	Henry Stamerjohann	Jamf Pro (jamfpro.ja...	Success
9/19/2019, 10:00:26 AM	Eric	Jamf Connect Azure ...	Success
9/19/2019, 9:57:52 AM	Eric	Jamf Connect Azure ...	Success
9/19/2019, 9:46:13 AM	Eric	Jamf Connect Azure ...	Success
9/19/2019, 9:38:08 AM	Eric	Jamf Connect Azure ...	Success
9/19/2019, 9:25:39 AM	Eric	Jamf Connect Azure ...	Success
9/18/2019, 10:08:25 PM	Henry Stamerjohann	Jamf Pro (jamfpro.ja...	Success

**Details**

Basic info	Device info	MFA info	Conditional Access
Request ID: 75d[REDACTED]00	IP address: 93.192.35		
Correlation ID: 512[REDACTED]38	Location: Frankfurt		
User: max muster	Date: 9/16/2019		
Username: max@zentral.pro	Status: Success		
User ID: 13d[REDACTED]bba	Client app: Mobile A		
Application: Microsoft Power Query for Excel			
Application ID: a67[REDACTED]51d			
Resource: Log Analytics API			
Resource ID: ca7f[REDACTED]ac5			

**Download Sign-ins**

You can download up to 250,000 records. If you want to download more, use reporting APIs. Click here to learn more.

Your download will be based on the filter selections you have made.

Format:  CSV  JSON  
File Name: Signins\_2019-09-13\_2019-09-21.csv

Download

Sign-in Logs (export json, csv)

# Event sources and types

Server / Cloud

► Outputs

► ATP Defender

The screenshot shows the Microsoft Defender Security Center interface for a MacBook. The left sidebar lists machine details and various filters. The main area displays a summary of alerts, user activity, and security assessments. A red box highlights the timeline events section, which shows three log entries from September 9, 2019, at 12:22 PM. An arrow points to the 'Export' button in the timeline header.

**Machine:** MacBook

**Risk level: Low**  
3 active alerts in 1 incident

**Logged on users:** 1 logged on user

**No data available:** Threat & Vulnerability Management currently supports only Windows 7, Windows 10 and Windows Server 2019 devices

**Timeline:**

Event time	Event	Additional information	Entities
Sep 9, 2019, 12:22:13.677 PM	Microsoft Defender ATP detected 'Trojan.MAC.Shlayer.E' malware		Malware
Sep 9, 2019, 12:22:13.677 PM	Install.dmg detected as Trojan.MAC.Shlayer.E by Antivirus		install.dmg > Install.dmg
Sep 9, 2019, 12:22:13.646 PM	Install.dmg detected as Trojan.MAC.Shlayer.E by Antivirus		install.dmg > Install.dmg

**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

The screenshot shows the Google Cloud Platform Stackdriver Logging interface. The top navigation bar includes the URL `console.cloud.google.com`, the project name `Jamf-AIO-prod`, and various navigation icons. The main area displays logs for a `GCE VM Instance` with the identifier `jamf.jamfsoftwareserver`. The logs are filtered to show entries from `7:41 AM to now (CEST)`. A specific log entry is highlighted with a red box:

```
2019-09-09 08:35:39.653 CEST Running AD CS Config Profile Renewal Task
2019-09-09 08:35:39.677 CEST Adding Configuration Profile install command for profile: OSXConfigurationProfile [ID=1, Name=11 DAYS] for device: ComputerShell [ID=1, Name=ladmin's MacBook] which has a certificate with expiration: 2019-09-18T07:34:05.000Z
```

Below the log entry, the JSON payload is expanded:

```
{
  "insertId": "uum27rag6ssp5oiob",
  "jsonPayload": {...},
  "labels": {...},
  "logName": "projects/jamf-aio-prod/logs/jamf.jamfsoftwareserver",
  "receiveTimestamp": "2019-09-09T06:35:57.648102190Z",
  "resource": {...},
  "severity": "INFO",
  "timestamp": "2019-09-09T06:35:39.677Z"
}
```

At the bottom of the log list, another entry is partially visible:

```
2019-09-09 08:35:52.207 CEST Running license monitor
```

# Ship and collect the events

## Existing Solutions

- ▶ Log Facilities
  - ▶ Stackdriver Logging

The screenshot shows the Google Cloud Platform Stackdriver Logging interface. The top navigation bar includes 'Google Cloud Platform', a project dropdown ('Jamf-AIO-prod'), and various icons for search, export, and metrics.

The main area displays logs for a 'GCE VM Instance' labeled 'jamf.jamfsoftware...'. A log entry from September 7, 2019, at 08:35:25.039 CEST is shown, indicating an error message about an incorrect keystore password.

A red box highlights the 'Error' dropdown menu, which lists the following log levels:

- Critical
- Error
- Warning
- Info
- Debug
- \* Any log level

On the right side of the log list, there are download and view options buttons, along with a context menu for the log entry.

# Ship and collect the events

## Existing Solutions

- ▶ Log Facilities
- ▶ Stackdriver Logging

The screenshot shows the Google Cloud Platform Logs Viewer interface. A modal dialog box is overlaid on the screen, prompting the user to download logs. The dialog title is "Download your 16 most recently loaded logs". It contains the following text: "Up to 300 log entries currently loaded into the Logs Viewer will be downloaded. If you need to download more logs, consider [exporting](#) your logs." Below this, there is a section titled "Log entry format" with two options: "JSON" (unchecked) and "CSV" (checked). At the bottom of the dialog, it says "Logs from 9/6/19, 10:26 AM to 9/8/19, 9:34 AM". The dialog has three buttons at the bottom: "CANCEL", "VIEW IN NEW TAB", and "DOWNLOAD". The "DOWNLOAD" button is highlighted with a red border. The background of the Logs Viewer shows a list of log entries for a "GCE VM Instance, yolo2" from September 6 to 8, 2019.

## 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

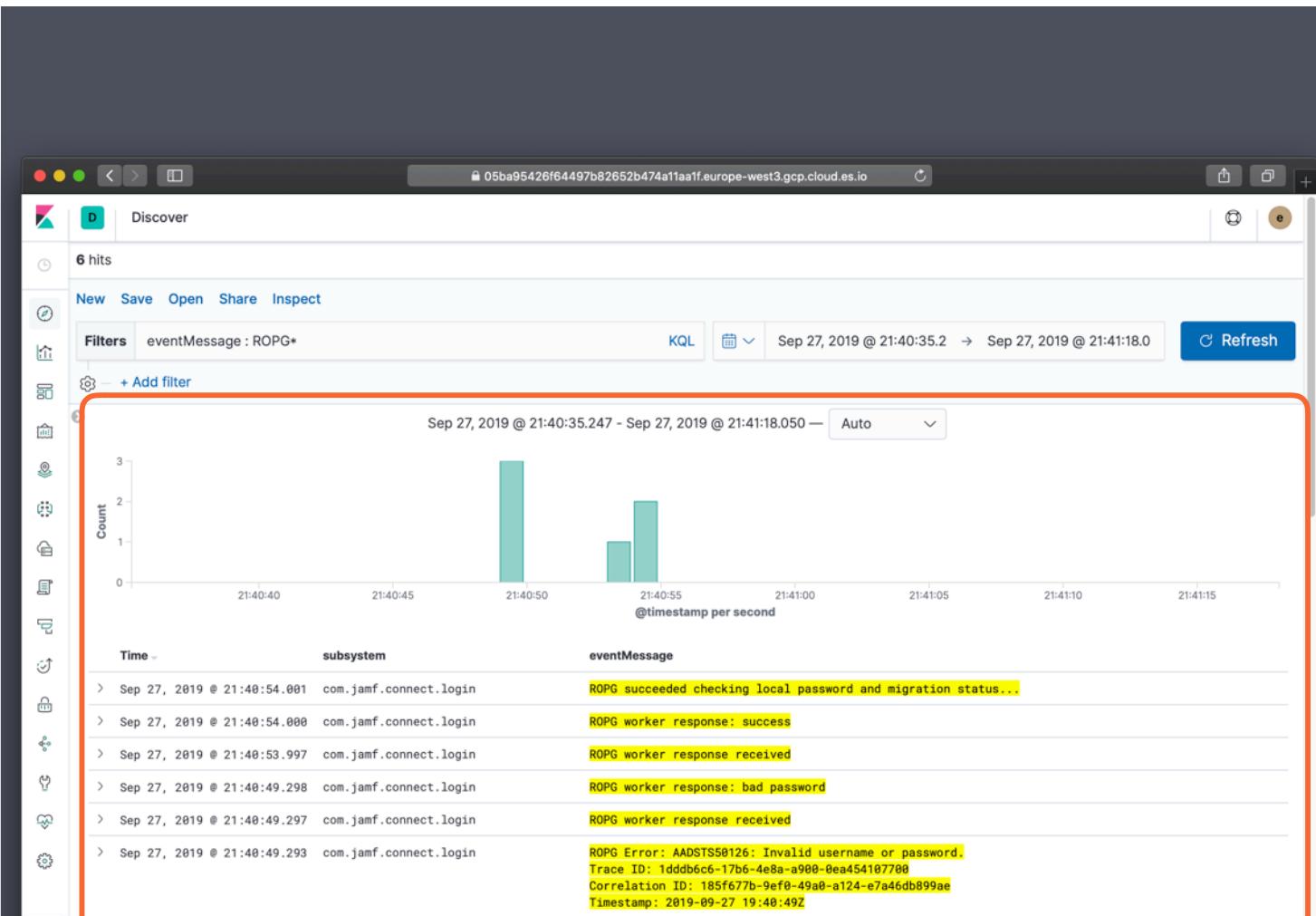
# Ship and collect the events

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)



- 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

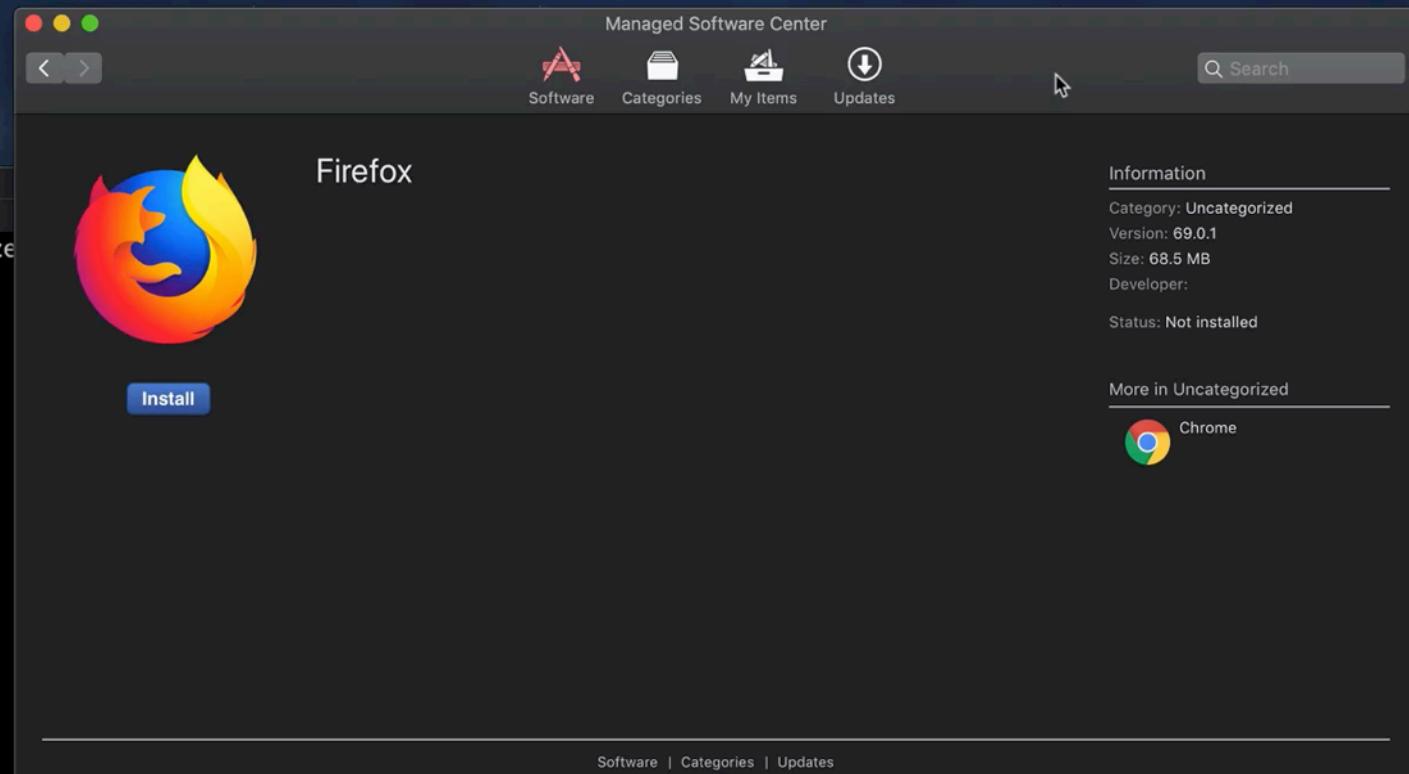
How to connect  
the sources

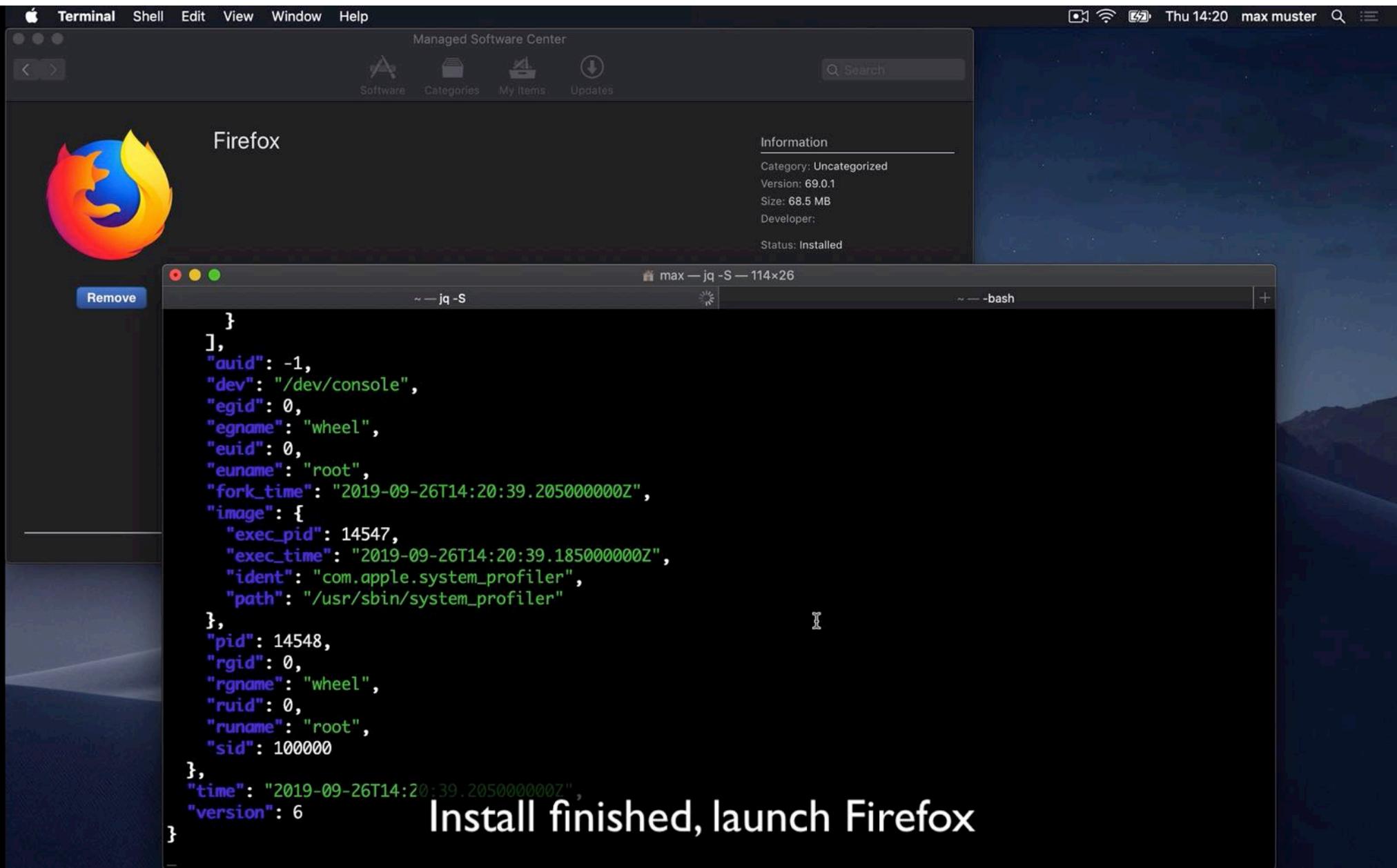
► Demo 1

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 signing information
- Ship the logs to Elastic Stack (*w/ FileBeat*)
- Run a quick filtering in Zentral
- See filtered Events in Kibana UI





A screenshot of a macOS desktop environment. At the top, there's a dark menu bar with the Apple logo and various menu items like Terminal, Shell, Edit, View, Window, Help. To the right of the menu bar are system status icons for battery, signal, and time (Thu 14:21). The main window in the foreground is a Terminal application window titled "max — -bash — 114x26". Inside the terminal, there is a large amount of JSON-like data output. A portion of the data is highlighted with a purple selection, showing details about a file named "plugin-container.app". The highlighted section includes fields such as "certcn", "ctime", "gid", "gname", "ident", "mode", "mtime", "origin", "path", "sha256", "signature", "size", "teamid", "uid", and "uname". Below this, another part of the JSON object is shown, starting with "subject": { "ancestors": [ { "exec\_pid": 14549, ... ] } ]. Above the terminal window, there's a browser window with a search bar containing the placeholder "Mit Google suchen oder Adresse eingeben".

```
"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": "618429dd3e7885853ecc578e8d9a7b62a3465a44f3d20ae1b18fff067455c3",
    "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 ▾

```
CCTOOLT : SIS
},
"time": "2019-09-26T14:20:54.797000000Z",
```

Safari File Edit View History Bookmarks Develop Window Help

Thu 14:22 max muster

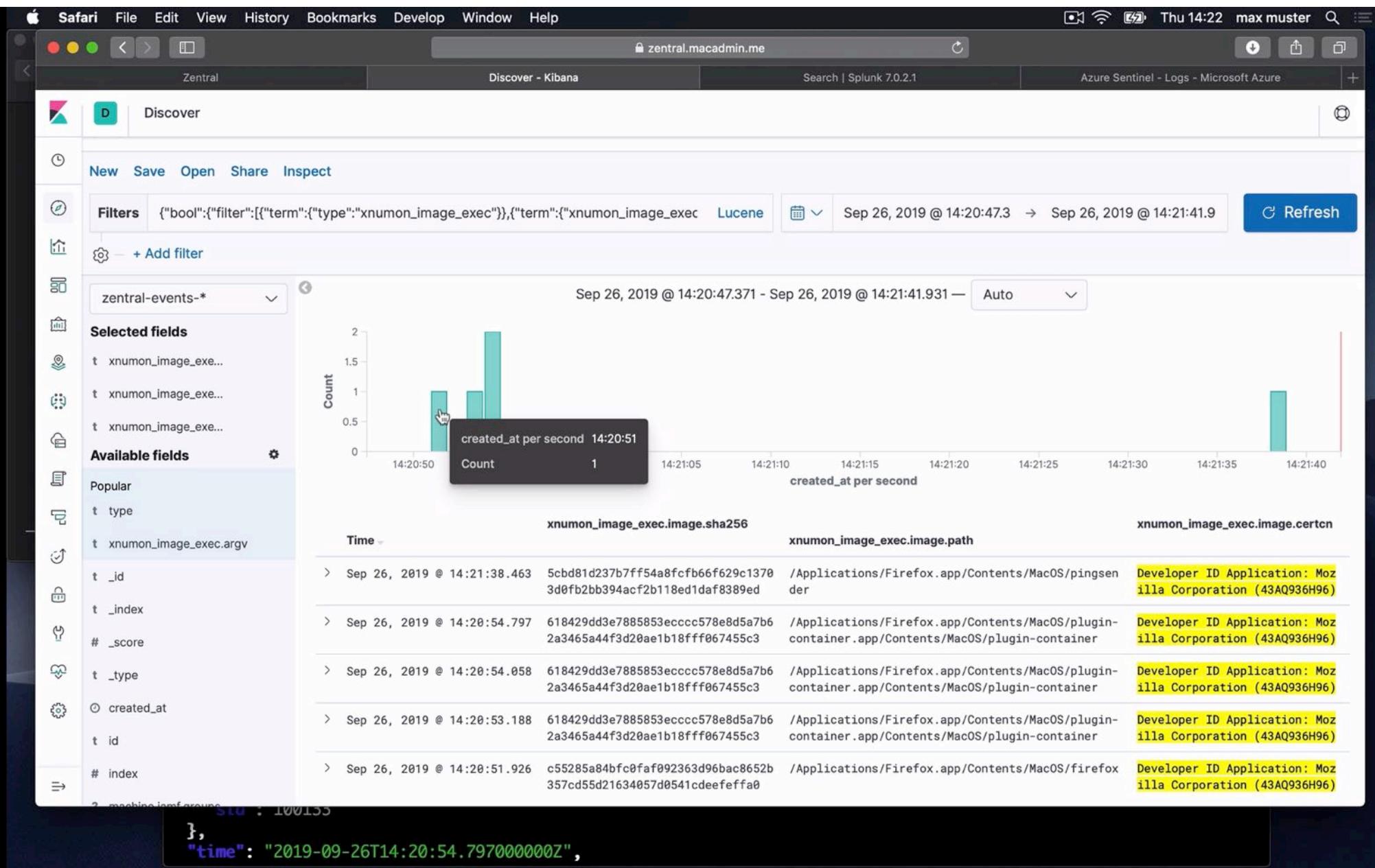
zentral.macadmin.me

Zentral Discover - Kibana Search | Splunk 7.0.2.1 Azure Sentinel - Logs - Microsoft Azure

Discover

# xnumon_image_exec.su...	t request.geo.region_iso_code	HH
① xnumon_image_exec.su...	t request.geo.region_name	Hamburg
t xnumon_image_exec.su...	□ request.ip	91.34.254.149
t xnumon_image_exec.su...	t request.user_agent	filebeat/7.3.0
t xnumon_image_exec.su...	t tags	xnumon
t xnumon_image_exec.su...	t type	xnumon_image_exec
t xnumon_image_exec.su...	t xnumon_image_exec.argv	/Applications/Firefox.app/Contents/MacOS/firefox
# xnumon_image_exec.su...	t xnumon_image_exec.cwd	/
# xnumon_image_exec.su...	② xnumon_image_exec.image.btime	Sep 17, 2019 @ 17:37:29.000
# xnumon_image_exec.su...	t xnumon_image_exec.image.cdhash	6f5f94e41aec7ae604ad0f70ced02b9082958292
t xnumon_image_exec.su...	🔍 * t xnumon_image_exec.image.certcn	Developer ID Application: Mozilla Corporation (43AQ936H96)
# xnumon_image_exec.su...	③ xnumon_image_exec.image.ctime	Sep 26, 2019 @ 14:20:37.964
t xnumon_image_exec.su...	# xnumon_image_exec.image.gid	80
t xnumon_image_exec.su...	t xnumon_image_exec.image.gname	admin
# xnumon_image_exec.su...	t xnumon_image_exec.image.ident	org.mozilla.firefox
# xnumon_image_exec.su...	t xnumon_image_exec.image.mode	0100755
# xnumon_image_exec.su...	④ xnumon_image_exec.image.mtime	Sep 17, 2019 @ 17:37:29.000
# xnumon_image_exec.ver...	t xnumon_image_exec.image.origin	devid
	t xnumon_image_exec.image.path	/Applications/Firefox.app/Contents/MacOS/firefox
	t xnumon_image_exec.image.sha256	c55285a84bf0faf092363d96bac8652b357cd55d21634057d0541cdeefffa0
	t xnumon_image_exec.image.signature	good
	# xnumon_image_exec.image.size	36,496
	t xnumon_image_exec.image.teamid	43AQ936H96
	# xnumon_image_exec.image.uid	0
	t xnumon_image_exec.image.uname	root
	? xnumon_image_exec.subject.ancestors	{

CC100T :  
},  
"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

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

zentral-events-\* Sep 26, 2019 @ 14:20:47.371 - Sep 26, 2019 @ 14:21:41.931 — Auto

**Selected fields**

- t xnumon\_image\_exec...
- t xnumon\_image\_exec...
- t xnumon\_image\_exec...

**Available fields**

- Popular
- t type
- t xnumon\_image\_exec.argv
- t \_id
- t \_index
- # \_score
- t \_type
- ⌚ created\_at
- t id
- # index
- ⌚ machine\_ids/groups

Count

created\_at per second 14:20:51 Count 1

xnumon\_image\_exec.image.sha256 xnumon\_image\_exec.image.path xnumon\_image\_exec.image.certcn

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	c55285a84bf0faf092363d96bac8652b357cd55d21634057d0541cdeefffa0	/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

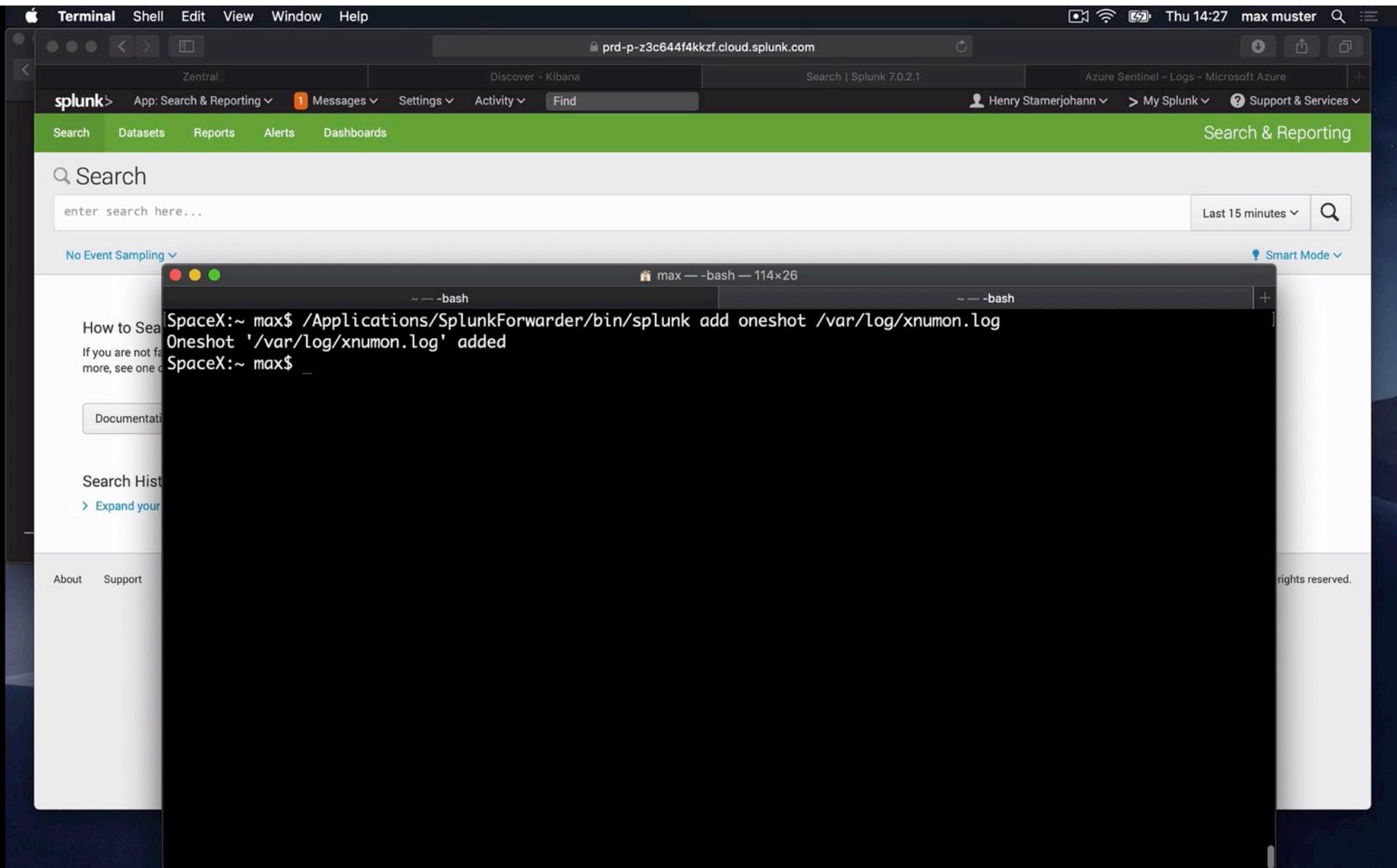
510,926 Events INDEXED	3 days ago EARLIEST EVENT	2 minutes ago LATEST EVENT
------------------------	---------------------------	----------------------------

[Data Summary](#)

### Search History

> [Expand your search history](#)

About Support File a Bug Documentation Privacy Policy © 2005-2019 Splunk Inc. All rights reserved.



Safari File Edit View History Bookmarks Develop Window Help

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

4 3 2 1

2:15 PM Thu Sep 26 2019 2:20 PM 2:25 PM

Table ▾ Format 20 Per Page ▾

< Hide Fields **All Fields**

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

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\_chash 3, image\_certcn 1, image\_ctime 3, image\_gid 1

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 argv0 /Applications/Firefox.app/Contents/MacOS/firefox  
cwd /  
eventcode 2  
image.btime 2019-09-17T17:37:29.000000000Z  
image.chash 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 c55285a84bfc0faf092363d96bac8652b357cd55d21634057d0541cdeefffa0  
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

Terminal Shell Edit View Window Help

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

max — bash — 114x26

~ -- bash ~ -- bash +

```
  "path": "/sbin/launchd"
}
],
"uid": 502,
"uname": "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": "c55285a84bf0faf092363d96bac8652b357cd55d21634057d0541cdeefffa0",
    "teamid": "43AQ936H96"
},
"pid": 14557,
"rgid": 20,
"rname": "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 Display time (UTC+00:00)

TABLE CHART Columns

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...	618429dd3e7885853ecc578e8d5a7b62a3465a44f3d20ae1b18fff067...
9/26/2019, 2:20:54.000 PM	91.34.254.149	xnumon_image_exec	/Applications/Firefox.app/Contents/MacOS/plugin-container.app/Conte...	618429dd3e7885853ecc578e8d5a7b62a3465a44f3d20ae1b18fff067...
9/26/2019, 2:20:53.000 PM	91.34.254.149	xnumon_image_exec	/Applications/Firefox.app/Contents/MacOS/plugin-container.app/Conte...	618429dd3e7885853ecc578e8d5a7b62a3465a44f3d20ae1b18fff067...
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

CCTOTALT : 515  
,  
"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 Display time (UTC+00:00)

TABLE CHART Columns

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/...	618429dd3e7885853ecc578e8d5a7b62a3465a44f3d20ae1b18fff067455c3
9/26/2019, 2:20:54.000 PM	91.34.254.149	santa_log	/Applications/Firefox.app/Contents/MacOS/plugin-container.app/Contents/...	618429dd3e7885853ecc578e8d5a7b62a3465a44f3d20ae1b18fff067455c3
9/26/2019, 2:20:53.000 PM	91.34.254.149	santa_log	/Applications/Firefox.app/Contents/MacOS/plugin-container.app/Contents/...	618429dd3e7885853ecc578e8d5a7b62a3465a44f3d20ae1b18fff067455c3
9/26/2019, 2:20:51.000 PM	91.34.254.149	santa_log	/Applications/Firefox.app/Contents/MacOS/firefox	c55285a84bf0faf092363d96bac8652b357cd55d21634057d0541cdeefffa0

Page 1 of 1 50 items per page 1 - 5 of 5 items

```
CCTOTALT : 515
},
"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 Microsoft Azure

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 Display time (UTC+00:00)

TABLE CHART Columns

Schema and Filter

Properties_fs_s	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

```
CCTOTALT : 01S
},
"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 Microsoft Azure

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 Display time (UTC+00:00)

TABLE .CHART Columns

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/Resour...	[ "python", "-m", "SimpleHTTPServer", "80" ]	/Users/Shared	good
91.34.254.149	xnumon_image_exec	/usr/bin/python	[ "python", "-m", "SimpleHTTPServer", "80" ]	/Users/Shared	good

Page 1 of 1 50 items per page 1 - 2 of 2 items

CCTOTALT : 01S  
},  
"time": "2019-09-26T14:20:54.797000000Z",

Schema and Filter

## 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“*



zentral.pro



[https://github.com/  
zentralopensource/  
MacSysAdmin-Conference-2019](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](mailto:hi@zentral.pro)

🌐 <https://int.zentral.pro>

🐦 [@zentral\\_io](https://zentral_io)



**zentral.pro**

# MacSysAdmin 2019