CROWDSTRIKE

Introducing the Next Generation of Mac Monitor

Brandon Dalton

Sr. Engineer – Threat Detection

CrowdStrike

Brandon Dalton

- Internals researcher
- Mac Developer
- OBTS v8.0 / OFTW v1.0 presenter
- Technical reviewer
- Lover of history
- @CrowdStrike – Sr. Engineer

github.com/Brandon7CC/mac-monitor

What made today possible...

A massive thank you to Matt Graeber and Keith McCammon!

"Without their support Mac Monitor would still be a closed project."

CROWDSTRIKE

And to CrowdStrike for sponsoring attendance!

Today's Talk

What is Mac Monitor?

Overview of core features.

Operationalizing Endpoint Security

Leveraging Endpoint Security in prod

v2.0 New Features!

What's new for this release?

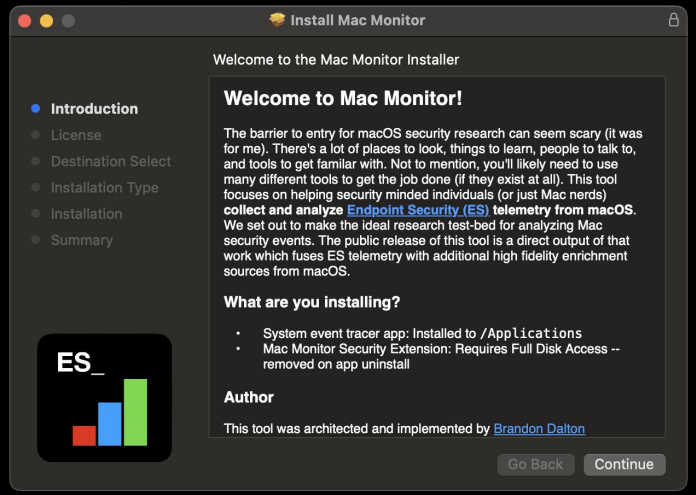
Quick Demo

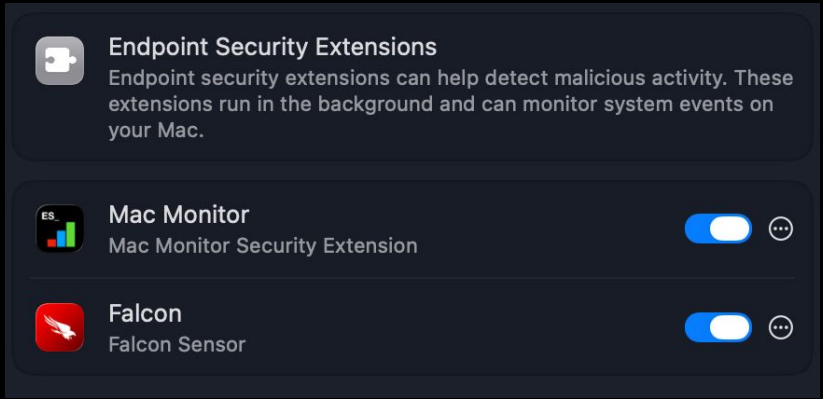
POSIX Atomic Test Harness

What is Mac Monitor?

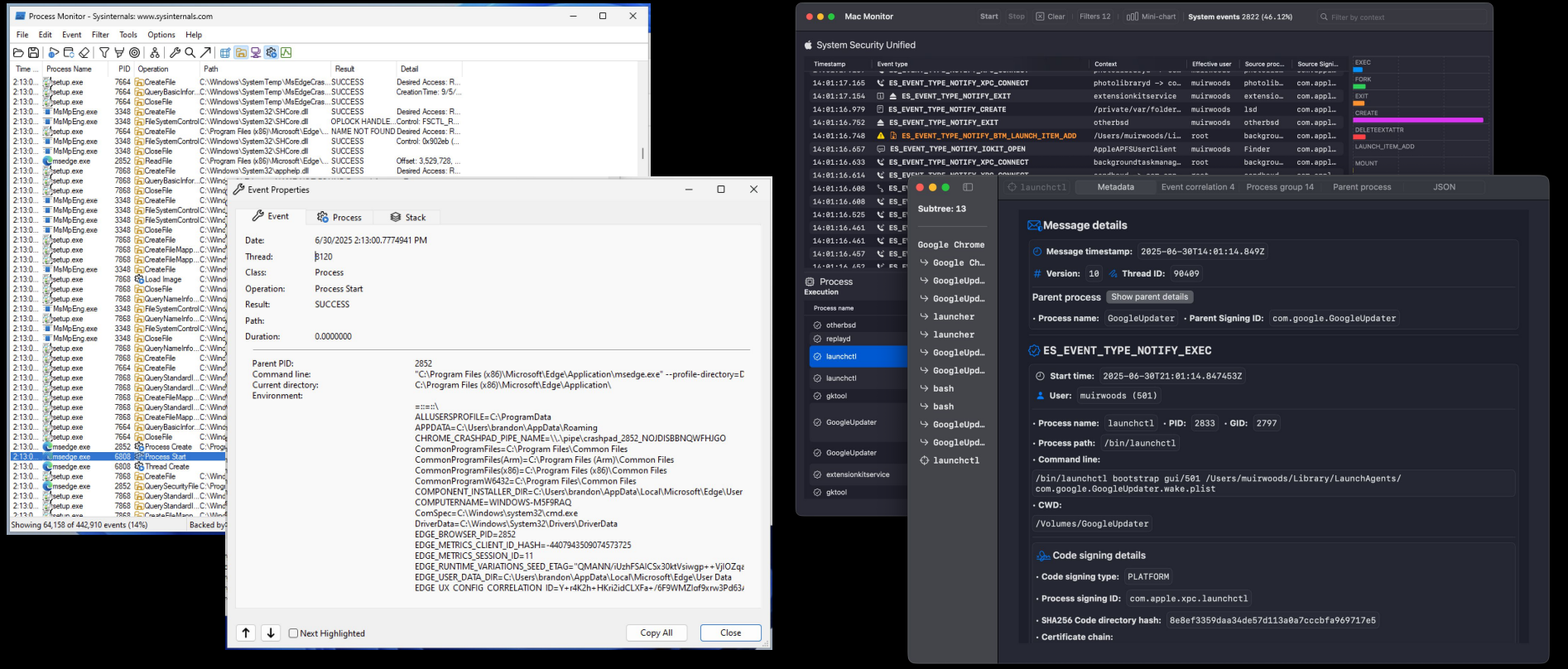
Mac Monitor `$ brew install --cask mac-monitor`

"The missing ProcMon for macOS": Mac Monitor records Endpoint Security events and displays them for analysis.

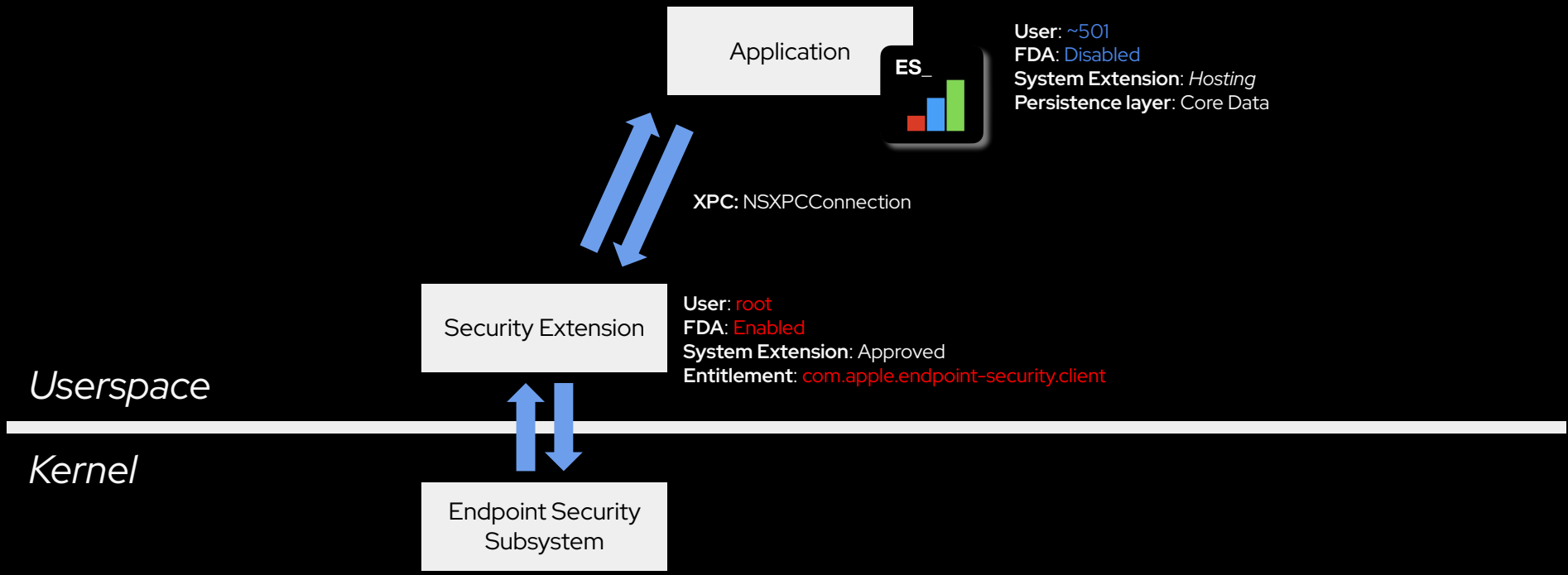




ProcMon and Mac Monitor



Architecture



⚡ Operationalizing Endpoint Security

CROWDSTRIKE

Event classes

Process	Interprocess	File system
File metadata	File system mounting	Code signing
Gatekeeper	XProtect	Kernel
Login	MDM	Memory mapping
OpenSSH	Socket	Authorization
Service Management	Link	TCC
Task port	XPC	Directory
File Provider	UID/GID	Clock

The API gives us?

Clients

ES Client

Subscribe and respond to events from ES

Event subscriptions

Event Type

NOTIFY / AUTH

(enumeration)

Message

Metadata, initiating process / thread, and event.

Event

Information about action on the system.

Response

ALLOW / DENY

Allow an event to continue or deny its action.

Muting

Initiating/target path literal

Mute a process literally by the full path.

Per-event

Target specific events.

Initiating/target path prefix

Mute a process by the path prefix.

Audit Token

Mute a process by its audit token.

Inversion

Suppress events not matching a path.

Dealing with noise (volume)

Muting

Initiating/target path literal

Mute a process literally by the full path.

Initiating/target path prefix

Mute a process by the path prefix.

Audit Token

Mute a process by its audit token.

Per-event

Target specific events.

Inversion

Suppress events not matching a path.

```
var eventRules = [
    (eventType: ES_EVENT_TYPE_NOTIFY_MMAP, muteType: ES_MUTE_PATH_TYPE_LITERAL, paths: [
        "/usr/bin/tailspin",
        "/usr/libexec/spindump",
        ...
    ]),
    (eventType: ES_EVENT_TYPE_NOTIFY_MMAP, muteType: ES_MUTE_PATH_TYPE_TARGET_PREFIX, paths:
[       "/Library/Caches/",
        "/private/var/db/",
        ...
    ])
]
```

```
let pathMute: es_return_t = es_mute_path(_:_:_:)
let pathEventsMute: es_return_t = es_mute_path_events(_:_:_:_:_:)
```

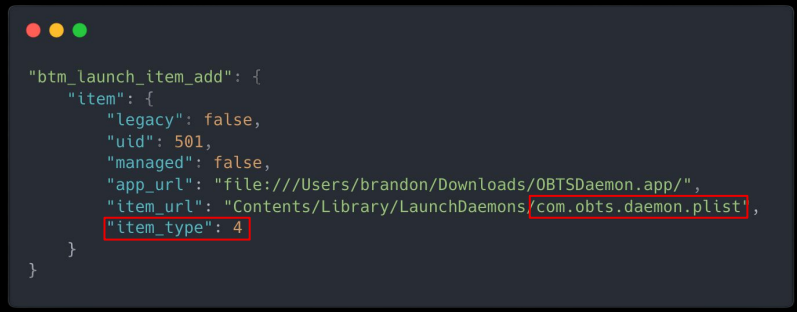
ESClient.h
ESTypes.h

Enrichment?

Example: API vs. *ESLogger*

In many cases, ES events, are not ready to go out of the box for threat detection.

- What's the plist contents?
- What's item_type=4?
- What's fdtype=1?
- What's cs_validation_category=1?
- If the process File Quarantine-aware?
- What are the code signing certs?



Why is Enrichment Necessary?

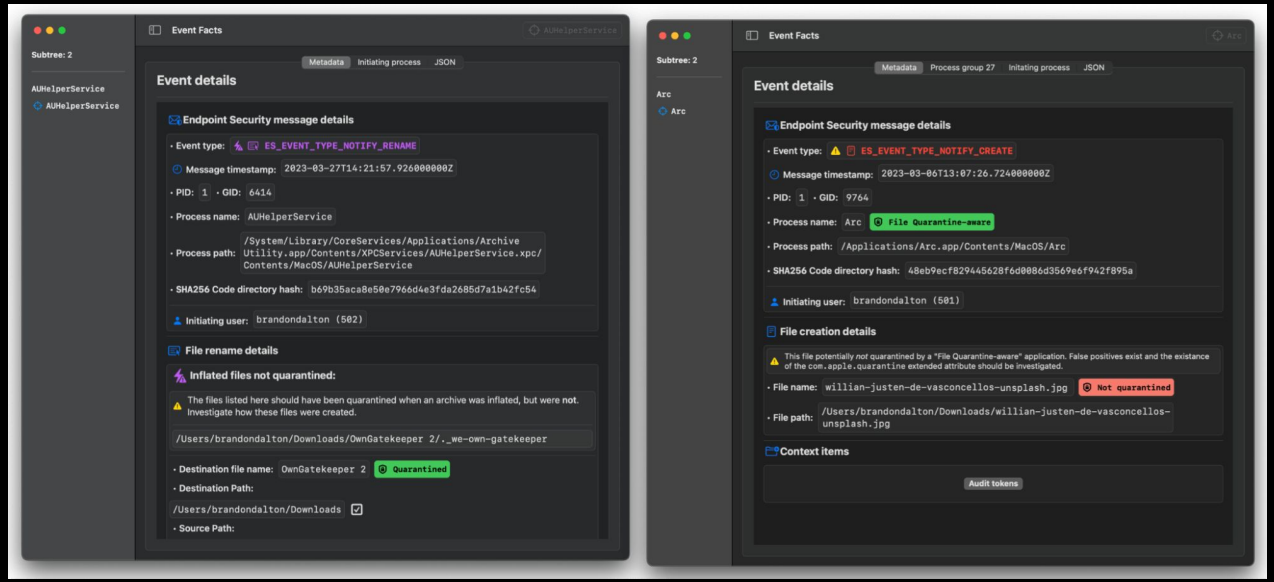
E.g., CVE-2023-27951 and CVE-2023-27943

Finding and reporting a Gatekeeper bypass exploit with help from Mac Monitor

Mac Monitor, our newly released free collection tool, helped us discover a pair of vulnerabilities that we disclosed to Apple

BRANDON DALTON

Originally published May 11, 2023. Last modified April 30, 2024.

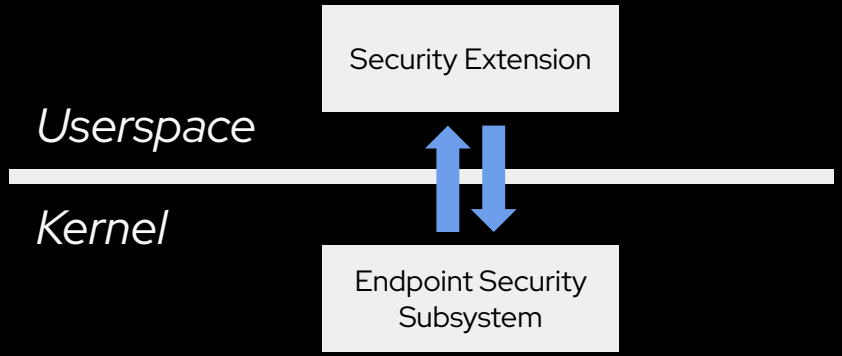


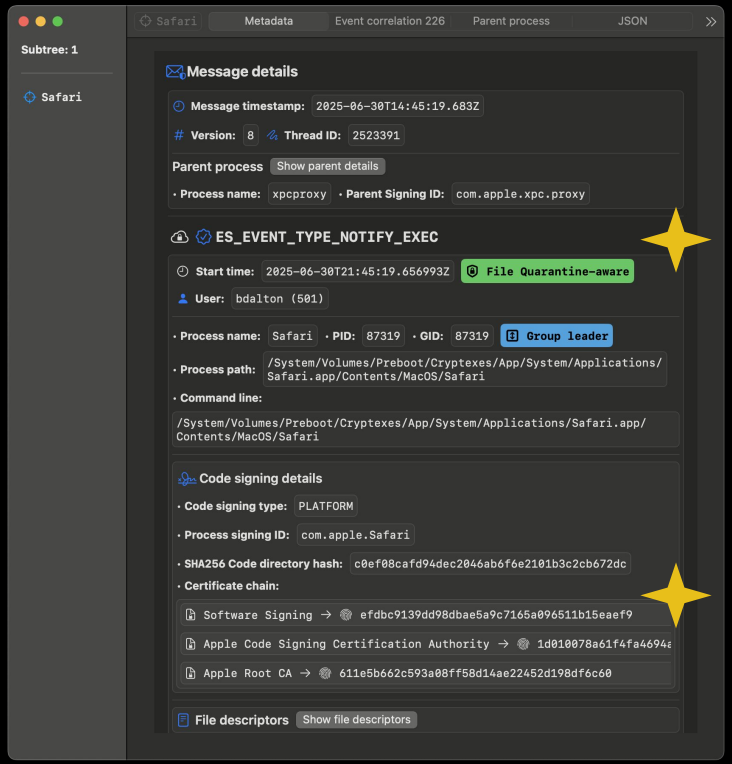
Mac Monitor Core features?

System Extension based

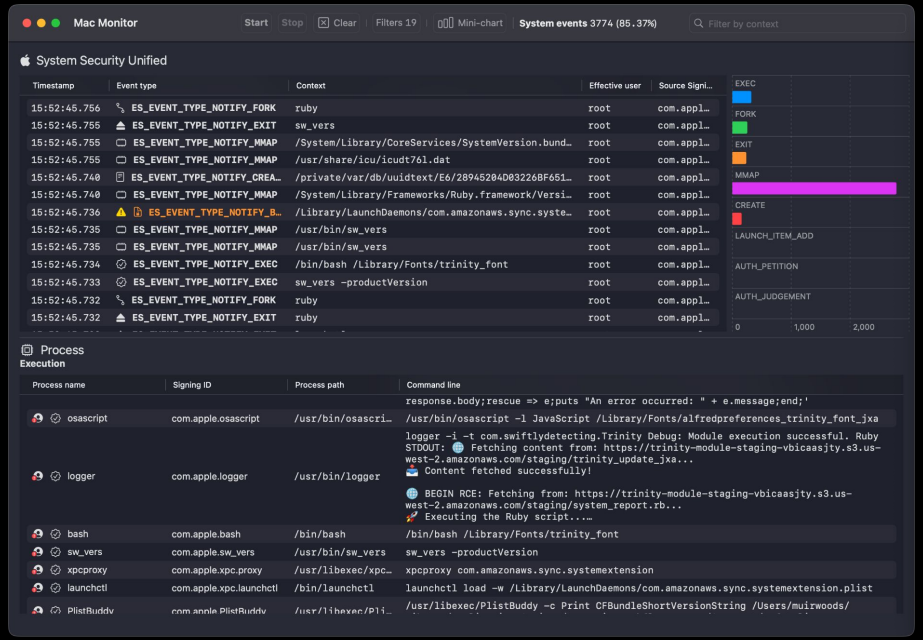
This is *not* an ESLogger proxy / front

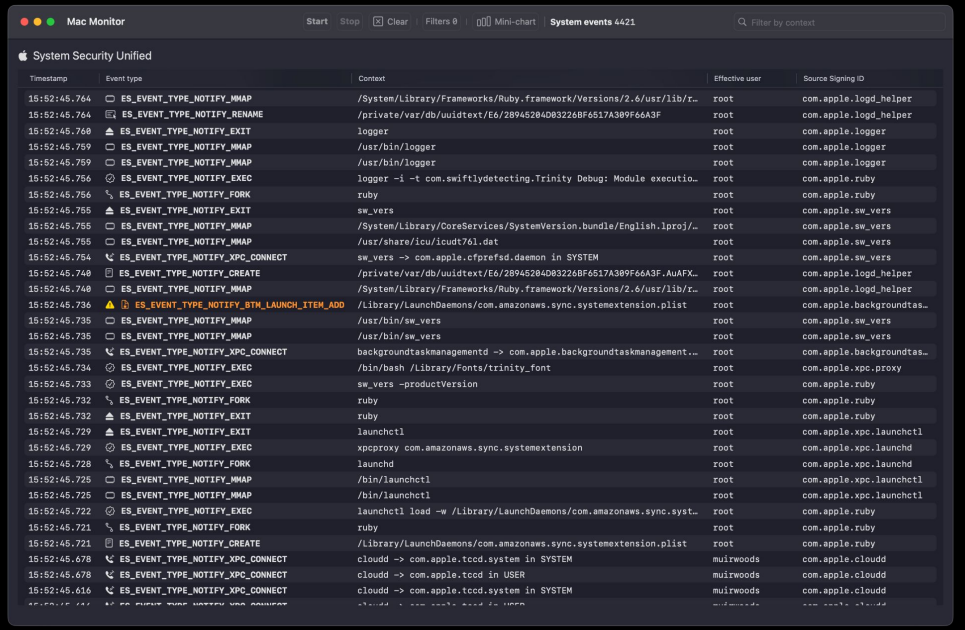
- Enables: tailored event models
  - Process File Quarantine-aware, X509 signing certs, PLIST, etc.
  - PoC enhancements to ES for threat detection





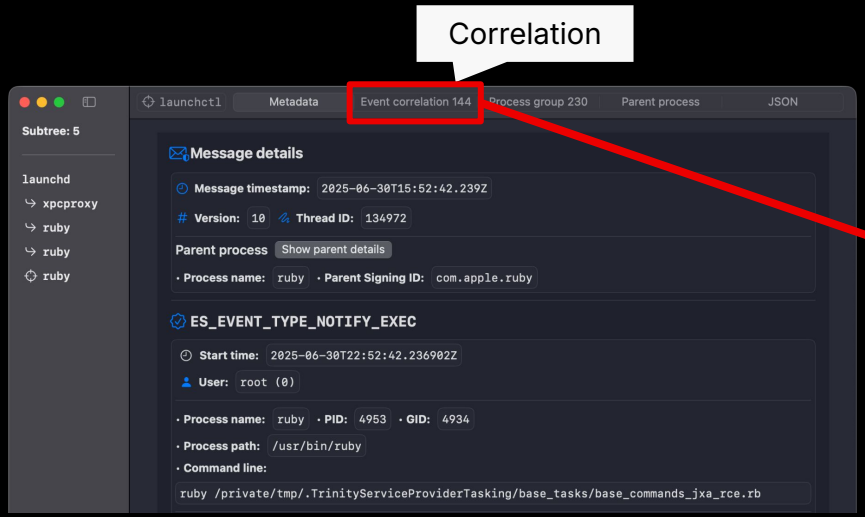
Intuitive UX



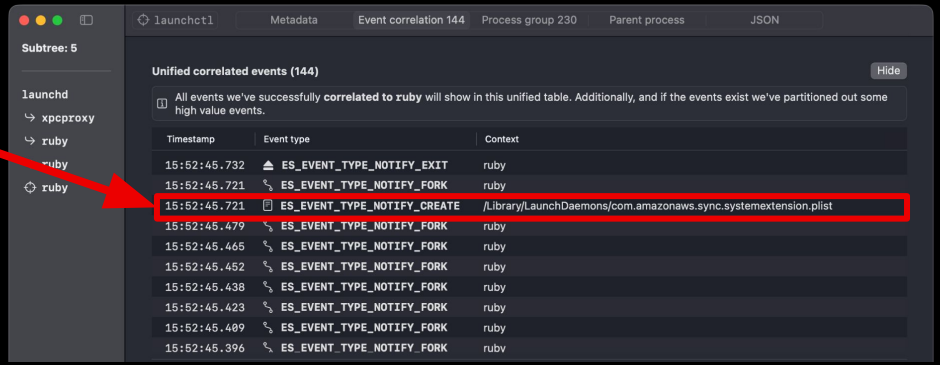


Event correlation

Event correlation (via audit token) – *"Which actions did this process take?"*

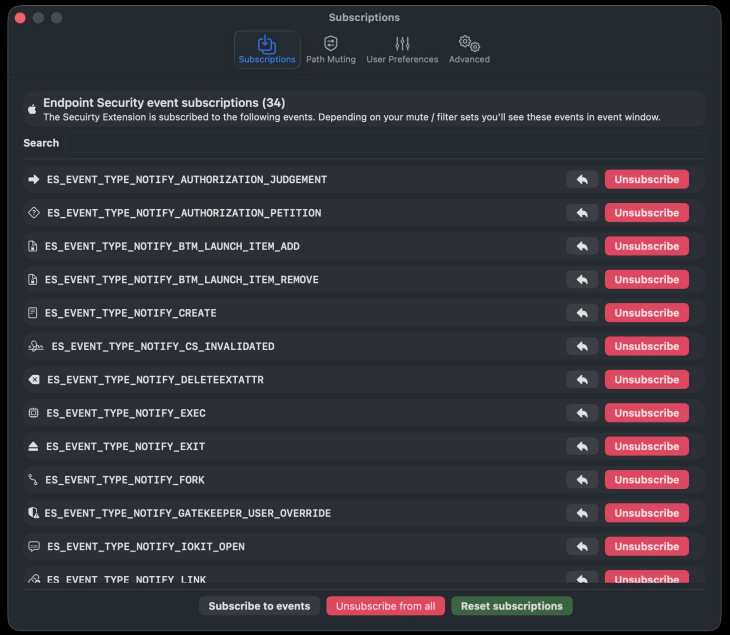


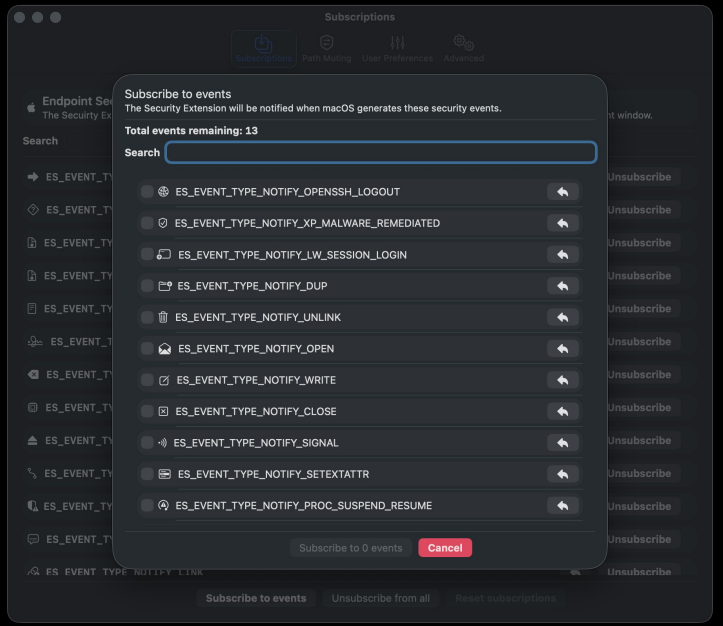
Created:
`com.amazonaws.sync.systemextension.plist`



Dynamic event subscriptions

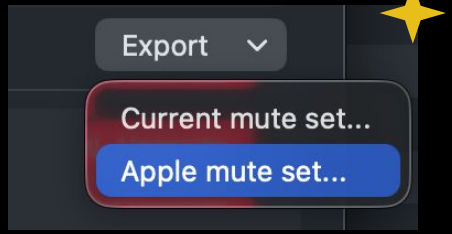
- Dynamic event subscriptions (47 *currently*) via the UI
  - Process, interprocess, code signing, memory, login, services, etc.

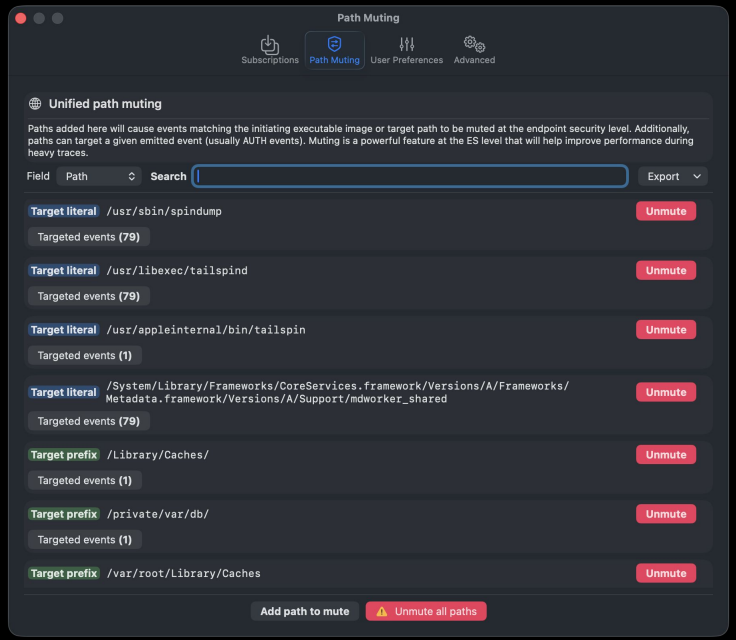


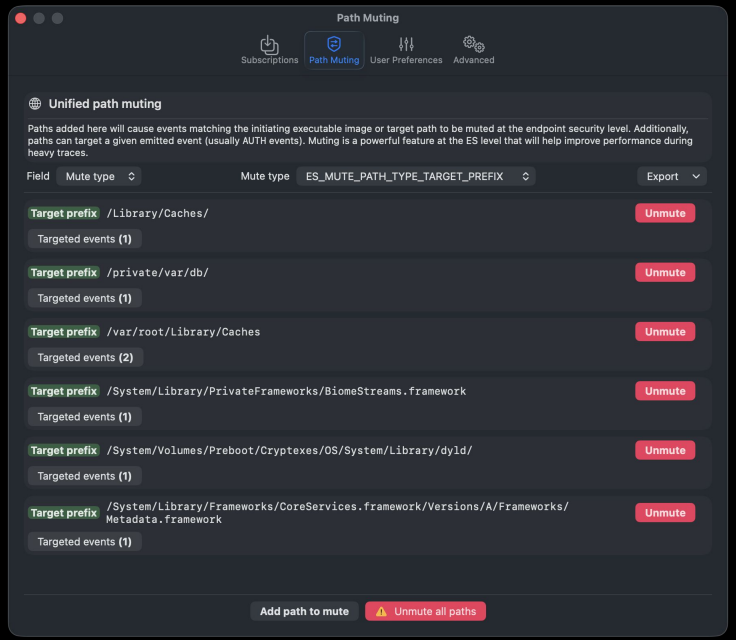


Path muting

- User configurable path muting via the UI
  - Performant noise reduction







BSD-3 Open Source!

README | BSD-3-Clause license

BSD 3-Clause License

Copyright (c) 2025, Red Canary, a Zscaler company

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

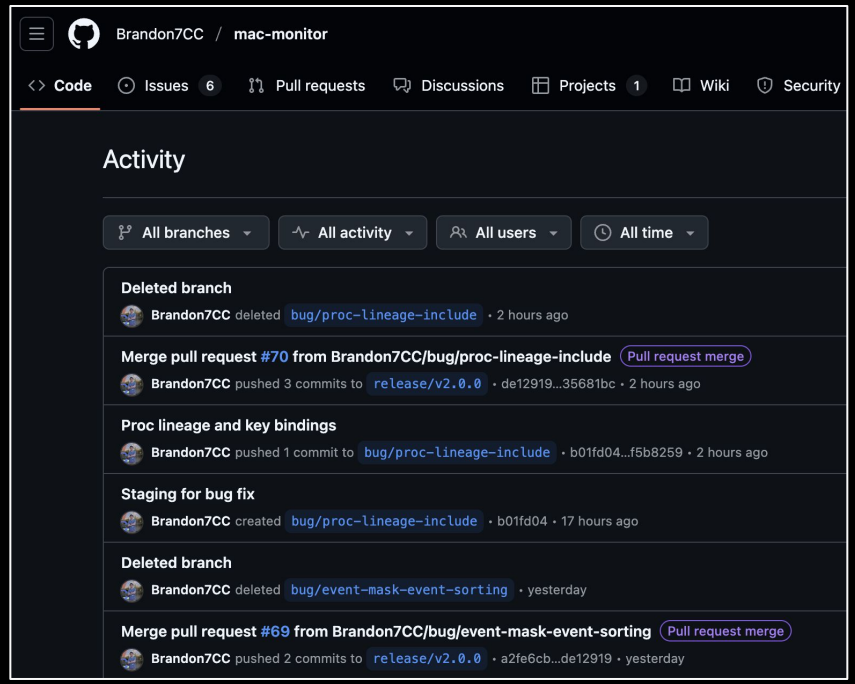
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. Neither the name of the copyright holder nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Send ideas

Help with dev :)



Open Development

What's new?

110+ PRs

Expanded key bindings

Event mask searching

Light / dark mode

BSD-3 License

ESLogger standardization

Process tree targeting

(New event) Set Mode

(New event) UIPC Bind

(New event) Gatekeeper User Override

Liquid Glass

Homebrew migration

Mute set searching

Export default Apple mute set

(New event) TCC Modify

Structured event facts UI

Live context search

(New event) UIPC Connect

Event subscriptions searching

Auto updates

Support Matrix

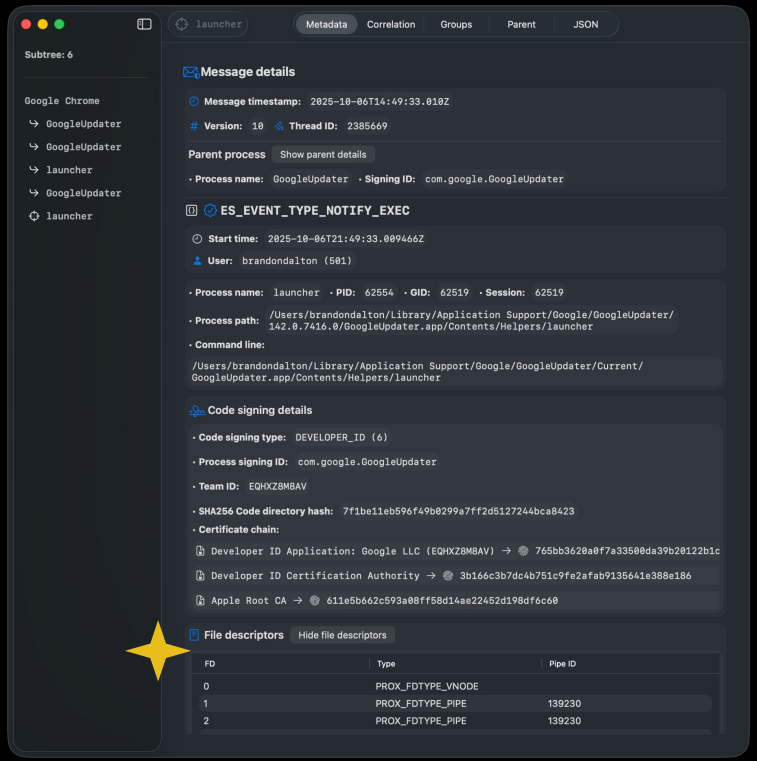
Session grouping

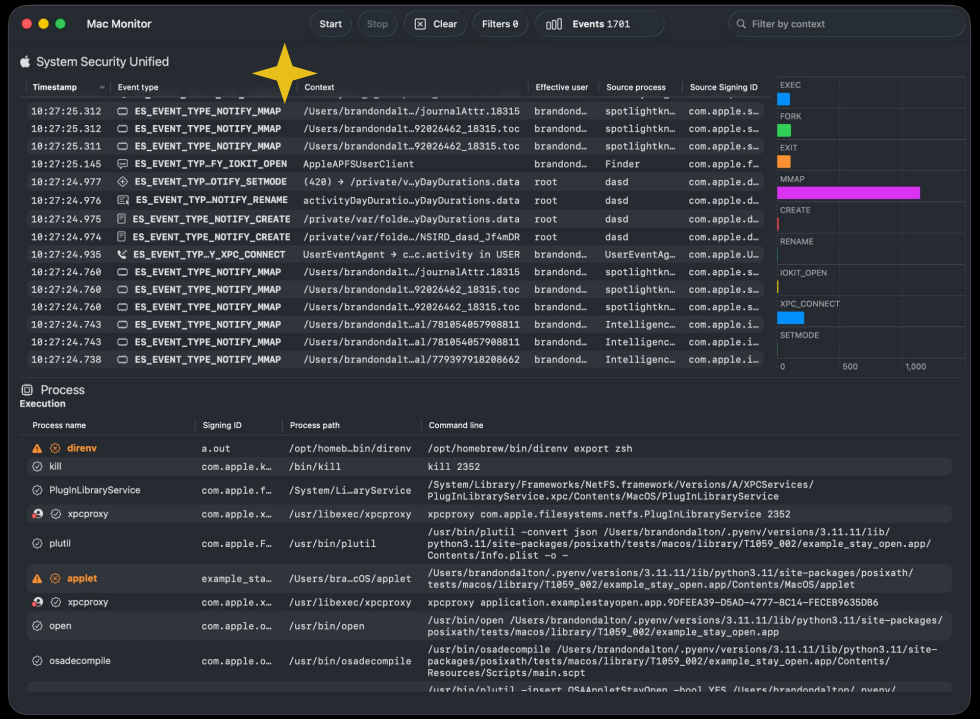
(New event) PTY Grant

Performance (Core Data)

SpriteTree compatibility

UI / UX updates (app wide)

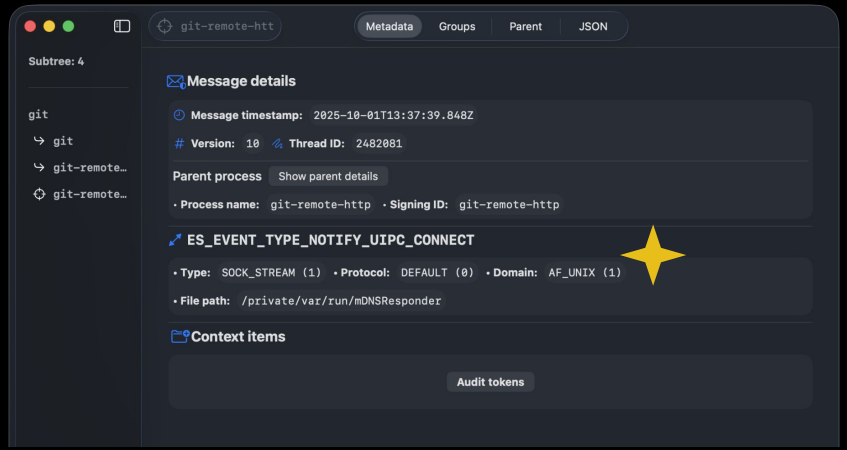


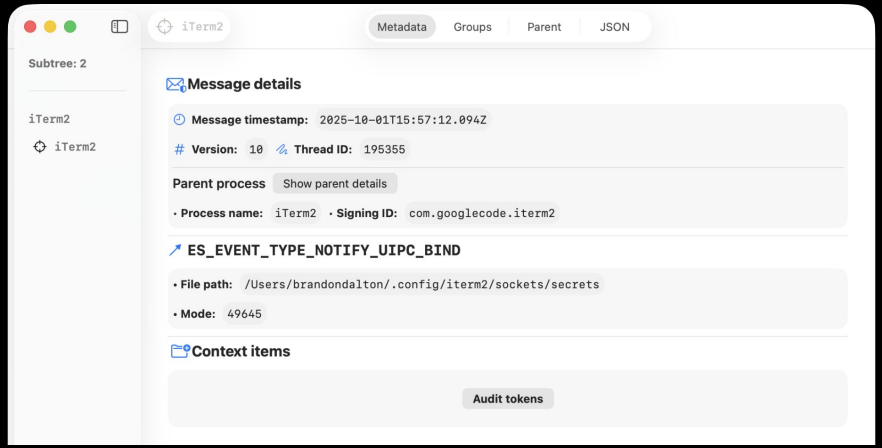


Socket events

- **UIPC Connect**: a UNIX-domain socket is about to be connected.
- **UIPC Bind**: UNIX-domain socket is about to be bound to a path.

Enables monitoring for anomalous IPC communication pipes
(e.g. to `mDNSResponder`)

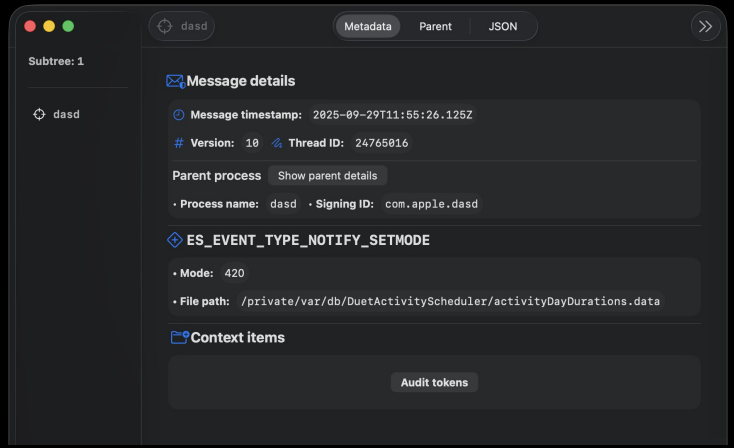


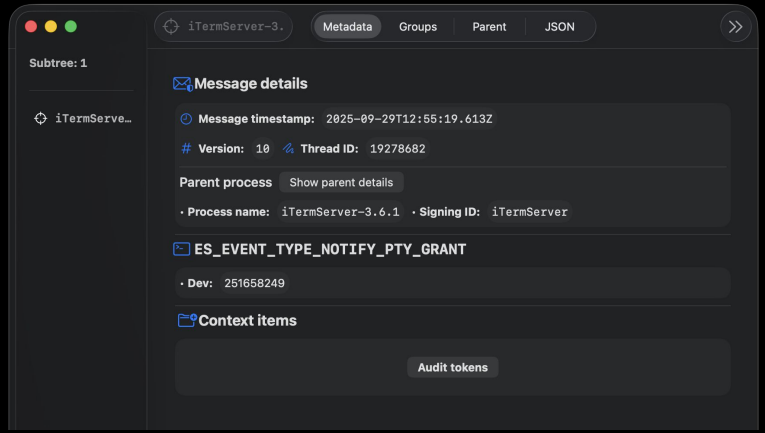


File Metadata events

- **Set Mode**: File mode modification.
  - ***Use case**: Attackers likely need to modify permissions for execution*

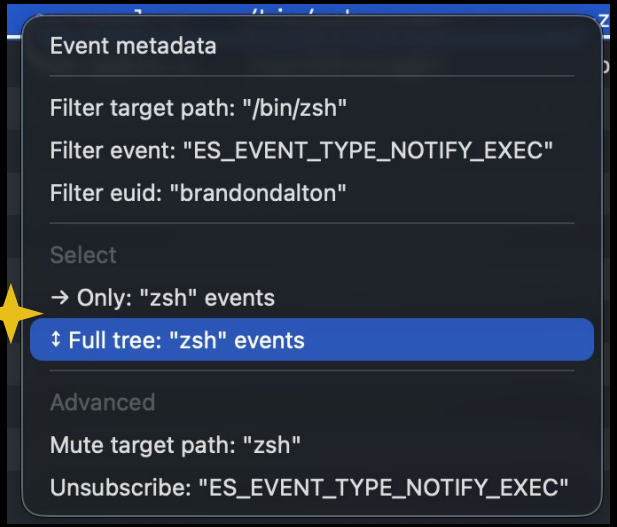
- **PTY Grant**: A pseudoterminal control device is granted
  - ***Use case**: PTYs granted outside of expected contexts*

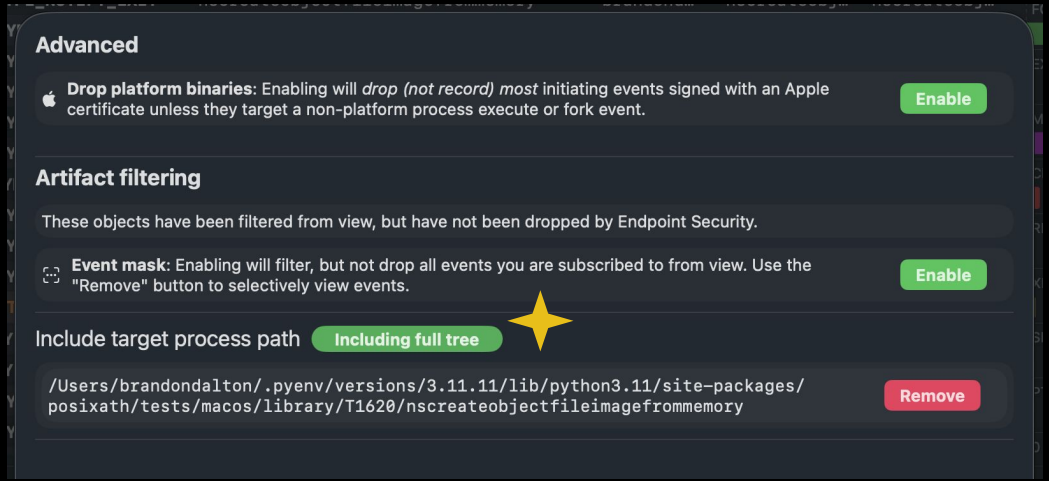




Targeting activity

Shoutout to Mitch Datka (@CrowdStrike) for the idea!





ESLogger standardization 🤒

Event overview

Events	v1.0.5	v1.9.0	v2.0.0
Process events	⚠	✅	✅
exec	⚠	✅	✅
fork	⚠	✅	✅
exit	⚠	✅	✅
signal	⚠	✅	✅
proc_suspend_resume	⚠	✅	✅
check	⚠	✅	✅
Interprocess events	⚠	⚠	✅
remote_thread_create	⚠	⚠	✅
trace	⚠	⚠	✅
File system events	⚠	⚠	✅
create	⚠	⚠	✅
rename	⚠	⚠	✅
write	⚠	⚠	✅
open	⚠	⚠	✅
close	⚠	⚠	✅
dup	⚠	⚠	✅
File system mounting	⚠	⚠	✅
mount	⚠	⚠	✅

Event overview

Events	v1.0.5	v1.9.0	v2.0.0
File metadata events	⚠	⚠	✅
deleteextattr	⚠	⚠	✅
setextattr	⚠	⚠	✅
pty_grant	❌	❌	✅
setmode	❌	❌	✅
Link events	⚠	⚠	✅
link	⚠	⚠	✅
unlink	⚠	⚠	✅
Code signing events	⚠	⚠	✅
code_signature_invalida	⚠	⚠	✅
Kernel events	⚠	⚠	✅
iokit_open	⚠	⚠	✅
Memory events	⚠	⚠	✅
mmap	⚠	⚠	✅
Task port events	⚠	⚠	✅
get_task	⚠	⚠	✅

Event overview

Events	v1.0.5	v1.9.0	v2.0.0
Socket events	❌	❌	✅
uipc_connect	❌	❌	✅
uipc_bind	❌	❌	✅
XPC events	⚠	⚠	✅
xpc_connect	⚠	⚠	✅
Service Management ev	⚠	⚠	✅
btm_launch_item_add	⚠	⚠	✅
btm_launch_item_remov	⚠	⚠	✅
Security authorization e	⚠	⚠	✅
authorization_petition	⚠	⚠	✅
authorization_judgemen	⚠	⚠	✅
Login events	⚠	⚠	✅
login_login	⚠	⚠	✅
lw_session_login	⚠	⚠	✅
lw_session_unlock	⚠	⚠	✅
OpenSSH events	⚠	⚠	✅
openssh_login	⚠	⚠	✅
openssh_logout	⚠	⚠	✅

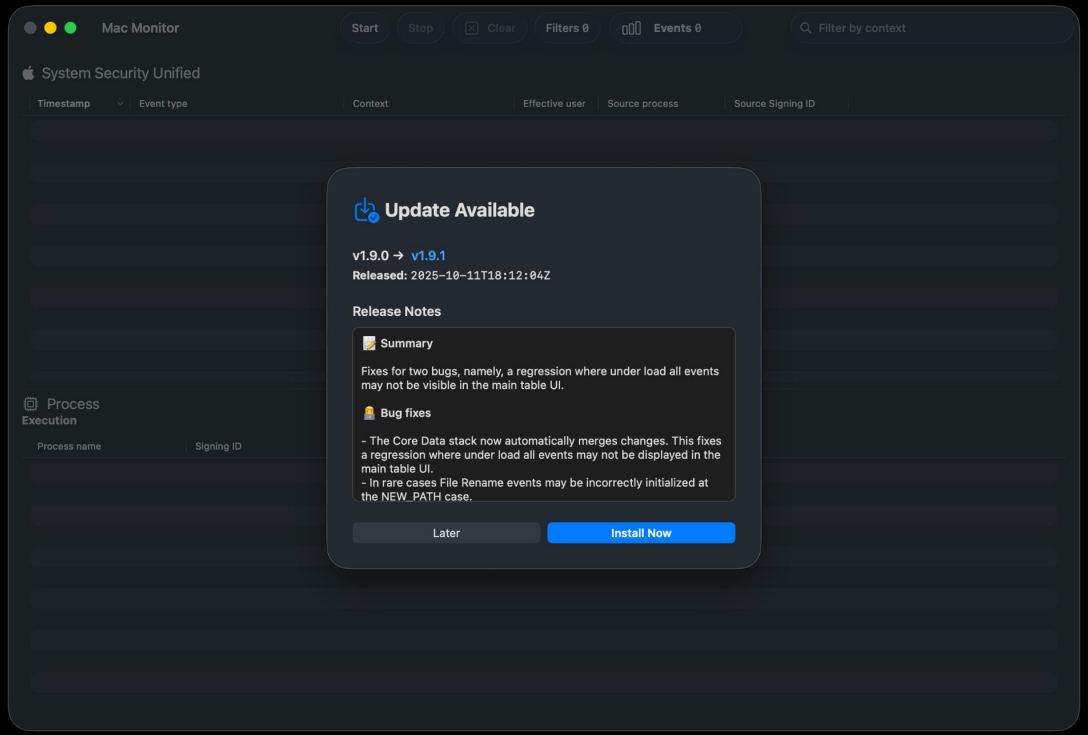
Event overview

Events	v1.0.5	v1.9.0	v2.0.0
MDM events	⚠	✅	✅
profile_add	⚠	✅	✅
XProtect events	⚠	⚠	✅
xp_malware_detected	⚠	⚠	✅
xp_malware_remediate	⚠	⚠	✅
TCC events	❌	✅	✅
tcc_modify	❌	✅	✅
Gatekeeper events	❌	✅	✅
gatekeeper_useroverride	❌	✅	✅
OpenDirectory events	⚠	⚠	⚠
od_create_user	⚠	⚠	⚠
od_group_add	⚠	⚠	⚠
od_modify_password	⚠	⚠	⚠
od_attribute_value_add	⚠	⚠	⚠
od_create_group	⚠	⚠	⚠

See GitHub for the link

CROWDSTRIKE

Auto updating!



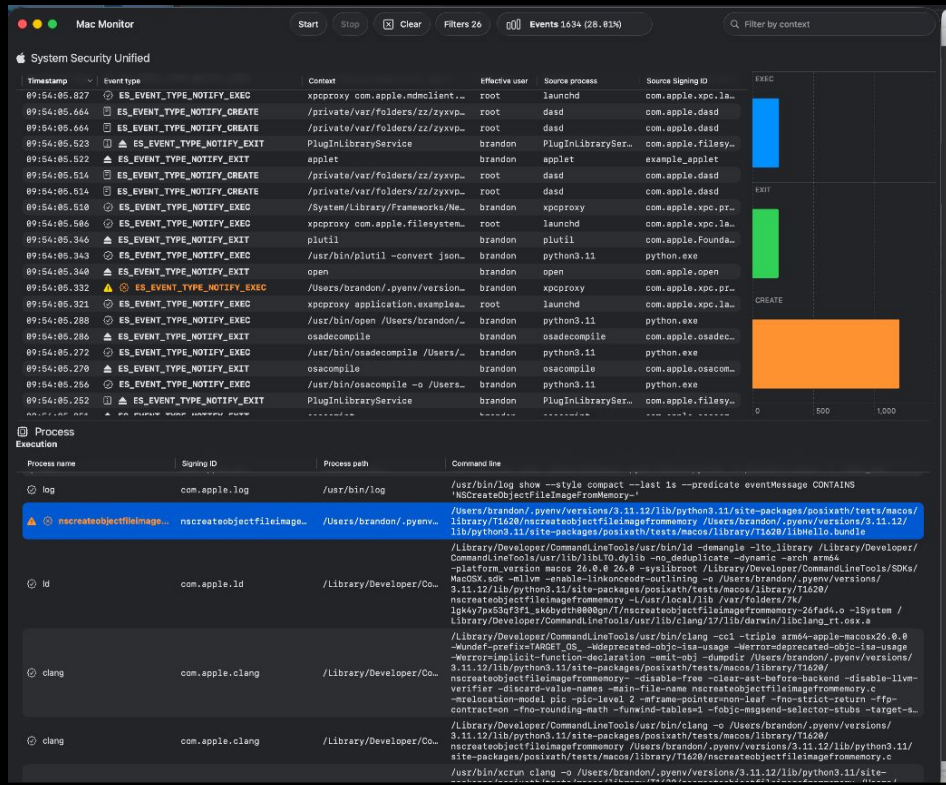
v1.9 feature

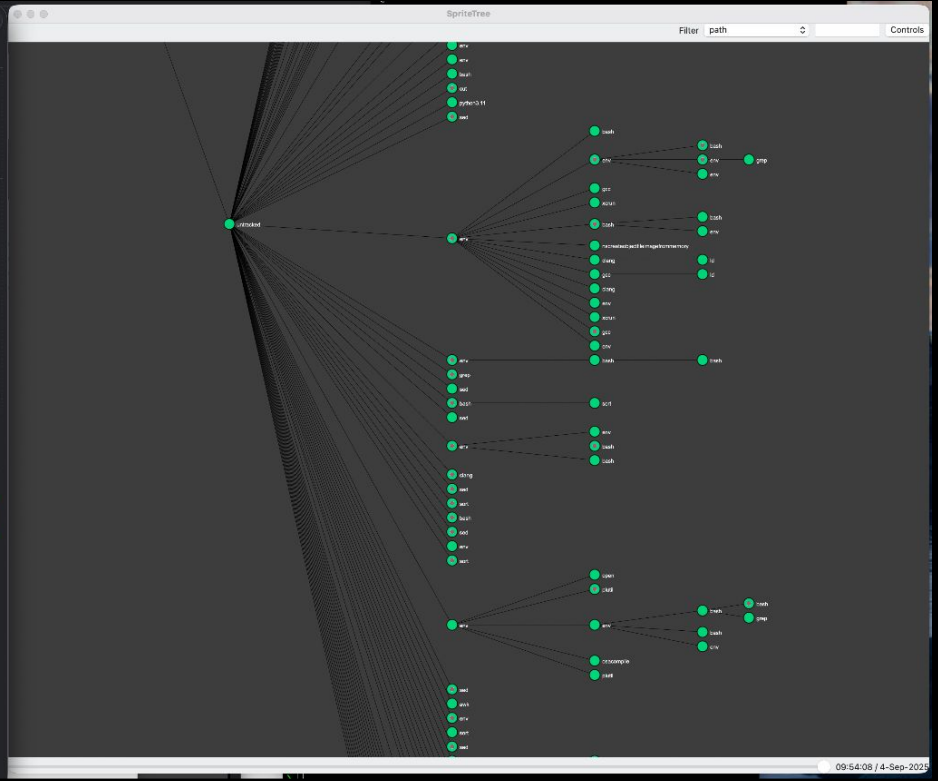
Demo and Release

Correlation w/AppleScript & Reflective Code Loading

```
$ pip install posixath
```

SpriteTree compatibility!





CROWDSTRIKE

$ brew install --cask mac-monitor

Brandon Dalton

CrowdStrike