MacOS Endpoint Security Framework (ESF)
Why its valuable and how to use it

Connor Morley
Senior Security Researcher

WITH secure

Who am I?

- Senior Researcher
- Threat Hunter for 4 years
- Whitepaper and POC maker
- BSc, OSCP, GREM
- Presented at DEFCON, BSIDES, STEELCON

WITH secure

Agenda

1. What is the Endpoint Security Framework (ESF)?
2. Why is the ESF important?
3. How can we use the ESF?
4. Issues with ESF use
5. Solutions to these issues
6. My Solution: ESFang
7. Meterpreter use case

What is ESF?

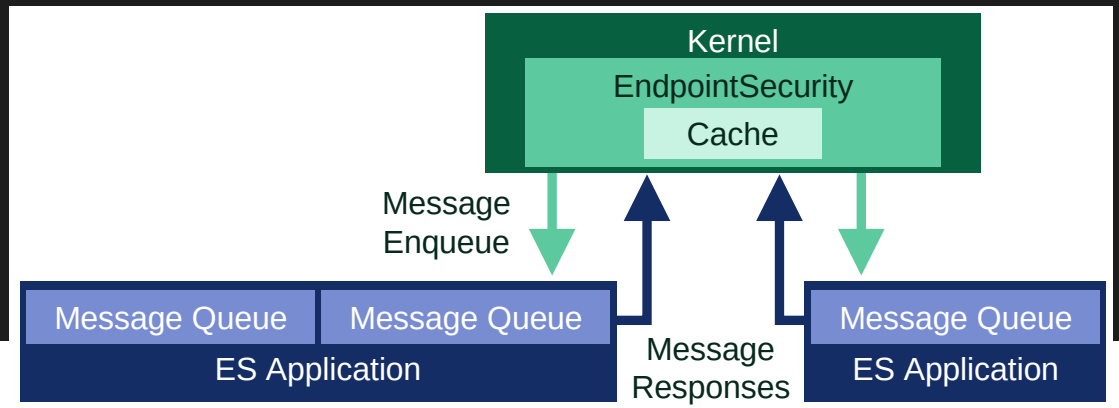
Endpoint security framework (ESF)

- Solution to security needs
- Succeeds OpenBSM
- Similar to Windows ETW
- Kernel Space
- Real Time events

What does this look like?


```
{
  "timestamp" : "2021-01-20T13:36:38.518Z",
  "eventtype" : "ES_EVENT_NOTIFY_EXEC",
  "metadata" : {
    "real_ppid" : 1196,
    "origin_platform_binary" : true,
    "uid" : 501,
    "origin_binarypath" : "\/bin\/bash",
    "origin_pid" : 45238,
    "oppid" : 42250,
    "origin_cdhash" : "508595E78370793873B546FDC6ED6B32422627EB",
    "ppid" : 42250,
    "origin_uid" : 501,
    "path" : "\/Users\/drt\/Desktop\/merlinAgent-Darwin-x64",
    "env_variables" : [
      "TERM_PROGRAM=Apple_Terminal",
      "TERM=xterm-256color",
      "SHELL=\/bin\/bash",
      "TMPDIR=\/var\/folders\/qc\/cvjw8vxj7l5218dc842sjcwh0000gn\/T\/",
      "TERM_PROGRAM_VERSION=433",
      "TERM_SESSION_ID=BB20D79A-5517-4288-A49B-374045F503EA",
      "USER=drt",
      "SSH_AUTH_SOCK=\/private\/tmp\/com.apple.launchd.ZbtHJekEWD\/Listeners",
      "PATH=\/usr\/local\/bin:\/usr\/bin:\/bin:\/usr\/sbin:\/sbin:\/usr\/local\/Cellar\/openvpn\/2.4.9\/sbin\/:\/Applications\/VMware Fusion.app\/Contents\/Public:\/Library\/Apple\/usr\/bin",
      "PWD=\/Users\/drt\/Desktop",
      "LANG=en_GB.UTF-8",
      "XPC_FLAGS=0x0",
      "XPC_SERVICE_NAME=0",
      "HOME=\/Users\/drt",
      "SHLVL=1",
      "LOGNAME=drt",
      "_=.\/merlinAgent-Darwin-x64",
      "OLDPWD=\/Users\/drt\/Desktop\/ESF_base\/proqmon"
    ],
    "sha1" : "0000000000000000000000000000000000000000",
    "ProcessArgs" : "https:\/\/192.168.1.69:443",
    "submitted_by" : {

    },
    "origin_ppid" : 42250,
    "parent_path" : "\/bin\/bash",
    "pid" : 45238,
    "origin_signingid" : "com.apple.bash",
    "origin_codesigningflags" : [
      "CS_VALID",
      "CS_SIGNED",
      "CS_RESTRICT",
```

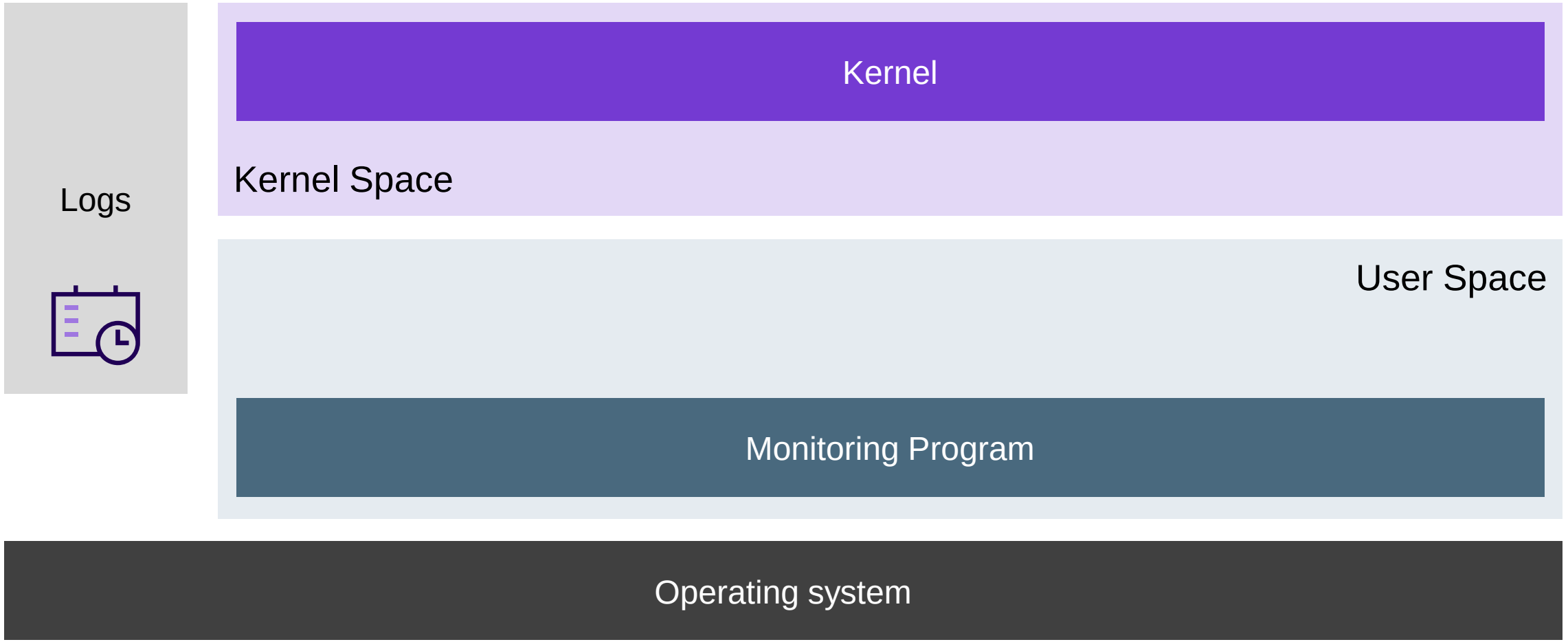
WITH secure

Why is the ESF important?

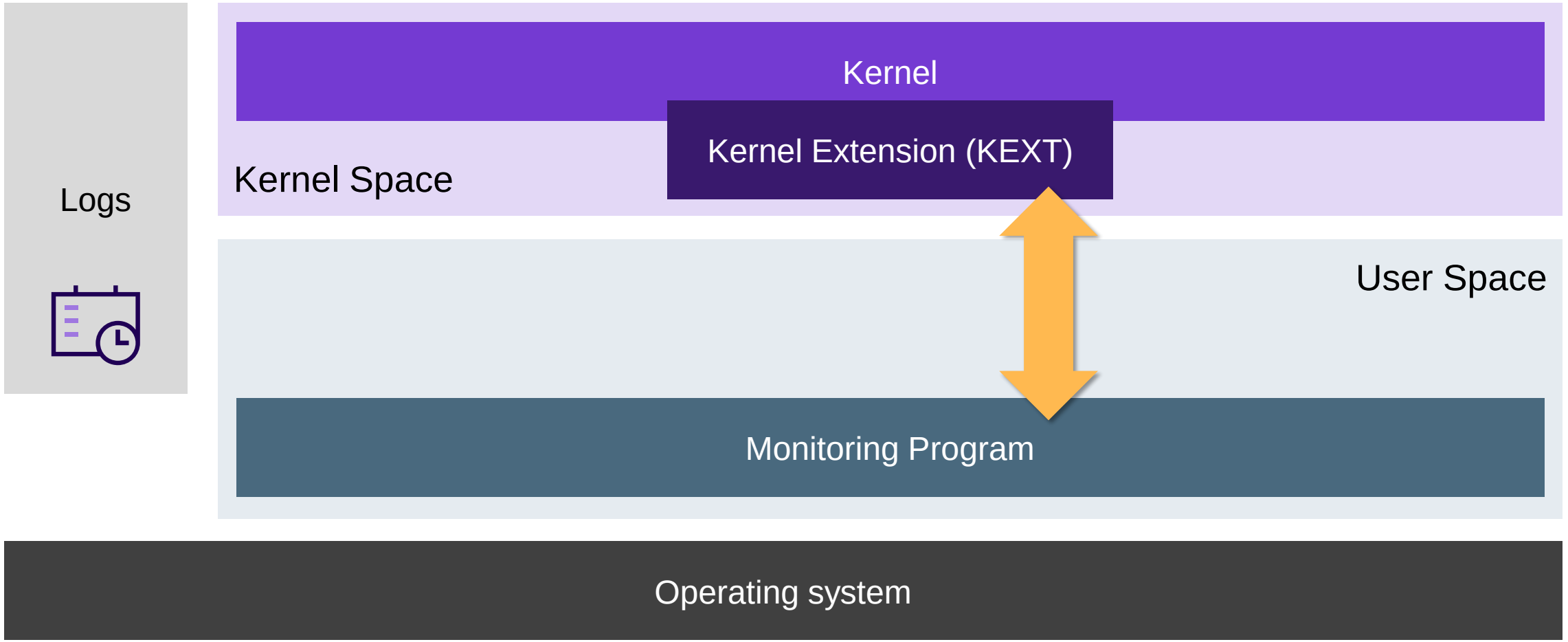
Restrictions and changes in macOS

- Deprecation of KEXT
- Migration to System Extensions
- OpenBSM was difficult to use, ESF is swift and real time

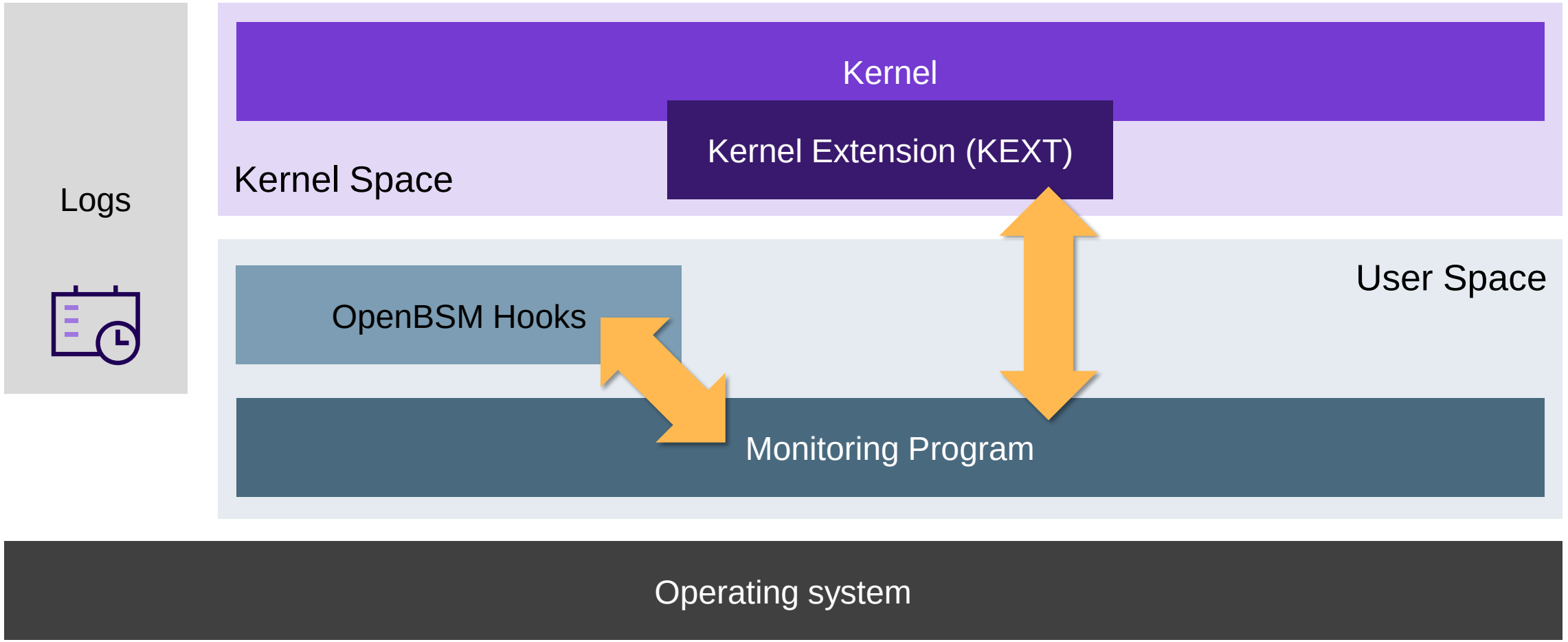
Old way of monitoring



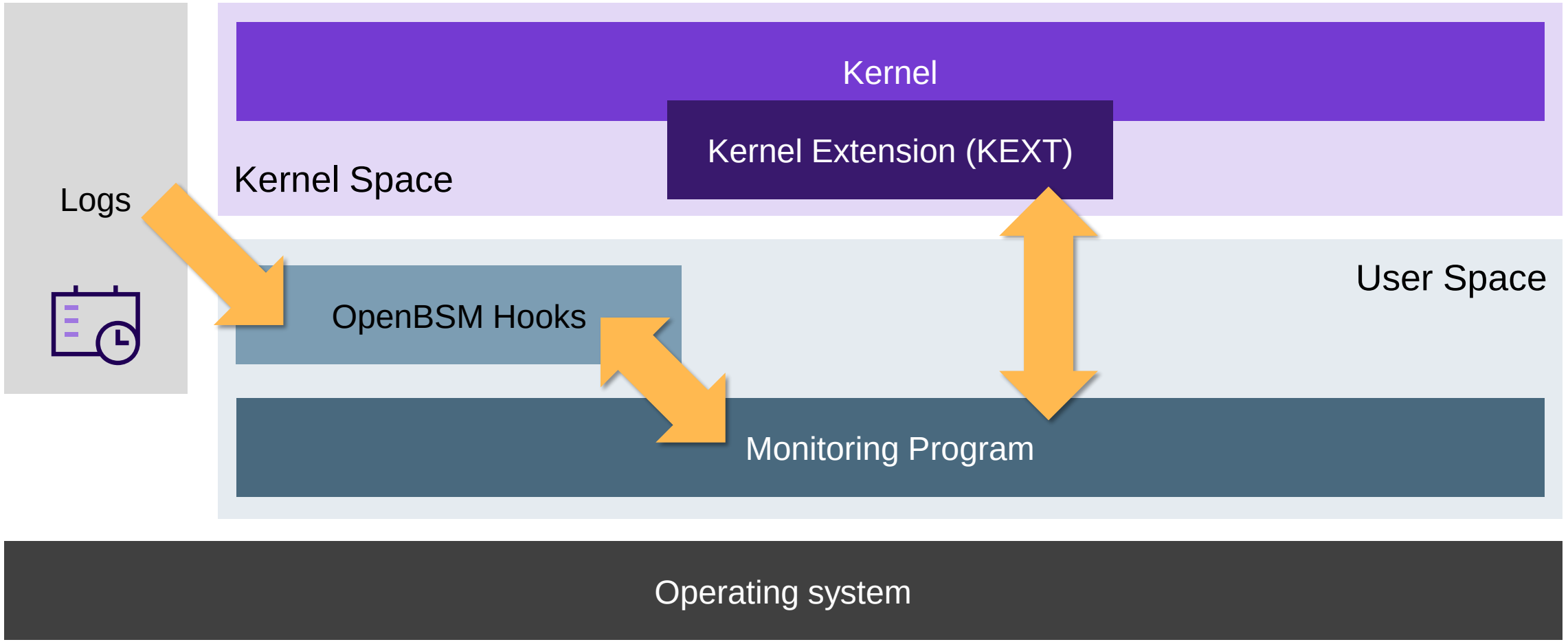
Old way of monitoring



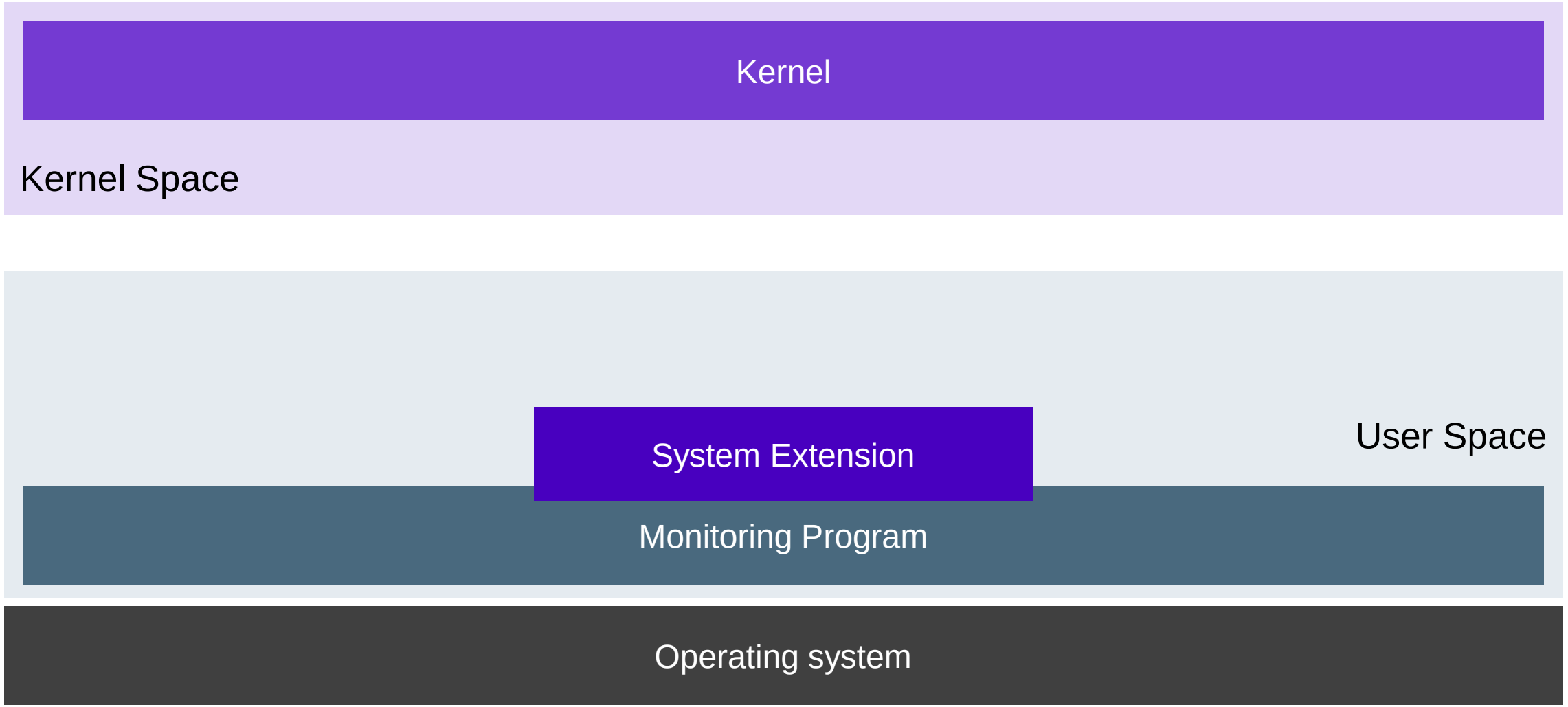
Old way of monitoring



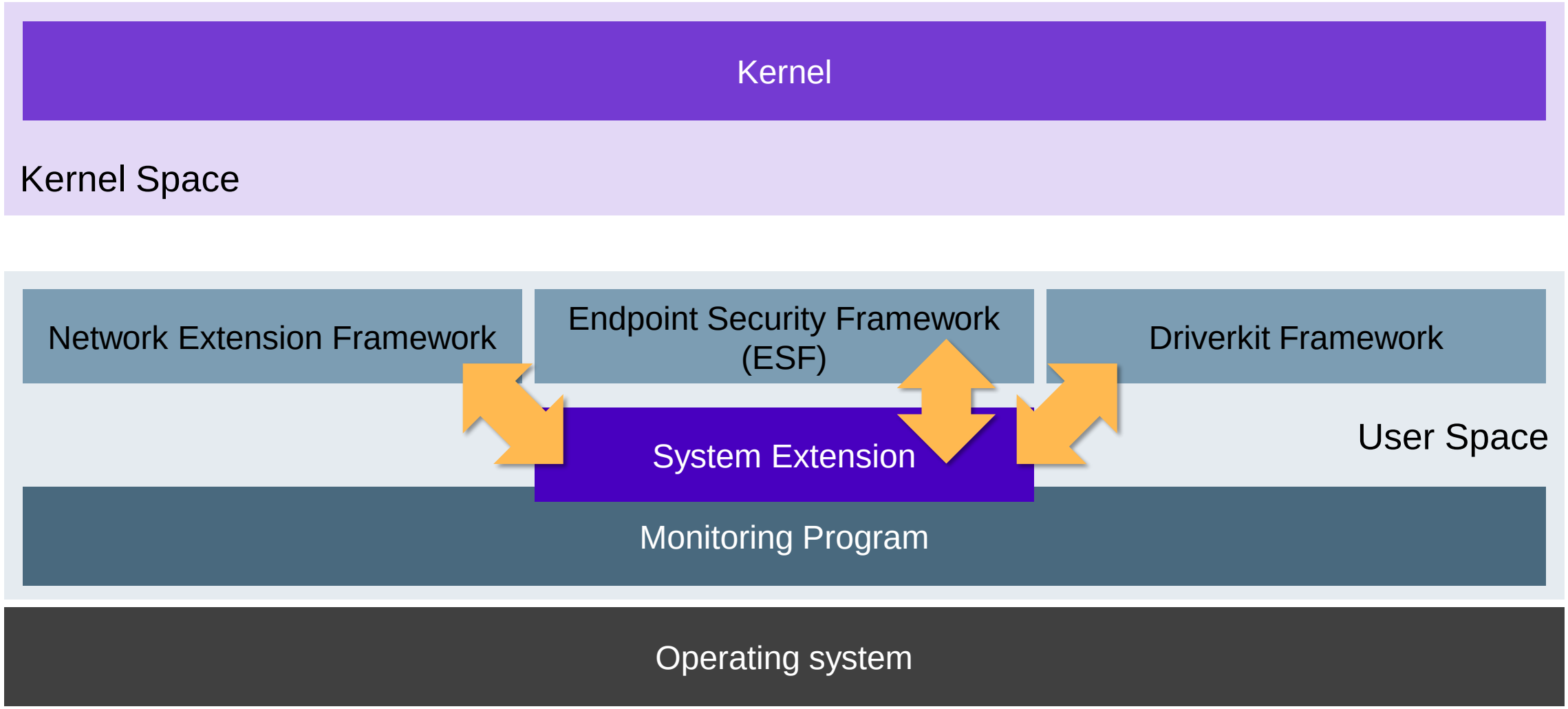
Old way of monitoring



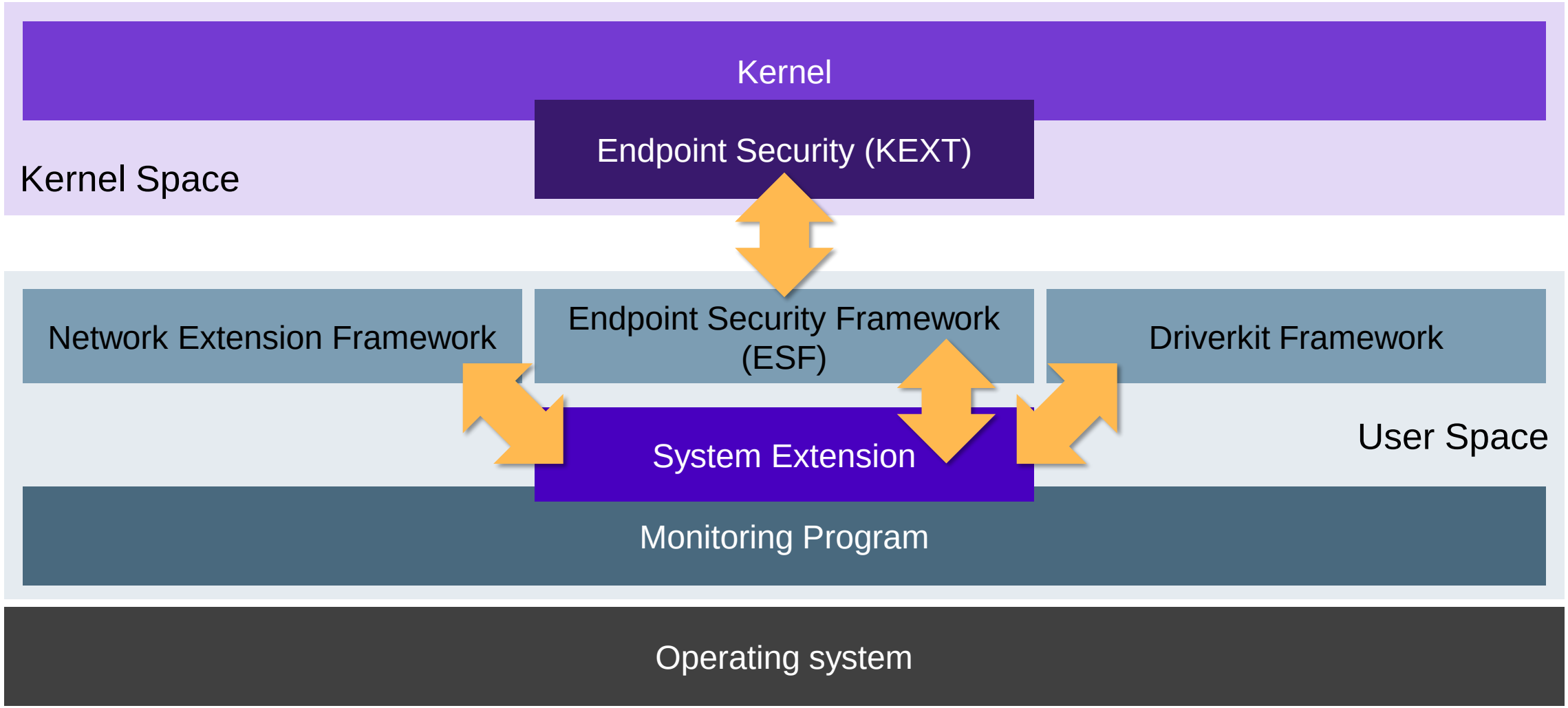
The new way


Kernel
Kernel Space
System Extension
User Space
Monitoring Program
Operating system

The new way


Kernel
Kernel Space
Network Extension Framework
Endpoint Security Framework (ESF)
Driverkit Framework
System Extension
User Space
Monitoring Program
Operating system

The new way


Kernel
Endpoint Security (KEXT)
Kernel Space
Network Extension Framework
Endpoint Security Framework (ESF)
Driverkit Framework
System Extension
User Space
Monitoring Program
Operating system

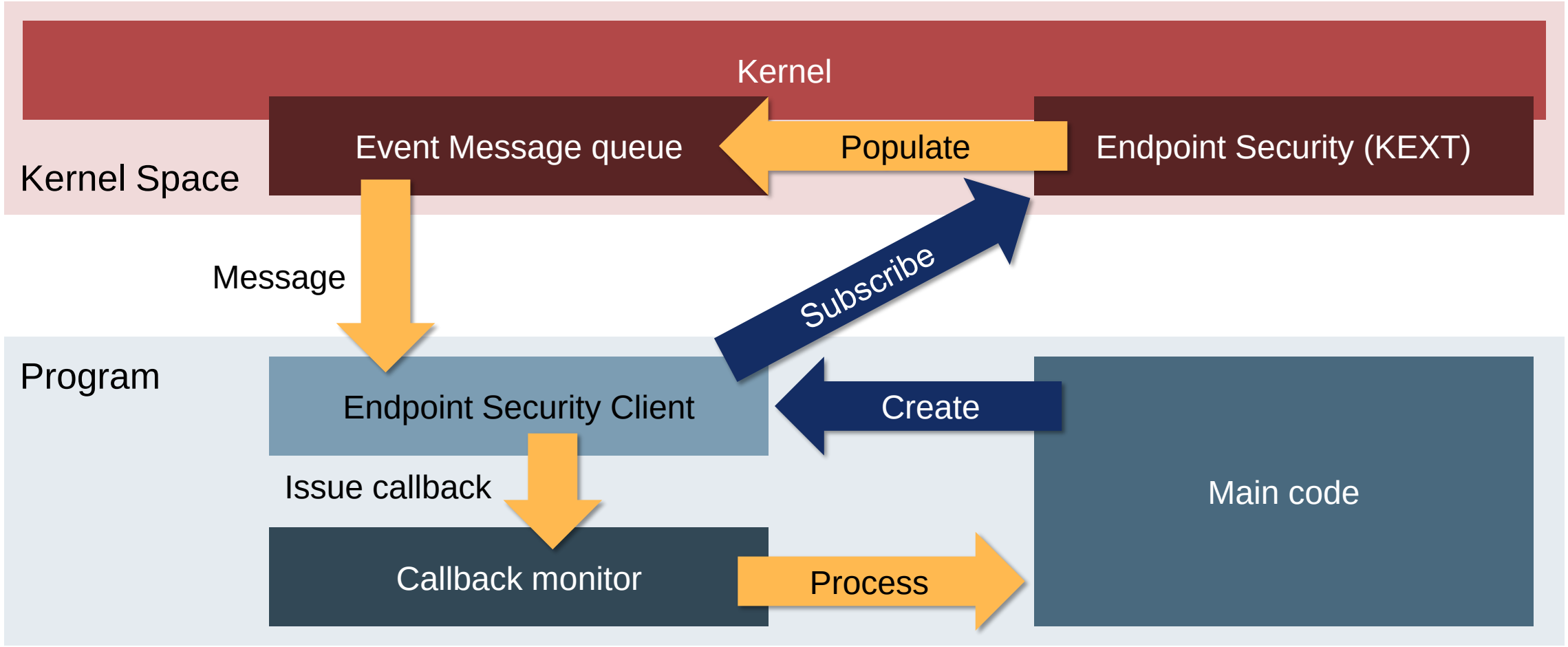
Why make the change?

- Increase stability and security
- Third party removed from Kernel Space
- Prevents BSOD and security issues
- KEXT can still be used with caveats

WITH secure

How can we use the ESF?

Basic architecture

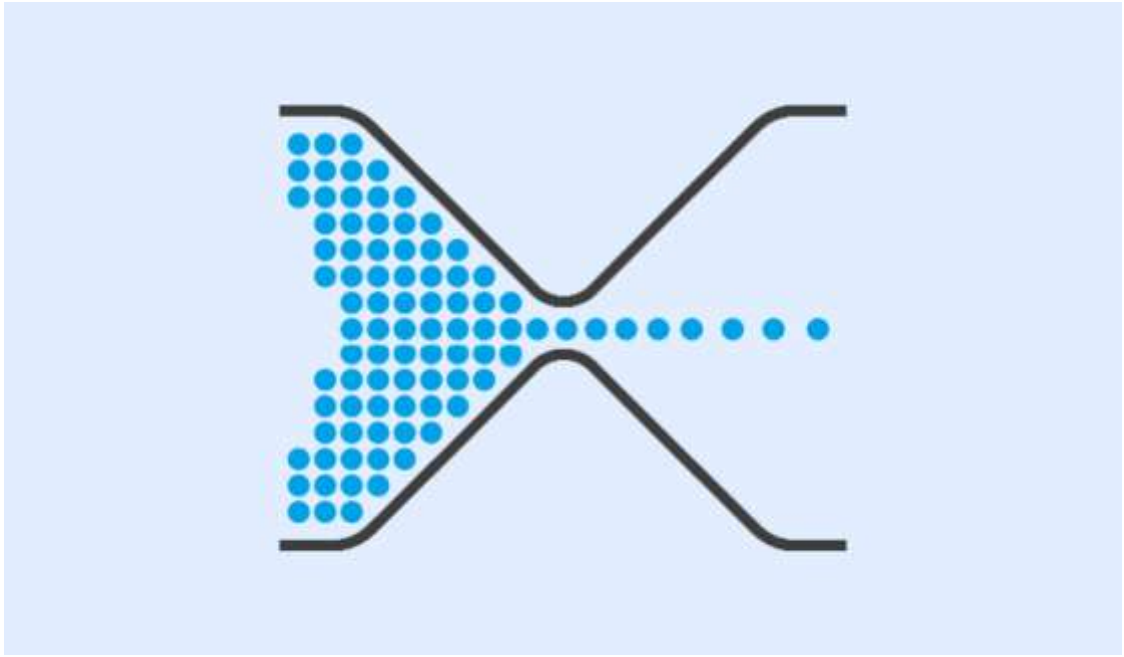


Issues with ESF use

Encountered issues

- Bottleneck in message queue
- SYSTEM verbosity
- Real Parent Process ID (PPID)

Bottleneck issue



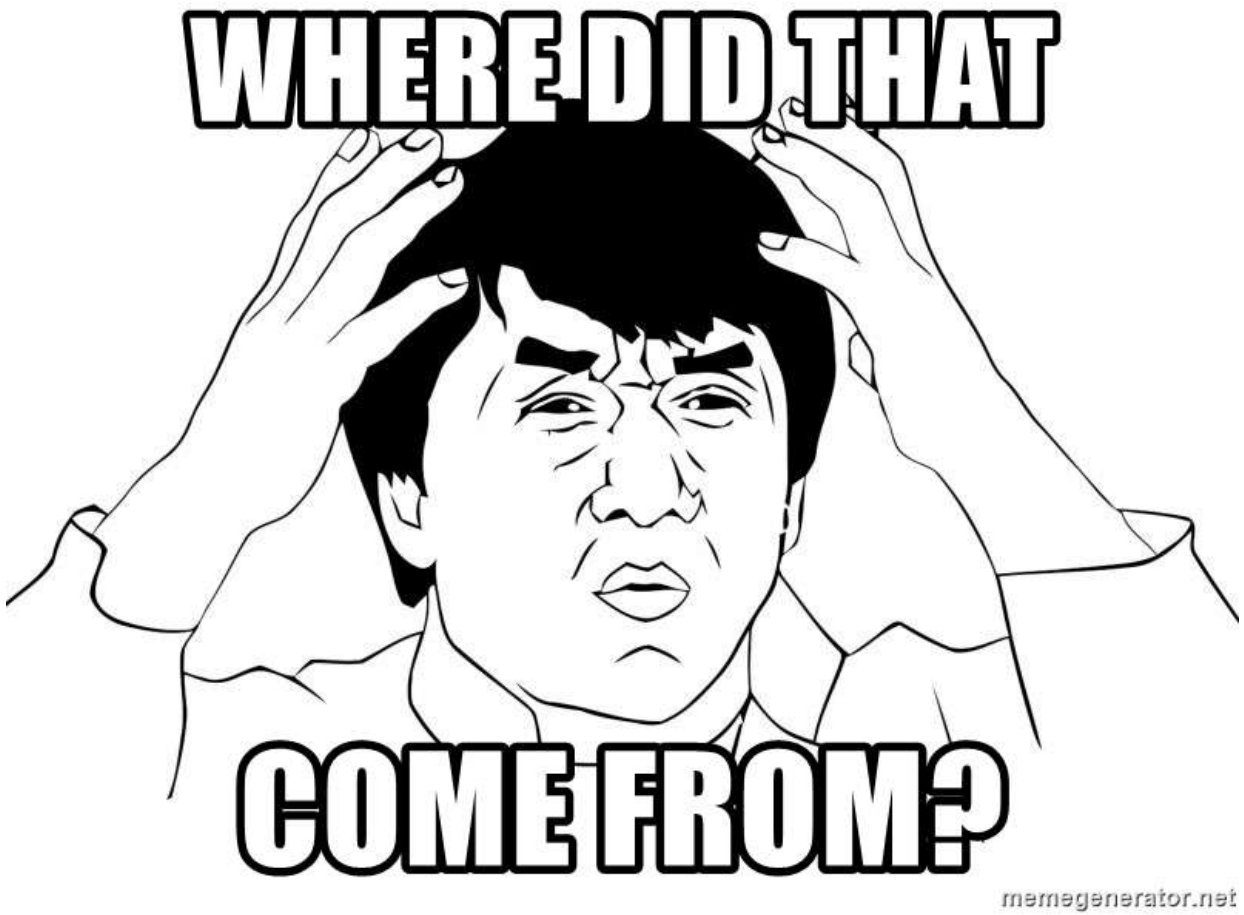
WITH secure

System verbosity issue


```
{
  "timestamp" : "2021-04-06T12:13:26.9772",
  "eventtype" : "ES_EVENT_TYPE_NOTIFY_CREATE",
  "metadata" : {
    "origin_platform_binary" : false,
    "origin_binarypath" : "\/usr\/local\/f-secure\/sensor\/sensord",
    "filesize" : 0,
    "origin_cdhash" : "D317FB56DD21489A4770C9A5227536B2B6F6C73",
    "origin_pid" : 97124,
    "origin_real_ppid" : 97124,
    "origin_uid" : 0,
    "origin_teamid" : "6KAL5AFZJC",
    "fileFullPath" : "\/usr\/local\/f-secure\/sensor\/dedup.db-wal",
    "origin_ppid" : 1,
    "origin_signingid" : "com.f-secure.ul.sensord",
    "origin_codesigningflags" : [
      "CS_VALID",
      "CS_SIGNED",
      "CS_RUNTIME",
      "CS_DYLD_PLATFORM",
      "CS_EXECSEG_MAIN_BINARY"
    ]
  }
}
{
  "timestamp" : "2021-04-06T12:13:26.9782",
  "eventtype" : "ES_EVENT_TYPE_NOTIFY_CREATE",
  "metadata" : {
    "origin_platform_binary" : false,
    "origin_binarypath" : "\/usr\/local\/f-secure\/sensor\/sensord",
    "filesize" : 0,
    "origin_cdhash" : "D317FB56DD21489A4770C9A5227536B2B6F6C73",
    "origin_pid" : 97124,
    "origin_real_ppid" : 97124,
    "origin_uid" : 0,
    "origin_teamid" : "6KAL5AFZJC",
    "fileFullPath" : "\/usr\/local\/f-secure\/sensor\/dedup.db-shm",
    "origin_ppid" : 1,
    "origin_signingid" : "com.f-secure.ul.sensord",
    "origin_codesigningflags" : [
      "CS_VALID",
      "CS_SIGNED",
      "CS_RUNTIME",
      "CS_DYLD_PLATFORM",
      "CS_EXECSEG_MAIN_BINARY"
    ]
  }
}
{
  "timestamp" : "2021-04-06T12:13:27.2412",
  "eventtype" : "ES_EVENT_TYPE_NOTIFY_CREATE",
  "metadata" : {
    "origin_platform_binary" : false,
    "origin_binarypath" : "\/usr\/local\/f-secure\/sensor\/sensord",
    "filesize" : 0,
    "origin_cdhash" : "D317FB56DD21489A4770C9A5227536B2B6F6C73",
    "origin_pid" : 97124,
    "origin_real_ppid" : 97124,
    "origin_uid" : 0,
    "origin_teamid" : "6KAL5AFZJC",
    "fileFullPath" : "\/usr\/local\/f-secure\/sensor\/event.db-wal",
    "origin_ppid" : 1,
    "origin_signingid" : "com.f-secure.ul.sensord",
    "origin_codesigningflags" : [
      "CS_VALID",
      "CS_SIGNED",
      "CS_RUNTIME",
      "CS_DYLD_PLATFORM",
      "CS_EXECSEG_MAIN_BINARY"
    ]
  }
}
```


WITH secure

Parent process id issue




```
"timestamp" : "2021-04-06T11:14:57.2482",
"eventtype" : "ES_EVENT_NOTIFY_EXEC",
"real_ppid" : 1,
"signing_id" : "com.apple.dt.Xcode.sourcecontrol.Git",
"procPid" : 81000,
"signingInformationFound" : "YES",
"origin_platform_binary" : true,
"origin_real_ppid" : 1,
"origin_cdhash" : "A4E72E326A81CF39ED9881205 3D7E2C2636954",
"env_variables" : [
"LaunchInstanceID=C86117AB-2781-4ADB-BCAD-9ECD1E579A3D",
"XPC_SERVICE_NAME=com.apple.dt.Xcode.sourcecontrol.Git",
"PATH=\/usr\/bin:\/bin:\/usr\/sbin:\/sbin",
"SSH_AUTH_SOCK=\/private\/tmp\/com.apple.launchd.g56tFwGuxg\/Listeners",
"HOME=\/Users\/drt",
"__CF_USER_TEXT_ENCODING=0x1F5:0:2",
"TMPDIR=\/var\/folders\/qc\/cvjw8vxj715218dcB42sjcw40000gn\/T\/",
"XPC_FLAGS=19",
"LOGNAME=drt",
"USER=drt",
"SHELL=\/bin\/bash"
],
"cd_hash" : "10E318A73B123D0873E5408EF0965D23E5832B41",
"procFileFullPath" : "\/Applications\/Xcode.app\/Contents\/SharedFrameworks\/DVTSourceControl.framework\/Ve
"origin_pid" : 81000,
"origin_uid" : 501,
"origin_signingid" : "com.apple.xpc.proxy",
"original_ppid" : 1,
"procUid" : 501,
"origin_codesigningflags" : [
"CS_KILL",
"CS_VALID",
"CS_SIGNED",
"CS_RUNTIME",
"CS_RESTRICT",
"CS_DYLD_PLATFORM",
"CS_EXECSEG_MAIN_BINARY"
],
"procCommandLine" : "\/Applications\/Xcode.app\/Contents\/SharedFrameworks\/DVTSourceControl.framework\/Ver
"sha1" : "72e32e3b6d5e4e4d7b420e4e6e61e1e6e54ca",
"submitted_by" : {
},
"origin_binarypath" : "\/usr\/libexec\/xpcproxy",
"parentProcFileFullPath" : "\/sbin\/launchd",
"origin_ppid" : 1,
"parentProcPid" : 1
},
{
"timestamp" : "2021-04-06T11:14:57.2642",
"eventtype" : "ES_EVENT_NOTIFY_EXEC",
"real_ppid" : 81001,
"signing_id" : "com.apple.xpc.proxy",
"procPid" : 81001,
"signingInformationFound" : "YES",
"origin_platform_binary" : true,
"origin_real_ppid" : 81001,
"origin_cdhash" : "7EC44859E464C47486B413EEF9E978263AF70D26",
"env_variables" : [
"XPC_FLAGS=0x100"
],
"cd_hash" : "A4E72E32A40A1C0F39ED9881205 3D7E2C2636954",
"procFileFullPath" : "\/usr\/libexec\/xpcproxy",
"origin_pid" : 81001,
"origin_uid" : 0,
"origin_signingid" : "com.apple.xpc.launchd",
"original_ppid" : 1,
"procUid" : 0,
"origin_codesigningflags" : [
"CS_KILL",
"CS_VALID",
"CS_SIGNED",
"CS_RUNTIME",
"CS_RESTRICT",
"CS_DYLD_PLATFORM",
"CS_EXECSEG_MAIN_BINARY"
],
"procCommandLine" : "xpcproxy com.apple.mbworker.shared.0D000000-0000-0000-0000-000000000000",
"sha1" : "0d5f91e5fa0d0034ba0e9d5efa6a05fc927d5f4",
"submitted_by" : {
"path" : "\/System\/Library\/LaunchAgents\/com.apple.mbworker.shared.plist"
},
"origin_binarypath" : "\/sbin\/launchd",
"parentProcFileFullPath" : "\/sbin\/launchd",
"origin_ppid" : 1,
"parentProcPid" : 1
}
```


WITH secure

Solutions to these issues

Bottleneck solutions

Bottleneck issue casued by kernel level queue overload

Potential solutions included:

- Multi-client system
- Event muting

In MacOS 10.15.4 an update was made to SDK 10.15 silently

- Within es_message_t the value “seq_num” was introduced

System verbosity solution

- Filter before or after collection
- Event muting is too general
- Client side filter may cause bottleneck
- SYSTEM filtering opens up SYSTEM level ignorance

PPID solution

There is no future proof solution for this, updates make solutions ineffective quickly

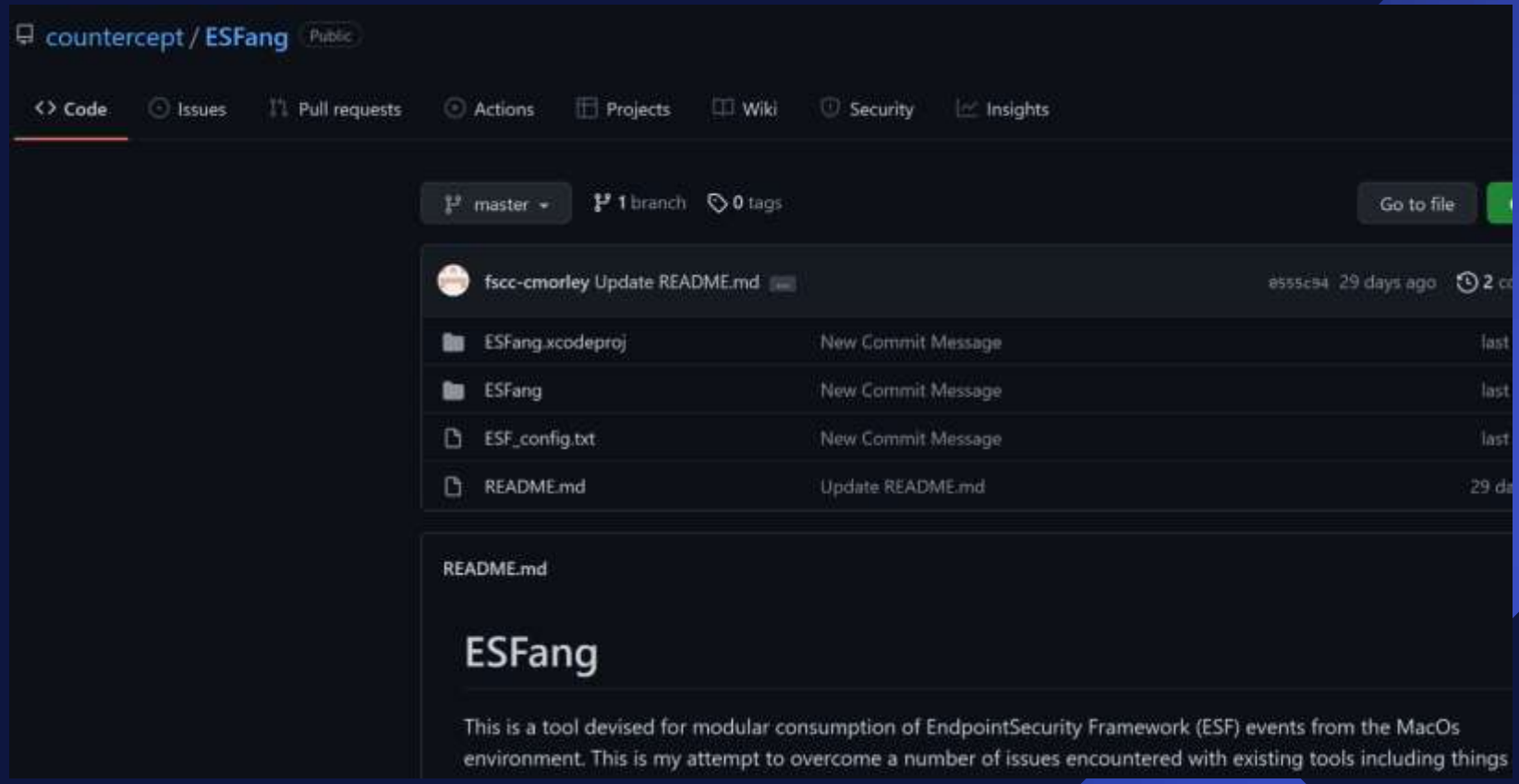
Current solutions include thing such as:

- TrueTree – Jaron Bradley
- launchdXPC – Patrick Wardle (ported from Jonathan Levin)

The latter is what is used in my solution but is only for launchd resolution, not Runningboard

My solution: ESFang

ESFang



Based heavily on the work of Patrick Wardle, Chris Ross and Omark-Ikram

WITH secure

ESFang

- 52 NOTIFY event types
- Type specific collection
- SIP disable required

```
NSString* event_type_str(const es_event_type_t event_type) {
    switch(event_type) {
        case ES_EVENT_TYPE_NOTIFY_GET_TASK: return @"ES_EVENT_TYPE_NOTIFY_GET_TASK";
        case ES_EVENT_TYPE_NOTIFY_MMAP: return @"ES_EVENT_TYPE_NOTIFY_MMAP";
        case ES_EVENT_TYPE_NOTIFY_MPROTECT: return @"ES_EVENT_TYPE_NOTIFY_MPROTECT";
        case ES_EVENT_TYPE_NOTIFY_EXEC: return @"ES_EVENT_NOTIFY_EXEC";
        case ES_EVENT_TYPE_NOTIFY_FORK: return @"ES_EVENT_NOTIFY_FORK";
        case ES_EVENT_TYPE_NOTIFY_EXIT: return @"ES_EVENT_NOTIFY_EXIT";
        case ES_EVENT_TYPE_NOTIFY_CHDIR: return @"ES_EVENT_TYPE_NOTIFY_CHDIR";
        case ES_EVENT_TYPE_NOTIFY_CHROOT: return @"ES_EVENT_TYPE_NOTIFY_CHROOT";
        case ES_EVENT_TYPE_NOTIFY_SIGNAL: return @"ES_EVENT_TYPE_NOTIFY_SIGNAL";
        case ES_EVENT_TYPE_NOTIFY_PROC_CHECK: return @"ES_EVENT_TYPE_NOTIFY_PROC_CHECK";
        case ES_EVENT_TYPE_NOTIFY_CREATE: return @"ES_EVENT_TYPE_NOTIFY_CREATE";
        case ES_EVENT_TYPE_NOTIFY_DUP: return @"ES_EVENT_TYPE_NOTIFY_DUP";
        case ES_EVENT_TYPE_NOTIFY_CLOSE: return @"ES_EVENT_TYPE_NOTIFY_CLOSE";
        case ES_EVENT_TYPE_NOTIFY_WRITE: return @"ES_EVENT_TYPE_NOTIFY_WRITE";
        case ES_EVENT_TYPE_NOTIFY_RENAME: return @"ES_EVENT_TYPE_NOTIFY_RENAME";
        case ES_EVENT_TYPE_NOTIFY_OPEN: return @"ES_EVENT_TYPE_NOTIFY_OPEN";
        case ES_EVENT_TYPE_NOTIFY_CLONE: return @"ES_EVENT_TYPE_NOTIFY_CLONE";
        case ES_EVENT_TYPE_NOTIFY_TRUNCATE: return @"ES_EVENT_TYPE_NOTIFY_TRUNCATE";
        case ES_EVENT_TYPE_NOTIFY_LOOKUP: return @"ES_EVENT_TYPE_NOTIFY_LOOKUP";
        case ES_EVENT_TYPE_NOTIFY_ACCESS: return @"ES_EVENT_TYPE_NOTIFY_ACCESS";
        case ES_EVENT_TYPE_NOTIFY_FCNTL: return @"ES_EVENT_TYPE_NOTIFY_FCNTL";
        case ES_EVENT_TYPE_NOTIFY_LINK: return @"ES_EVENT_TYPE_NOTIFY_LINK";
        case ES_EVENT_TYPE_NOTIFY_UNLINK: return @"ES_EVENT_TYPE_NOTIFY_UNLINK";
        case ES_EVENT_TYPE_NOTIFY_READLINK: return @"ES_EVENT_TYPE_NOTIFY_READLINK";
        case ES_EVENT_TYPE_NOTIFY_EXCHANGEDATA: return @"ES_EVENT_TYPE_NOTIFY_EXCHANGEDATA";
        case ES_EVENT_TYPE_NOTIFY_KEXTLOAD: return @"ES_EVENT_TYPE_NOTIFY_KEXTLOAD";
        case ES_EVENT_TYPE_NOTIFY_KEXTUNLOAD: return @"ES_EVENT_TYPE_NOTIFY_KEXTUNLOAD";
        case ES_EVENT_TYPE_NOTIFY_IOKIT_OPEN: return @"ES_EVENT_TYPE_NOTIFY_IOKIT_OPEN";
        case ES_EVENT_TYPE_NOTIFY_SETATTRLIST: return @"ES_EVENT_TYPE_NOTIFY_SETATTRLIST";
        case ES_EVENT_TYPE_NOTIFY_GETATTRLIST: return @"ES_EVENT_TYPE_NOTIFY_GETATTRLIST";
        case ES_EVENT_TYPE_NOTIFY_GETEXTATTR: return @"ES_EVENT_TYPE_NOTIFY_GETEXTATTR";
        case ES_EVENT_TYPE_NOTIFY_LISTEXTATTR: return @"ES_EVENT_TYPE_NOTIFY_LISTEXTATTR";
        case ES_EVENT_TYPE_NOTIFY_DELETEEXTATTR: return @"ES_EVENT_TYPE_NOTIFY_DELETEEXTATTR";
        case ES_EVENT_TYPE_NOTIFY_SETOWNER: return @"ES_EVENT_TYPE_NOTIFY_SETOWNER";
        case ES_EVENT_TYPE_NOTIFY_SETEXTATTR: return @"ES_EVENT_TYPE_NOTIFY_SETEXTATTR";
        case ES_EVENT_TYPE_NOTIFY_SETFLAGS: return @"ES_EVENT_TYPE_NOTIFY_SETFLAGS";
        case ES_EVENT_TYPE_NOTIFY_SETMODE: return @"ES_EVENT_TYPE_NOTIFY_SETMODE";
        case ES_EVENT_TYPE_NOTIFY_SETACL: return @"ES_EVENT_TYPE_NOTIFY_SETACL";
        case ES_EVENT_TYPE_NOTIFY_UTIMES: return @"ES_EVENT_TYPE_NOTIFY_UTIMES";
        case ES_EVENT_TYPE_NOTIFY_READDIR: return @"ES_EVENT_TYPE_NOTIFY_READDIR";
        case ES_EVENT_TYPE_NOTIFY_FSGETPATH: return @"ES_EVENT_TYPE_NOTIFY_FSGETPATH";
        case ES_EVENT_TYPE_NOTIFY_STAT: return @"ES_EVENT_TYPE_NOTIFY_STAT";
        case ES_EVENT_TYPE_NOTIFY_UIPC_BIND: return @"ES_EVENT_TYPE_NOTIFY_UIPC_BIND";
        case ES_EVENT_TYPE_NOTIFY_UIPC_CONNECT: return @"ES_EVENT_TYPE_NOTIFY_UIPC_CONNECT";
        case ES_EVENT_TYPE_NOTIFY_PTY_GRANT: return @"ES_EVENT_TYPE_NOTIFY_PTY_GRANT";
        case ES_EVENT_TYPE_NOTIFY_PTY_CLOSE: return @"ES_EVENT_TYPE_NOTIFY_PTY_CLOSE";
        case ES_EVENT_TYPE_NOTIFY_MOUNT: return @"ES_EVENT_TYPE_NOTIFY_MOUNT";
        case ES_EVENT_TYPE_NOTIFY_UNMOUNT: return @"ES_EVENT_TYPE_NOTIFY_UNMOUNT";
        case ES_EVENT_TYPE_NOTIFY_FILE_PROVIDER_MATERIALIZE: return @"ES_EVENT_TYPE_NOTIFY_FILE_PROVIDER_MATERIALIZE";
```

ESFang

- Single/multiple types
- JSON output
- Upstream integration design

WITH secure

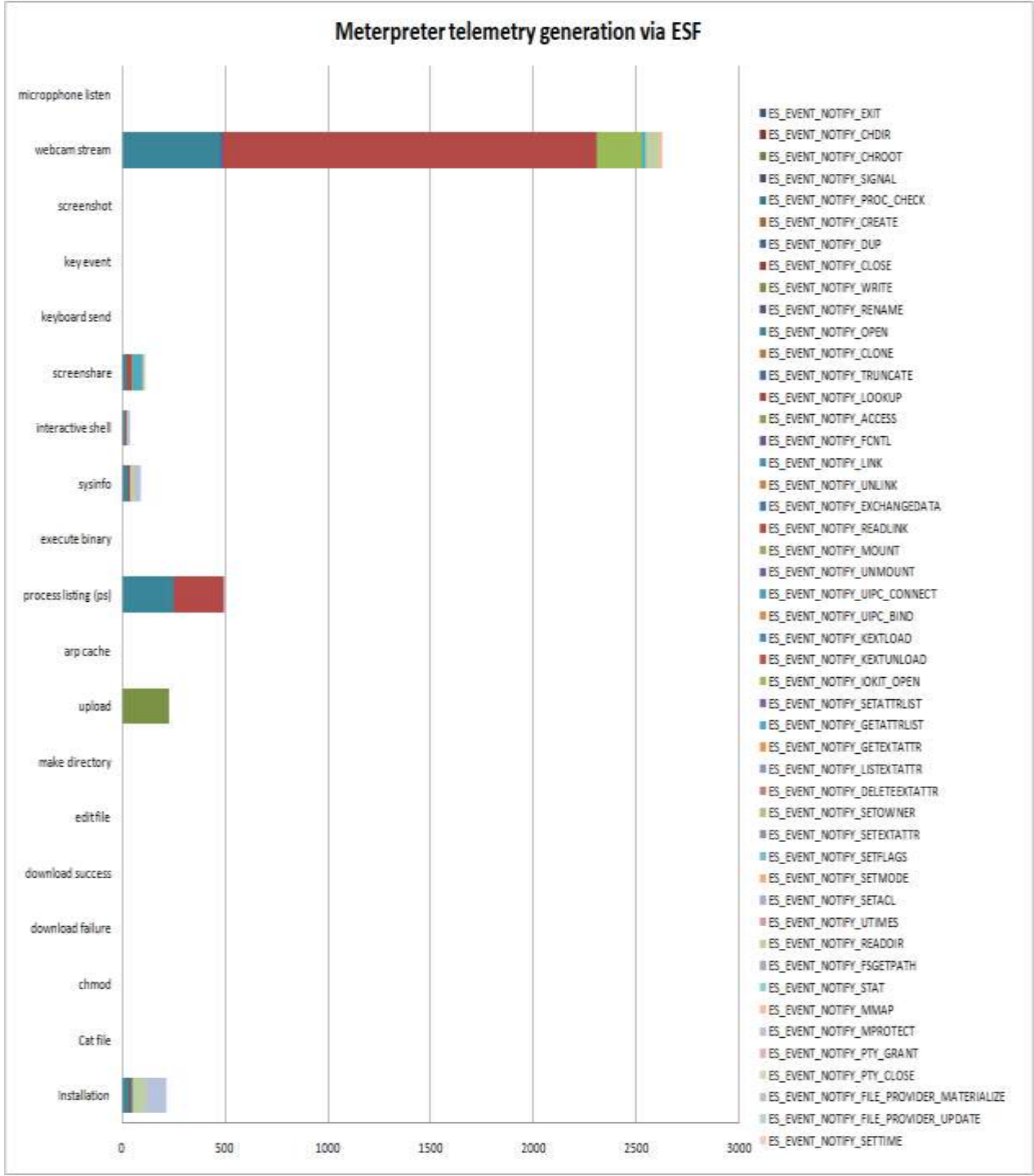
Meterpreter use case

WITH secure

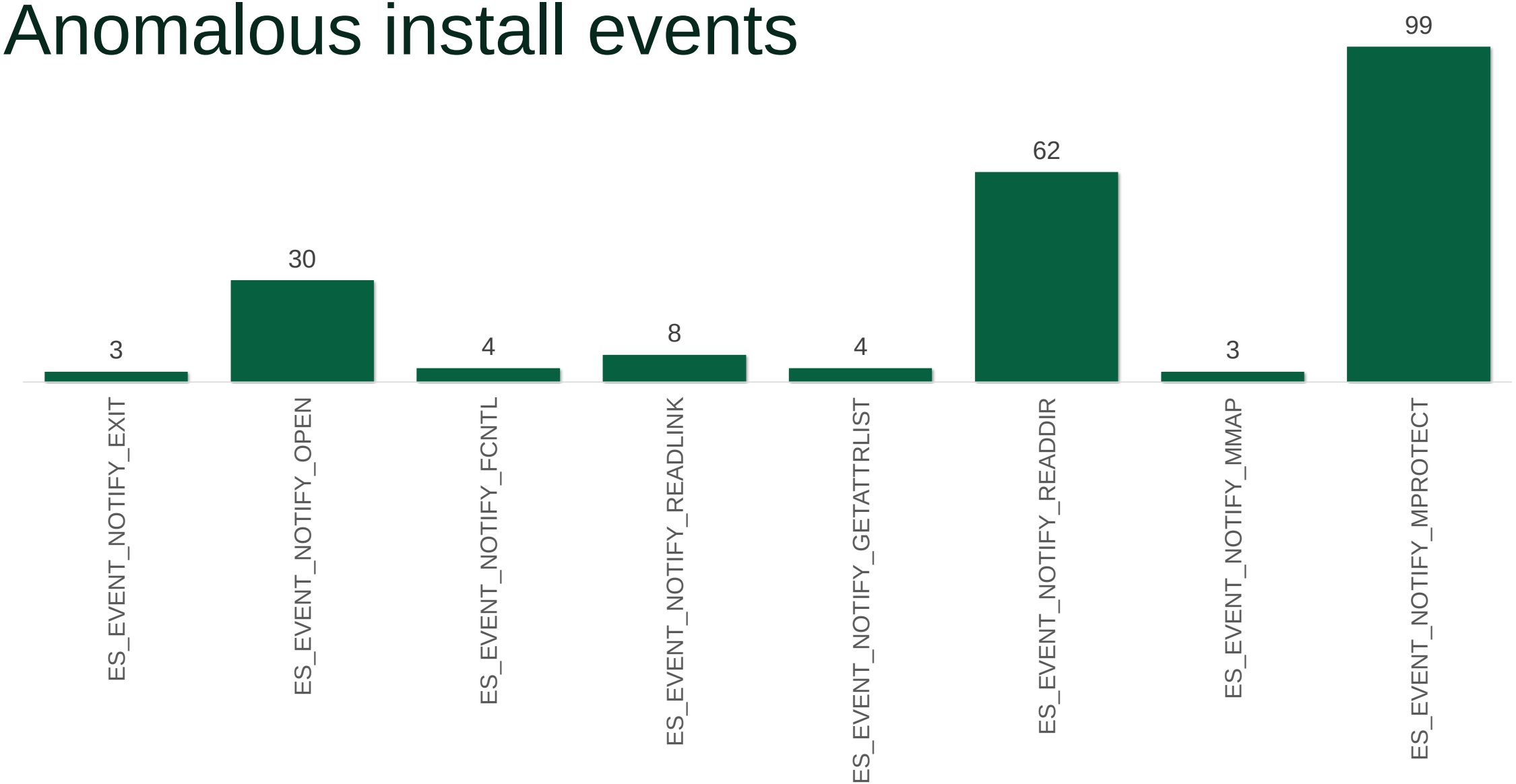
Use case outline

- Tested on MacOS 11.2.2
- ESFang collection
- Agent only test
- Post-exploit phase only
- Single host test

Overall findings



Anomalous install events



WITH secure

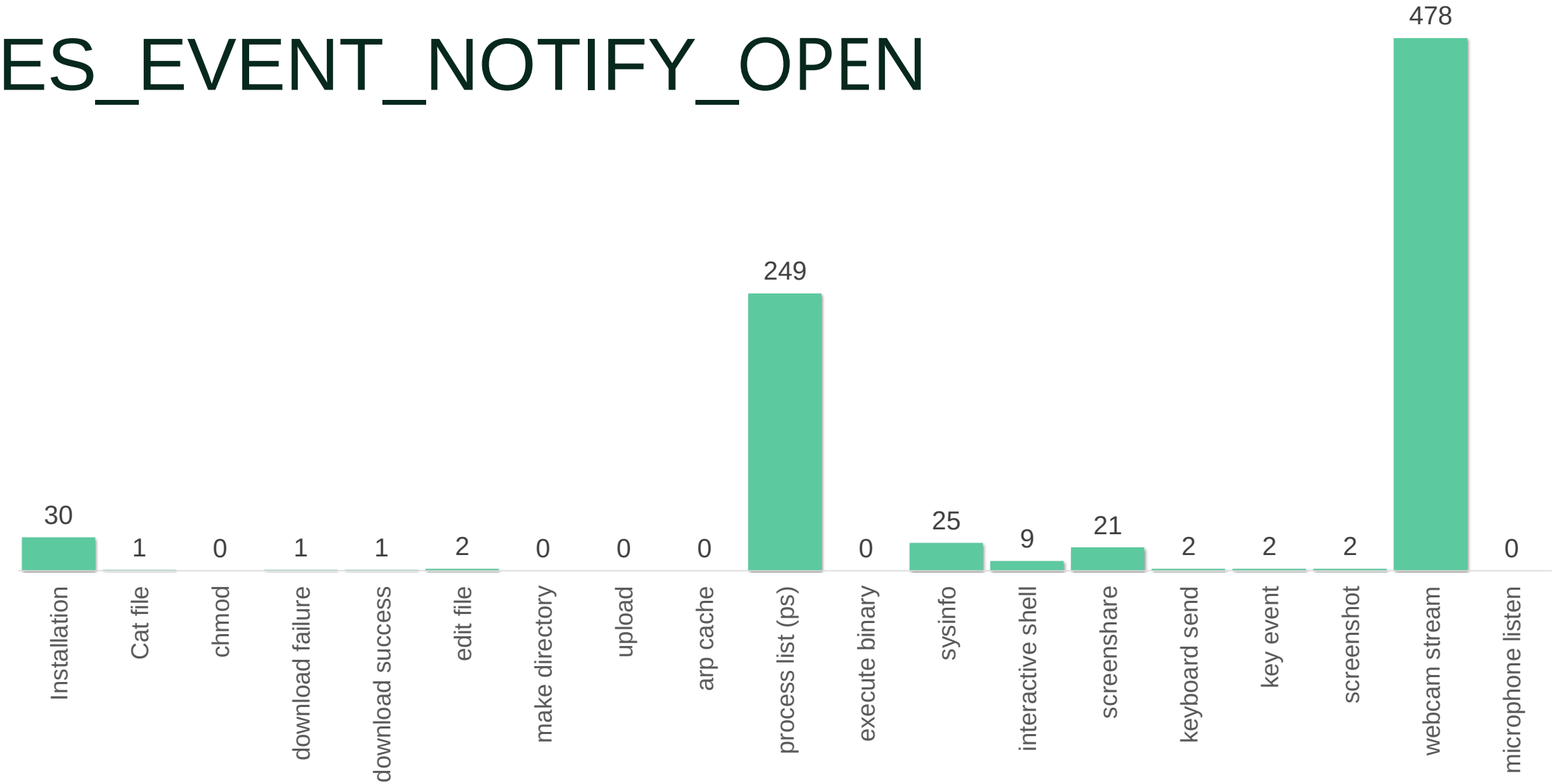
Breaking this down

Installation has 259 data points

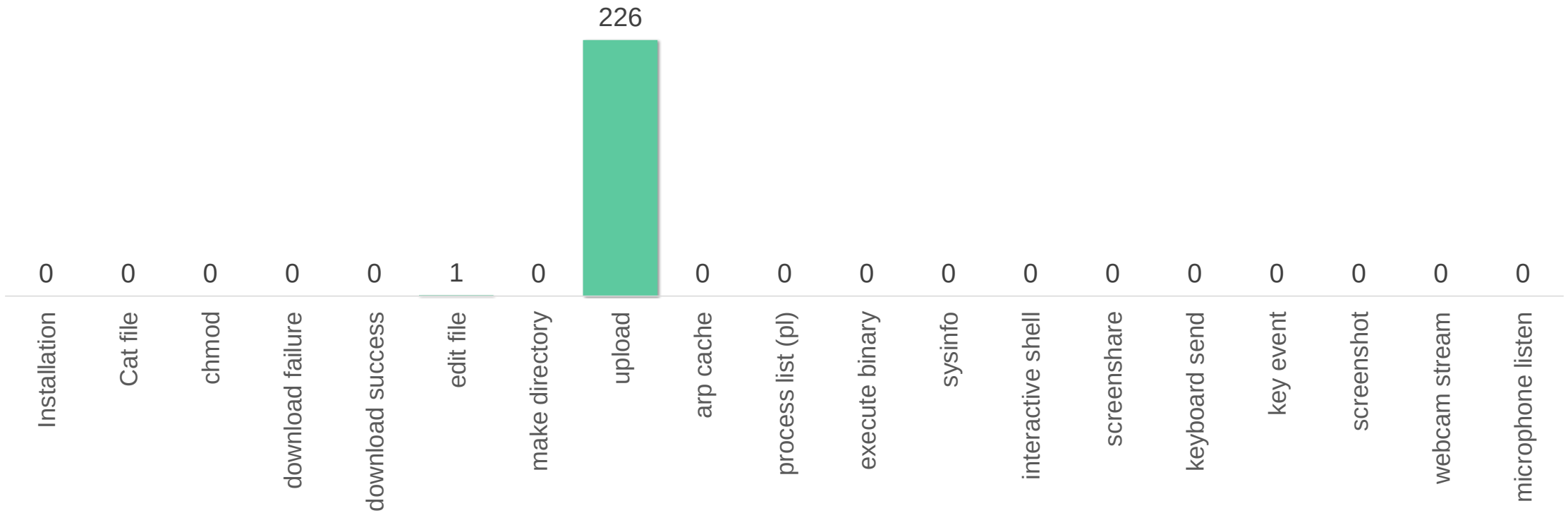
Quantity is not always a good thing, but allows for better cross referencing and accuracy

Let's look at some of the more valuable event types in detail…

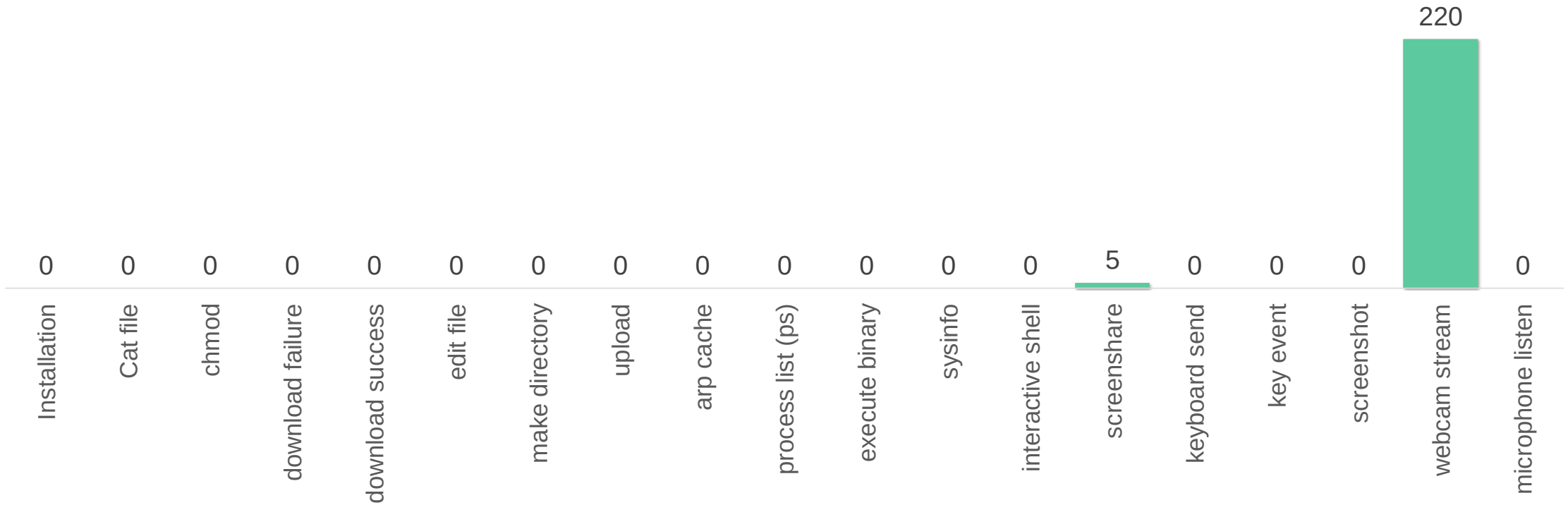
ES_EVENT_NOTIFY_OPEN



ES_EVENT_NOTIFY_WRITE



ES_EVENT_NOTIFY_IOKIT_OPEN



Full list of valued types

Valuable event types for detection:

- ES_EVENT_TYPE_NOTIFY_EXEC
- ES_EVENT_TYPE_NOTIFY_FORK
- ES_EVENT_TYPE_NOTIFY_OPEN
- ES_EVENT_TYPE_NOTIFY_CREATE
- ES_EVENT_TYPE_NOTIFY_FCNTL
- ES_EVENT_TYPE_ NOTIFY_WRITE
- ES_EVENT_TYPE_ NOTIFY_READLINK
- ES_EVENT_TYPE_ NOTIFY_MMAP
- ES_EVENT_TYPE_ NOTIFY_MPROTECT
- ES_EVENT_TYPE_ NOTIFY_IOKIT_OPEN
- ES_EVENT_TYPE_ NOTIFY_UIPC_CONNEC
- ES_EVENT_TYPE_NOTIFY_PTY_GRANT
- ES_EVENT_TYPE_NOTIFY_DUP
- ES_EVENT_TYPE_NOTIFY_STAT
- ES_EVENT_TYPE_NOTIFY_RENAME
- ES_EVENT_TYPE_NOTIFY_SETMODE
- ES_EVENT_TYPE_NOTIFY_SETEXTATTR

Summary

- Powerful and regularly updated
- No choice in its use
- Teething issues
- Stable and easy to use
- High detection capability
- Filtering is essential

Questions?

WITH®

secure