



Introducing the Next Generation of Mac Monitor

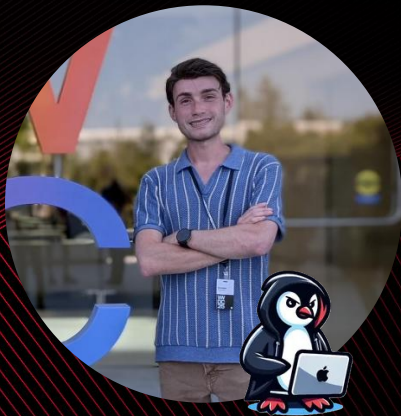
Brandon Dalton

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."



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

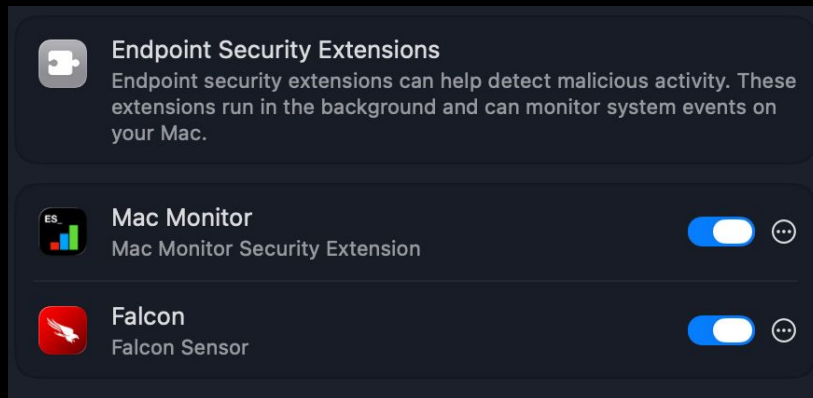
POSIX Atomic Test Harness

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.



The screenshot displays the Windows Process Monitor (ProcMon) application. The main window shows a list of events with columns for Time, Process Name, PID, Operation, Path, Result, and Detail. The events are filtered to show 'Process Create' operations. The 'Event Properties' window is open, showing details for a specific event where 'setup.exe' created 'msedge.exe'.

Time	Process Name	PID	Operation	Path	Result	Detail
21:30...	setup.exe	7654	CreateFile	C:\Windows\SystemTemp\MsEdgeCra...	SUCCESS	Desired Access: R...
21:30...	setup.exe	7654	QueryBasicInfor...	C:\Windows\SystemTemp\MsEdgeCra...	SUCCESS	CreationTime: 5/5/...
21:30...	setup.exe	7654	CreateFile	C:\Windows\SystemTemp\MsEdgeCra...	SUCCESS	
21:30...	MsEdge.exe	3348	CreateFile	C:\Windows\System32\SHCore.dll	SUCCESS	Desired Access: R...
21:30...	MsEdge.exe	3348	FileSystemControl...	C:\Program Files (x86)\Microsoft Edg...	OPLOCK HANDLE...	Control: FSCTL_R...
21:30...	setup.exe	7654	CreateFile	C:\Windows\System32\SHCore.dll	NAME NOT FOUND	Desired Access: R...
21:30...	MsEdge.exe	3348	FileSystemControl...	C:\Windows\System32\SHCore.dll	SUCCESS	Control: 0x00b0 (...)
21:30...	MsEdge.exe	3348	CreateFile	C:\Windows\System32\SHCore.dll	SUCCESS	
21:30...	msedge.exe	2852	Process Create	C:\Program Files (x86)\Microsoft Edge\...	SUCCESS	Offset: 3,529,728...
21:30...	setup.exe	7658	CreateFile	C:\Windows\System32\api-ms-win-...	SUCCESS	Desired Access: R...
21:30...	setup.exe	7658	QueryBasicInfor...	C:\Wind...		
21:30...	setup.exe	7658	CreateFile	C:\Wind...		
21:30...	MsEdge.exe	3348	CreateFile	C:\Wind...		
21:30...	MsEdge.exe	3348	FileSystemControl...	C:\Wind...		
21:30...	MsEdge.exe	3348	CreateFile	C:\Wind...		
21:30...	setup.exe	7658	CreateFile	C:\Wind...		
21:30...	setup.exe	7658	CreateFileMap...	C:\Wind...		
21:30...	MsEdge.exe	3348	CreateFile	C:\Wind...		
21:30...	setup.exe	7658	Load Image	C:\Wind...		
21:30...	setup.exe	7658	CreateFile	C:\Wind...		
21:30...	setup.exe	7658	QueryNameInfo...	C:\Wind...		
21:30...	MsEdge.exe	3348	FileSystemControl...	C:\Wind...		
21:30...	setup.exe	7658	QueryNameInfo...	C:\Wind...		
21:30...	MsEdge.exe	3348	CreateFile	C:\Wind...		
21:30...	setup.exe	7658	QueryNameInfo...	C:\Wind...		
21:30...	setup.exe	7658	CreateFile	C:\Wind...		
21:30...	setup.exe	7658	QueryStandard...	C:\Wind...		
21:30...	setup.exe	7658	QueryStandard...	C:\Wind...		
21:30...	setup.exe	7658	CreateFileMap...	C:\Wind...		
21:30...	setup.exe	7658	QueryStandard...	C:\Wind...		
21:30...	setup.exe	7658	QueryBasicInfor...	C:\Wind...		
21:30...	setup.exe	7658	CreateFile	C:\Wind...		
21:30...	msedge.exe	2852	Process Create	C:\Program Files (x86)\Microsoft Edge\...		
21:30...	msedge.exe	6808	Thread Create			
21:30...	setup.exe	7658	CreateFile	C:\Wind...		
21:30...	msedge.exe	2852	QuerySecurityFile...	C:\Prog...		
21:30...	setup.exe	7658	QueryStandard...	C:\Wind...		
21:30...	setup.exe	7658	QueryStandard...	C:\Wind...		
21:30...	setup.exe	7658	QueryBasicInfor...	C:\Wind...		

Event Properties

- Event:** Process
- Stack:**
- Date:** 6/30/2025 21:30:07.7774941 PM
- Thread:** 0
- Class:** Process
- Operation:** Process Start
- Result:** SUCCESS
- Path:**
- Duration:** 0.0000000
- Parent PID:** 2852
- Command line:** "C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --profile-directory=C:\Program Files (x86)\Microsoft\Edge\Application\
- Current directory:**
- Environment:**

```

===A
ALLUSERSPROFILE=C:\ProgramData
APPDATA=C:\Users\brandon\AppData\Local\Roaming
CHROME_CRASHPAD_PIPE_NAME=\\pipe\crashpad_2852_NOIDISBNCWFHGO
COMMONPROGRAMFILES=C:\Program Files (x86)\Common Files
COMMONPROGRAMFILES(X86)=C:\Program Files (x86)\Common Files
COMMONPROGRAMFILES(ARM)=C:\Program Files (ARM)\Common Files
COMMONPROGRAMFILES(ARM64)=C:\Program Files (ARM64)\Common Files
COMPONENT_INSTALLER_DIR=C:\Users\brandon\AppData\Local\Microsoft\Edge\User
COMPUTERNAME=WINDOWS-M5F9RAQ
CONSPEC=C:\Windows\system32\cmd.exe
DRIVERDATA=C:\Windows\System32\Drivers\DriverData
EDGE_BROWSER_PID=2852
EDGE_METRICS_CLIENT_ID_HASH=440794350907457325
EDGE_METRICS_SESSION_ID=11
EDGE_RUNTIME_VARIATIONS_SEED_ETAG=0xMANIN\UshFSAicSx30k\wvgr+~+VjQZqZ
EDGE_USER_DATA_DIR=C:\Users\brandon\AppData\Local\Microsoft\Edge\User
EDGE_USR_CONFIG_CORRELATION_ID=y+rk2h~HkizdCLXf+~6F9W\WZl0frnw3Pd63

```

The screenshot shows the 'System Security' window on a Mac. The 'Process Execution' section is active, displaying a list of processes. The 'launchctl' process is selected, and its details are shown on the right. The details include message timestamp, version, thread ID, parent process, start time, user, process name, path, command line, and code signing details.

Timestamp	Event type	Context	Effective user	Source proc.	Source Sign.	EXEC
14:01:17.165	ES_EVENT_TYPE_NOTIFY_XPC_CONNECT	photolibraryd -> co.	muirwoods	photolib.	com.apple.	EXEC
14:01:17.154	ES_EVENT_TYPE_NOTIFY_EXIT	extensionkitservice	muirwoods	extensio.	com.apple.	EXIT
14:01:16.979	ES_EVENT_TYPE_NOTIFY_CREATE	/private/var/folder.	muirwoods	lsd	com.apple.	CREATE
14:01:16.752	ES_EVENT_TYPE_NOTIFY_EXIT	otherbsd	muirwoods	otherbsd	com.apple.	DELETEEXTATB
14:01:16.748	ES_EVENT_TYPE_NOTIFY_BTM_LAUNCH_ITEM_ADD	/Users/muirwoods/Li.	root	backgrou.	com.apple.	LAUNCH_ITEM_ADD
14:01:16.657	ES_EVENT_TYPE_NOTIFY_IOKIT_OPEN	AppleAPFSUserClient	muirwoods	Finder	com.apple.	MOUNT
14:01:16.633	ES_EVENT_TYPE_NOTIFY_XPC_CONNECT	backgroundtaskmanag.	root	backgrou.	com.apple.	
14:01:16.614	ES_EVENT_TYPE_NOTIFY_XPC_CONNECT					
14:01:16.608	ES_E					
14:01:16.608	ES_E					
14:01:16.525	ES_E					
14:01:16.461	ES_E					
14:01:16.461	ES_E					
14:01:16.457	ES_E					
14:01:16.453	ES_E					

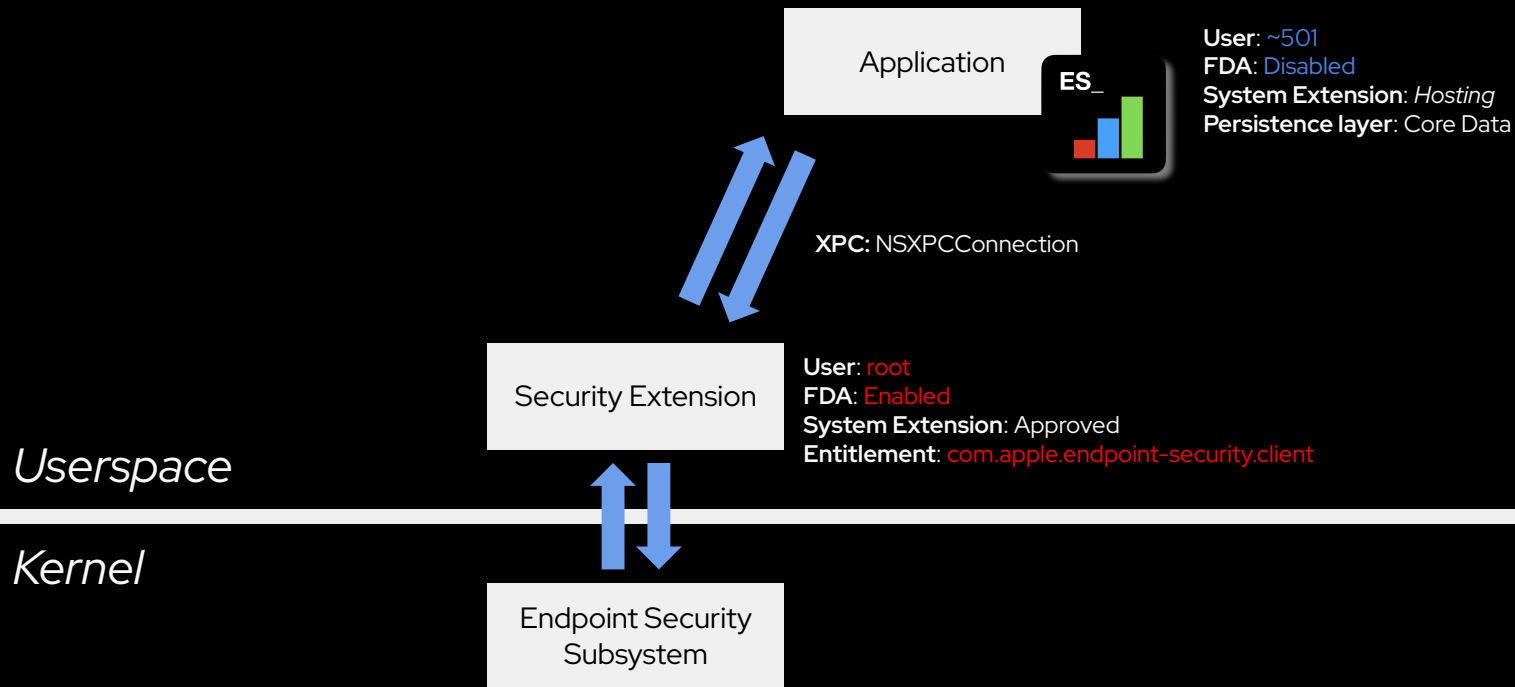
Subtree: 13

- Process Execution
 - Process name
 - otherbsd
 - replayd
 - launchctl**
 - launchctl
 - gktool
 - GoogleUpdater
 - GoogleUpdater
 - extensionkitservice
 - gktool

Message details

- Message timestamp: 2025-06-30T14:01:14.849Z
- Version: 10 Thread ID: 90489
- Parent process: [Show parent details](#)
 - Process name: GoogleUpdater
 - Parent Signing ID: com.google.GoogleUpdater
- ES_EVENT_TYPE_NOTIFY_EXEC
 - Start time: 2025-06-30T21:01:14.847453Z
 - User: muirwoods (501)
 - Process name: launchctl PID: 2833 GID: 2797
 - Process path: /bin/launchctl
 - Command line: /bin/launchctl bootstrap gui/501 /Users/muirwoods/Library/LaunchAgents/com.google.GoogleUpdater.wake.plist
 - CWD: /Volumes/GoogleUpdater
- Code signing details
 - Code signing type: PLATFORM
 - Process signing ID: com.apple.xpc.launchctl
 - SHA256 Code directory hash: 8e8ef3359daa34de57d113a8a7cccba969717e5
 - Certificate chain:

Architecture



Operationalizing Endpoint Security

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.

[illegible]

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?

```
"exec": {
  "args": [
    "ls",
    "-lah0"
  ],
  "cwd": {
    "path": "\\Users\\brandon"
  },
  "fds": [
    {
      "fd": 0,
      "fdtype": 1
    }
  ],
  "target": {
    "tty": {
      "path": "\\dev\\ttys007"
    },
    "executable": {
      "path": "\\bin\\ls"
    },
    "cs_validation_category": 1,
    "signing_id": "com.apple.ls",
    "is_platform_binary": true,
    "codesigning_flags": 637601793
  },
  "env": [ ... ]
}
```

```
"btm_launch_item_add": {
  "item": {
    "legacy": false,
    "uid": 501,
    "managed": false,
    "app_url": "file:///Users/brandon/Downloads/OBTSDaemon.app/",
    "item_url": "Contents/Library/LaunchDaemons/com.obts.daemon.plist",
    "item_type": 4
  }
}
```

Why is Enrichment Necessary?



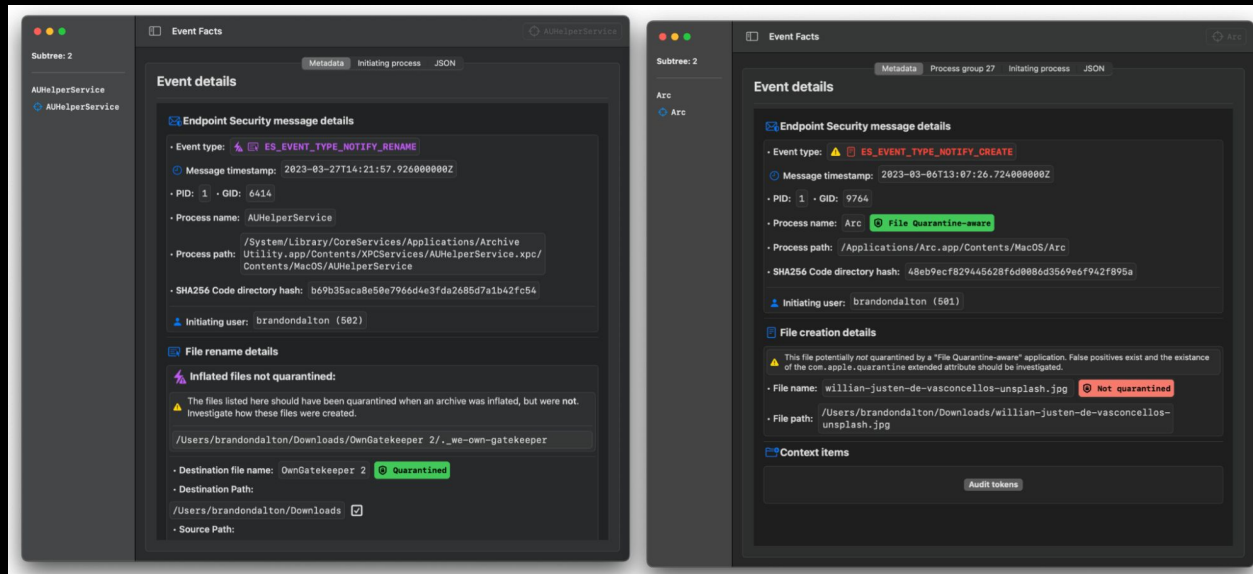
E.g., CVE-2023-27951 and CVE-2023-27943

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.



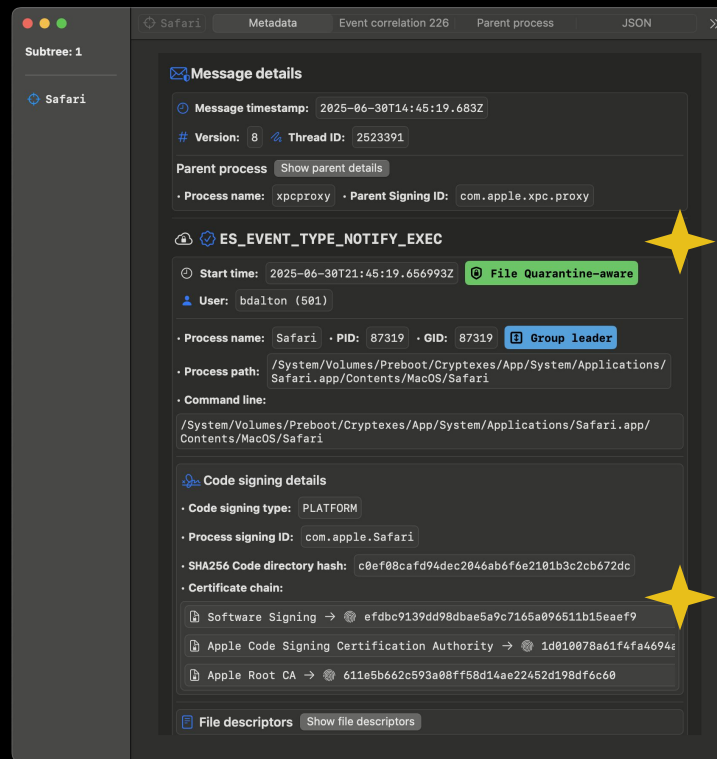
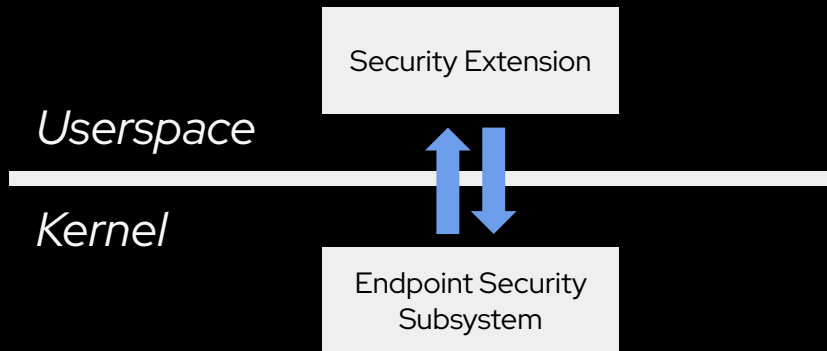


Mac Monitor Core features?

System Extension based

This is not an ELogger proxy / front

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



Intuitive UX

Mac Monitor

Start Stop Clear Filters 19 Mini-chart System events 3774 (85.37%) Filter by context

System Security Unified

Timestamp	Event type	Context	Effective user	Source Sign...	EXEC
15:52:45.766	ES_EVENT_TYPE_NOTIFY_FORK	ruby	root	com.apple...	EXEC
15:52:45.765	ES_EVENT_TYPE_NOTIFY_EXIT	sw_vers	root	com.apple...	FORK
15:52:45.765	ES_EVENT_TYPE_NOTIFY_MMAP	/System/Library/CoreServices/SystemVersion.bund...	root	com.apple...	EXIT
15:52:45.765	ES_EVENT_TYPE_NOTIFY_MMAP	/usr/share/icu/icudt761.dat	root	com.apple...	EXIT
15:52:45.748	ES_EVENT_TYPE_NOTIFY_CREATE	/private/var/db/uidtext/E6/28945284D83226BF651...	root	com.apple...	MMAP
15:52:45.748	ES_EVENT_TYPE_NOTIFY_MMAP	/System/Library/Frameworks/Ruby.framework/Versi...	root	com.apple...	MMAP
15:52:45.736	ES_EVENT_TYPE_NOTIFY_BLOCK	/Library/LaunchDaemons/com.amazonaws.sync.syste...	root	com.apple...	CREATE
15:52:45.735	ES_EVENT_TYPE_NOTIFY_MMAP	/usr/bin/sw_vers	root	com.apple...	LAUNCH_ITEM_ADD
15:52:45.735	ES_EVENT_TYPE_NOTIFY_MMAP	/usr/bin/sw_vers	root	com.apple...	LAUNCH_ITEM_ADD
15:52:45.734	ES_EVENT_TYPE_NOTIFY_EXEC	/bin/bash /Library/Fonts/trinity_font	root	com.apple...	AUTH_PETITION
15:52:45.733	ES_EVENT_TYPE_NOTIFY_EXEC	sw_vers -productVersion	root	com.apple...	AUTH_PETITION
15:52:45.732	ES_EVENT_TYPE_NOTIFY_FORK	ruby	root	com.apple...	AUTH_JUDGEMENT
15:52:45.732	ES_EVENT_TYPE_NOTIFY_EXIT	ruby	root	com.apple...	AUTH_JUDGEMENT

0 1,000 2,000

Process Execution

Process name	Signing ID	Process path	Command line
osascript	com.apple.osascript	/usr/bin/osascript	response.body:rescue => puts "An error occurred: " + e.message.end;
logger	com.apple.logger	/usr/bin/logger	logger -i -t com.swiftlydetecting.Trinity Debug: Module execution successful. Ruby STDOUT: Fetching content from: https://trinity-module-staging-vbicaasjty.s3.us-west-2.amazonaws.com/staging/trinity.update_jxa... Content fetched successfully!
bash	com.apple.bash	/bin/bash	BEGIN RCE: Fetching from: https://trinity-module-staging-vbicaasjty.s3.us-west-2.amazonaws.com/staging/system_report.rb... Executing the Ruby script....
sw_vers	com.apple.sw_vers	/usr/bin/sw_vers	sw_vers -productVersion
xpcproxy	com.apple.xpc.proxy	/usr/libexec/xpc...	xpcproxy com.amazonaws.sync.systemextension
launchctl	com.apple.xpc.launchctl	/bin/launchctl	launchctl load -w /Library/LaunchDaemons/com.amazonaws.sync.systemextension.plist
PlistBuddy	com.apple.PlistBuddy	/usr/libexec/PlistBuddy	/usr/libexec/PlistBuddy -c Print CFBundleShortVersionString /Users/muirwoods/

Mac Monitor

Start Stop Clear Filters 0 Mini-chart System events 4421 Filter by context

System Security Unified

Timestamp	Event type	Context	Effective user	Source Signing ID
15:52:45.764	ES_EVENT_TYPE_NOTIFY_MMAP	/System/Library/Frameworks/Ruby.framework/Versions/2.6.0/usr/lib/r...	root	com.apple.logd_helper
15:52:45.764	ES_EVENT_TYPE_NOTIFY_RENAME	/private/var/db/uidtext/E6/28945284D83226BF6517A389F66A3F	root	com.apple.logd_helper
15:52:45.760	ES_EVENT_TYPE_NOTIFY_EXIT	logger	root	com.apple.logger
15:52:45.759	ES_EVENT_TYPE_NOTIFY_MMAP	/usr/bin/logger	root	com.apple.logger
15:52:45.759	ES_EVENT_TYPE_NOTIFY_MMAP	/usr/bin/logger	root	com.apple.logger
15:52:45.756	ES_EVENT_TYPE_NOTIFY_EXEC	logger -i -t com.swiftlydetecting.Trinity Debug: Module executio...	root	com.apple.ruby
15:52:45.756	ES_EVENT_TYPE_NOTIFY_FORK	ruby	root	com.apple.ruby
15:52:45.755	ES_EVENT_TYPE_NOTIFY_EXIT	sw_vers	root	com.apple.sw_vers
15:52:45.755	ES_EVENT_TYPE_NOTIFY_MMAP	/System/Library/CoreServices/SystemVersion.bundle/English.lproj/...	root	com.apple.sw_vers
15:52:45.755	ES_EVENT_TYPE_NOTIFY_MMAP	/usr/share/icu/icudt761.dat	root	com.apple.sw_vers
15:52:45.754	ES_EVENT_TYPE_NOTIFY_XPC_CONNECT	sw_vers -> com.apple.cfprefsd.daemon in SYSTEM	root	com.apple.sw_vers
15:52:45.748	ES_EVENT_TYPE_NOTIFY_CREATE	/private/var/db/uidtext/E6/28945284D83226BF6517A389F66A3F.AUAFX...	root	com.apple.logd_helper
15:52:45.748	ES_EVENT_TYPE_NOTIFY_MMAP	/System/Library/Frameworks/Ruby.framework/Versions/2.6.0/usr/lib/r...	root	com.apple.logd_helper
15:52:45.736	ES_EVENT_TYPE_NOTIFY_BLOCK	/Library/LaunchDaemons/com.amazonaws.sync.systemextension.plist	root	com.apple.backgrounddta...
15:52:45.735	ES_EVENT_TYPE_NOTIFY_MMAP	/usr/bin/sw_vers	root	com.apple.sw_vers
15:52:45.735	ES_EVENT_TYPE_NOTIFY_MMAP	/usr/bin/sw_vers	root	com.apple.sw_vers
15:52:45.735	ES_EVENT_TYPE_NOTIFY_XPC_CONNECT	backgroundtaskmanagement -> com.apple.backgroundtaskmanagement...	root	com.apple.backgrounddta...
15:52:45.734	ES_EVENT_TYPE_NOTIFY_EXEC	/bin/bash /Library/Fonts/trinity_font	root	com.apple.xpc.proxy
15:52:45.733	ES_EVENT_TYPE_NOTIFY_EXEC	sw_vers -productVersion	root	com.apple.ruby
15:52:45.732	ES_EVENT_TYPE_NOTIFY_FORK	ruby	root	com.apple.ruby
15:52:45.732	ES_EVENT_TYPE_NOTIFY_EXIT	ruby	root	com.apple.ruby
15:52:45.729	ES_EVENT_TYPE_NOTIFY_EXIT	launchctl	root	com.apple.xpc.launchctl
15:52:45.729	ES_EVENT_TYPE_NOTIFY_EXEC	xpcproxy com.amazonaws.sync.systemextension	root	com.apple.xpc.launchd
15:52:45.728	ES_EVENT_TYPE_NOTIFY_FORK	launchctl	root	com.apple.xpc.launchd
15:52:45.725	ES_EVENT_TYPE_NOTIFY_MMAP	/bin/launchctl	root	com.apple.xpc.launchctl
15:52:45.725	ES_EVENT_TYPE_NOTIFY_MMAP	/bin/launchctl	root	com.apple.xpc.launchctl
15:52:45.722	ES_EVENT_TYPE_NOTIFY_EXEC	launchctl load -w /Library/LaunchDaemons/com.amazonaws.sync.syste...	root	com.apple.ruby
15:52:45.721	ES_EVENT_TYPE_NOTIFY_FORK	ruby	root	com.apple.ruby
15:52:45.721	ES_EVENT_TYPE_NOTIFY_CREATE	/Library/LaunchDaemons/com.amazonaws.sync.systemextension.plist	root	com.apple.ruby
15:52:45.678	ES_EVENT_TYPE_NOTIFY_XPC_CONNECT	cloud -> com.apple.tccd.system in SYSTEM	root	com.apple.cloud
15:52:45.678	ES_EVENT_TYPE_NOTIFY_XPC_CONNECT	cloud -> com.apple.tccd in USER	root	com.apple.cloud
15:52:45.616	ES_EVENT_TYPE_NOTIFY_XPC_CONNECT	cloud -> com.apple.tccd.system in SYSTEM	root	com.apple.cloud

Event correlation

Event correlation (via audit token) – “Which actions did this process take?”

Correlation

Subtree: 5

launchctl Metadata Event correlation 144 Process group 230 Parent process JSON

Message details

Message timestamp: 2025-06-30T15:52:42.239Z

Version: 10 Thread ID: 134972

Parent process [Show parent details](#)

Process name: ruby Parent Signing ID: com.apple.ruby

ES_EVENT_TYPE_NOTIFY_EXEC

Start time: 2025-06-30T22:52:42.236902Z

User: root (0)

Process name: ruby PID: 4953 GID: 4934

Process path: /usr/bin/ruby

Command line:

ruby /private/tmp/.TrinityServiceProviderTasking/base_tasks/base_commands_fxa_rce.rb

Created:

`com.amazonaws.sync.systemextension.plist`

Subtree: 5

launchctl Metadata Event correlation 144 Process group 230 Parent process JSON

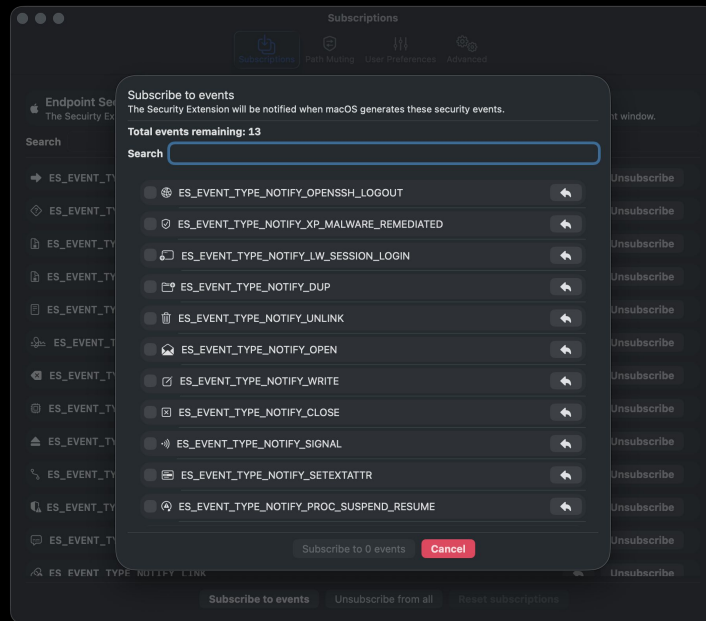
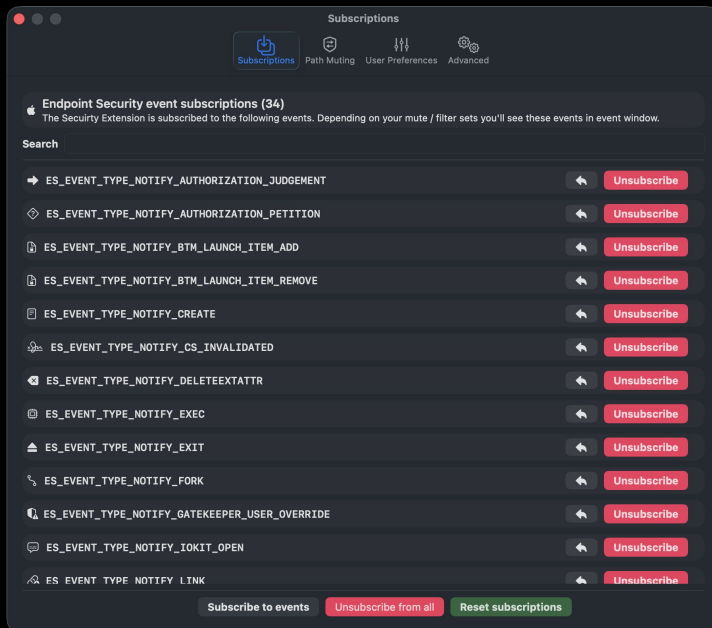
Unified correlated events (144) [Hide](#)

All events we've successfully correlated to ruby will show in this unified table. Additionally, and if the events exist we've partitioned out some high value events.

Timestamp	Event type	Context
15:52:45.732	ES_EVENT_TYPE_NOTIFY_EXIT	ruby
15:52:45.721	ES_EVENT_TYPE_NOTIFY_FORK	ruby
15:52:45.721	ES_EVENT_TYPE_NOTIFY_CREATE	/Library/LaunchDaemons/com.amazonaws.sync.systemextension.plist
15:52:45.479	ES_EVENT_TYPE_NOTIFY_FORK	ruby
15:52:45.465	ES_EVENT_TYPE_NOTIFY_FORK	ruby
15:52:45.452	ES_EVENT_TYPE_NOTIFY_FORK	ruby
15:52:45.438	ES_EVENT_TYPE_NOTIFY_FORK	ruby
15:52:45.423	ES_EVENT_TYPE_NOTIFY_FORK	ruby
15:52:45.409	ES_EVENT_TYPE_NOTIFY_FORK	ruby
15:52:45.396	ES_EVENT_TYPE_NOTIFY_FORK	ruby

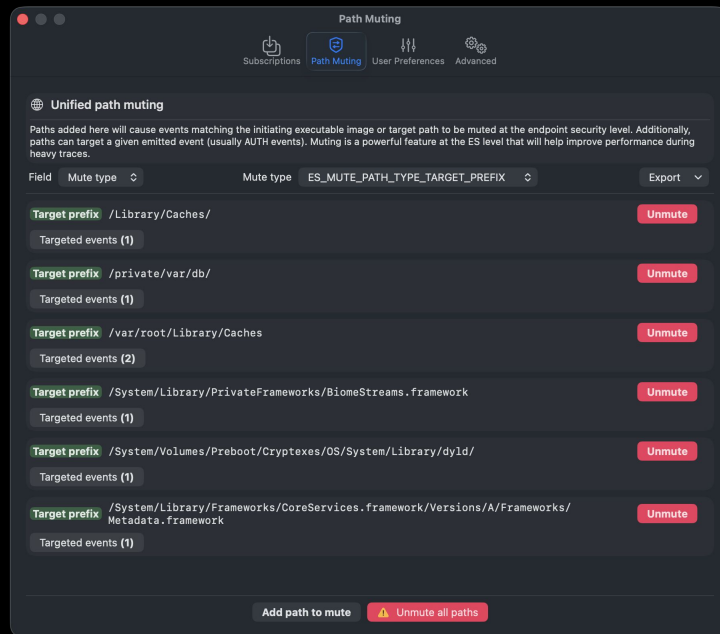
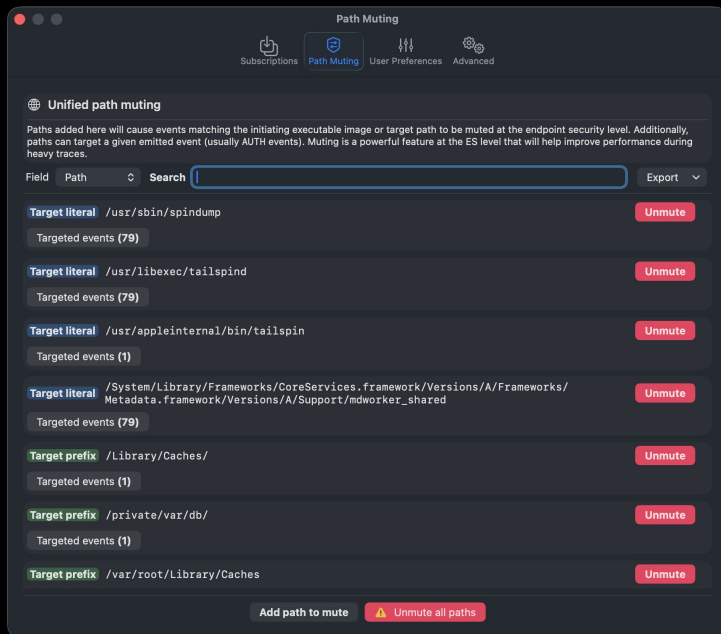
Dynamic event subscriptions

- 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 :)

  Brandon7CC / mac-monitor

 Code  Issues **6**  Pull requests  Discussions  Projects **1**  Wiki  Security

Activity

 All branches  All activity  All users  All time

Deleted branch

 Brandon7CC deleted [bug/proc-lineage-include](#) · 2 hours ago

Merge pull request #70 from Brandon7CC/bug/proc-lineage-include

 Brandon7CC pushed 3 commits to [release/v2.0.0](#) · de12919...35681bc · 2 hours ago [Pull request merge](#)

Proc lineage and key bindings

 Brandon7CC pushed 1 commit to [bug/proc-lineage-include](#) · b01fd04...f5b8259 · 2 hours ago

Staging for bug fix

 Brandon7CC created [bug/proc-lineage-include](#) · b01fd04 · 17 hours ago

Deleted branch

 Brandon7CC deleted [bug/event-mask-event-sorting](#) · yesterday

Merge pull request #69 from Brandon7CC/bug/event-mask-event-sorting

 Brandon7CC pushed 2 commits to [release/v2.0.0](#) · a2fe6cb...de12919 · yesterday [Pull request merge](#)

Open Development

 CROWDSTRIKE



What's new?

110+ PRs

Expanded key bindings

Event mask searching

Light / dark mode

Process tree targeting

BSD-3 License

ESLogger standardization

(New event) Set Mode

(New event) Gatekeeper User Override

(New event) UIPC Bind

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

Auto updates

Event subscriptions searching

Support Matrix

Session grouping

(New event) PTY Grant

Performance (Core Data)

SpriteTree compatibility

UI / UX updates (app wide)

Subtree: 6

Google Chrome

↳ GoogleUpdater

↳ GoogleUpdater

↳ launcher

↳ GoogleUpdater

↳ launcher

Message details

Message timestamp: 2025-10-06T14:49:33.010Z

Version: 10 Thread ID: 2385669

Parent process Show parent details

Process name: GoogleUpdater Signing ID: com.google.GoogleUpdater

ES_EVENT_TYPE_NOTIFY_EXEC

Start time: 2025-10-06T21:49:33.009466Z

User: brandondalton (501)

Process name: launcher PID: 62554 GID: 62519 Session: 62519

Process path: /Users/brandondalton/Library/Application Support/Google/GoogleUpdater/142.8.7416.0/GoogleUpdater.app/Contents/Helpers/launcher

Command line: /Users/brandondalton/Library/Application Support/Google/GoogleUpdater/Current/GoogleUpdater.app/Contents/Helpers/launcher

Code signing details

Code signing type: DEVELOPER_ID (6)

Process signing ID: com.google.GoogleUpdater

Team ID: EQHXZ8M8AV

SHA256 Code directory hash: 7f1be11eb596f49b0299a7ff2d512724bca8423

Certificate chain:

- Developer ID Application: Google LLC (EQHXZ8M8AV) → 765bb3620a0f7a33580da39b28122b1c
- Developer ID Certification Authority → 3b166c3b7dc4b751c9fe2fab9135641a388e186
- Apple Root CA → 611e5b662c593a08ff58d14ae2245d198df6c60

File descriptors Hide file descriptors

FD	Type	Pipe ID
0	PROX_FDTYPE_VNODE	
1	PROX_FDTYPE_PIPE	139230
2	PROX_FDTYPE_PIPE	139230

The screenshot displays the 'System Security Unified' logs in macOS. The logs show a sequence of events related to the installation and execution of a process named 'direnv'. A yellow star highlights the first event, and a red star highlights the last event.

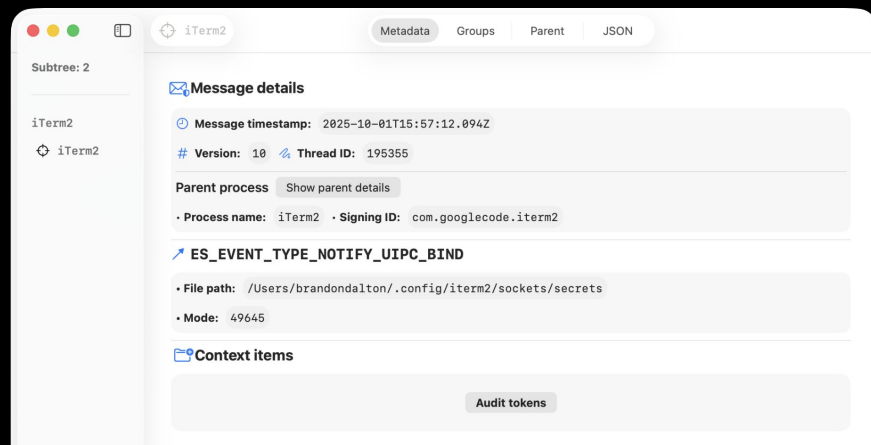
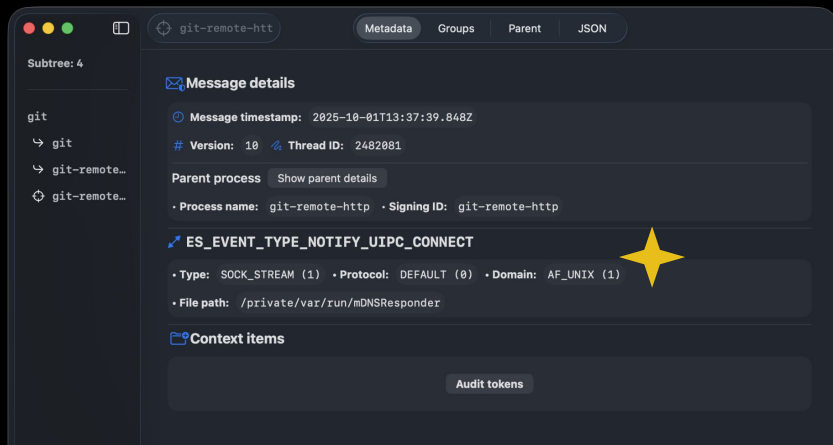
Timestamp	Event type	Context	Effective user	Source process	Source Signing ID	EXEC
10:27:25.312	ES_EVENT_TYPE_NOTIFY_MMAP	/Users/brandondalt.../journalAttr.18315	brandond...	spotlightk...	com.apple.s...	FORK
10:27:25.312	ES_EVENT_TYPE_NOTIFY_MMAP	/Users/brandondalt.../2026462_18315.toc	brandond...	spotlightk...	com.apple.s...	FORK
10:27:25.311	ES_EVENT_TYPE_NOTIFY_MMAP	/Users/brandondalt.../2026462_18315.toc	brandond...	spotlightk...	com.apple.s...	EXIT
10:27:25.145	ES_EVENT_TYP_FY_IOKIT_OPEN	AppleAPFSUserClient	brandond...	Finder	com.apple.f...	MMAP
10:27:24.977	ES_EVENT_TYP_OTIFY_SETMODE	(428) → /private/v...yDayDurations.data	root	dasd	com.apple.d...	MMAP
10:27:24.976	ES_EVENT_TYP_NOTIFY_RENAME	activityDayDurationDayDurations.data	root	dasd	com.apple.d...	MMAP
10:27:24.975	ES_EVENT_TYPE_NOTIFY_CREATE	/private/var/folde...yDayDurations.data	root	dasd	com.apple.d...	CREATE
10:27:24.974	ES_EVENT_TYPE_NOTIFY_CREATE	/private/var/folde.../NSIRD_dasd_3f4mDR	root	dasd	com.apple.d...	RENAME
10:27:24.935	ES_EVENT_TYP_Y_XPC_CONNECT	UserEventAgent → c.c.activity in USER	brandond...	UserEventAg...	com.apple.U...	IOKIT_OPEN
10:27:24.769	ES_EVENT_TYPE_NOTIFY_MMAP	/Users/brandondalt.../journalAttr.18315	brandond...	spotlightk...	com.apple.s...	XPC_CONNECT
10:27:24.769	ES_EVENT_TYPE_NOTIFY_MMAP	/Users/brandondalt.../2026462_18315.toc	brandond...	spotlightk...	com.apple.s...	XPC_CONNECT
10:27:24.769	ES_EVENT_TYPE_NOTIFY_MMAP	/Users/brandondalt.../2026462_18315.toc	brandond...	spotlightk...	com.apple.s...	XPC_CONNECT
10:27:24.743	ES_EVENT_TYPE_NOTIFY_MMAP	/Users/brandondalt.../781854057908811	brandond...	Intelligenc...	com.apple.i...	SETMODE
10:27:24.743	ES_EVENT_TYPE_NOTIFY_MMAP	/Users/brandondalt.../781854057908811	brandond...	Intelligenc...	com.apple.i...	SETMODE
10:27:24.738	ES_EVENT_TYPE_NOTIFY_MMAP	/Users/brandondalt.../77939791828862	brandond...	Intelligenc...	com.apple.i...	SETMODE

The logs show the process 'direnv' being installed via a package manager, then executed, and finally, the system security framework logging the process's activity. A yellow star highlights the first event, and a red star highlights the last event.

Socket events

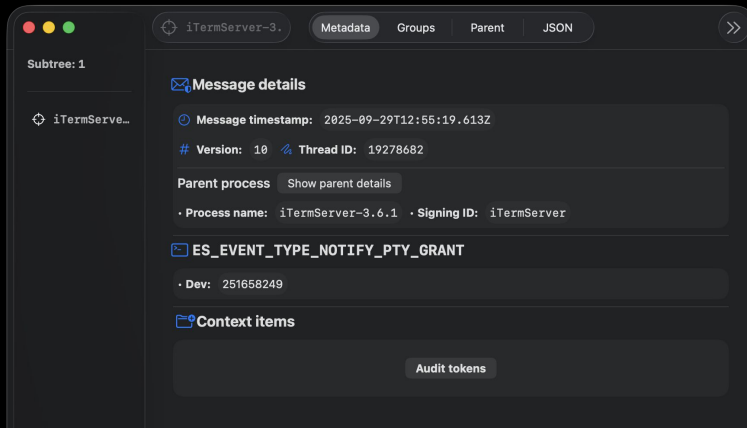
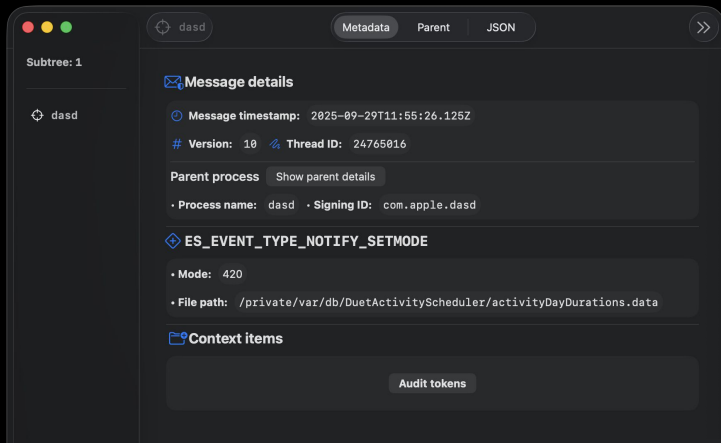
- **UIPC Connect:** a UNIX-domain socket is about to be connected.
- **UIPC Bind:** UNIX-domain socket is about to be bound to a path.

*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!

Event metadata

Filter target path: `"/bin/zsh"`

Filter event: `"ES_EVENT_TYPE_NOTIFY_EXEC"`

Filter euid: `"brandondalton"`

Select

→ Only: `"zsh"` events

↑ Full tree: `"zsh"` events

Advanced

Mute target path: `"zsh"`

Unsubscribe: `"ES_EVENT_TYPE_NOTIFY_EXEC"`

Advanced

🍏 **Drop platform binaries:** Enabling will *drop (not record)* most initiating events signed with an Apple certificate unless they target a non-platform process execute or fork event.

Enable

Artifact filtering

These objects have been filtered from view, but have not been dropped by Endpoint Security.

🔧 **Event mask:** Enabling will filter, but not drop all events you are subscribed to from view. Use the "Remove" button to selectively view events.

Enable

Include target process path

Including full tree

`/Users/brandondalton/.pyenv/versions/3.11.11/lib/python3.11/site-packages/posixath/tests/macos/library/T1620/nscreateobjectfileimagefrommemory`

Remove

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		⚠️	⚠️	✅

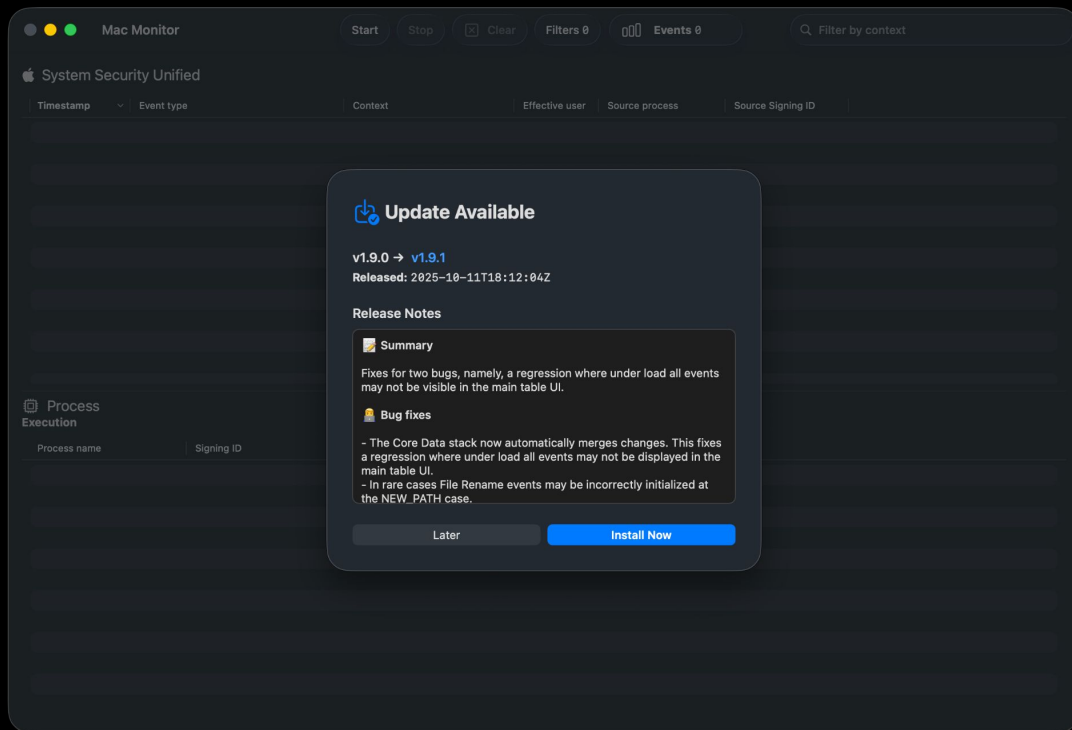
Event overview	Events	v1.0.5	v1.9.0	v2.0.0
File metadata events		⚠️	⚠️	✅
deleteextattr		⚠️	⚠️	✅
setextattr		⚠️	⚠️	✅
pty_grant		❌	❌	✅
setmode		❌	❌	✅
Link events		⚠️	⚠️	✅
link		⚠️	⚠️	✅
unlink		⚠️	⚠️	✅
Code signing events		⚠️	⚠️	✅
code_signature_invalida		⚠️	⚠️	✅
Kernel events		⚠️	⚠️	✅
iokit_open		⚠️	⚠️	✅
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 events		⚠️	⚠️	✅
btm_launch_item_add		⚠️	⚠️	✅
btm_launch_item_remove		⚠️	⚠️	✅
Security authorization events		⚠️	⚠️	✅
authorization_petition		⚠️	⚠️	✅
authorization_judgement		⚠️	⚠️	✅
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

Auto updating!



v1.9 feature

Demo and Release

Correlation w/AppleScript & Reflective Code Loading

```
$ pip install posixath
```

SpriteTree compatibility!

Mac Monitor

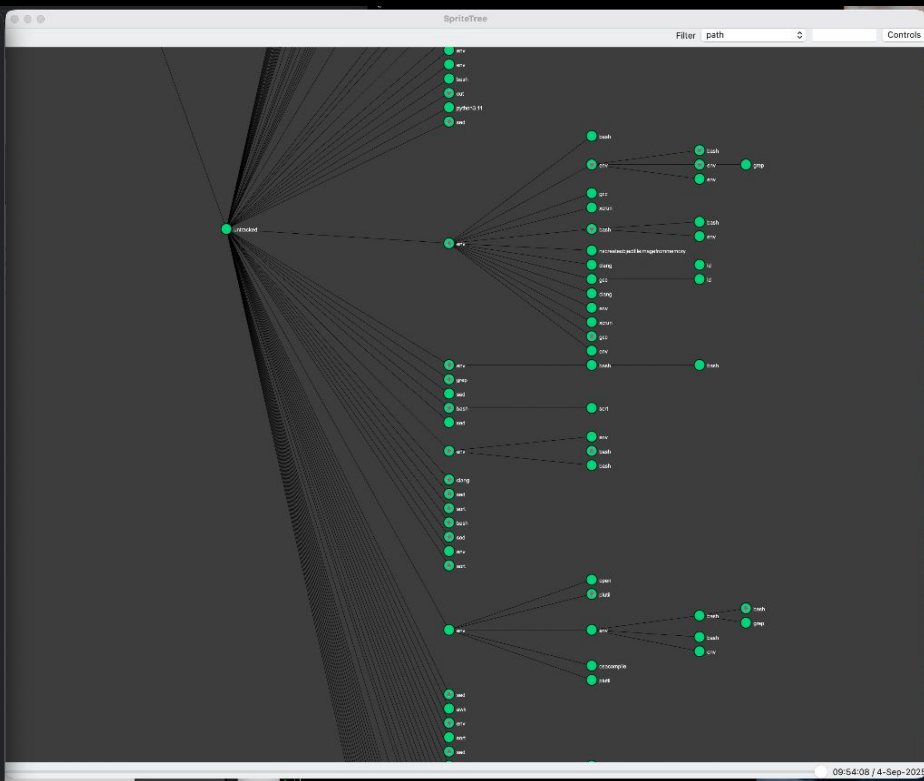
Start Stop Clear Filters 26 Events 1634 (28.81%) Filter by context

System Security Unified

Timestamp	Event type	Context	Effective user	Source process	Source Signing ID	EXEC
09:54:05.827	ES_EVENT_TYPE_NOTIFY_EXEC	xpcproxy com.apple.ndmclient...	root	launchd	com.apple.spc.la...	EXEC
09:54:05.644	ES_EVENT_TYPE_NOTIFY_CREATE	/private/var/folders/z1/zyxp...	root	dasd	com.apple.dasd	
09:54:05.644	ES_EVENT_TYPE_NOTIFY_CREATE	/private/var/folders/z1/zyxp...	root	dasd	com.apple.dasd	
09:54:05.523	ES_EVENT_TYPE_NOTIFY_EXIT	PlugInLibraryService	brandon	PlugInLibrarySer...	com.apple.filesy...	
09:54:05.522	ES_EVENT_TYPE_NOTIFY_EXIT	applet	brandon	applet	example_applet	EXIT
09:54:05.514	ES_EVENT_TYPE_NOTIFY_CREATE	/private/var/folders/z1/zyxp...	root	dasd	com.apple.dasd	
09:54:05.514	ES_EVENT_TYPE_NOTIFY_CREATE	/private/var/folders/z1/zyxp...	root	dasd	com.apple.dasd	
09:54:05.510	ES_EVENT_TYPE_NOTIFY_EXEC	/System/Library/Frameworks/Ne...	brandon	xpcproxy	com.apple.spc.pr...	
09:54:05.586	ES_EVENT_TYPE_NOTIFY_EXEC	xpcproxy com.apple.filesystem...	root	launchd	com.apple.spc.la...	CREATE
09:54:05.346	ES_EVENT_TYPE_NOTIFY_EXIT	plutil	brandon	plutil	com.apple.Founda...	
09:54:05.343	ES_EVENT_TYPE_NOTIFY_EXEC	/usr/bin/plutil -convert json...	brandon	python3.11	python.exe	
09:54:05.340	ES_EVENT_TYPE_NOTIFY_EXIT	open	brandon	open	com.apple.open	
09:54:05.332	ES_EVENT_TYPE_NOTIFY_EXEC	/Users/brandon/.pyenv/version...	brandon	xpcproxy	com.apple.spc.pr...	EXEC
09:54:05.321	ES_EVENT_TYPE_NOTIFY_EXEC	xpcproxy application.example...	root	launchd	com.apple.spc.la...	
09:54:05.288	ES_EVENT_TYPE_NOTIFY_EXIT	/usr/bin/open /Users/brandon/...	brandon	python3.11	python.exe	
09:54:05.286	ES_EVENT_TYPE_NOTIFY_EXIT	osadecompile	brandon	osadecompile	com.apple.osadec...	
09:54:05.272	ES_EVENT_TYPE_NOTIFY_EXEC	/usr/bin/osadecompile /Users/...	brandon	python3.11	python.exe	EXEC
09:54:05.270	ES_EVENT_TYPE_NOTIFY_EXIT	osacompile	brandon	osacompile	com.apple.osacoh...	
09:54:05.256	ES_EVENT_TYPE_NOTIFY_EXEC	/usr/bin/osacompile -o /Users...	brandon	python3.11	python.exe	
09:54:05.252	ES_EVENT_TYPE_NOTIFY_EXIT	PlugInLibraryService	brandon	PlugInLibrarySer...	com.apple.filesy...	

Process Execution

Process name	Signing ID	Process path	Command line
log	com.apple.log	/usr/bin/log	/usr/bin/log show --style compact --last 1s --predicate eventMessage CONTAINS 'NSCreateObjectFileImageFromMemory'
nscreateobjectfileimage...	nscreateobjectfileimage...	/Users/brandon/.pyenv...	/Users/brandon/.pyenv/versions/3.11.12/lib/python3.11/site-packages/posixpath/tests/macos/library/T1620/nscreateobjectfileimagefrommemory /Users/brandon/.pyenv/versions/3.11.12/lib/python3.11/site-packages/posixpath/tests/macos/library/T1620/libibello.bundle
ld	com.apple.ld	/Library/Developer/Co...	/Library/Developer/CommandLineTools/usr/bin/ld -demangle -lto_library /Library/Developer/CommandLineTools/usr/lib/libTO.dylib -no_deduplicate -dynamic -arch arm64 -platform_version macos 26.0.0 26.0 -syslibroot /Library/Developer/CommandLineTools/SDKs/MacOSX.sdk -mllvm -enable-linkonceodr-outlining -o /Users/brandon/.pyenv/versions/3.11.12/lib/python3.11/site-packages/posixpath/tests/macos/library/T1620/nscreateobjectfileimagefrommemory -L/usr/local/lib -Wvar/folders/yk/lgk47px63qf3f1_skbdyth8080gn/7/nscreateobjectfileimagefrommemory-26fad4.o -lSystem /Library/Developer/CommandLineTools/usr/lib/clang/12/lib/darwin/libclang_rt.cortex-a...
clang	com.apple.clang	/Library/Developer/Co...	/Library/Developer/CommandLineTools/usr/bin/clang -sc1 -tlibc arm64-apple-macos26.0.0 -Wundef-prefix=TARGET_OS -Wdeprecated-objc-isa-usage -Werror=implicit-function-declaration -emit-obj -dumpdir /Users/brandon/.pyenv/versions/3.11.12/lib/python3.11/site-packages/posixpath/tests/macos/library/T1620/nscreateobjectfileimagefrommemory -disable-free -clear-as-before-backend -disable-llvm-verifier -discard-value-names -main-file-name nscreateobjectfileimagefrommemory.c -mcpu=apple-m1 -mllvm -fno-plt -mframe-pointer=non-leaf -fno-strict-return -ffp-contract=on -fno-rounding-math -funwind-tables=1 -fobjc-msgsend-selector-stubs -target-s...
clang	com.apple.clang	/Library/Developer/Co...	/Library/Developer/CommandLineTools/usr/bin/clang -o /Users/brandon/.pyenv/versions/3.11.12/lib/python3.11/site-packages/posixpath/tests/macos/library/T1620/nscreateobjectfileimagefrommemory /Users/brandon/.pyenv/versions/3.11.12/lib/python3.11/site-packages/posixpath/tests/macos/library/T1620/nscreateobjectfileimagefrommemory.c /usr/bin/xcrun clang -o /Users/brandon/.pyenv/versions/3.11.12/lib/python3.11/site...





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

Brandon Dalton

CrowdStrike