

Technical Overview of **cmd Reporter**

Dan Griggs, CEO cmdSecurity Inc.
Jun 19, 2019



cmdReporter is a security monitoring tool for macOS.

Using native built-in resources, it collects the **data IT security teams need** to hunt threats on macOS computers in real time.



What cmdReporter Solves

- Regulatory auditing and logging requirements.
- Data loss prevention (DLP) requirements.
- Security team visibility into macOS.
- Historical threat hunting.
- Security tool instability.

What cmdReporter does



Who we are

Jamf certified macOS and security experts

Presented at JNUC 2017

Author/contributor to multiple versions of:

- DISA STIGs
- CIS benchmarks
- Cybersecurity Campaign Playbook

Deployed or defended Macs at:

- NIST
- The Pentagon
- NASA
- NASA JPL
- JHUAPL
- Pharmaceutical Firms
- FinTech Firms

What we are trying to do

- Extend, don't replace macOS security features.
- User-experience-focused security.
- Provide the enterprise-grade security tools macOS deserves.

What's built into cmdReporter



Regulatory
Compliance



JSON output



Continuously
streaming data



No kernel extension



Light footprint



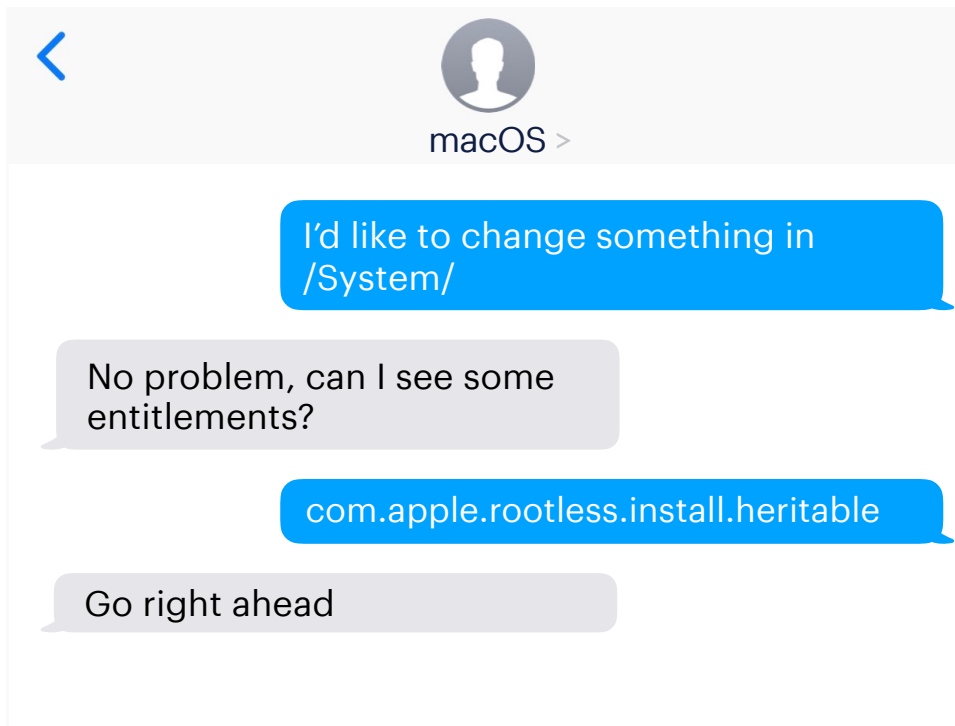
Modern
Management

100% Configuration Profile Coverage



MACF

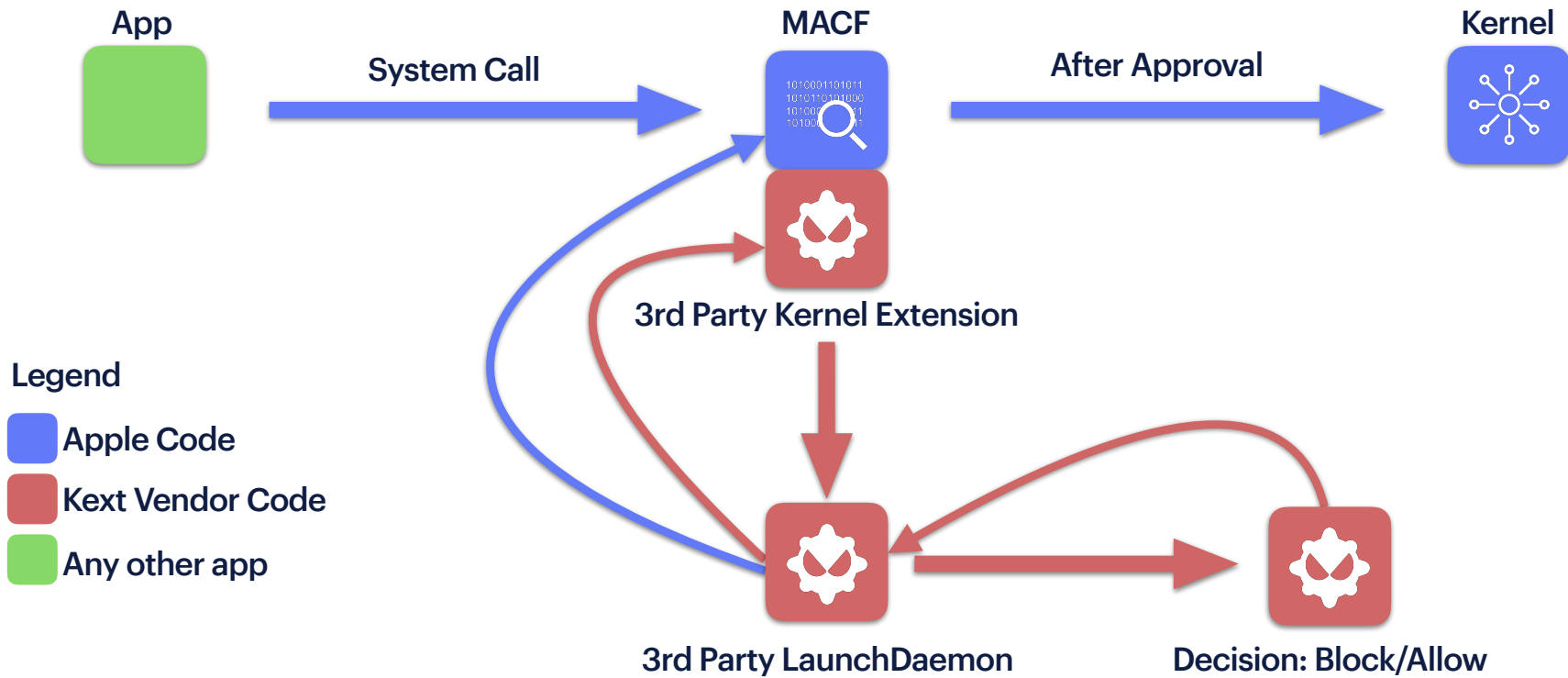
Mandatory Access Control Framework



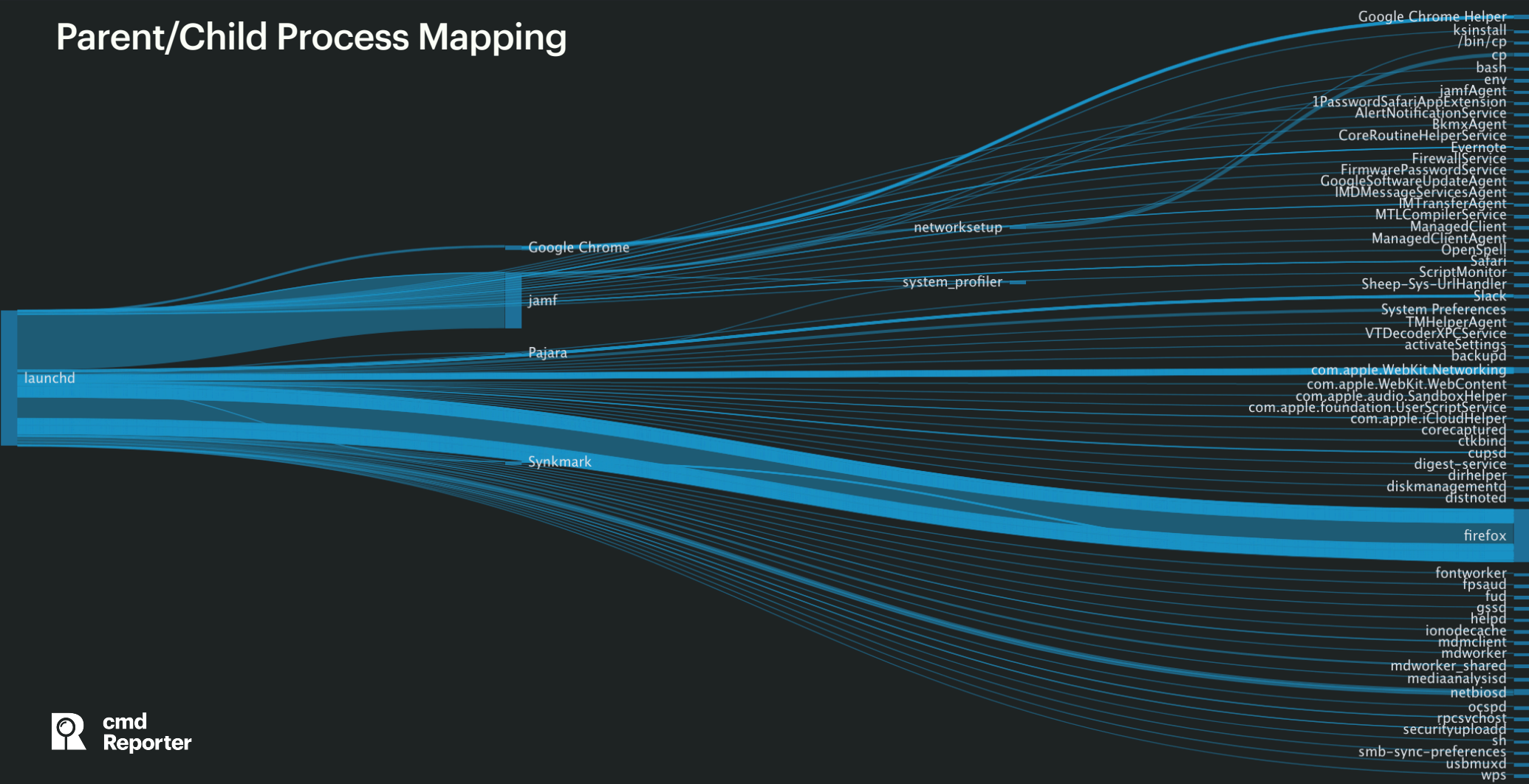
- Every system call, for any app or process requires MACF approval.
- TCC controls around Contacts, Photos, and Mail? MACF.
- MACF **blocks** a system call until approval is received.
- Major component of current macOS app sandboxing
- MACF Policy Plugins



Why kexts slow down macOS



Parent/Child Process Mapping



What terminal users see

```
$ sudo fdesetup list
dan,3F6E4B3A-9285-4E7E-9A0C-C3B62DC379DF
```

What macOS OpenBSM would log

```
header,140,11,AUE_DARWIN_sudo,0,Tue Feb 19 10:14:40 2019, + 636 msec
subject_ex,morty,root,staff,root,wheel,384,384,50331650,0.0.0.0
exec_arg,fdesetup,list
return,success,0
identity,1,com.apple.sudo,complete,,complete,0x9d683833e4e38e482a32fa6953bee2e21bffb3d8
trailer,140
```



What cmdReporter logs



What terminal users see

```
$ sudo fdesetup list
dan,3F6E4B3A-9285-4E7E-9A0C-C3B62DC379DF
```

What macOS OpenBSM would log

```
header,140,11,AUIE_DARWIN_sudo,0,Tue Feb 19 10:14:40 2019, + 636 msec
subject_ex,morty,root,staff,root,wheel,384,384,50331650,0.0.0.0
exec_arg,fdesetup,list
return,success,0
identity,1,com.apple.sudo,complete,,complete,0x9d683383e4e38e482a32fa6953bee2e21bffb3d8
trailer,140
```



```
identity : {
  "cd_hash": "1d9c8250bfb6114b29404a8bb2dacc78aeb46f66",
  "signer_id": "com.apple.zsh",
  "signer_id_truncated": 0,
  "signer_type": 1,
  "team_id": "",
  "team_id_truncated": 0
},
"path": [
  "/Users/morty/bin/fdesetup"
],
"return": {
  "description": "success",
  "error": 0,
  "return_value": 0
},
"subject": {
  "audit_id": 502,
  "audit_user_name": "morty",
  "effective_group_id": 20,
  "effective_group_name": "staff",
  "effective_user_id": 502,
  "effective_user_name": "dan",
  "group_id": 20,
  "group_name": "staff",
  "process_id": 40210,
  "process_name": "/usr/bin/sudo",
  "session_id": 100009,
  "terminal_id": {
    "addr": [
      0
    ],
    "ip_address": "0.0.0.0",
```

What terminal users see



```
$ sudo fdesetup list
dan,3F6E4B3A-9285-4E7E-9A0C-C3B62DC379DF
```

What macOS OpenBSM would log



```
header,140,11,AUE DARWIN_sudo,0,Tue Feb 19 10:14:40 2019, + 636 msec
subject_ex,morty,root,staff,root,wheel,384,384,50331650,0.0.0.0
exec_arg,fdesetup,list
return,success,0
identity,1,com.apple.sudo,complete,,complete,0x9d683383e4e38e482a32fa6953bee2e21bffb3d8
trailer,140
```



```
"signer_id_truncated": 0,
"signer_type": 1,
"team_id": "",
"team_id_truncated": 0
},
"path": [
  "/Users/morty/bin/fdesetup"
],
"return": {
  "description": "success",
  "error": 0,
  "return_value": 0
},
"subject": {
  "audit_id": 502,
  "audit_user_name": "morty",
  "effective_group_id": 20,
  "effective_group_name": "staff",
  "effective_user_id": 502,
  "effective_user_name": "dan",
  "group_id": 20,
  "group_name": "staff",
  "process_id": 40210,
  "process_name": "/usr/bin/sudo",
  "session_id": 100009,
  "terminal_id": {
    "addr": [
      0
    ],
    "ip_address": "0.0.0.0",
    "port": 50331650,
    "type": 0
  }
},
```

What terminal users see

```
$ sudo fdesetup list
dan,3F6E4B3A-9285-4E7E-9A0C-C3B62DC379DF
```

What macOS OpenBSM would log

```
header,140,11,AUE_DARWIN_sudo,0,Tue Feb 19 10:14:40 2019, + 636 msec
subject ex,morty,root,staff,root,wheel,384,384,50331650,0.0.0.0
exec_arg,fdesetup,list
return,success,0
identity,1,com.apple.sudo,complete,,complete,0x9d683383e4e38e482a32fa6953bee2e21bffb3d8
trailer,140
```



```
"is_non_attributeable_event": false,
"time_milliseconds_offset": 441,
"time_seconds_epoch": 1550763610,
"version": 11
},
"host_info": {
  "host_name": "Hogwarts",
  "host_uuid": "3F6E4B3A-9285-4E7E-9A0C-C3B62DC379DF",
  "primary_mac_address": "38:f9:e8:15:5a:82",
  "serial_number": "C03XY889JHG3"
},
"identity": {
  "cd_hash": "1d9c8250bfb6114b29404a8bb2dacc78aeb46f66",
  "signer_id": "com.apple.zsh",
  "signer_id_truncated": 0,
  "signer_type": 1,
  "team_id": "",
  "team_id_truncated": 0
},
"path": [
  "/Users/morty/bin/fdesetup"
],
"return": {
  "description": "success",
  "error": 0,
  "return_value": 0
},
"subject": {
  "audit_id": 502,
  "audit_user_name": "morty",
  "effective_group_id": 20,
  "effective_group_name": "staff",
  "effective_user_id": 502,
```

What terminal users see

```
$ sudo fdesetup list
dan,3F6E4B3A-9285-4E7E-9A0C-C3B62DC379DF
```

What macOS OpenBSM would log

```
header,140,11,AUE_DARWIN_sudo,0,Tue Feb 19 10:14:40 2019, + 636 msec
subject_ex,morty,root,staff,root,wheel,384,384,50331650,0.0.0.0
exec_arg,fdesetup,list
return,success,0
identity,1,com.apple.sudo,complete,,complete,0x9d683383e4e38e482a32fa6953bee2e21bffb3d8
trailer,140
```



```
"env": {
  "Apple_PubSub_Socket_Render": "/private/tmp/com.apple.launchd...",
  "COLORFGBG": "15;0",
  "COLORTERM": "truecolor",
  "COMMAND_MODE": "unix2003",
  "HOME": "/Users/morty",
  "ITERM_PROFILE": "TopScreen",
  "ITERM_SESSION_ID": "w0t0p2:63E5B91A-6AB3-49A6-86CA-B2D3F...",
  "LANG": "en_US.UTF-8",
  "LC_CTYPE": "en_US.UTF-8",
  "LESS": "-R",
  "LOGNAME": "morty",
  "LSCOLORS": "Gxfxcxdxbxegedabagacad",
  "OLDPWD": "/Users/morty/git-content/cmdReporter",
  "PAGER": "less",
  "PATH": "/Users/morty/bin:/usr/local/bin:/usr/libexec:/u...",
  "PWD": "/Users/morty/git-content/cmdReporter/deployment_p...",
  "SECURITYSESSIONID": "186a9",
  "SHELL": "/bin/bash",
  "SHLVL": "1",
  "SSH_AUTH_SOCK": "/private/tmp/com.apple.launchd.agq0W55F...",
  "TERM": "xterm-256color",
  "TERM_PROGRAM": "iTerm.app",
  "TERM_PROGRAM_VERSION": "3.2.7",
  "TERM_SESSION_ID": "w0t0p2:63E5B91A-6AB3-49A6-86CA-B2D3F...",
  "TMPDIR": "/var/folders/y1/_qx51bb12qgbj1w28d08f20h0000gp...",
  "USER": "morty",
  "XPC_FLAGS": "0x0",
  "XPC_SERVICE_NAME": "0",
  "ZSH": "/Users/morty/.oh-my-zsh",
  "_": "/usr/bin/sudo",
  "CF_USER_TEXT_ENCODING": "0x1F6:0x0:0x0"
```


TA-cmdReporter Popular Event Types

cmdrep
cmdrep_interactive_event
cmdrep_non_interactive_event
cmdrep_acc
cmdrep_acc_group
cmdrep_acc_group_create
cmdrep_acc_group_delete
cmdrep_acc_user
cmdrep_acc_user_delete

cmdrep_acc_group_modify

cmdrep_acc_user_create

cmdrep_acc_user_modify

cmdrep_audit
cmdrep_authorization_check
cmdrep_auth
cmdrep_auth_failure
cmdrep_auth_success
cmdrep_auth_failure_password
cmdrep_auth_failure_touchid
cmdrep_auth_login_piv
cmdrep_auth_login_piv_success
cmdrep_auth_login_piv_failed

cmdrep_auth_login_service_acct

cmdrep_auth_login_service_acct_failure
cmdrep_auth_login_service_acct_success
cmdrep_auth_success_password
cmdrep_auth_success_touchid
cmdrep_auth_escalated_priv
cmdrep_auth_preference_sharing
cmdrep_auth_sudo
cmdrep_priv_shell_action
cmdrep_diskvol
cmdrep_diskvol_mount
cmdrep_diskvol_unmount
cmdrep_exec
cmdrep_exec_rootbg
cmdrep_exec_firewall

cmdrep_exec_user_sudo

cmdrep_exec_background_sudo

cmdrep_priv_actions

cmdrep_exec_user

cmdrep_priv_action_on_system_folder

cmdrep_exec_interactive
cmdrep_exec_non_interactive
cmdrep_service_action
cmdrep_priv_shell_action

cmdrep_file
cmdrep_file_crontab

cmdrep_file_etc

cmdrep_file_etc_hosts
cmdrep_file_loginprefs
cmdrep_file_startupitems
cmdrep_file_airdrop_send
cmdrep_hardware
cmdrep_hardware_removable
cmdrep_hardware_usb
cmdrep_hardware_usb_connected
cmdrep_hardware_usb_disconnected
cmdrep_internal
cmdrep_internal_license
cmdrep_internal_signal

cmdrep_listen

cmdrep_misc
cmdrep_network
cmdrep_network_system
cmdrep_network_user
cmdrep_ptrace
cmdrep_service
cmdrep_session
cmdrep_task
cmdrep_time

Reporting for every risk, every level

	LEVEL 1	LEVEL 2	LEVEL 3
Login	✓	✓	✓
Authorization	✓	✓	✓
User and group account creation/modify events	✓	✓	✓
Hardware change events	✓	✓	✓
System operation events, such as mounting external drives	✓	✓	✓
Network and firewall changes	✓	✓	✓
Process (.app) execution	✓	✓	✓
Terminal and Shell script actions	✓	✓	✓
X-Protect and Gatekeeper evaluations	✓	✓	✓
System and User apps listening for network connections	✓	✓	✓
Non-browser user network connections		✓	✓
System-level network communications		✓	✓
File system events in system configuration folders	✓	✓	✓
File system events on external drives	○	○	○
All network traffic including user browser traffic			✓

Know who is sending data

```
{
  "host_info": {
    "host_name": "Dan_macbook_pro",
    "host_uuid": "3F6E4B3A-9285-4E7E-9A0C-C3B62DC379DF",
    "osversion": "Version 10.14.5 (Build 18F203)",
    "primary_mac_address": "38:f9:e8:15:5a:82",
    "serial_number": "C03XY889JHG3"
  },
  "identity": {
    "cd_hash": "9f09a16813b35dcd110d58c43cb04b9fbb26a60d",
    "signer_id": "com.sublimetext.3",
    "signer_id_truncated": 0,
    "signer_type": 0,
    "team_id": "Z6D26JE4Y4",
    "team_id_truncated": 0
  }
}
```

What cmdReporter Solves

- Regulatory auditing and logging requirements.
- Data loss prevention (DLP) tools required.
- Security team visibility into macOS usage.
- Historical threat hunting

Pricing is simple.

\$15 per computer, per year.

8x5 Technical support included.

Demo:
cmdReporter data on Splunk-built Windows
endpoint dashboards.

Network Traffic [Show Filters](#)

[Edit](#)[Export](#)[...](#)

Blocked Connections

2,200

Allowed Connections

13,601

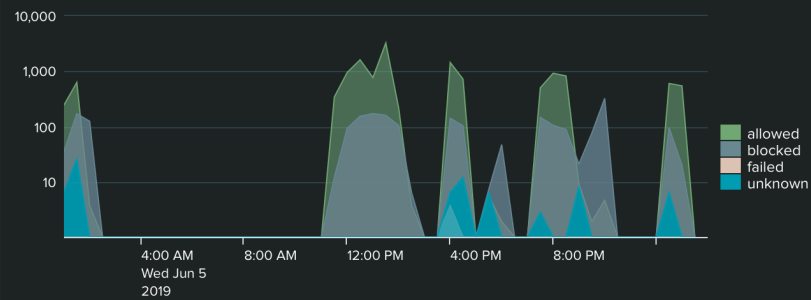
Traffic Sources

1

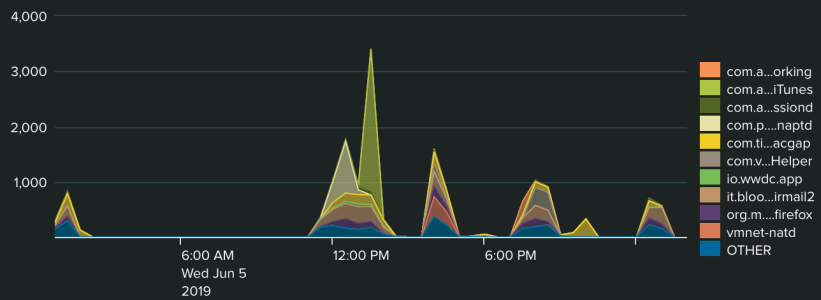
Traffic Destinations

1,087

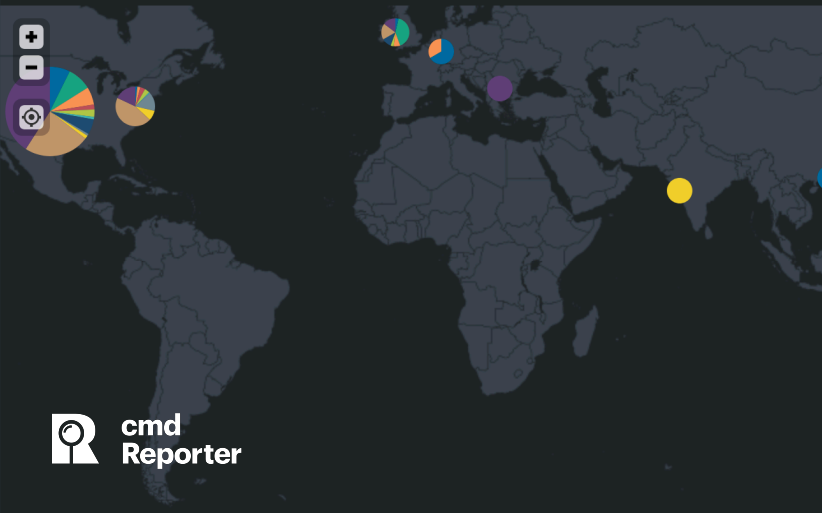
Network Traffic by Action (Logarithmic Scale)



Traffic by App/Protocol

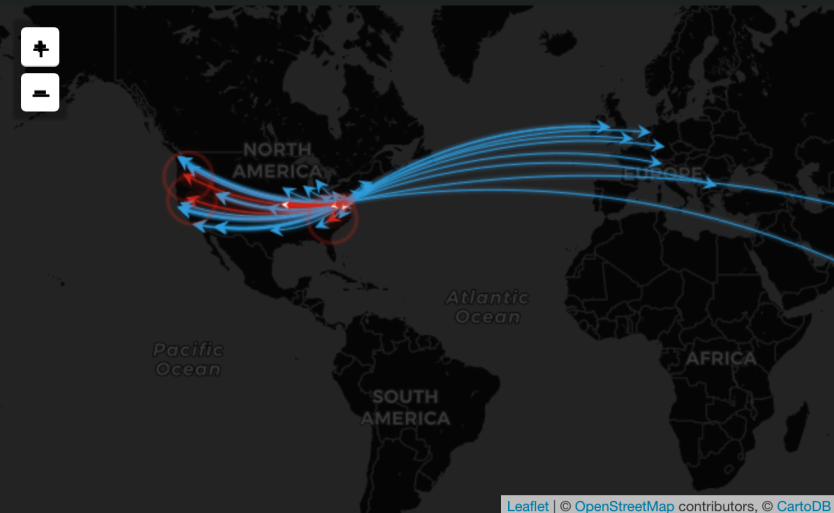


Outgoing Traffic by Application



cmd Reporter

Outgoing Traffic by Location



Leaflet | © OpenStreetMap contributors, © CartoDB

User Investigation

Edit
Export
...

User (Wildcards Accepted)

Authentication Success/Failure

_softwareupdate

Last 30 days

All

Hide Filters

Access over Time by Action

Access over Time by App

Account Changes

No results found.

Access by Source

src	dest	timechart
Dan_macbook_pro	Dan_macbook_pro	

User Authentications

count	app	user	src_u
book_pro 16	SoftwareUpdateConfigData	_softwareupdate	_soft

Events with User Name

entity	data source	count
	cmdreporter:network	228
	cmdreporter:auth	178
	cmdreporter:exec	12
	cmdreporter:session	4
	cmdreporter:listen	2
vm-remote-lock-command	cmdreporter:session	2

Authentications Map (Map Shows up to 250 Authentication Destinations)

Process Map Filters

Process Filter

Endpoint Name Filter

Endpoints Process Ran on

Select Time Range

*

17*

Any number of endpoints

Last 24 hours



Processes (with Filters Applied)

process_name	endpoints
ccloud	14
trustd	16
com.apple.geod	17
CalendarAgent	22
nsurlsessiond	59

Endpoints (with Filters Applied)

endpoint	count
17.134.127.249	1
17.134.127.250	1
17.134.62.30	1
17.142.169.199	1
17.142.169.200	1

< prev 1 2 3 4 5 next >

< prev 1 2 3 4 5 6 7 8 9 10 next >

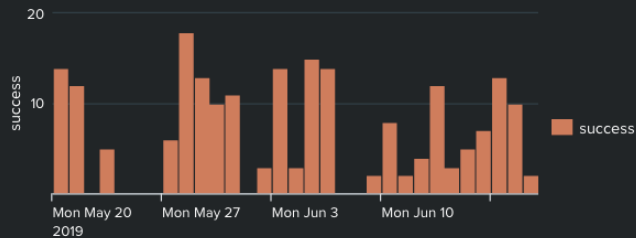
Q ↓ i ↺ 1m ago

Parent/Child Processes (Map Shows up to 250 Connections)

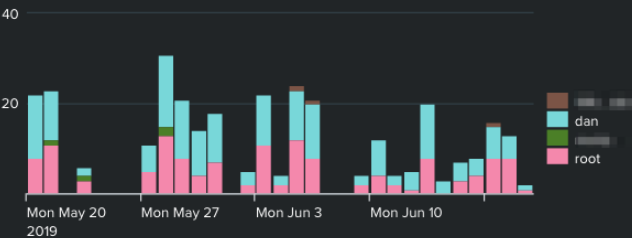


Authentications and Changes

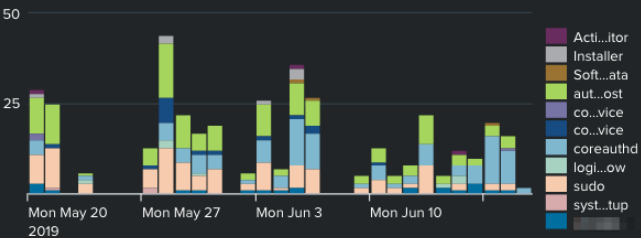
Authentications by Action



Authentications by User



Authentications by App



Asset Authentications

_time ↕	src ↕	dest ↕	action ↕	app ↕	count ↕	user ↕	src_user ↕
2019-06-11 23:44:32	Dan_macbook_pro		success	sudo	370	root	dan
2019-05-20 21:28:16			success	Activity Monitor Installer com.apple.preference.security.remoteservice com.apple.preferences.sharing.remoteservice com.apple.preferences.users.remoteservice coreauthd	252	dan	dan
2019-06-18 22:33:46	Dan_macbook_pro	Dan_macbook_pro	success	sudo	186	root	dan
2019-05-23 23:00:34			success	sudo	160	root	dan
2019-06-12 14:54:12	Dan_macbook_pro		success	Apple Configurator 2 Autoupdate Finder GitHub Desktop Installer com.apple.preferences.configurationprofiles.remoteservice coreauthd lldb-rpc-server storedownload	153	dan	dan

Network Communication Map Filters

Protocol/App Filter

*

Source/Dest. Host Name or IP

17.*

Allowed/Blocked

All

Host Connected to

1 host or more

Select Time Range

Last 24 hours

Applications/Protocols (with Filters Applied)

app	communications
com.apple.CalendarAgent	32
com.apple.cloudsd	16
com.apple.syncdefaults	15
com.apple.imtransferservices.IMTransferAgent	12
com.apple.apsd	11

« prev 1 2 3 4 5 next »

of Destinations Connected to by Source (with Filters Applied)



Dan_macbook_pro

Source and Destination (with Filters Applied)

source&destination	communications
Dan_macbook_pro 17.167.194.149	23
Dan_macbook_pro 17.134.127.249	22
Dan_macbook_pro 17.142.171.9	21

« prev 1 2 3 4 5 6 7 8 9 10 next »

Communications Map (Map Shows up to 250 Connections)



cmdSecurity / TA-cmdReporter
Unwatch 1 Star 1 Fork 1

Code Issues 0 Pull requests 0 Projects 0 Wiki Security Insights Settings

Splunk Technology Add-on for cmdReporter for CIM compliance.
Edit

Manage topics


25 commits 3 branches 0 releases 2 contributors GPL-3.0

Branch: master New pull request Create new file Upload files Find File Clone or download

danCmdsec Merge pull request #2 from skhopkins/master Latest commit 280da34 8 days ago

TA-cmdreporter	Merge pull request #2 from skhopkins/master	8 days ago
.gitignore	Update .gitignore	20 days ago
LICENSE	Initial commit	last month
README.md	Update README.md	last month

README.md


cmd Reporter

cmdReporter Add-on for Splunk Enterprise and Splunk Enterprise Security

Splunk Technology Add-on for cmdReporter for CIM compliance and data normalization.

Special Thanks: Stuart Hopkins
Add-on Version: 0.3

Note: This add-on is still in beta

Use caution when installing this add-on in production environments.



<https://github.com/cmdSecurity/TA-cmdReporter>

Dan Griggs

dan@cmdsec.com

MacAdmins Slack:
#cmdreporter

