hello (again)

Henry Stamerjohann
Apfelwerk GmbH & Co. KG

Twitter: @head_min
Slack: @henry

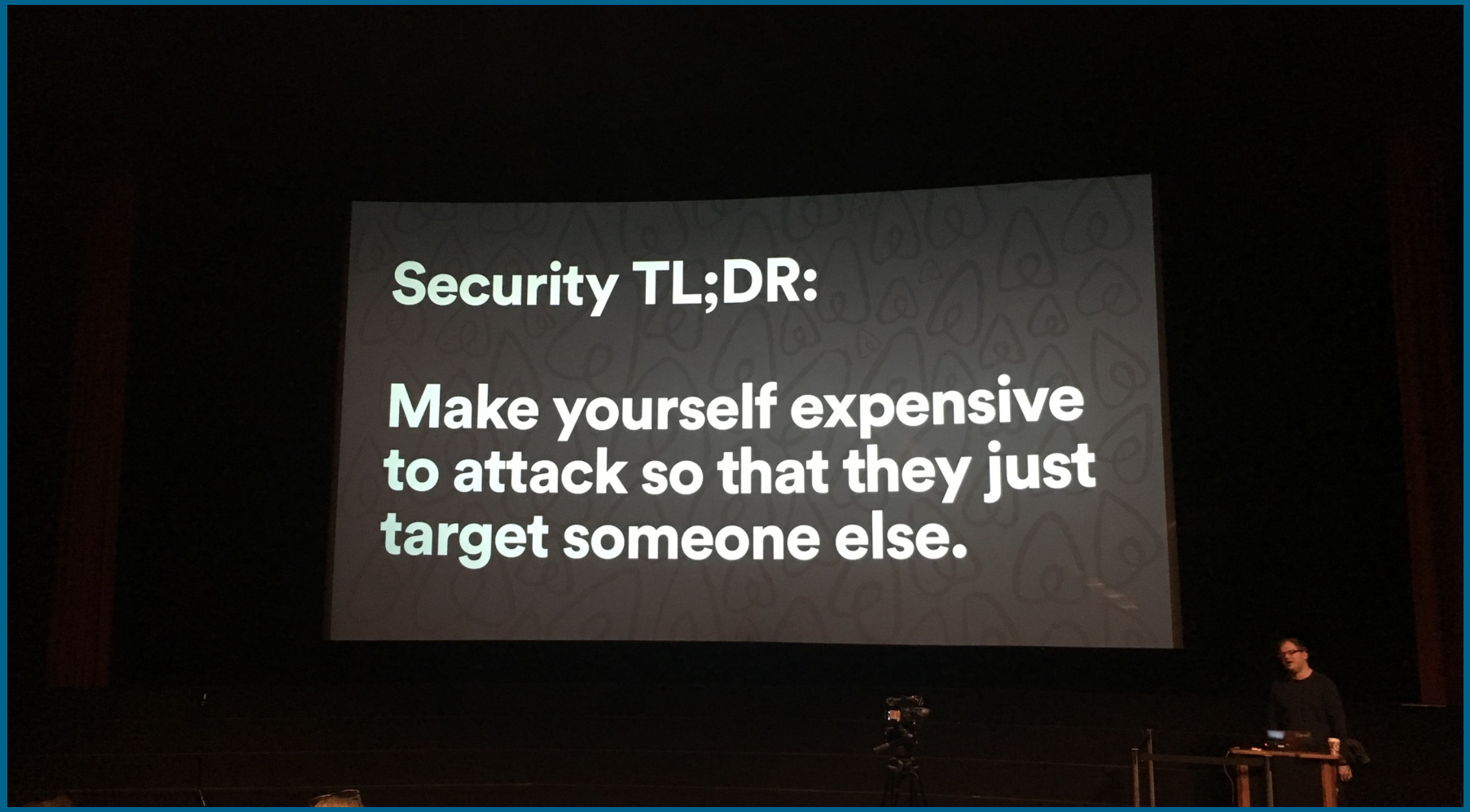
Building your macOS Baseline Requirements

Today

- Wide variety of endpoints in a mobile world
- Mission to secure Hardware / Software configurations
- Continuous Vulnerability Assessment
- We are responsible for data *(GDPR / EU-DSGVO)*

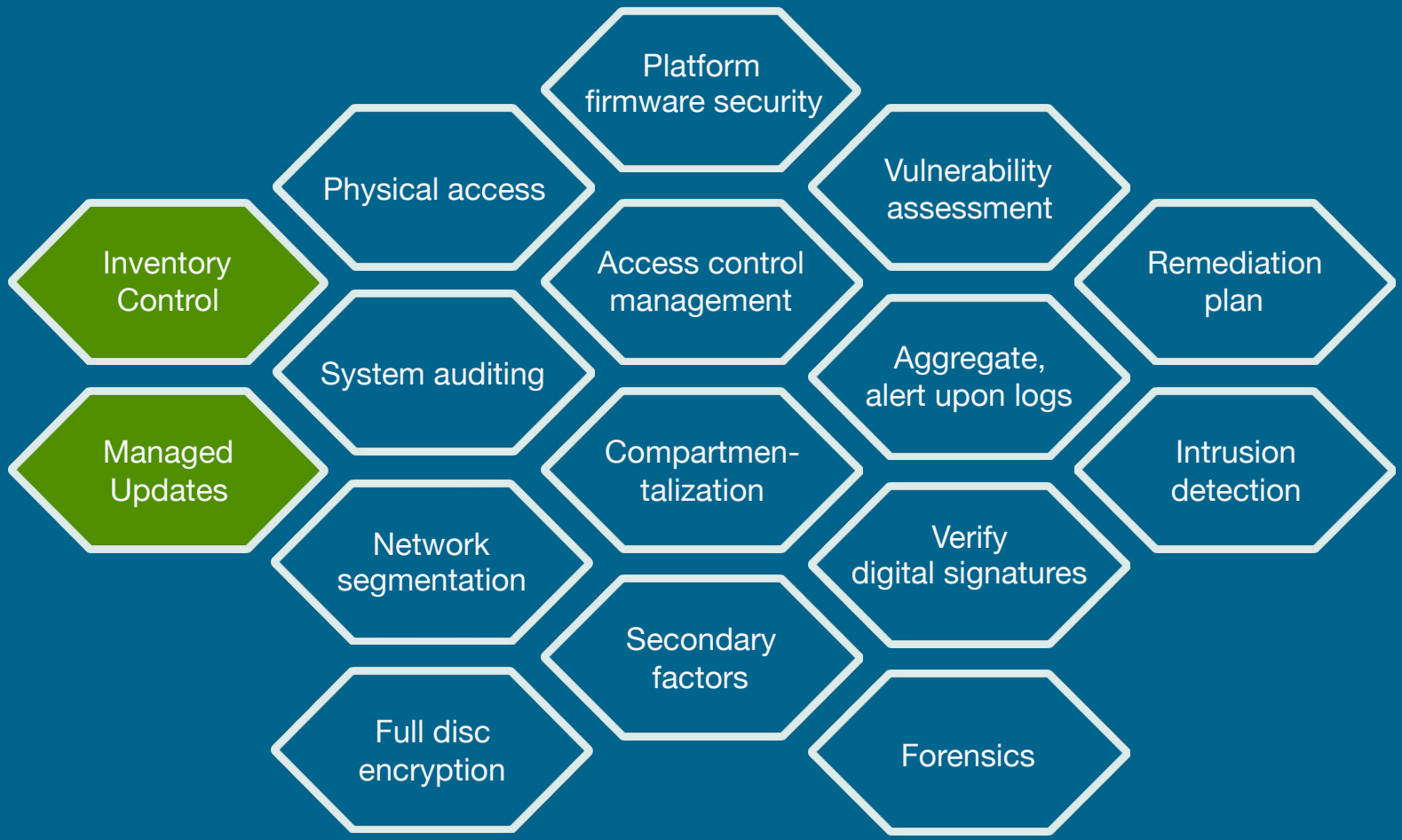
Imagine

- You’re asked to apply a Windows Security guideline to Macs
- You’re questioned how Group Policy Objects (GPOs) can apply to Macs
- You’re glued into looping-discussion how MDM / APNs works
- InfoSec challenges you with: **"Why should we trust 17.0.0.0/8"**

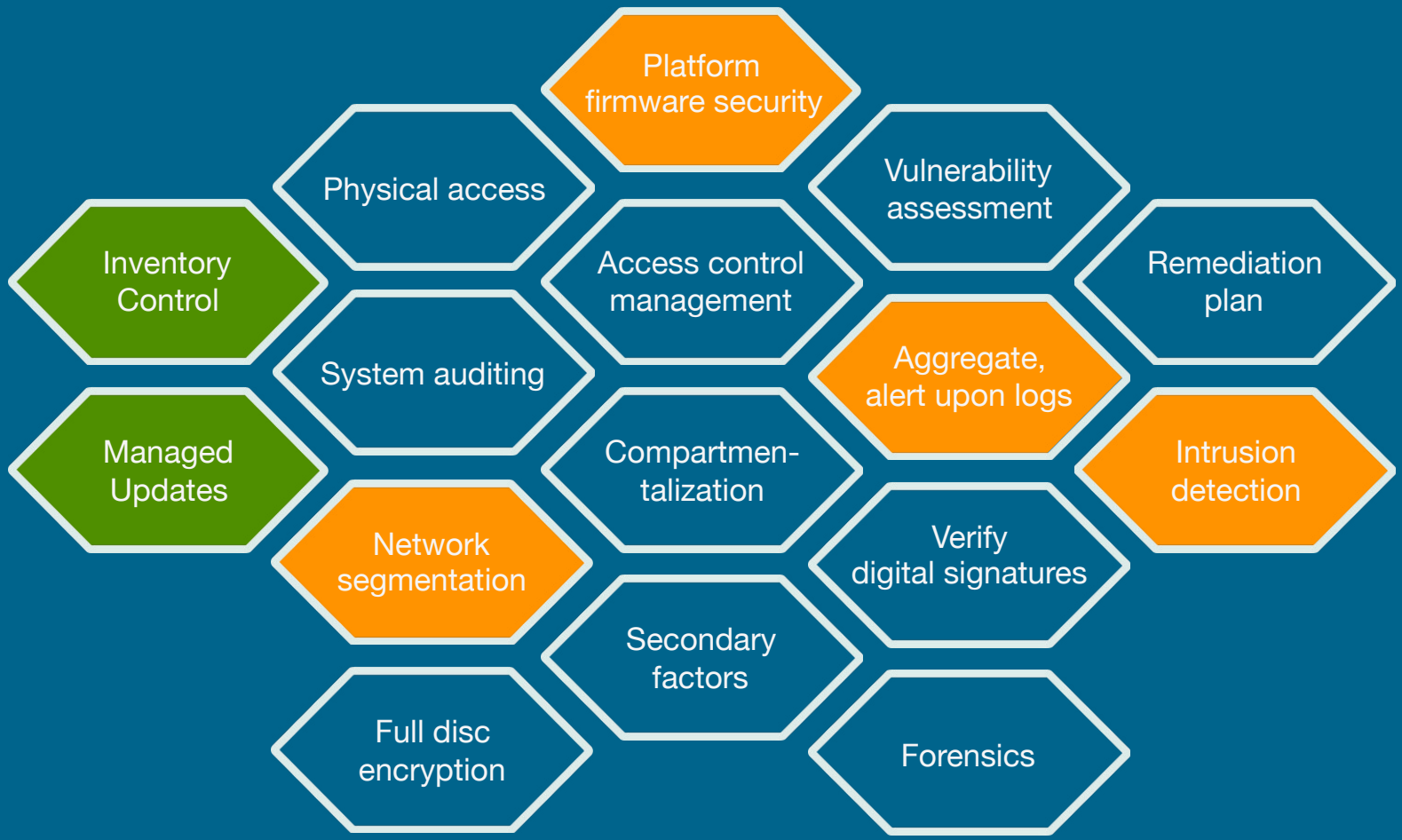

Security TL;DR:
Make yourself expensive to attack so that they just target someone else.

Security Baseline

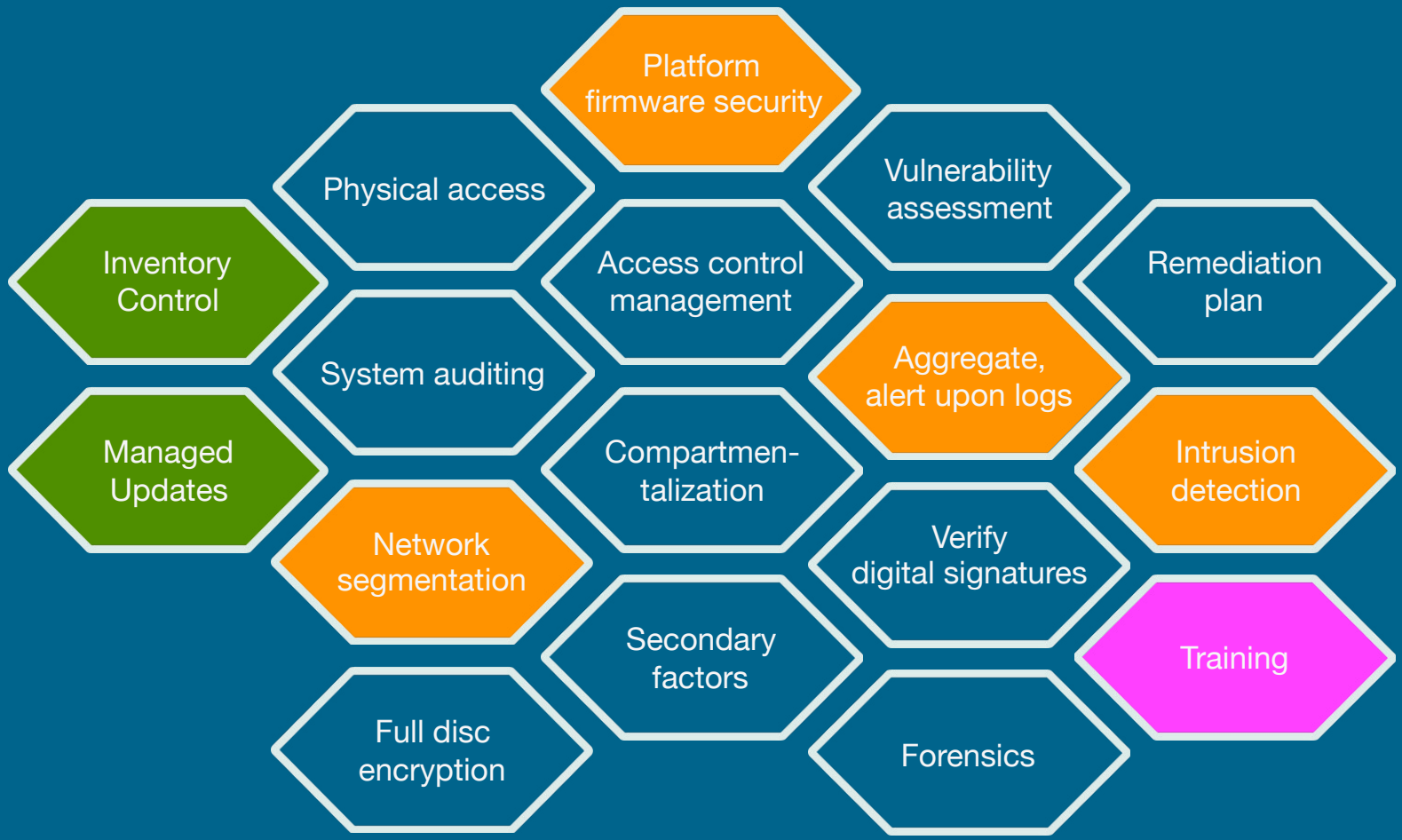
Components


Platform firmware security
Physical access
Vulnerability assessment
Inventory Control
Access control management
Remediation plan
System auditing
Aggregate, alert upon logs
Managed Updates
Compartmen-talization
Intrusion detection
Network segmentation
Verify digital signatures
Secondary factors
Full disc encryption
Forensics

Components


Platform firmware security
Physical access
Vulnerability assessment
Inventory Control
Access control management
Remediation plan
System auditing
Aggregate, alert upon logs
Managed Updates
Compartmen-talization
Intrusion detection
Network segmentation
Verify digital signatures
Secondary factors
Full disc encryption
Forensics

Components


Platform firmware security
Physical access
Vulnerability assessment
Inventory Control
Access control management
Remediation plan
System auditing
Aggregate, alert upon logs
Managed Updates
Compartmen-talization
Intrusion detection
Network segmentation
Verify digital signatures
Secondary factors
Training
Full disc encryption
Forensics

Essentials

- Basic (security) plan for IT systems
- Identify and implement security measures
- Complete for operational environment
- Specific implementation documents

Objectives

- Enforce compliance standards
- Appropriate strategy to address security and end-user productivity
- Include (simple) post-incident templates
- Your security posture

Procedures

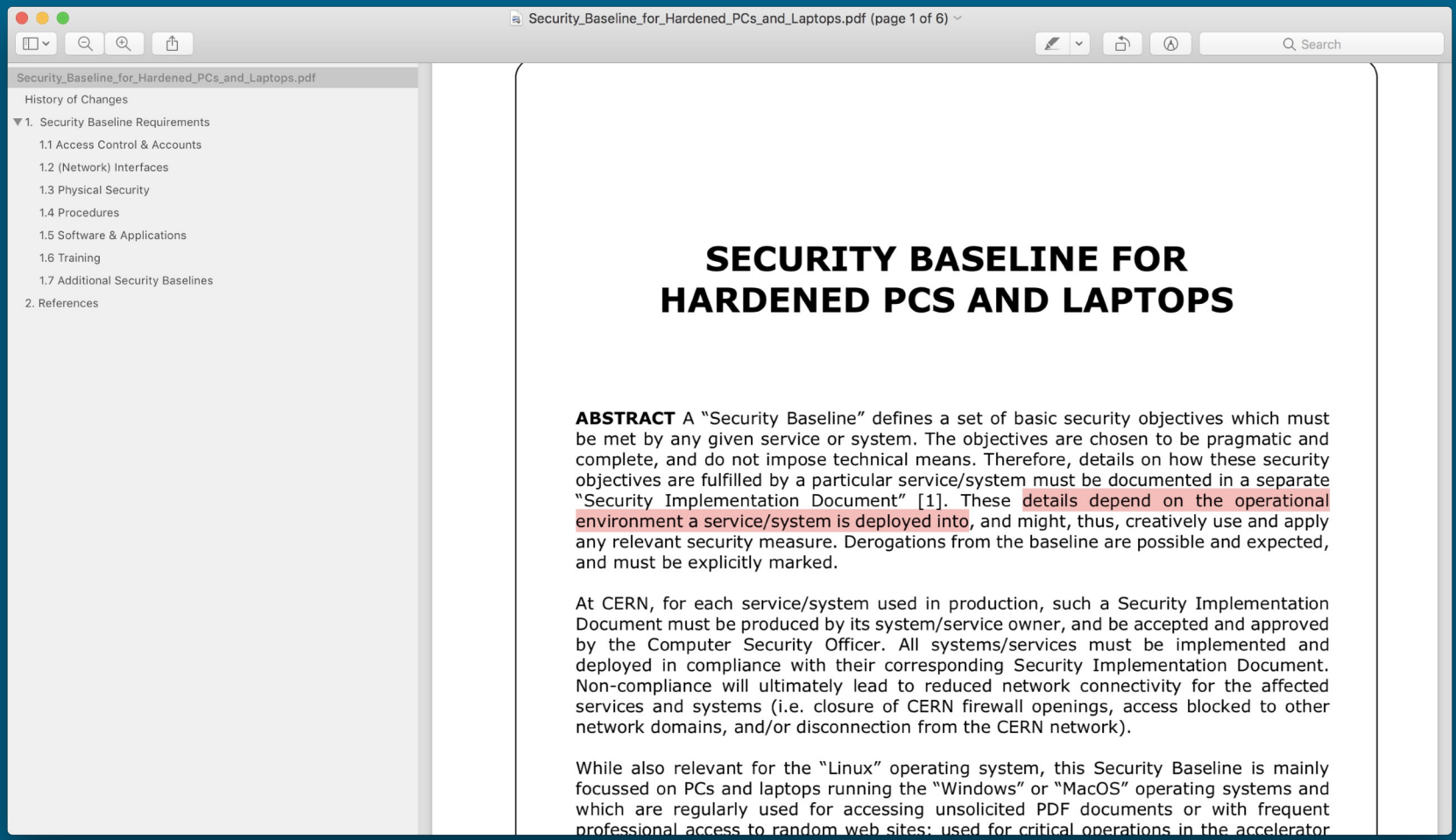
- Patch your systems and software frequently
- Disable services and limit access where possible
- Ensure configuration settings stay compliant
- Close the gaps when detected & keep improving

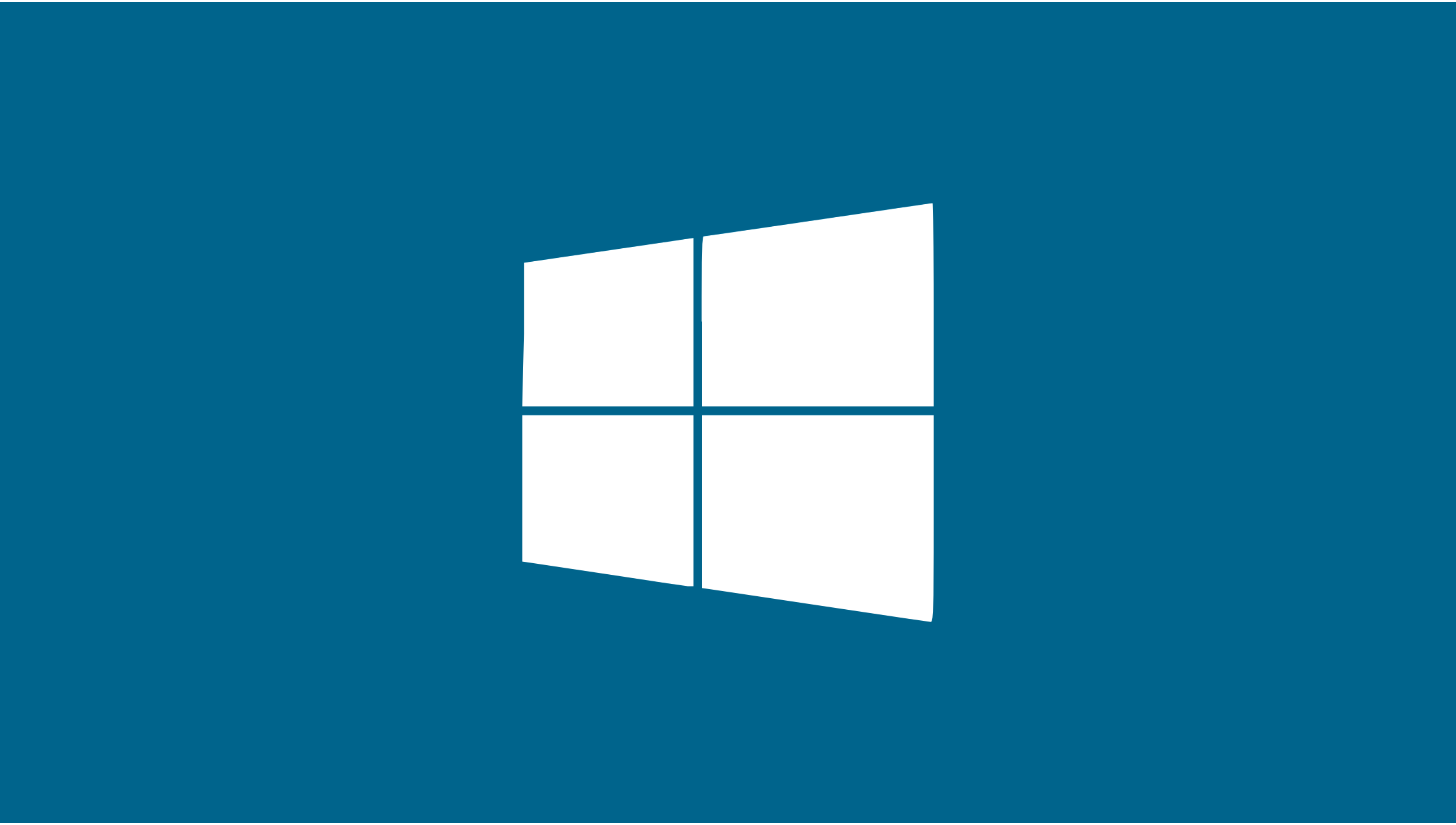
Creating policies too rigid,
you'll be taking the risk to fail !

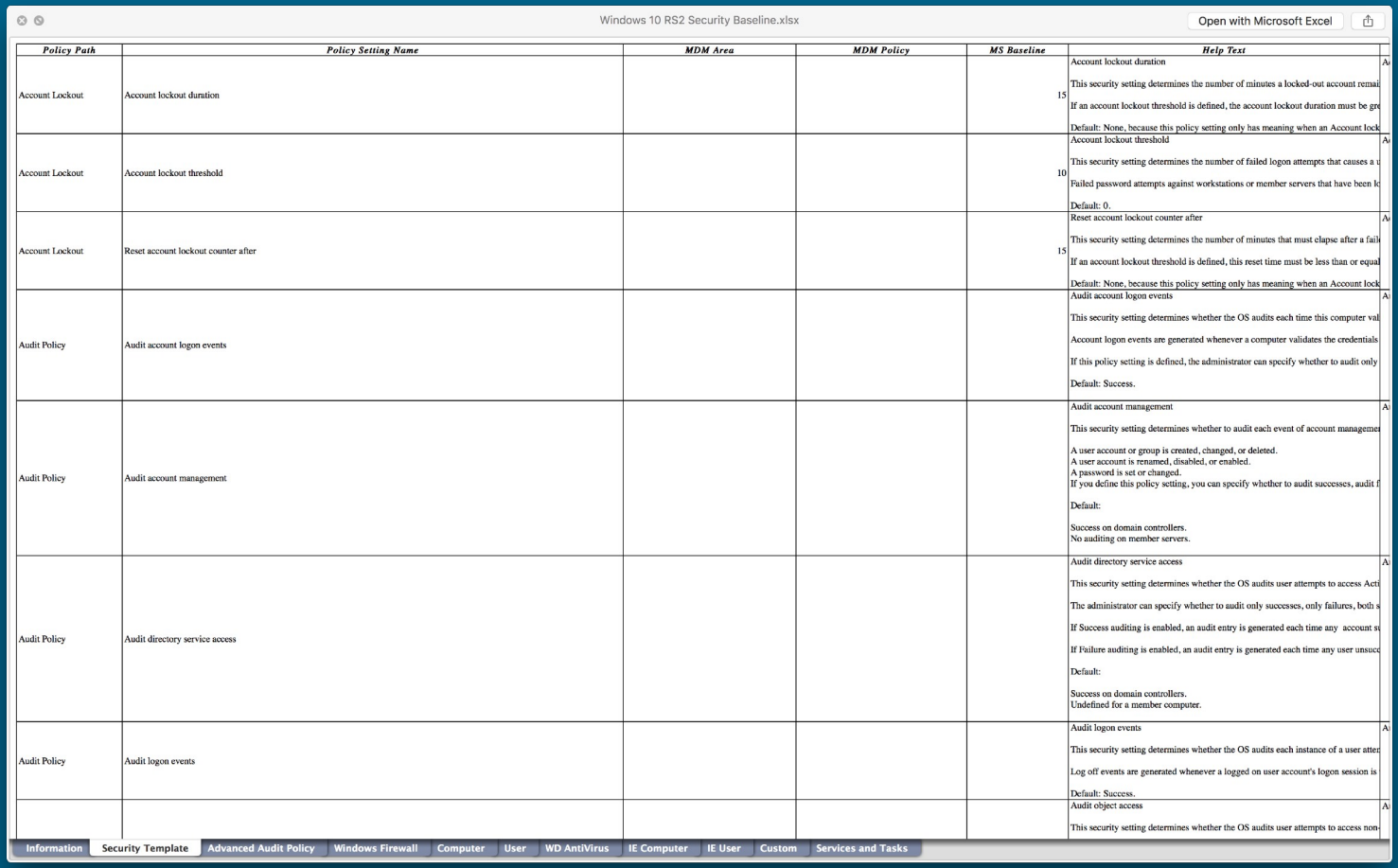
Structure

```
# Baseline Technical Standards Outline

I.      Introduction
II.     Proper base OS install
III.    Modifications to file/directory permissions
IV.     Services to disable
V.      Approved Protocols
VI.     Account Policies
VII.    Password Policies
VIII.   System Auditing


## Source: SANS Institute 2000 - 2002
```

Example: Security Baseline from CERN



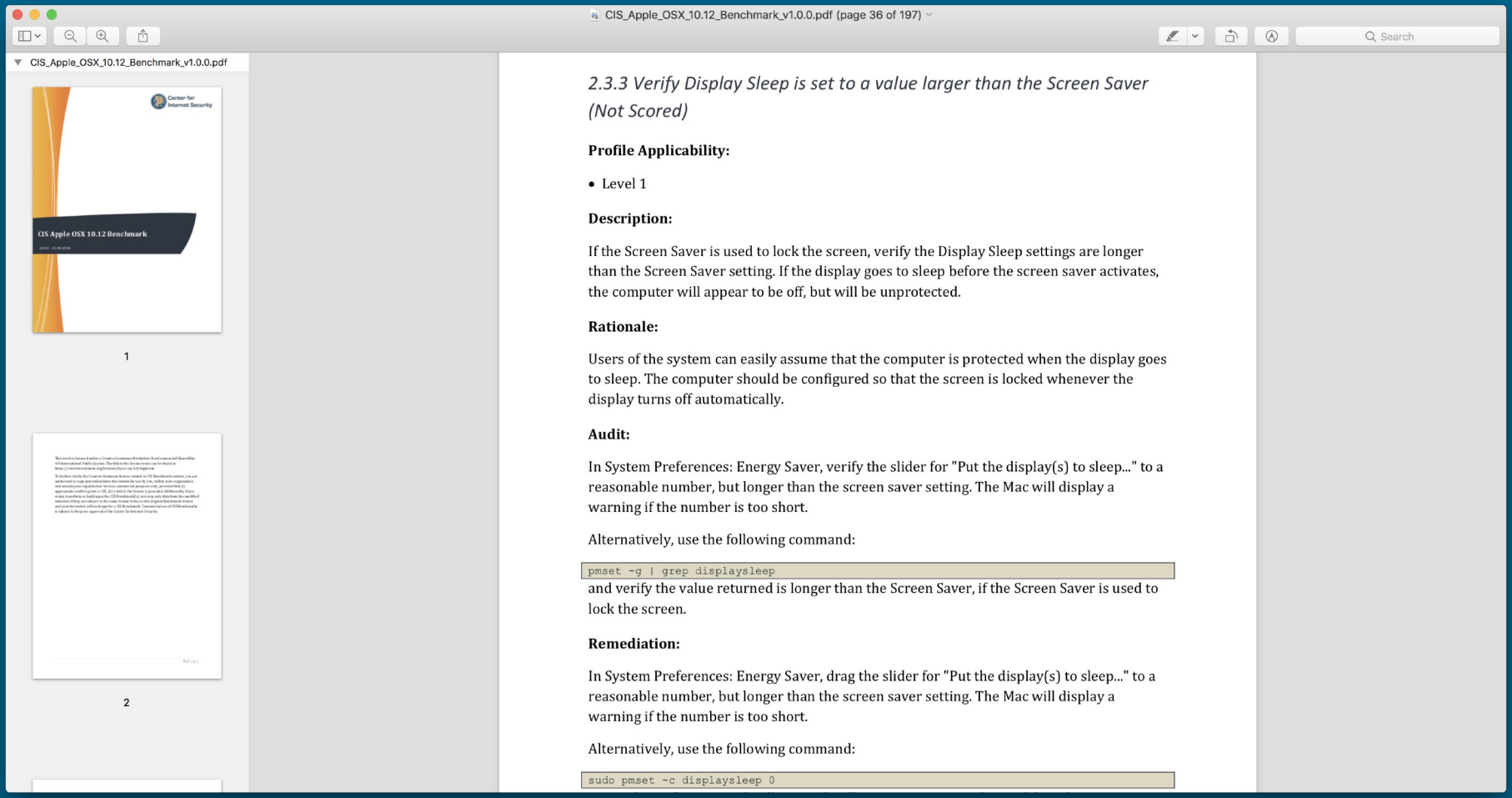




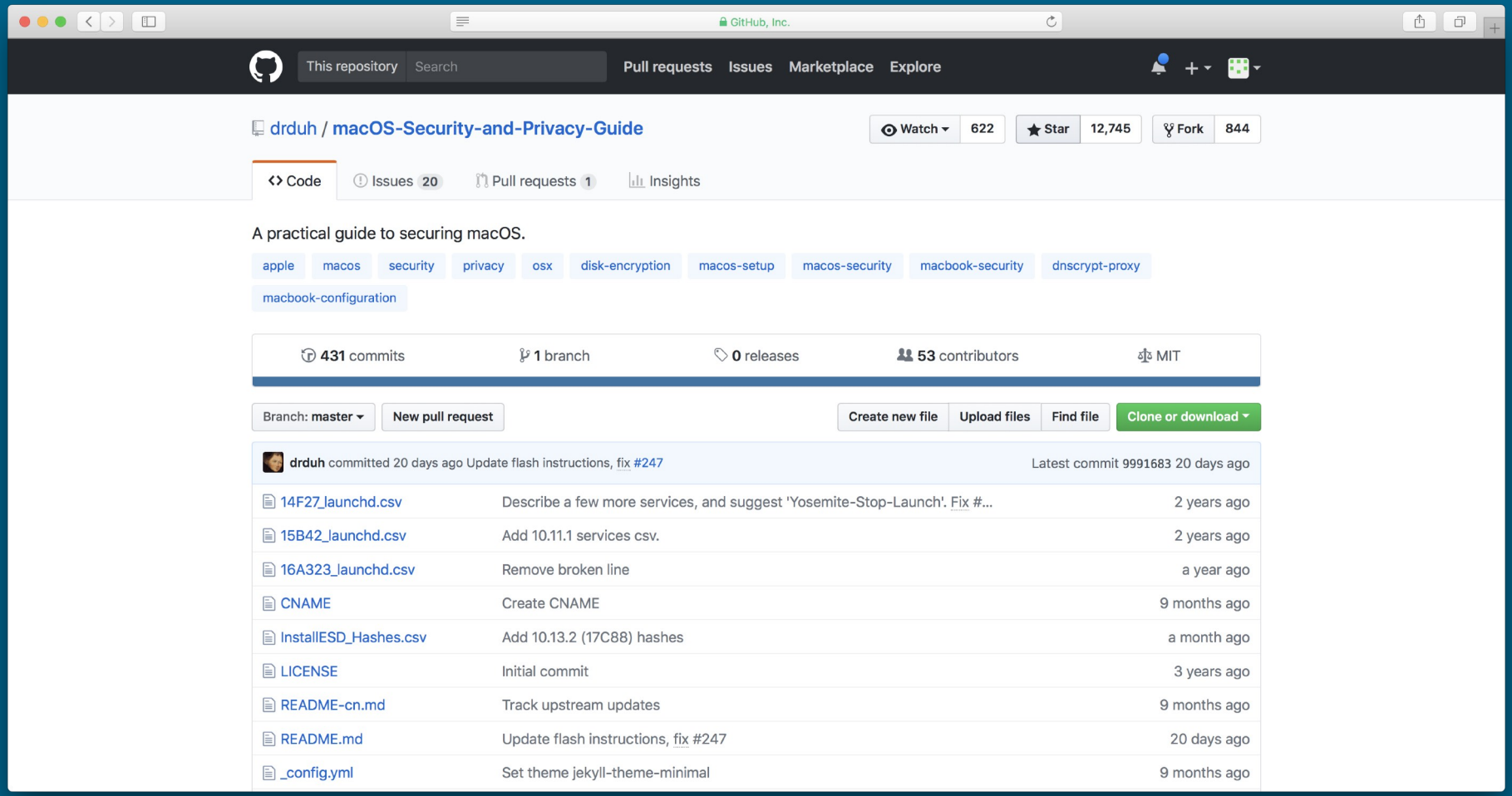
Policy Path	Policy Setting Name	MDM Area	MDM Policy	MS Baseline	Help Text
Account Lockout	Account lockout duration			15	Account lockout duration This security setting determines the number of minutes a locked-out account remai If an account lockout threshold is defined, the account lockout duration must be gr Default: None, because this policy setting only has meaning when an Account lock
Account Lockout	Account lockout threshold			10	Account lockout threshold This security setting determines the number of failed logon attempts that causes a u Failed password attempts against workstations or member servers that have been l Default: 0.
Account Lockout	Reset account lockout counter after			15	Reset account lockout counter after This security setting determines the number of minutes that must elapse after a fail If an account lockout threshold is defined, this reset time must be less than or equal Default: None, because this policy setting only has meaning when an Account lock
Audit Policy	Audit account logon events				Audit account logon events This security setting determines whether the OS audits each time this computer val Account logon events are generated whenever a computer validates the credentials If this policy setting is defined, the administrator can specify whether to audit only Default: Success.
Audit Policy	Audit account management				Audit account management This security setting determines whether to audit each event of account manageme A user account or group is created, changed, or deleted. A user account is renamed, disabled, or enabled. A password is set or changed. If you define this policy setting, you can specify whether to audit successes, audit f Default: Success on domain controllers. No auditing on member servers.
Audit Policy	Audit directory service access				Audit directory service access This security setting determines whether the OS audits user attempts to access Acti The administrator can specify whether to audit only successes, only failures, both s If Success auditing is enabled, an audit entry is generated each time any account s If Failure auditing is enabled, an audit entry is generated each time any user unsucc Default: Success on domain controllers. Undefined for a member computer.
Audit Policy	Audit logon events				Audit logon events This security setting determines whether the OS audits each instance of a user atte Log off events are generated whenever a logged on user account's logon session is Default: Success.
					Audit object access This security setting determines whether the OS audits user attempts to access non-

Microsoft Security Compliance Toolkit

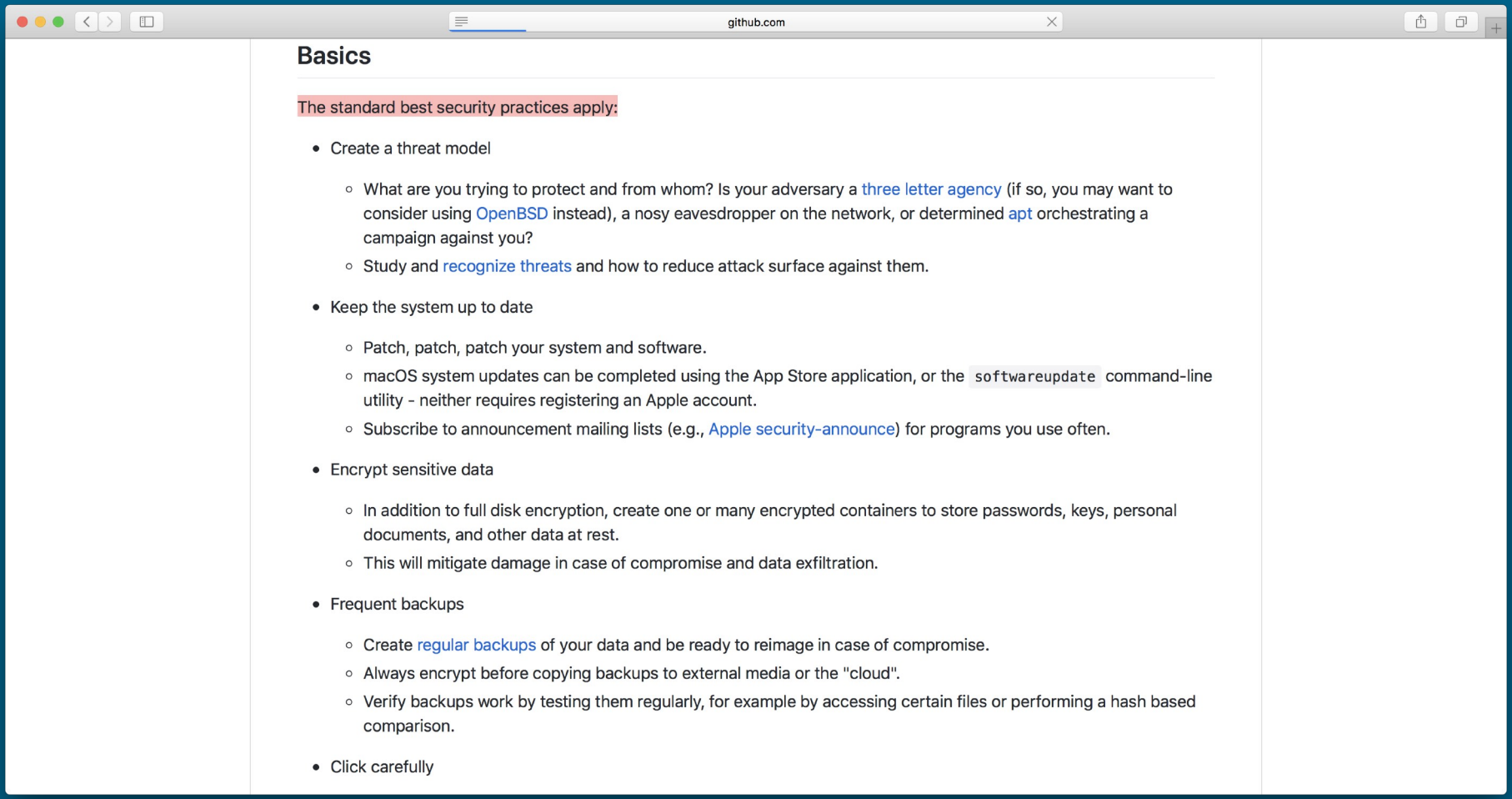
www.cisecurity.org/benchmark/apple_os/



github.com/drduh/macOS-Security-and-Privacy-Guide



github.com/drduh/macOS-Security-and-Privacy-Guide



Basics

The standard best security practices apply:

- Create a threat model
  - What are you trying to protect and from whom? Is your adversary a three letter agency (if so, you may want to consider using OpenBSD instead), a nosy eavesdropper on the network, or determined apt orchestrating a campaign against you?
  - Study and recognize threats and how to reduce attack surface against them.
- Keep the system up to date
  - Patch, patch, patch your system and software.
  - macOS system updates can be completed using the App Store application, or the `softwareupdate` command-line utility - neither requires registering an Apple account.
  - Subscribe to announcement mailing lists (e.g., Apple security-announce) for programs you use often.
- Encrypt sensitive data
  - In addition to full disk encryption, create one or many encrypted containers to store passwords, keys, personal documents, and other data at rest.
  - This will mitigate damage in case of compromise and data exfiltration.
- Frequent backups
  - Create regular backups of your data and be ready to reimage in case of compromise.
  - Always encrypt before copying backups to external media or the "cloud".
  - Verify backups work by testing them regularly, for example by accessing certain files or performing a hash based comparison.
- Click carefully

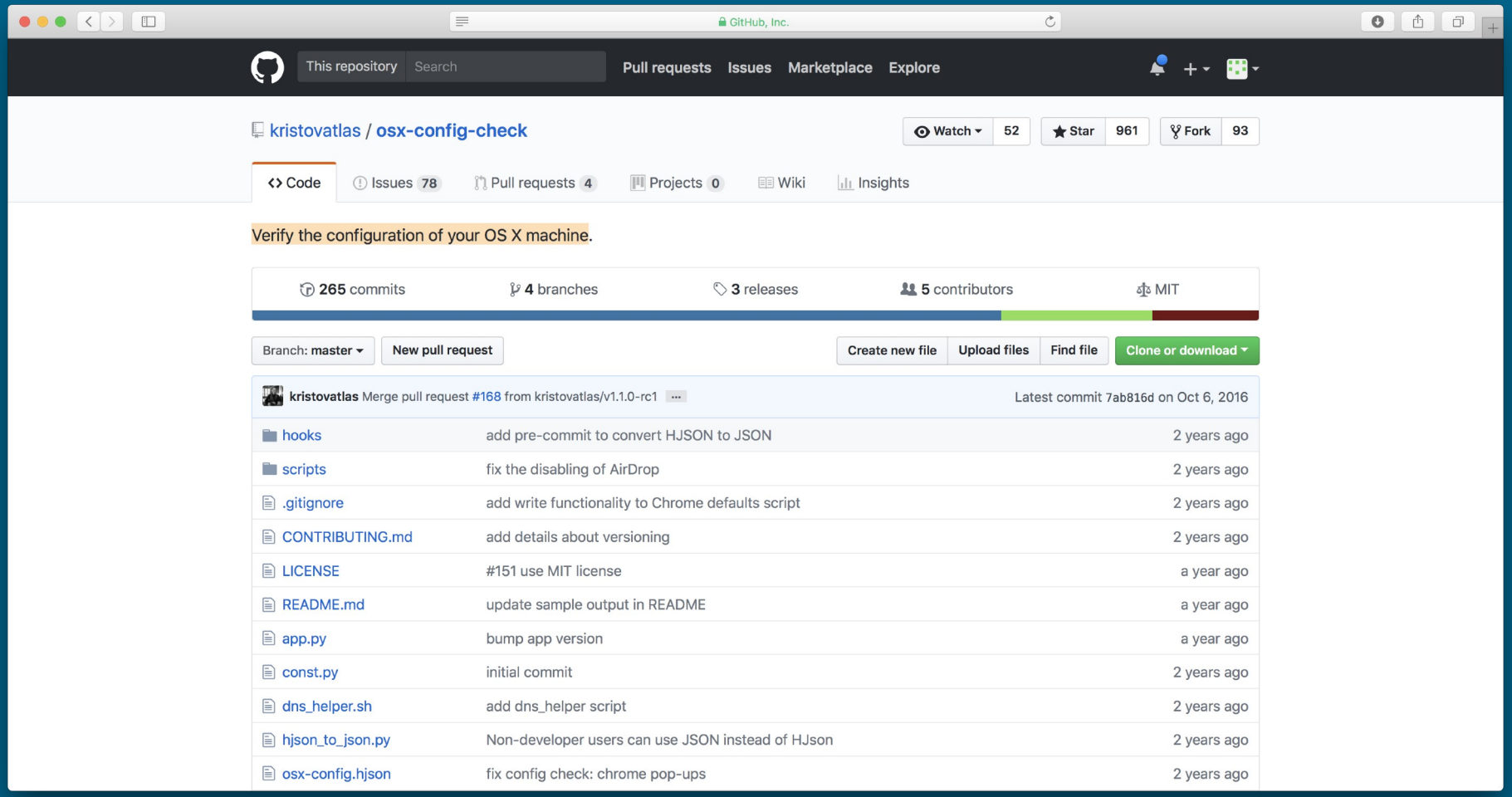
Configuration elements

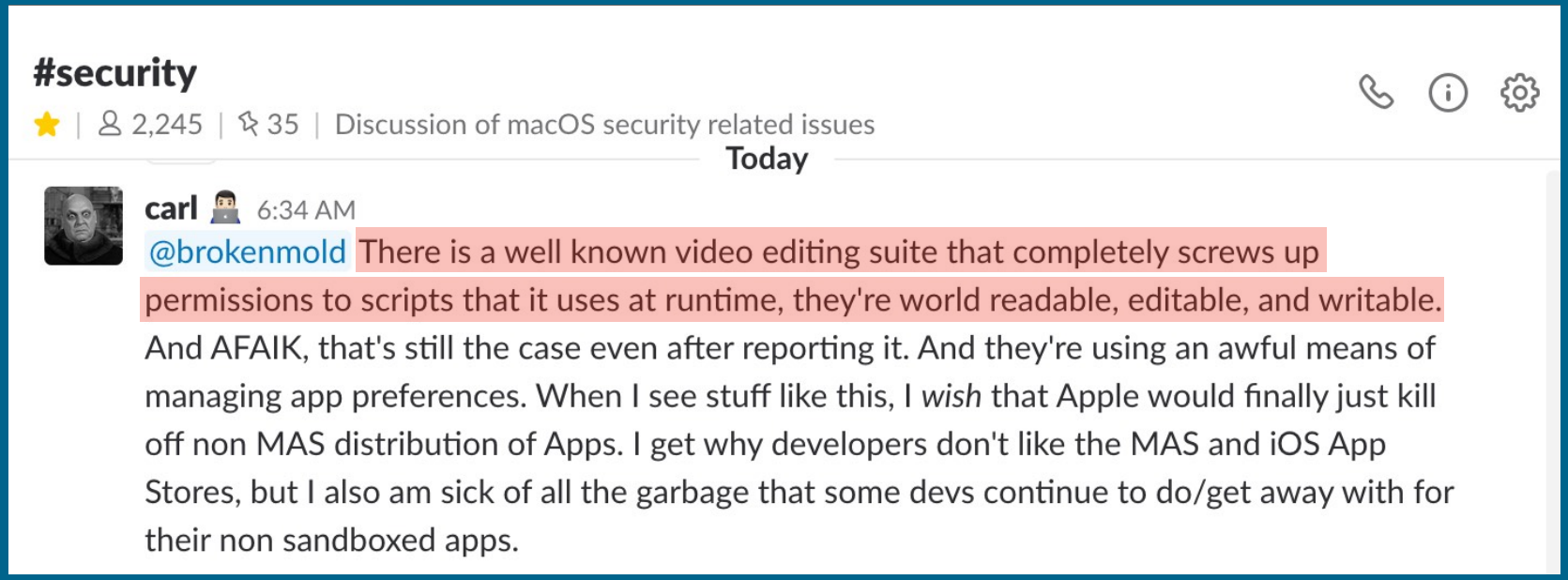
- Config Profiles (MDM, manually deployed)
- Scripts / CLI tools / Software
- Conditionals / Extension Attributes
- MDM commands (wipe/lock)

Control Facilities

- Inventory information, management system
- Scheduled intervals
- Reporting / Dashboards / Logging
- Change Detection, Alerting
- Automation / programmed remediation

github.com/kristovatlas/osx-config-check

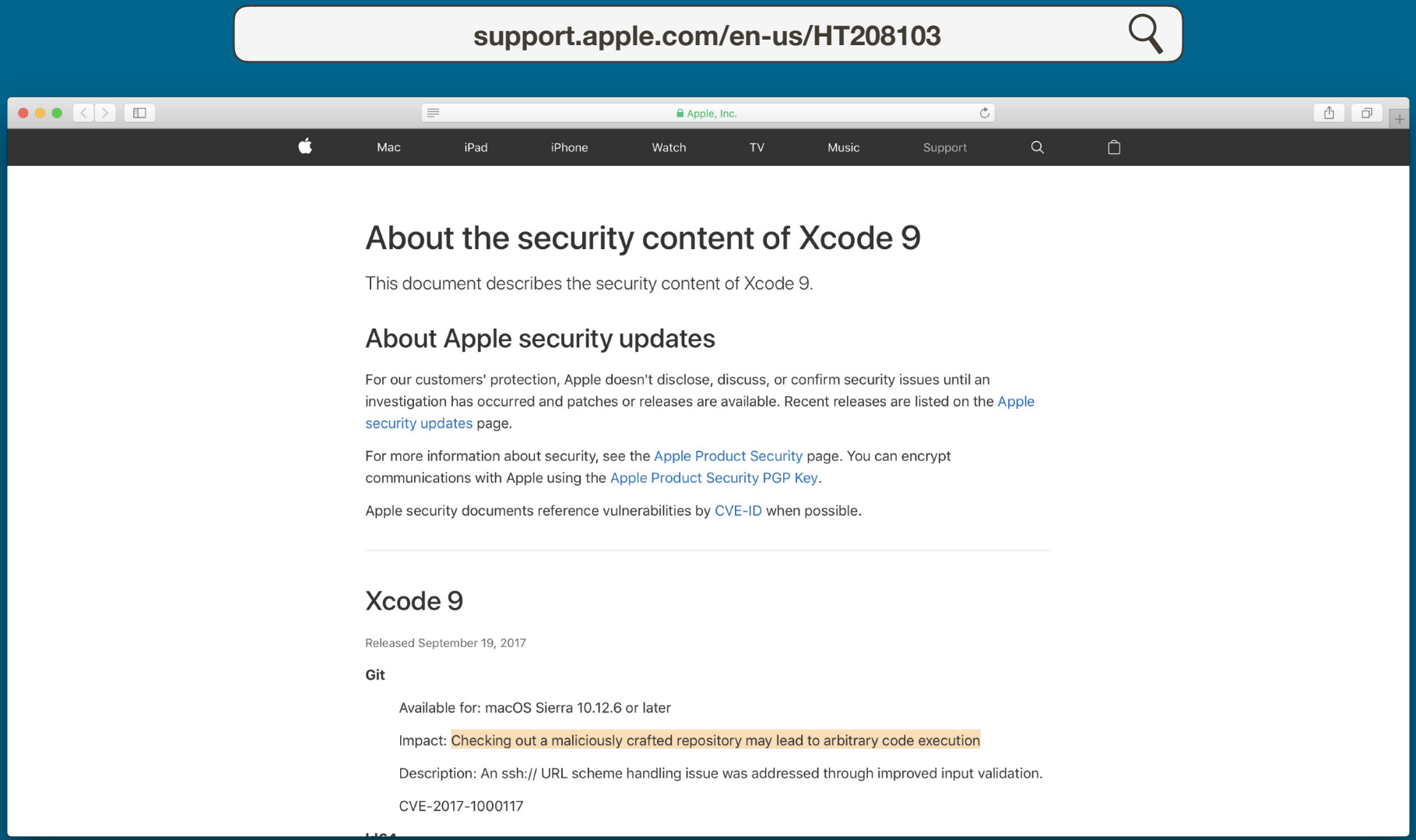



#security
2,245 | 35 | Discussion of macOS security related issues
Today
carl 6:34 AM
@brokenmold There is a well known video editing suite that completely screws up permissions to scripts that it uses at runtime, they're world readable, editable, and writable. And AFAIK, that's still the case even after reporting it. And they're using an awful means of managing app preferences. When I see stuff like this, I *wish* that Apple would finally just kill off non MAS distribution of Apps. I get why developers don't like the MAS and iOS App Stores, but I also am sick of all the garbage that some devs continue to do/get away with for their non sandboxed apps.

Executable Bingo!

How many binaries and scripts inside?

App	Binaries	Scripts
Firefox.app	**8**	**-**
Google Chrome.app	**12**	**6** (bash)
Atom.app	**30**	**144** (bash, python, node,..)
Xcode.app	**1224**	**270** (bash, python, perl, node,..)

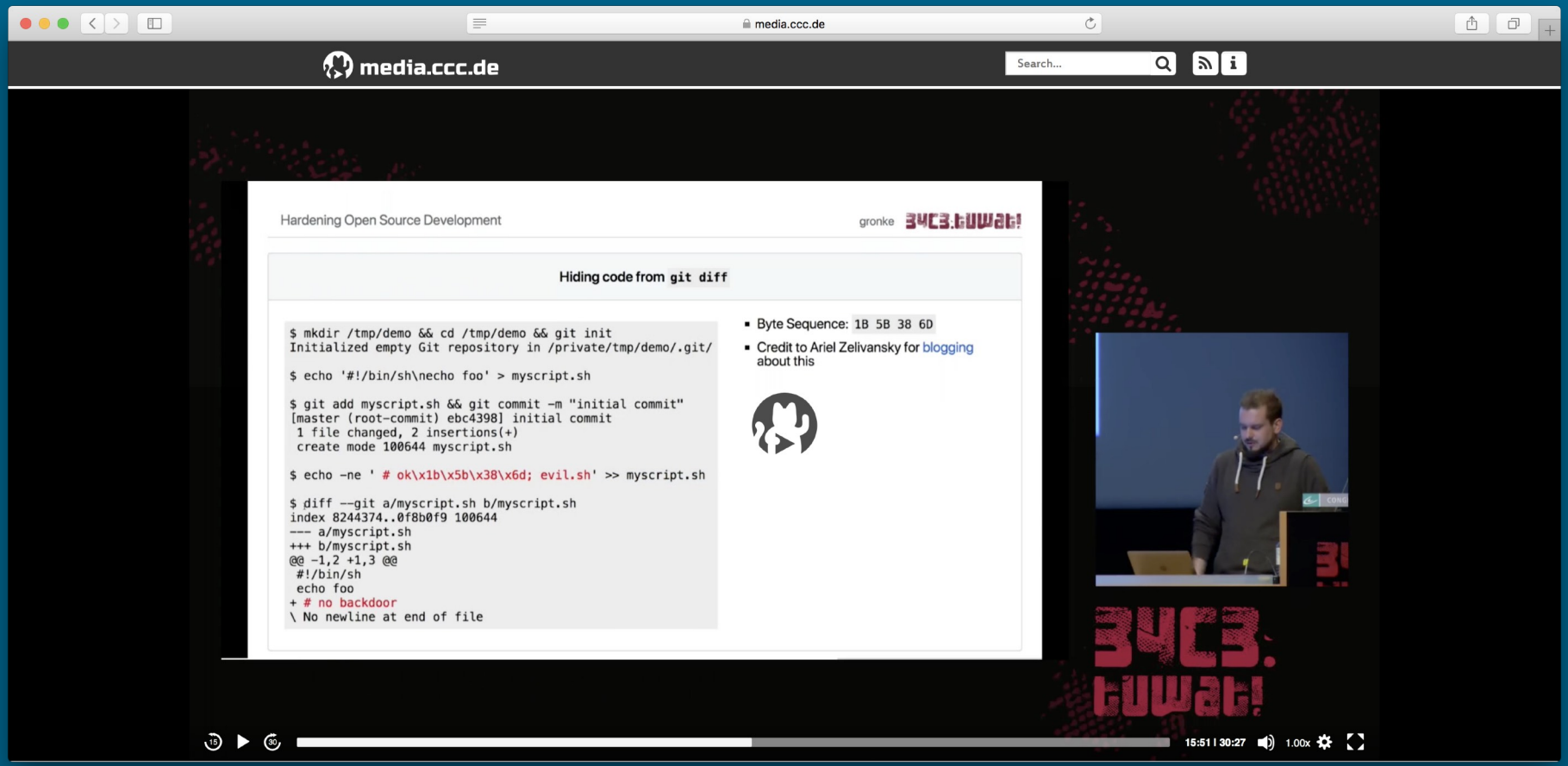

support.apple.com/en-us/HT208103
Apple, Inc.
Mac
iPad
iPhone
Watch
TV
Music
Support
About the security content of Xcode 9
This document describes the security content of Xcode 9.
About Apple security updates
For our customers' protection, Apple doesn't disclose, discuss, or confirm security issues until an investigation has occurred and patches or releases are available. Recent releases are listed on the Apple security updates page.
For more information about security, see the Apple Product Security page. You can encrypt communications with Apple using the Apple Product Security PGP Key.
Apple security documents reference vulnerabilities by CVE-ID when possible.
Xcode 9
Released September 19, 2017
Git
Available for: macOS Sierra 10.12.6 or later
Impact: Checking out a maliciously crafted repository may lead to arbitrary code execution
Description: An ssh:// URL scheme handling issue was addressed through improved input validation.
CVE-2017-1000117

Repercussions

Acknowledge risk of executing malicious binaries

Developers could blindly insert "bad code" or "backdoor mechanism", etc.

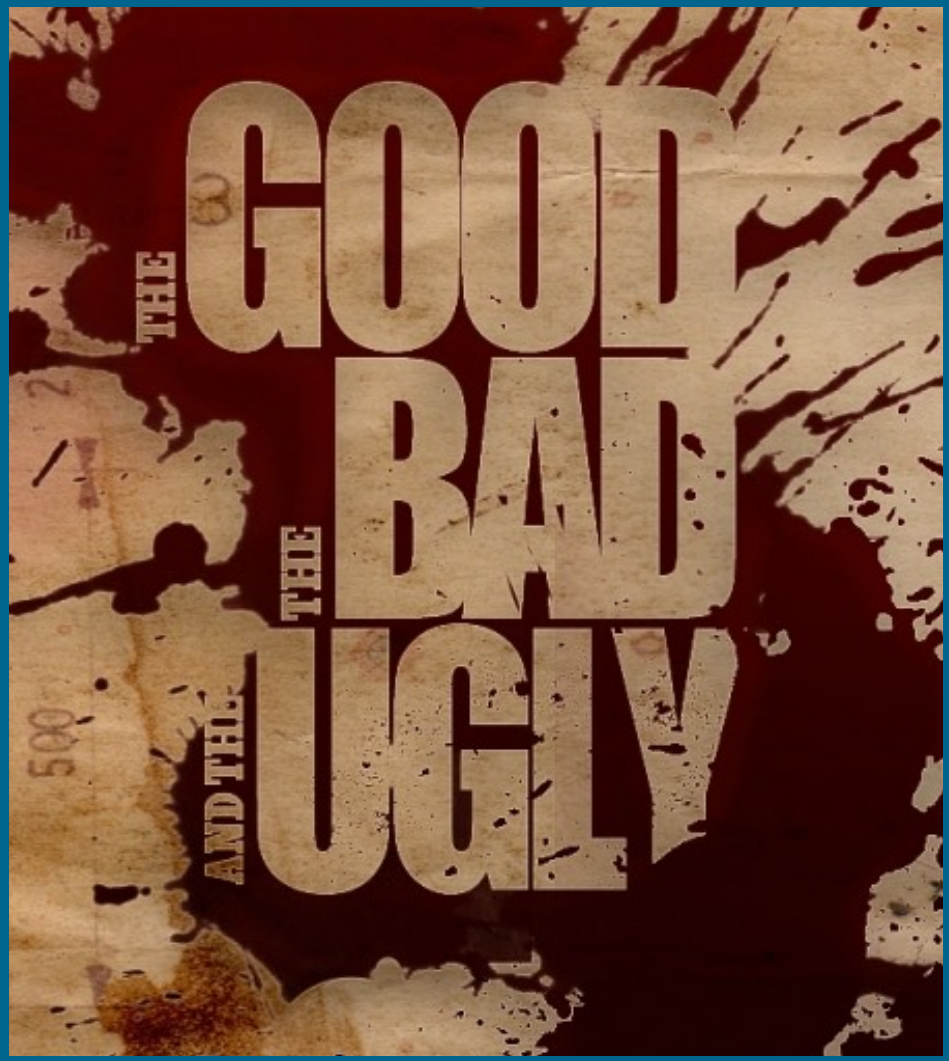
media.ccc.de/v/34c3-9249-hardening_open_source_development



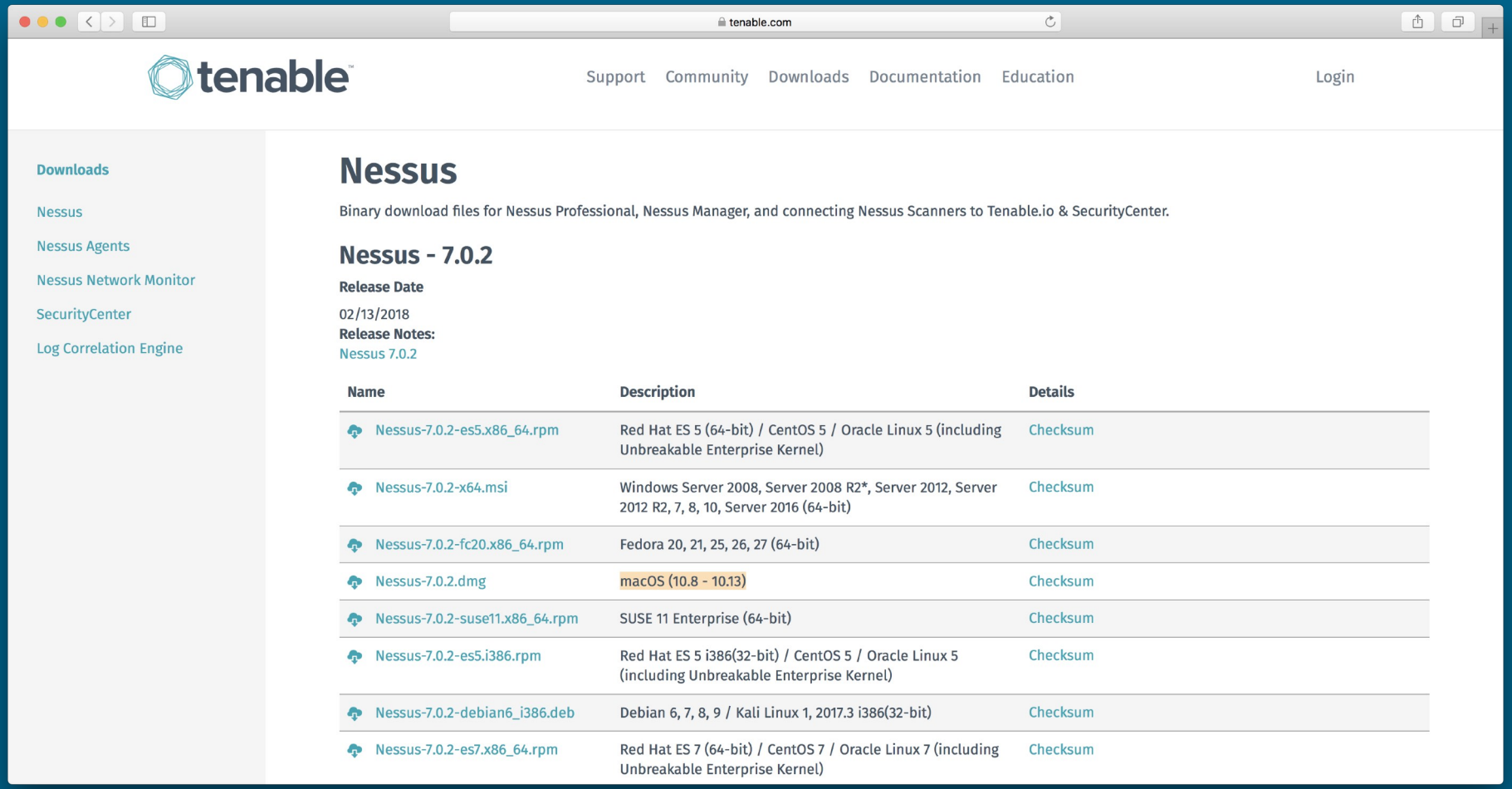
34C3

Devs …what can go wrong ?

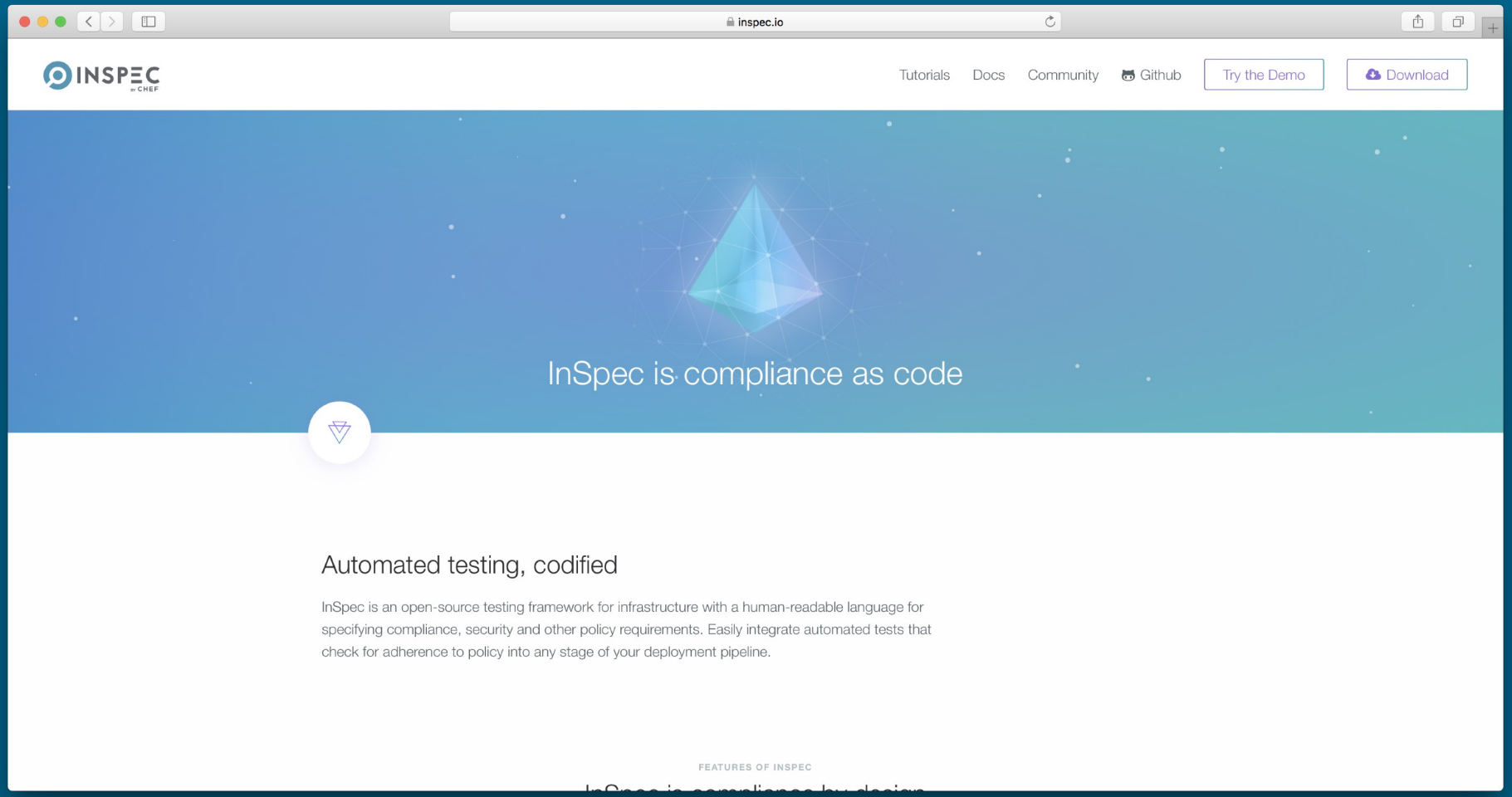
- Flaws in development toolchains
- Risk of code execution
  - Package managers (npm, hombrew)
  - Code or build scripts compromised
  - Hiding code from git diff (UTF-8 Character spoofing)
  - ASCII control characters copy/paste compromised

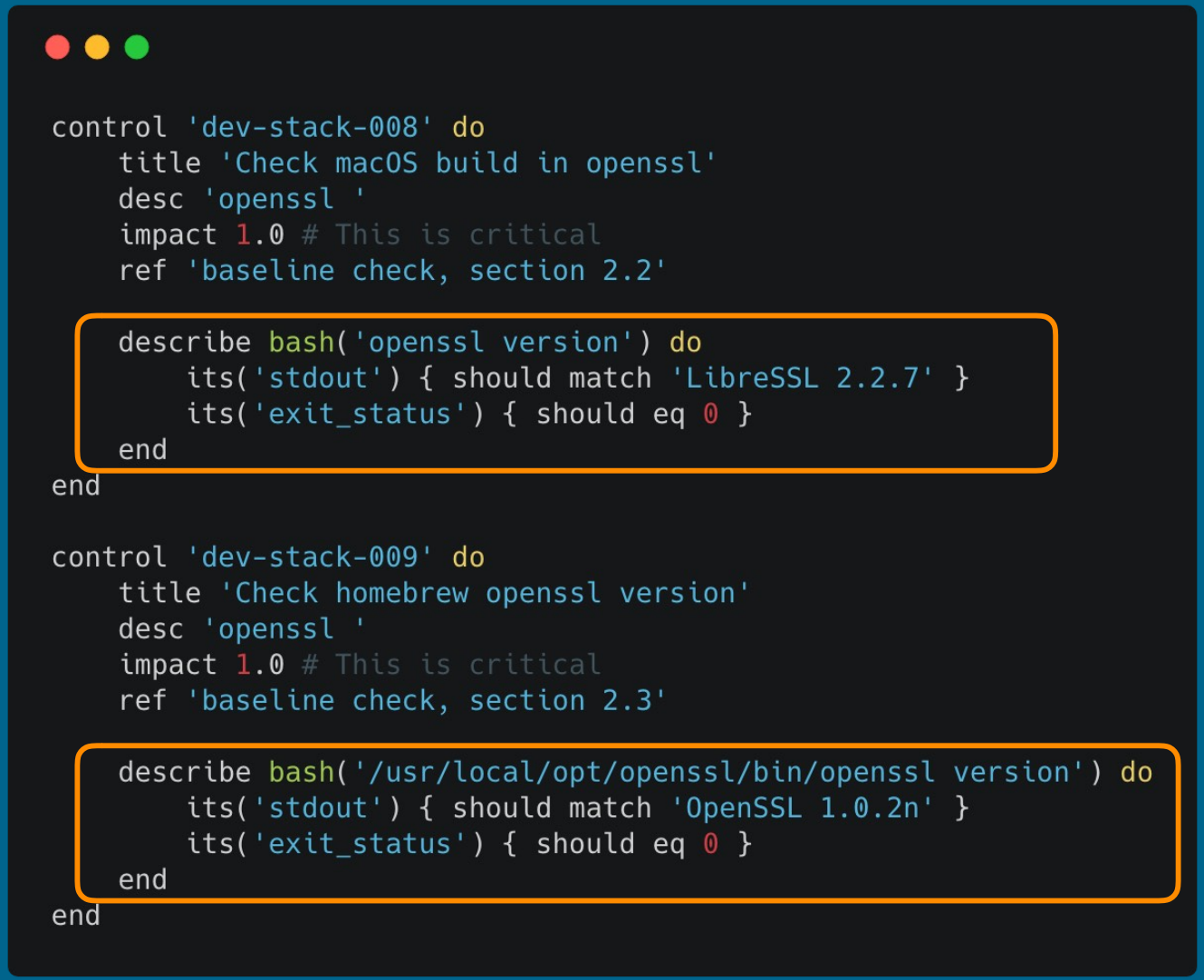

THE GOOD
THE BAD
AND THE UGLY

www.tenable.com/products/nessus/nessus-professional

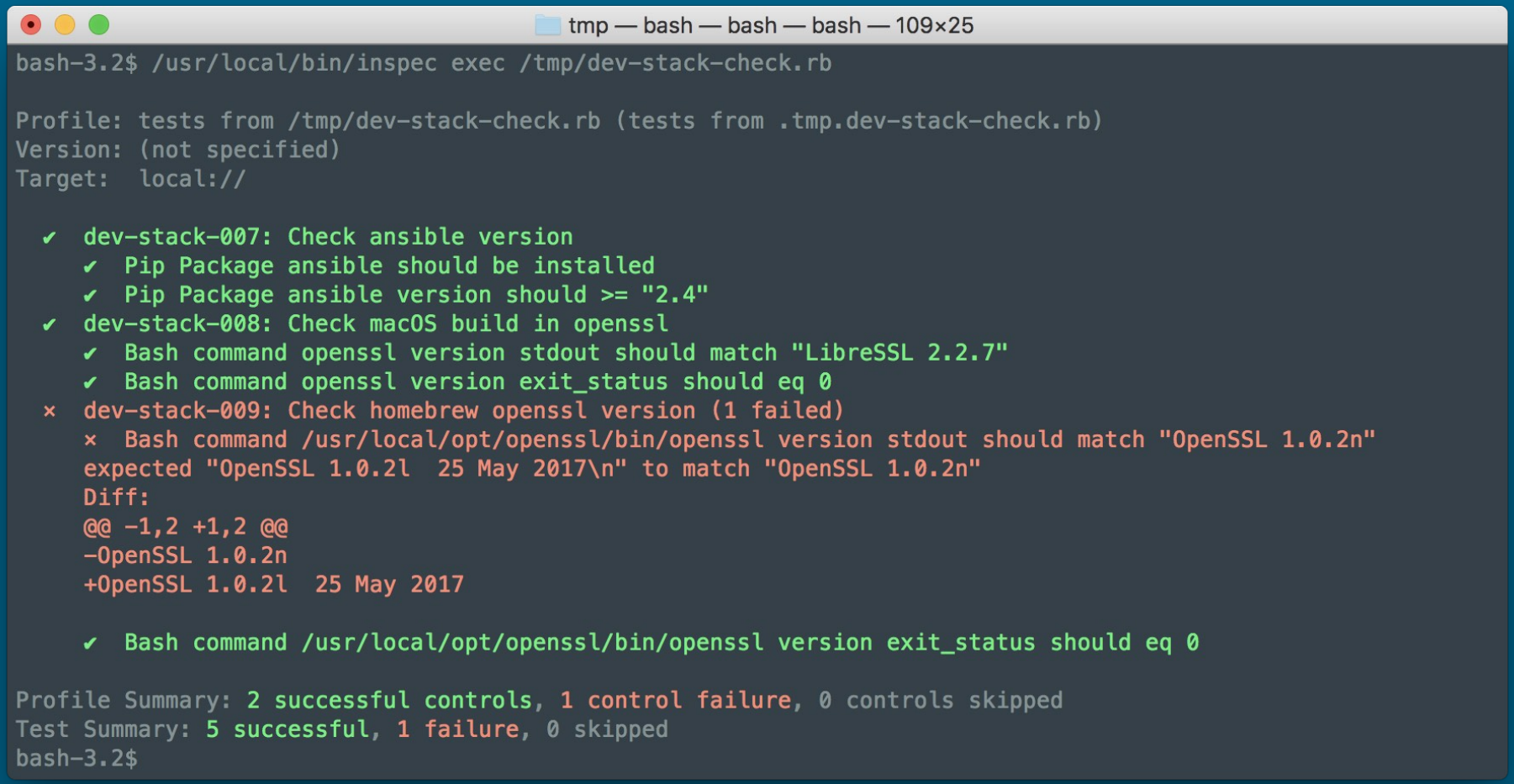


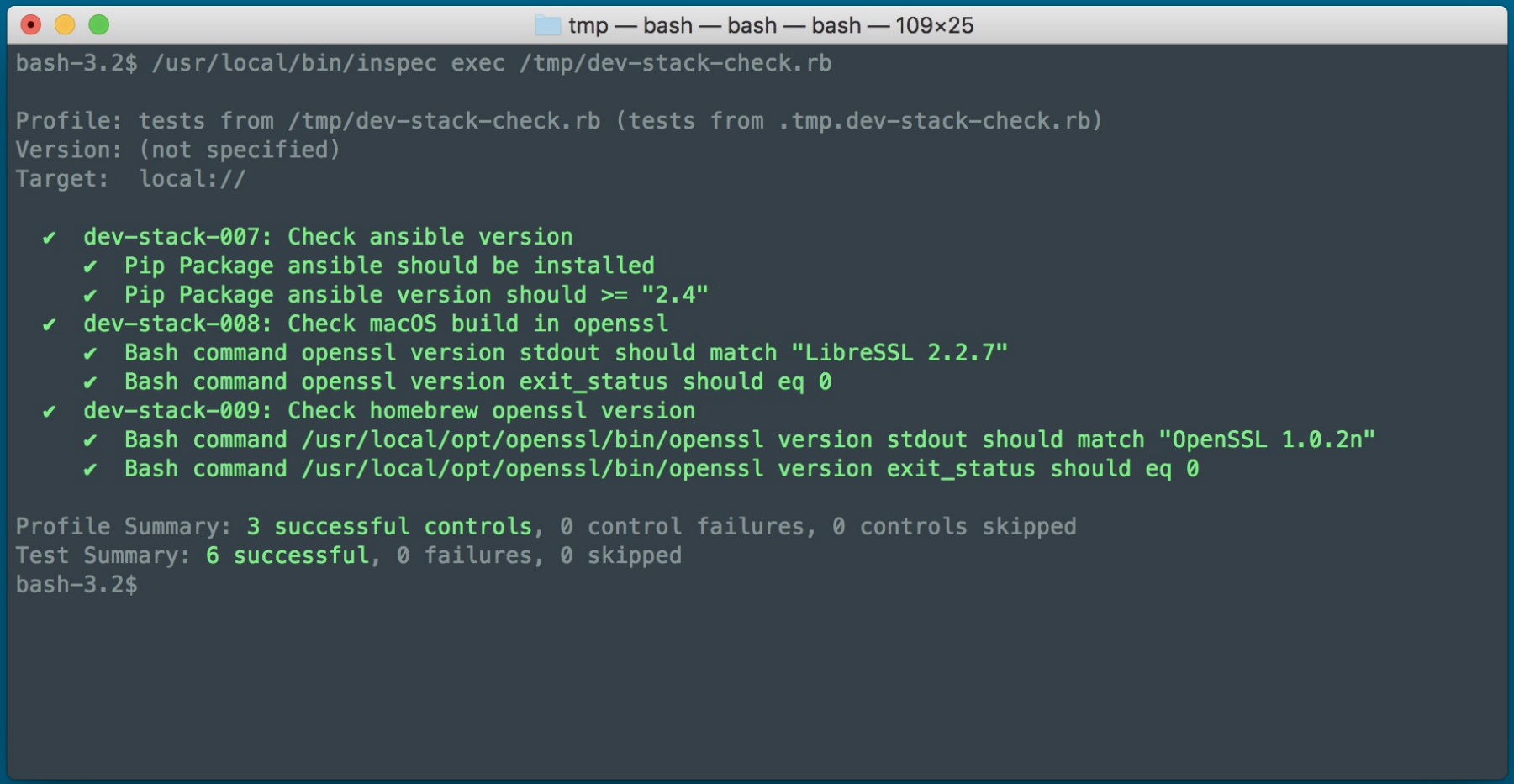
https://www.inspec.io



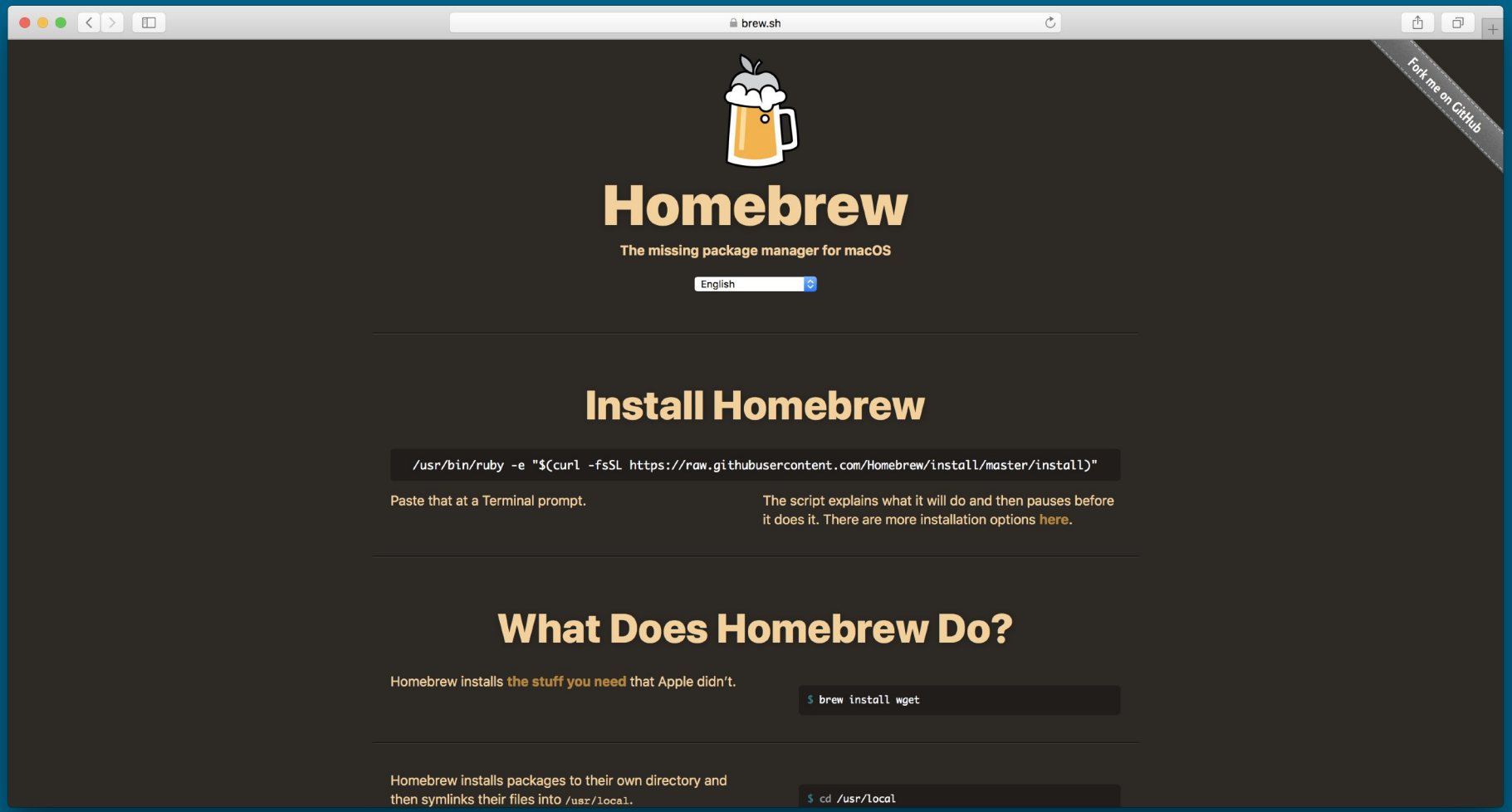


```
control 'dev-stack-008' do
    title 'Check macOS build in openssl'
    desc 'openssl '
    impact 1.0 # This is critical
    ref 'baseline check, section 2.2'

    describe bash('openssl version') do
        its('stdout') { should match 'LibreSSL 2.2.7' }
        its('exit_status') { should eq 0 }
    end
end

control 'dev-stack-009' do
    title 'Check homebrew openssl version'
    desc 'openssl '
    impact 1.0 # This is critical
    ref 'baseline check, section 2.3'

    describe bash('/usr/local/opt/openssl/bin/openssl version') do
        its('stdout') { should match 'OpenSSL 1.0.2n' }
        its('exit_status') { should eq 0 }
    end
end
```


tmp — bash — bash — bash — 109×25
bash-3.2$ /usr/local/bin/inspec exec /tmp/dev-stack-check.rb
Profile: tests from /tmp/dev-stack-check.rb (tests from .tmp.dev-stack-check.rb)
Version: (not specified)
Target: local://
✔ dev-stack-007: Check ansible version
✔ Pip Package ansible should be installed
✔ Pip Package ansible version should >= "2.4"
✔ dev-stack-008: Check macOS build in openssl
✔ Bash command openssl version stdout should match "LibreSSL 2.2.7"
✔ Bash command openssl version exit_status should eq 0
× dev-stack-009: Check homebrew openssl version (1 failed)
× Bash command /usr/local/opt/openssl/bin/openssl version stdout should match "OpenSSL 1.0.2n"
expected "OpenSSL 1.0.2l 25 May 2017\n" to match "OpenSSL 1.0.2n"
Diff:
@@ -1,2 +1,2 @@
-OpenSSL 1.0.2n
+OpenSSL 1.0.2l 25 May 2017
✔ Bash command /usr/local/opt/openssl/bin/openssl version exit_status should eq 0
Profile Summary: 2 successful controls, 1 control failure, 0 controls skipped
Test Summary: 5 successful, 1 failure, 0 skipped
bash-3.2$

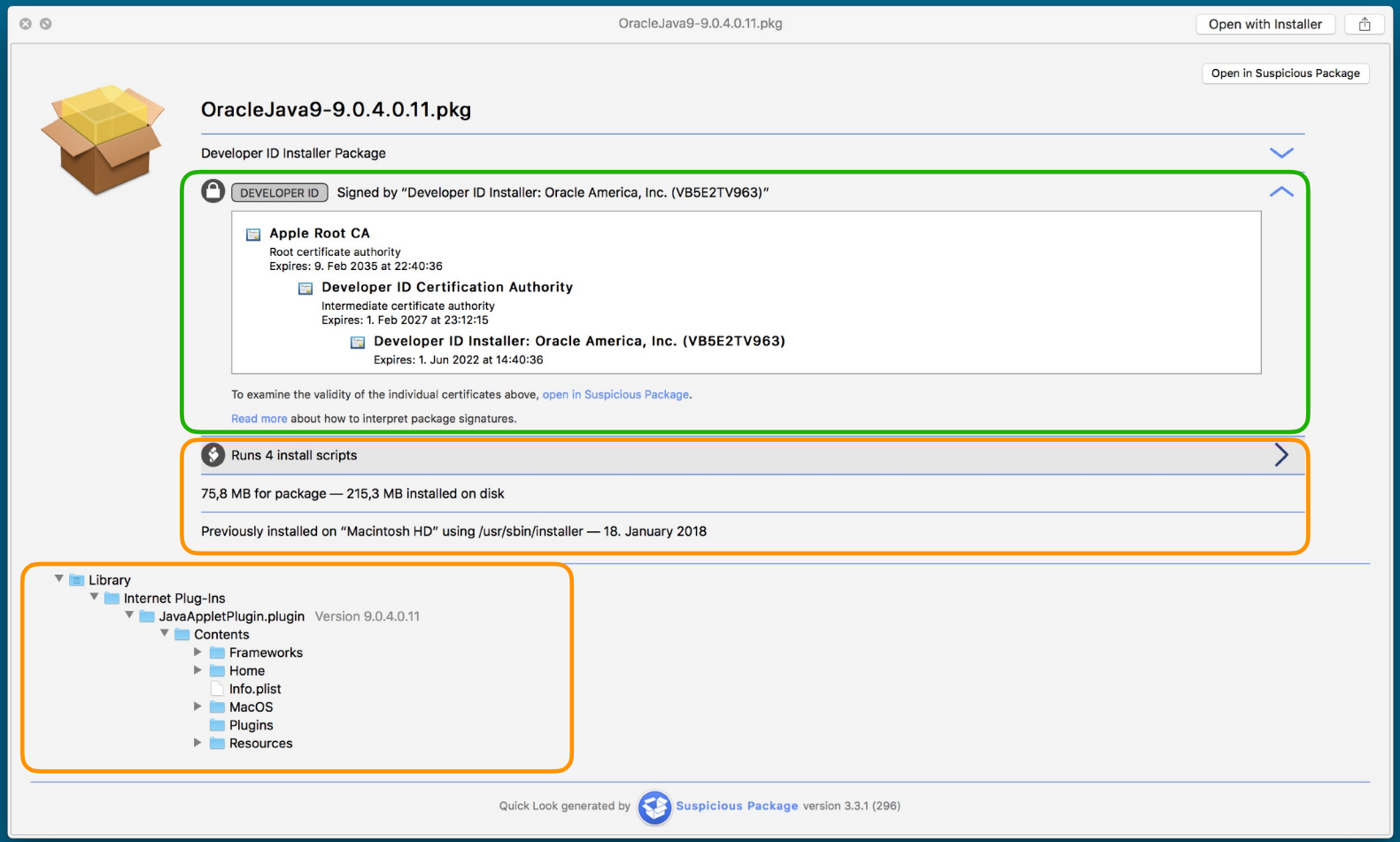

tmp — bash — bash — bash — 109×25
bash-3.2$ /usr/local/bin/inspec exec /tmp/dev-stack-check.rb
Profile: tests from /tmp/dev-stack-check.rb (tests from .tmp.dev-stack-check.rb)
Version: (not specified)
Target: local://
✔ dev-stack-007: Check ansible version
✔ Pip Package ansible should be installed
✔ Pip Package ansible version should >= "2.4"
✔ dev-stack-008: Check macOS build in openssl
✔ Bash command openssl version stdout should match "LibreSSL 2.2.7"
✔ Bash command openssl version exit_status should eq 0
✔ dev-stack-009: Check homebrew openssl version
✔ Bash command /usr/local/opt/openssl/bin/openssl version stdout should match "OpenSSL 1.0.2n"
✔ Bash command /usr/local/opt/openssl/bin/openssl version exit_status should eq 0
Profile Summary: 3 successful controls, 0 control failures, 0 controls skipped
Test Summary: 6 successful, 0 failures, 0 skipped
bash-3.2$

brew.sh


brew.sh
Fork me on GitHub
Homebrew
The missing package manager for macOS
English
Install Homebrew
/usr/bin/ruby -e "$(curl -fsSL https://raw.githubusercontent.com/Homebrew/install/master/install)"
Paste that at a Terminal prompt.
The script explains what it will do and then pauses before it does it. There are more installation options here.
What Does Homebrew Do?
Homebrew installs the stuff you need that Apple didn't.
$ brew install wget
Homebrew installs packages to their own directory and then symlinks their files into /usr/local.
$ cd /usr/local

Application Lifecycle & Change management

Inspect content



Fingerprint binaries

OracleJava9-9.0.1.0.11.pkg

java-9.0.1.0.11.csv — Open with Numbers

name	path	interprete	sha256	main_bundle_exec
				1
unpack200	/Library/Internet Plug-Ins/JavaAppletPlugin.plugin/Contents/Home/bin		cdc164f6ea631d6f8548c3271297e4b8fcf1997b5bee3d476f83f7645df3c20d	0
appletviewer	/Library/Internet Plug-Ins/JavaAppletPlugin.plugin/Contents/Home/bin		a158a7d2736df860cb8039239bf2f651c41ef95a6e53f4fd0e1a621476da0f5d	0
idlj	/Library/Internet Plug-Ins/JavaAppletPlugin.plugin/Contents/Home/bin		6e8a4ca0a6f4d5eb8ca4108e19aa1be84493ad26341813e61a52dbe405a06367	0
rmid	/Library/Internet Plug-Ins/JavaAppletPlugin.plugin/Contents/Home/bin		b387d4ae8f575dd0e112d1a061037323ecb62d44668cd9b1429508e3e146b8b3	0
rmiregistry	/Library/Internet Plug-Ins/JavaAppletPlugin.plugin/Contents/Home/bin		9837957fc8af6a20c654b434341f2789f4f495ac39348c4023f7b82460544b02	0
jrunscript	/Library/Internet Plug-Ins/JavaAppletPlugin.plugin/Contents/Home/bin		940e4a0a3c16d0e0a4cd826f958a26bc7b85611d13804eecca8bc640a65d2b5f	0
java	/Library/Internet Plug-Ins/JavaAppletPlugin.plugin/Contents/Home/bin		c47b724b24b65301166283cc0c636f00e7f2f223b7ad6b4ae8f7332698a37fb0	0
jweblauncher	/Library/Internet Plug-Ins/JavaAppletPlugin.plugin/Contents/Home/bin		6961251adda4d9317f37d8b6fa7046cd061b2d2946dc428f3b40432b72fa62a9	0
javaws	/Library/Internet Plug-Ins/JavaAppletPlugin.plugin/Contents/Home/bin		d473aefd5690447149de80e40e29ee1325c092160a8555a44562807a9c52a935	0
servertool	/Library/Internet Plug-Ins/JavaAppletPlugin.plugin/Contents/Home/bin		6ee25d34b365b42b13364c5e4fa56bc42ca75c07dbe145d76b90668f0959f844	0
orbd	/Library/Internet Plug-Ins/JavaAppletPlugin.plugin/Contents/Home/bin		2655a6f979e2dc0a5bd3931cab9291015d7a4d0661505cb2bfff88bf306b52a4	0
keytool	/Library/Internet Plug-Ins/JavaAppletPlugin.plugin/Contents/Home/bin		84b706d85182024dbf5105f39f2e7c6591cbcd88c8609837e85171be931971b1	0
pack200	/Library/Internet Plug-Ins/JavaAppletPlugin.plugin/Contents/Home/bin		3b6874748fe0a593de93a63cc8e4ce14a1356e26574cfa10574b1601b043ecfb	0
jjs	/Library/Internet Plug-Ins/JavaAppletPlugin.plugin/Contents/Home/bin		7d298591edf77b6f3ee7d81549b494f3f61b9f6b4b3fa9b907aa97d043310c9f	0
tnameserv	/Library/Internet Plug-Ins/JavaAppletPlugin.plugin/Contents/Home/bin		d2ec61d606044f6c7313852f4d87fff007b20de2bc823f2e6a4ad83547d39bee	0
jcontrol	/Library/Internet Plug-Ins/JavaAppletPlugin.plugin/Contents/Home/bin		ba5212c07edc29a377068022236fa0820863b098f4e0ffd93b43acee306cc8f6	0
JavaWSApplicationStub	/Library/Internet Plug-Ins/JavaAppletPlugin.plugin/Contents/Home/lib/shortcuts		64a414ff9f3699fca07c8b8b77852a892d8890f6ba9a1eb6f8158ff7bbaa1b6c	0
jspawnhelper	/Library/Internet Plug-Ins/JavaAppletPlugin.plugin/Contents/Home/lib		ef683342502005f896c3c377fb76aba360129e0b16f3835bd8ed39cde1ca052f	0
JavaUpdater	/Library/Internet Plug-Ins/JavaAppletPlugin.plugin/Contents/Resources/JavaUpdater.app/Contents/MacOS		f51f084d8c15b18070ab5a17b33e3ec589c8298c67dc291d194ec974314c62f3	0
Helper-Tool	/Library/Internet Plug-Ins/JavaAppletPlugin.plugin/Contents/Resources	/bin/bash	7a2c6e84bb1ff121196777056c1504d31a8348d70acb3f0d67334c9fe4f2a2a0	0
JavawsLauncher	/Library/Internet Plug-Ins/JavaAppletPlugin.plugin/Contents/Resources/JavawsLauncher.app/Contents/MacOS		7f723fd0926746800d17183859346ce5f47719753e099d126f02737e94bc8ea7	0
JavaControlPanelHelper	/Library/Internet Plug-Ins/JavaAppletPlugin.plugin/Contents/Resources		3f9229c15dcca316594c1e62eeb36aa643533daaa1d91da1b9fa5d61975d0668	0
finish_installation	/Library/Internet Plug-Ins/JavaAppletPlugin.plugin/Contents/Frameworks/Sparkle.framework/Versions/A/Resources/finish_installation.app/Contents/MacOS		38e3063bba8a45ca07ec3d1b69fd8c3d643a8e6039dc2c4a44ac989e4c8567b3	0
com.oracle.java.JavaUpdateHelper	/Library/Internet Plug-Ins/JavaAppletPlugin.plugin/Contents/Frameworks/Sparkle.framework/Versions/A/Resources/finish_installation.app/Contents/Library/LaunchServices		f9eff9d098debfcd65e81216d14ac5a09d8366e2fa18d0a400f72fb9133bc3eb	0

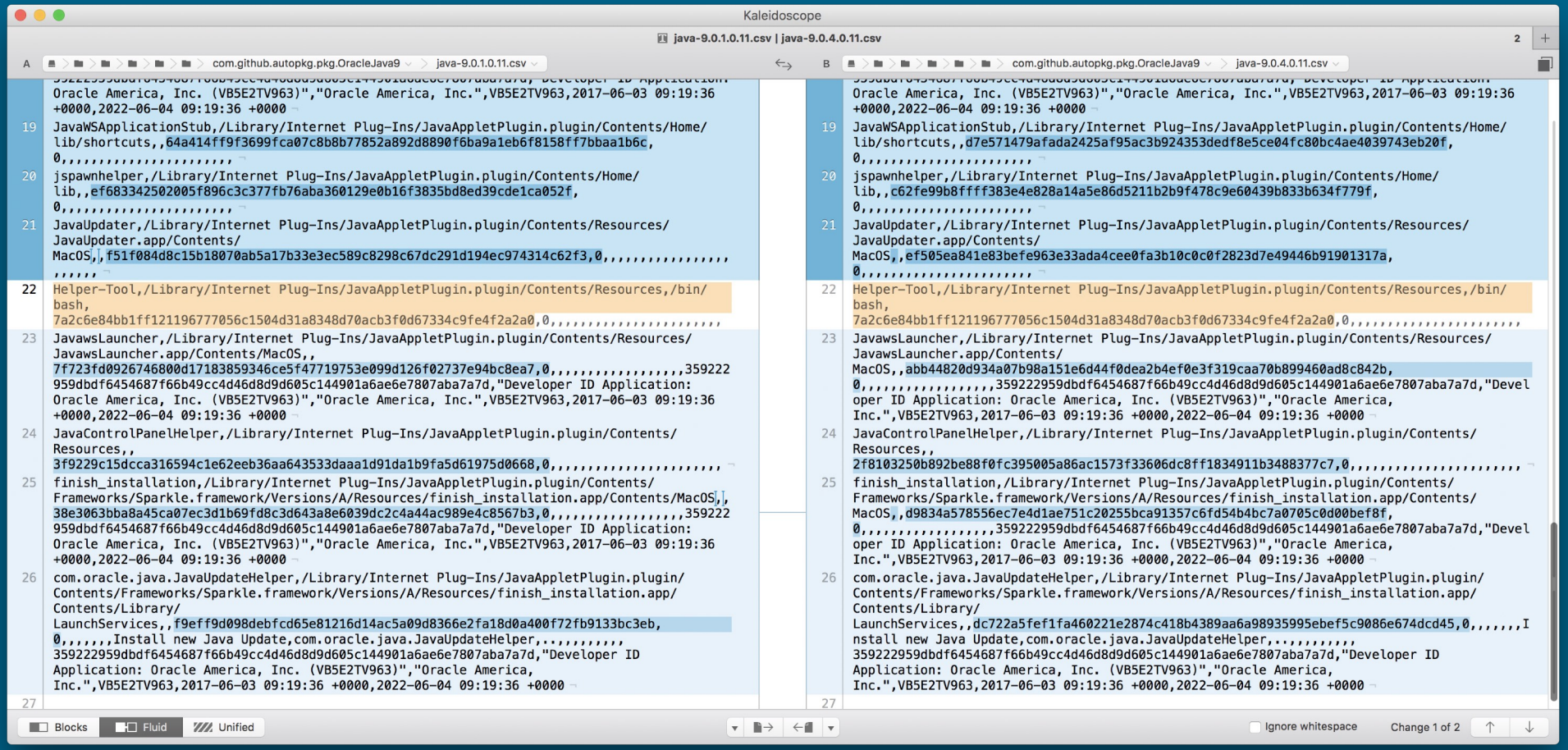
Fingerprint binaries

OracleJava9-9.0.4.0.11.pkg

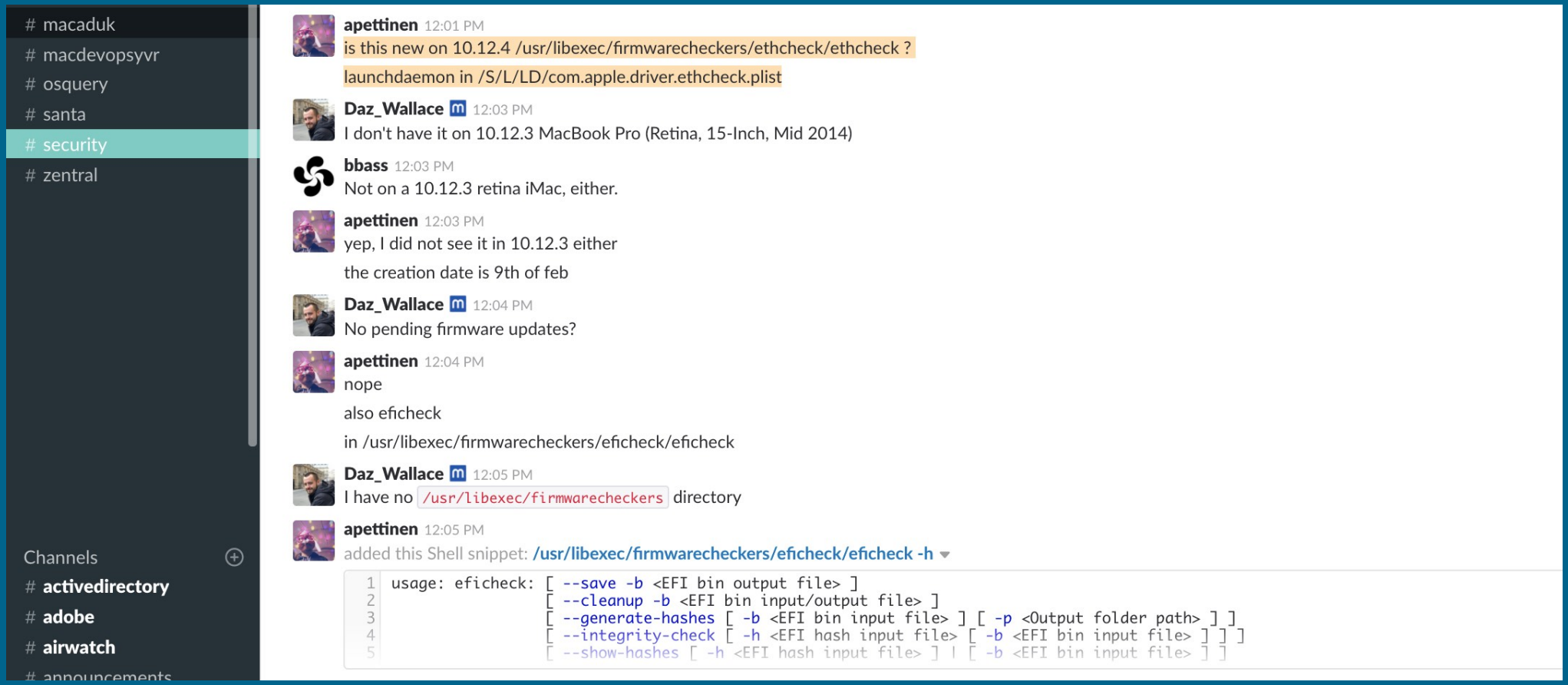
java-9.0.4.0.11.csv — Open with Numbers

name	path	interprete	sha256	main_bundle_exec
				1
unpack200	/Library/Internet Plug-Ins/JavaAppletPlugin.plugin/Contents/Home/bin		e74c0d918b09aeef73d5439ff1782f2758713266ec7157ac52d234d44da508dc	0
appletviewer	/Library/Internet Plug-Ins/JavaAppletPlugin.plugin/Contents/Home/bin		e0dd56ff44e5a045a0e1993286e05436d3af2efa2833c6cd6605686b2ee7b719	0
idlj	/Library/Internet Plug-Ins/JavaAppletPlugin.plugin/Contents/Home/bin		0df27abf854d6187819f99b346fe1f1263c472f32029a2b205f80738db874dd3	0
rmid	/Library/Internet Plug-Ins/JavaAppletPlugin.plugin/Contents/Home/bin		0b3a412e5c9f25d5a32ef23b09d6c7b16d9a306d3d1aa7d822cfc98dd35b9dfa	0
rmiregistry	/Library/Internet Plug-Ins/JavaAppletPlugin.plugin/Contents/Home/bin		aa6efdd405f6d1dd6961ba8cb37c46151e4b878c75cc25fe16ceac61af1588ba	0
jrunscript	/Library/Internet Plug-Ins/JavaAppletPlugin.plugin/Contents/Home/bin		5e08613e91b61c566e2db9f9ad47bbfb297b0105f1225b02910e164b051a1985	0
java	/Library/Internet Plug-Ins/JavaAppletPlugin.plugin/Contents/Home/bin		55bb6a3085ef5cfa486b5a3957e6ec018065324a8d99b61bf0cc060a29fc7746	0
jweblauncher	/Library/Internet Plug-Ins/JavaAppletPlugin.plugin/Contents/Home/bin		f7a6a03562f3909d59a50e9b54d3a5a73b05f8a97871709cc2f2eca5536428c4	0
javaws	/Library/Internet Plug-Ins/JavaAppletPlugin.plugin/Contents/Home/bin		f227bd9dd7ded2add9bad57f0c721d53bacf88c49b37c11511276bc9811e8373	0
servertool	/Library/Internet Plug-Ins/JavaAppletPlugin.plugin/Contents/Home/bin		6a096375f30f37a9af5d846e8cef45ef259456d52a62c6272bbaa167eff64de3	0
orbd	/Library/Internet Plug-Ins/JavaAppletPlugin.plugin/Contents/Home/bin		329761ec52c699d8fcf6eff2e11ef87c8ae7b0baf99d12ff9b6a2a1b6a71b1b5	0
keytool	/Library/Internet Plug-Ins/JavaAppletPlugin.plugin/Contents/Home/bin		15f40bb7682a066c98d1fa146fb29d203abea525d9e029c8ae5832a3e93e8148	0
pack200	/Library/Internet Plug-Ins/JavaAppletPlugin.plugin/Contents/Home/bin		483936605e4760b5bc8fc9ed7526b513569e6f5b0828e02495600066fd9f10bf	0
jjs	/Library/Internet Plug-Ins/JavaAppletPlugin.plugin/Contents/Home/bin		799c9d86f921250c3d43862c228cb5a974411051c4daf0418570cf52626f9e36	0
tnameserv	/Library/Internet Plug-Ins/JavaAppletPlugin.plugin/Contents/Home/bin		1f9bb289bdc5af5421903f97d03cd9788280b82b0fab28f2a94b4b16d9debaa6	0
jcontrol	/Library/Internet Plug-Ins/JavaAppletPlugin.plugin/Contents/Home/bin		60bb74c8c421ce536bbc49efd8a4741d70d8e84a06a61ce4f5f618e5682c5010	0
JavaWSApplicationStub	/Library/Internet Plug-Ins/JavaAppletPlugin.plugin/Contents/Home/lib/shortcuts		d7e571479afada2425af95ac3b924353dedf8e5ce04fc80bc4ae4039743eb20f	0
jspawnhelper	/Library/Internet Plug-Ins/JavaAppletPlugin.plugin/Contents/Home/lib		c62fe99b8ffff383e4e828a14a5e86d5211b2b9f478c9e60439b833b634f779f	0
JavaUpdater	/Library/Internet Plug-Ins/JavaAppletPlugin.plugin/Contents/Resources/JavaUpdater.app/Contents/MacOS		ef505ea841e83befe963e33ada4cee0fa3b10c0c0f2823d7e49446b91901317a	0
Helper-Tool	/Library/Internet Plug-Ins/JavaAppletPlugin.plugin/Contents/Resources	/bin/bash	7a2c6e84bb1ff121196777056c1504d31a8348d70acb3f0d67334c9fe4f2a2a0	0
JavawsLauncher	/Library/Internet Plug-Ins/JavaAppletPlugin.plugin/Contents/Resources/JavawsLauncher.app/Contents/MacOS		abb44820d934a07b98a151e6d44f0dea2b4ef0e3f319caa70b899460ad8c842b	0
JavaControlPanelHelper	/Library/Internet Plug-Ins/JavaAppletPlugin.plugin/Contents/Resources		2f8103250b892be88f0fc395005a86ac1573f33606dc8ff1834911b3488377c7	0
finish_installation	/Library/Internet Plug-Ins/JavaAppletPlugin.plugin/Contents/Frameworks/Sparkle.framework/Versions/A/Resources/finish_installation.app/Contents/MacOS		d9834a578556ec7e4d1ae751c20255bca91357c6fd54b4bc7a0705c0d00bef8f	0
com.oracle.java.JavaUpdateHelper	/Library/Internet Plug-Ins/JavaAppletPlugin.plugin/Contents/Frameworks/Sparkle.framework/Versions/A/Resources/finish_installation.app/Contents/Library/LaunchServices		dc722a5fef1fa460221e2874c418b4389aa6a98935995ebef5c9086e674dcd45	0

Inspect for difference in detail



Discuss responsibly




Johnny Random
@random-twitter-dude
Follow
Dear @AppleSupport, we noticed a *HUGE* security issue at MacOS High Sierra. Anyone can login as "root" with empty password after clicking on login button several times. Are you aware of it @Apple?
10:38 AM - 28 Nov 2017
12,696 Retweets 15,595 Likes
1.2K
13K
16K

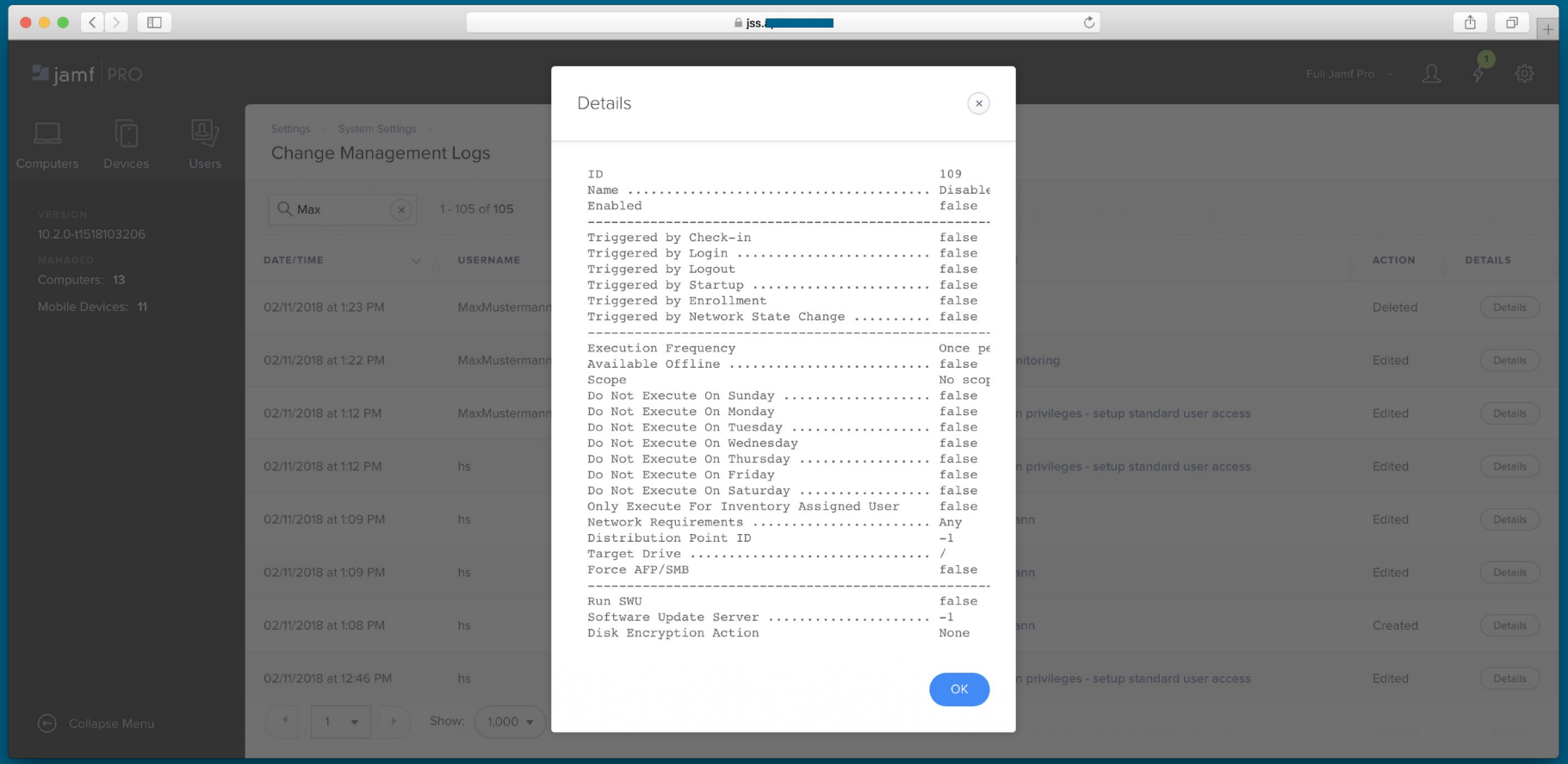
Security Baseline

(Management infrastructure)

Management services

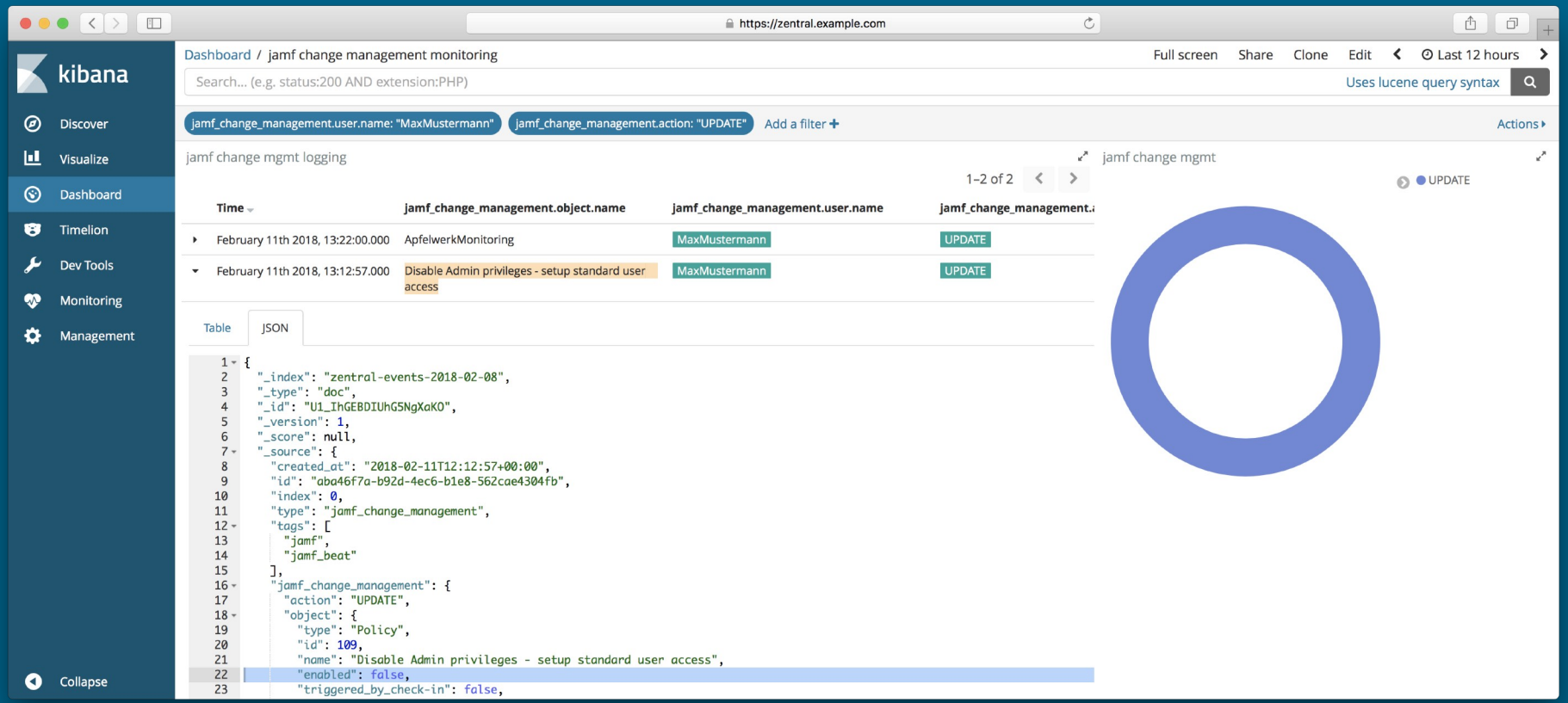
- Configuration management to control server state
- Build Multiple layers of defense
- Limit access / API access
- Use logging and intrusion detection

Local logs

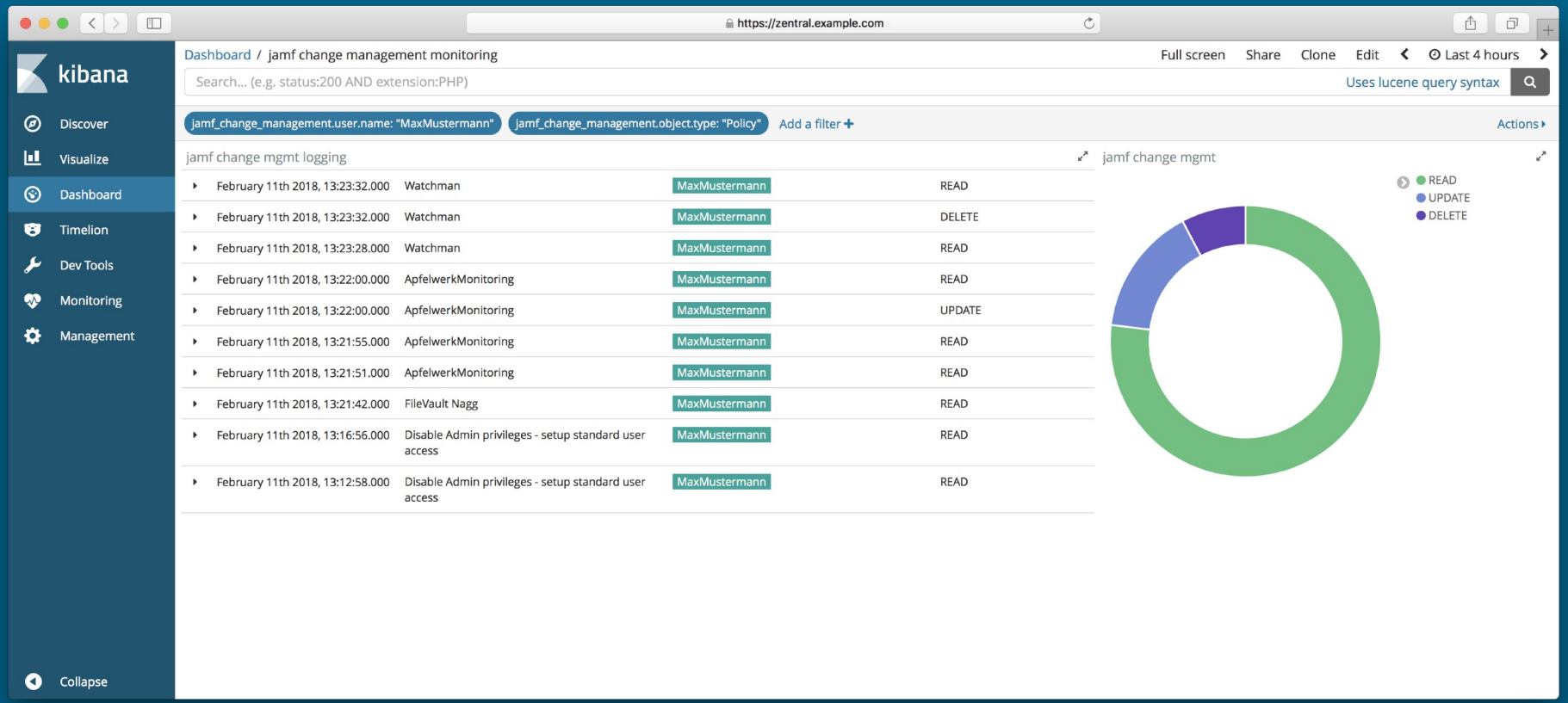

jamf PRO
Full Jamf Pro
Computers
Devices
Users
Settings
System Settings
Change Management Logs
Max
1 - 105 of 105
DATE/TIME
USERNAME
ACTION
DETAILS
02/11/2018 at 1:23 PM
MaxMustermann
Deleted
Details
02/11/2018 at 1:22 PM
MaxMustermann
Edited
Details
02/11/2018 at 1:12 PM
MaxMustermann
Edited
Details
02/11/2018 at 1:12 PM
hs
Edited
Details
02/11/2018 at 1:09 PM
hs
Edited
Details
02/11/2018 at 1:09 PM
hs
Edited
Details
02/11/2018 at 1:08 PM
hs
Created
Details
02/11/2018 at 12:46 PM
hs
Edited
Details
VERSION
10.2.0-t1518103206
MANAGED
Computers: 13
Mobile Devices: 11
Collapse Menu
Show:
1,000
Details
ID 109
Name ..... Disable
Enabled false
Triggered by Check-in false
Triggered by Login ..... false
Triggered by Logout false
Triggered by Startup ..... false
Triggered by Enrollment false
Triggered by Network State Change ..... false
Execution Frequency Once pe
Available Offline ..... false
Scope No scop
Do Not Execute On Sunday ..... false
Do Not Execute On Monday false
Do Not Execute On Tuesday ..... false
Do Not Execute On Wednesday false
Do Not Execute On Thursday ..... false
Do Not Execute On Friday false
Do Not Execute On Saturday ..... false
Only Execute For Inventory Assigned User false
Network Requirements ..... Any
Distribution Point ID -1
Target Drive ..... /
Force AFP/SMB false
Run SWU false
Software Update Server ..... -1
Disk Encryption Action None
OK

```
#  Log lines read out from ElasticStack / Kibana 6.2
{
  "_index": "zentral-events-2018-02-21",
  "_type": "doc",
...
    "type": "jamf_change_management",
    "tags": [
      "jamf",
      "jamf_beat"
    ],
    "jamf_change_management": {
      "action": "UPDATE",
      "object": {
        "type": "Policy",
        "id": 109,
        "name": "Disable Admin privileges - setup standard user access",
        "enabled": false,
...
      },
      "jamf_instance": {
        "host": "jamfpro.example.com",
        "path": "/JSSResource",
        "port": 8443
      },
      "user": {
        "id": 23,
        "name": "max mustermann"
      }
    }
...
}
```

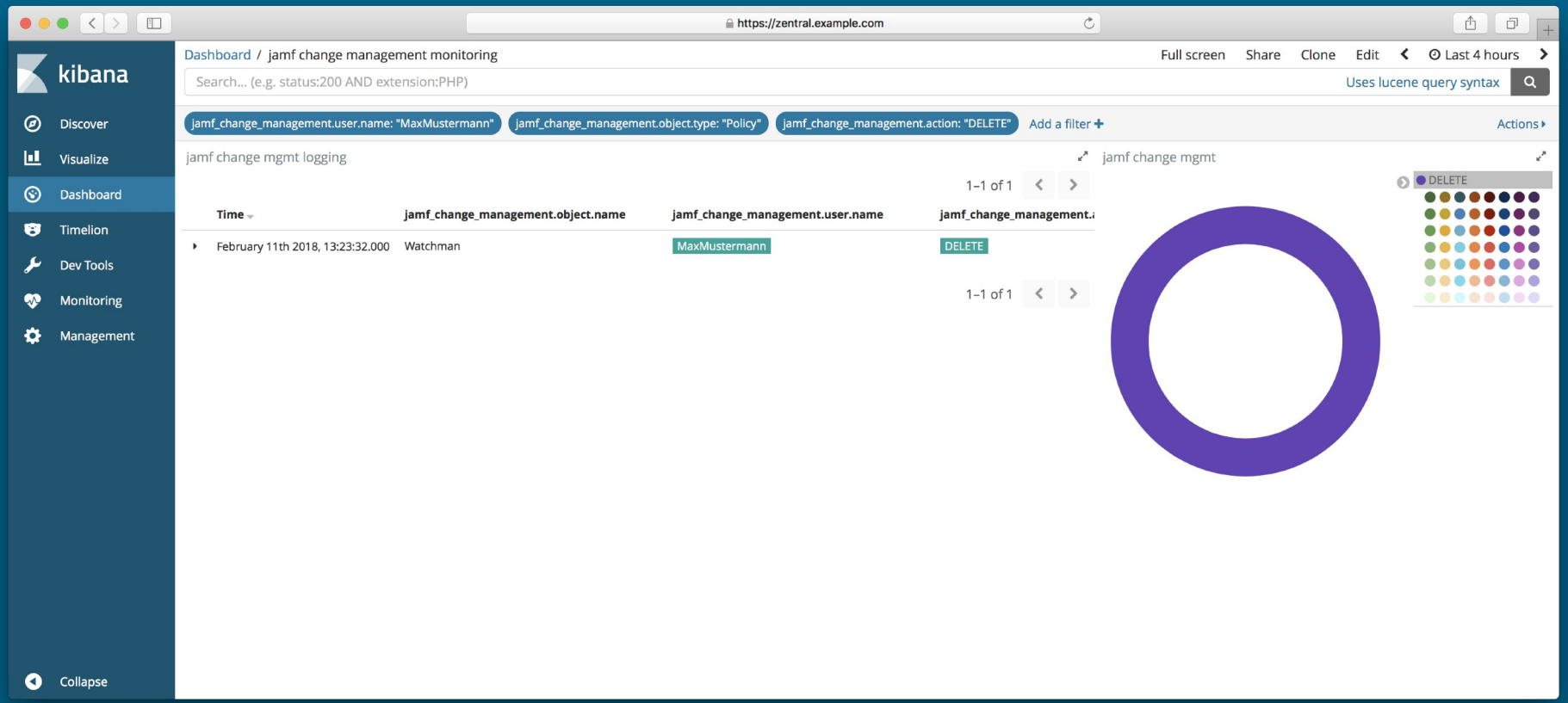
Log aggregation



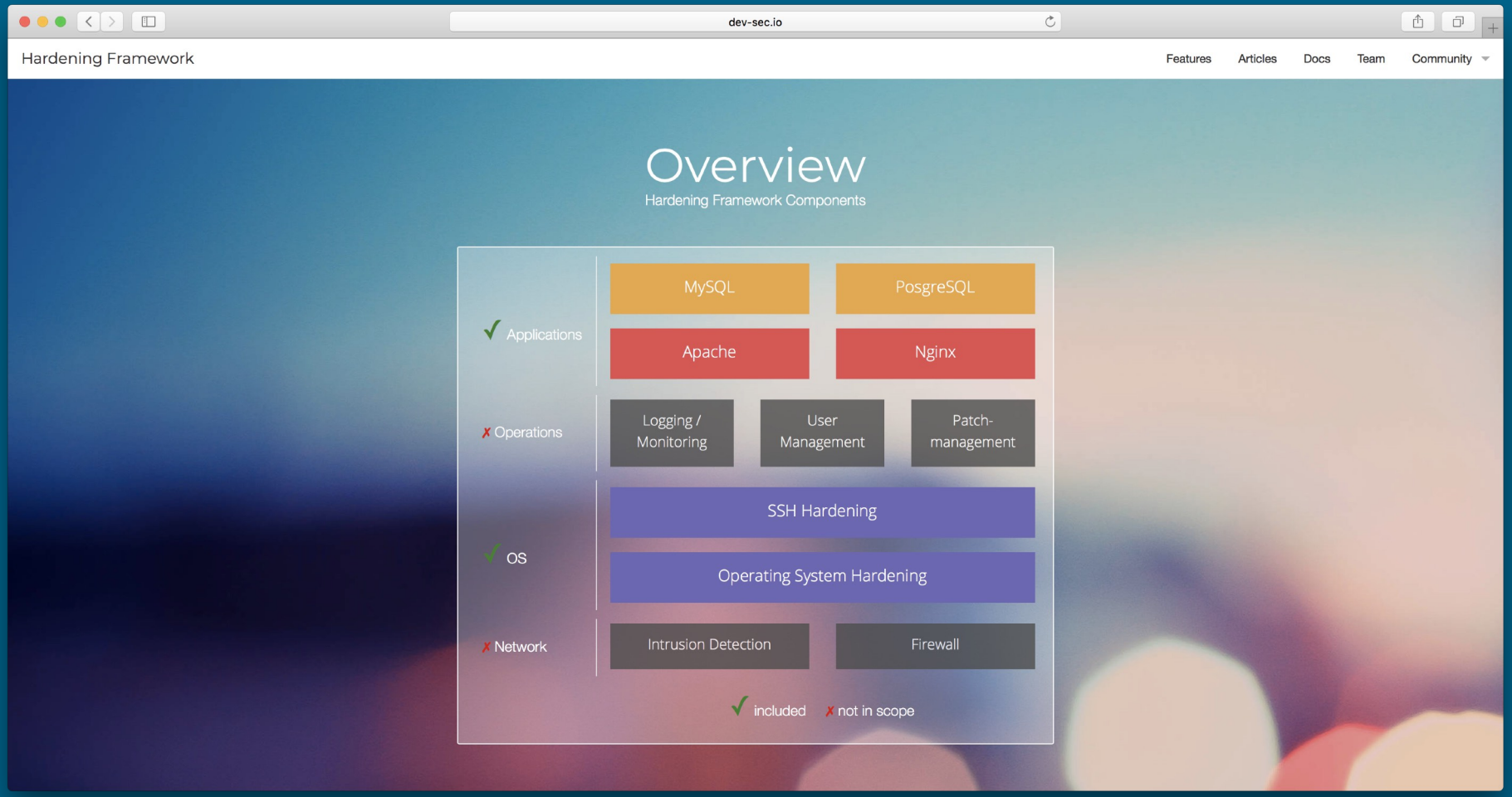
Log aggregation



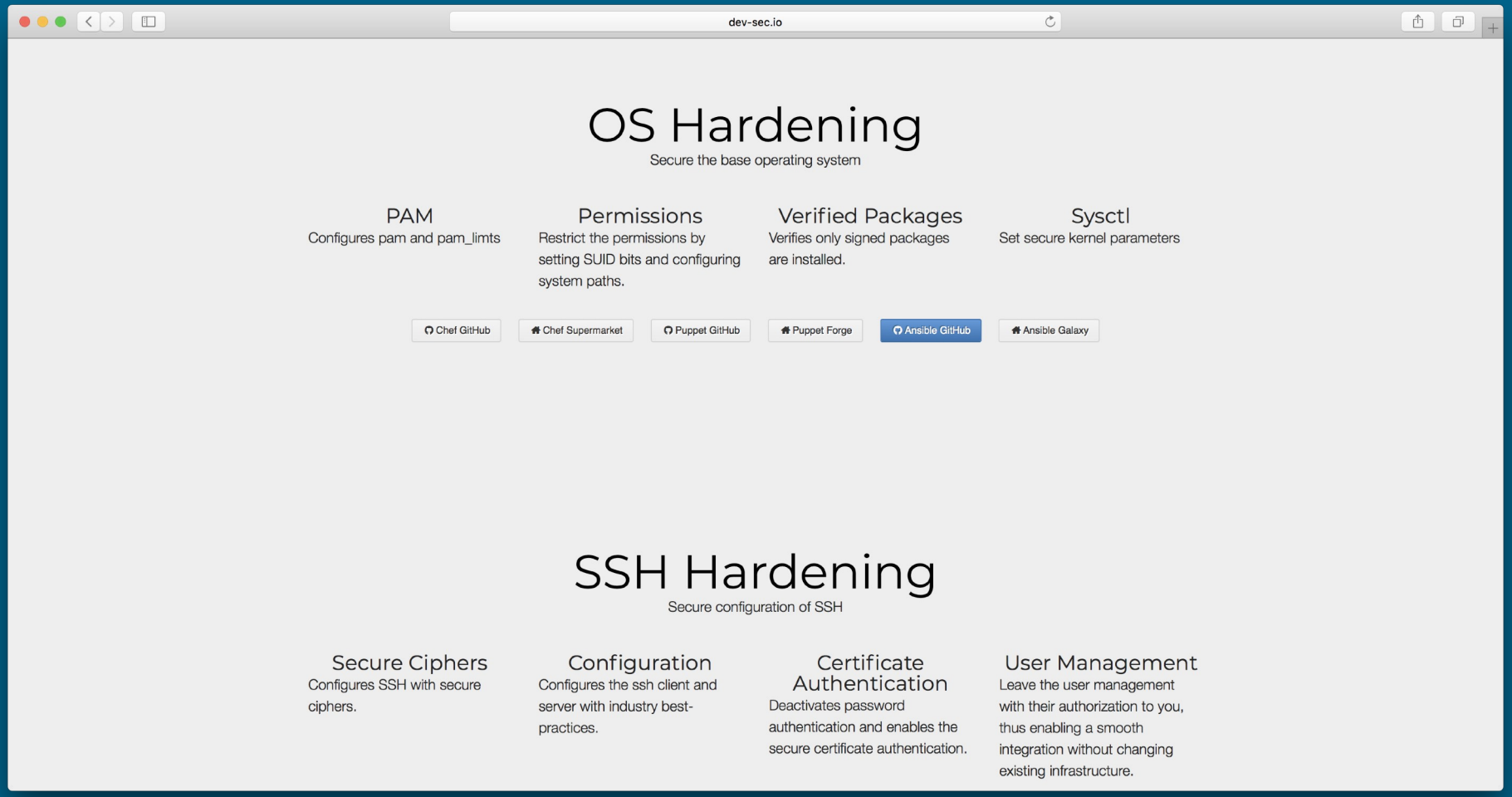
Log aggregation



http://dev-sec.io



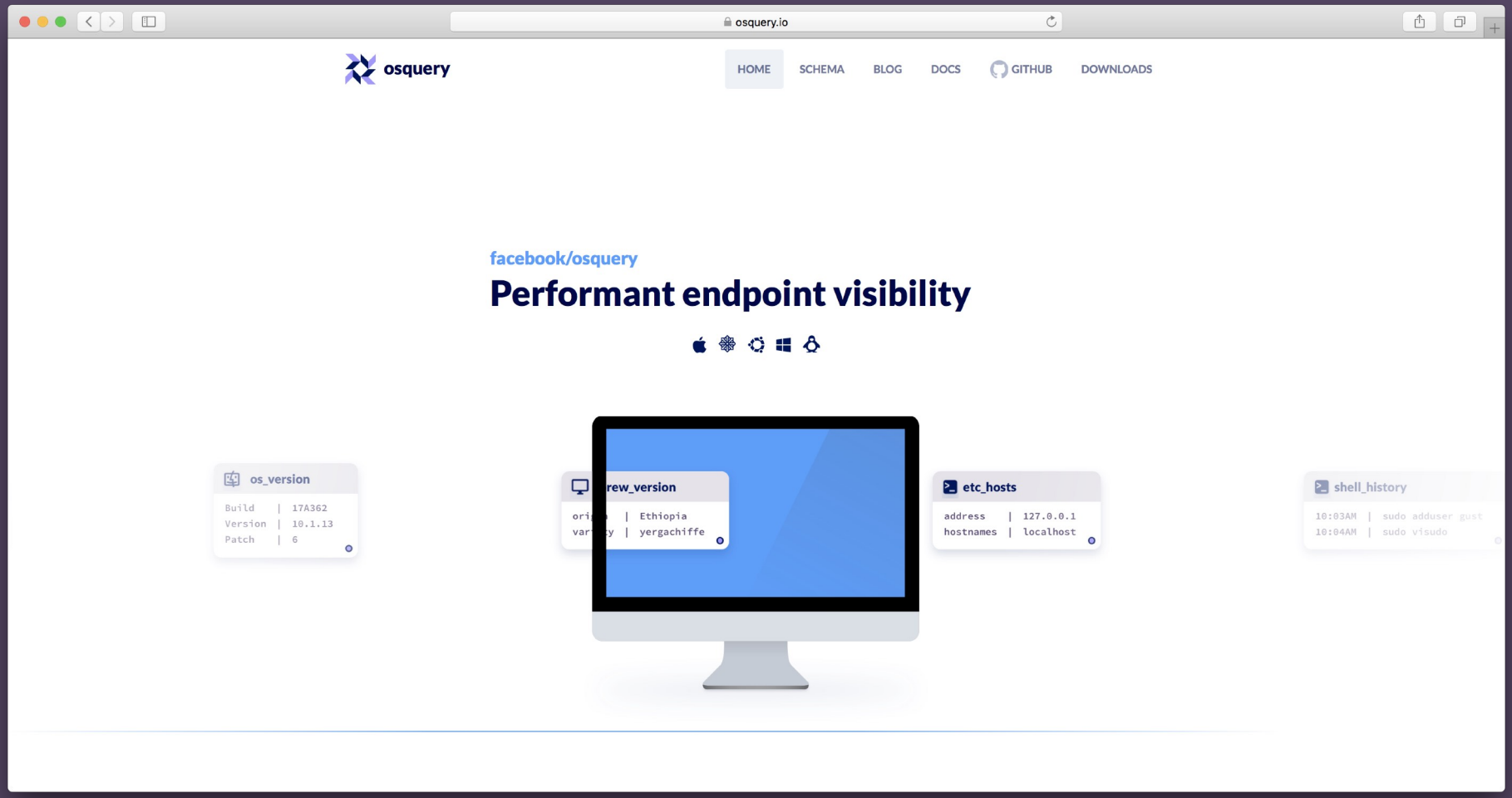
http://dev-sec.io



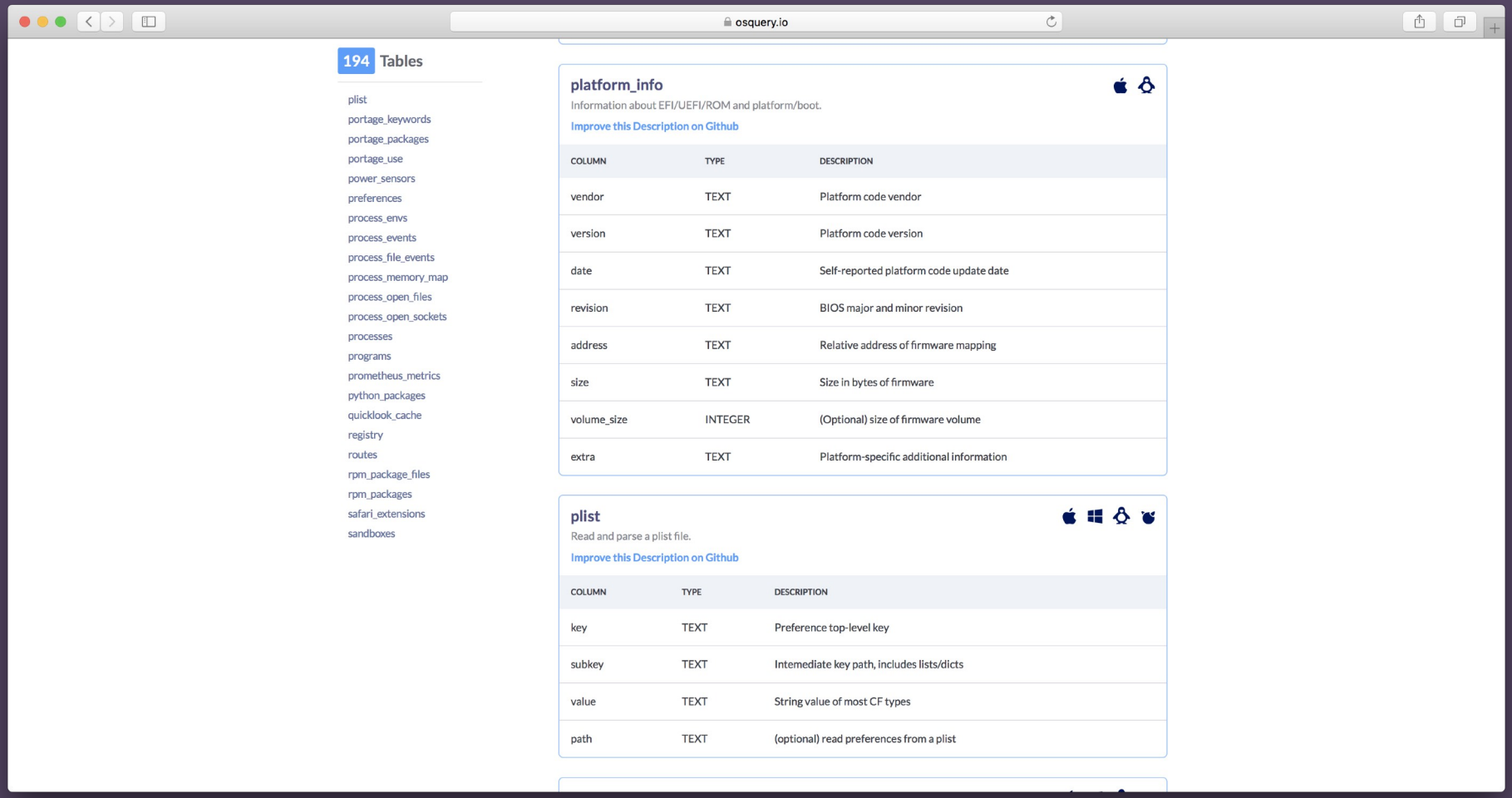
OSQuery

(Change detection)

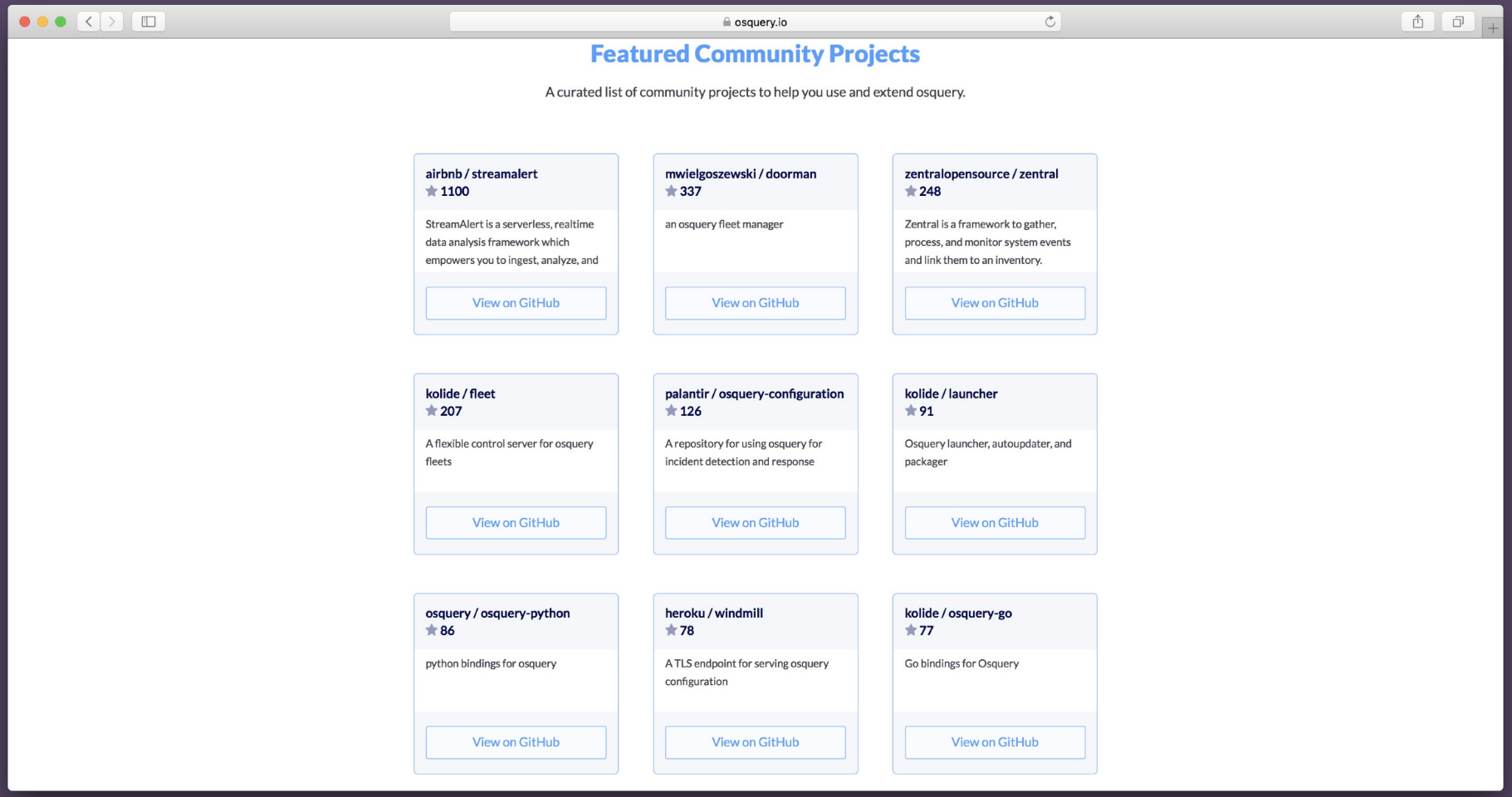
https://osquery.io



https://osquery.io



https://osquery.io



Recurring check

```
SELECT '/private/var/db/ConfigurationProfiles/MDM_ComputerPrefs.plist' AS
OMG_missing_profile WHERE NOT EXISTS (SELECT value FROM plist
WHERE path = '/private/var/db/ConfigurationProfiles/MDM_ComputerPrefs.plist'
AND subkey LIKE '%ProfileUUID%');
```

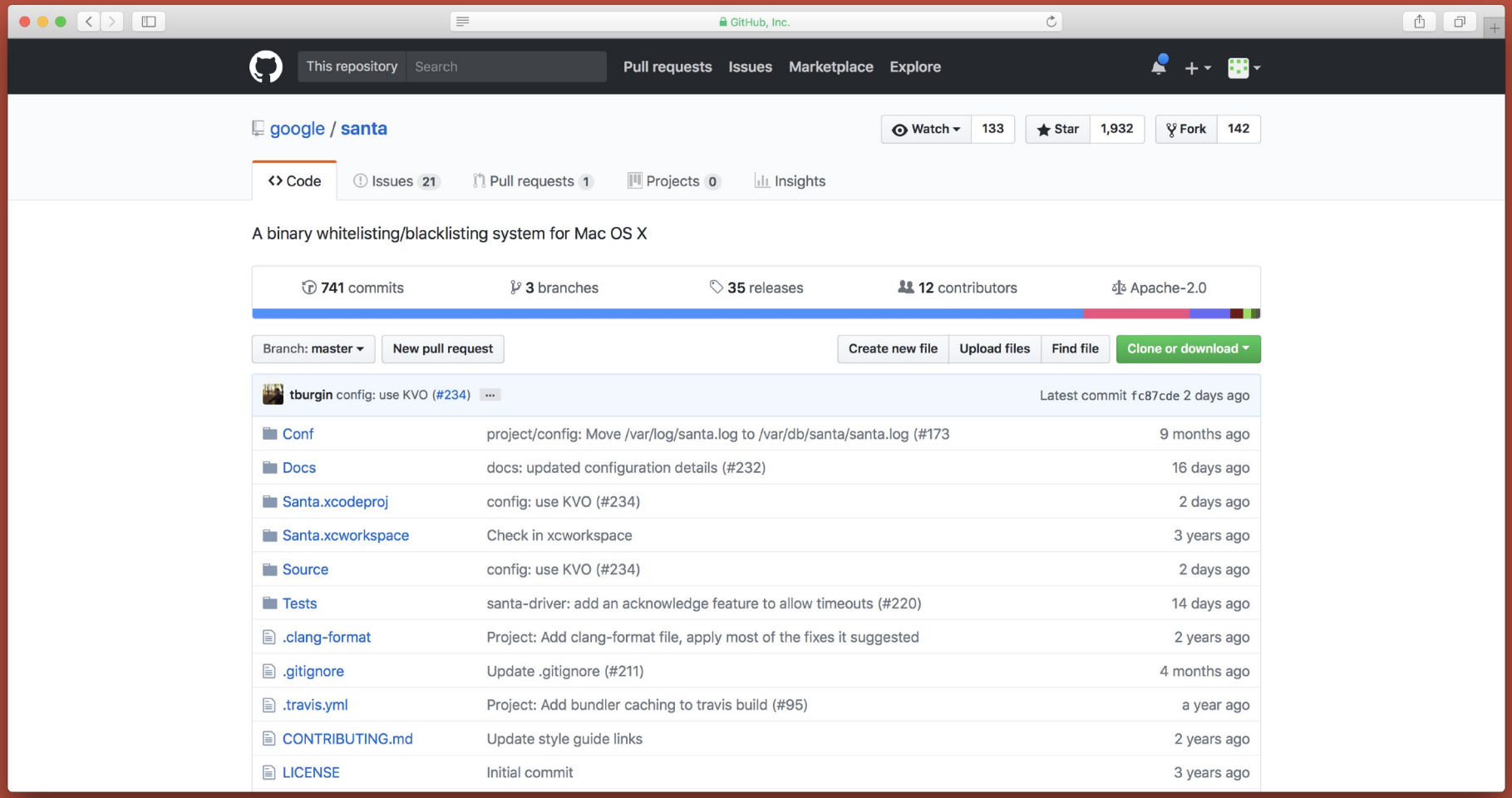
Recurring check

```
SELECT '/private/var/db/ConfigurationProfiles/MDM_ComputerPrefs.plist' AS
OMG_missing_profile WHERE NOT EXISTS (SELECT value FROM plist
WHERE path = '/private/var/db/ConfigurationProfiles/MDM_ComputerPrefs.plist'
AND subkey LIKE '%ProfileUUID%');
+-----------------------------------------------------------------+
| OMG_missing_profile                                             |
+-----------------------------------------------------------------+
| /private/var/db/ConfigurationProfiles/MDM_ComputerPrefs.plist |
+-----------------------------------------------------------------+
```

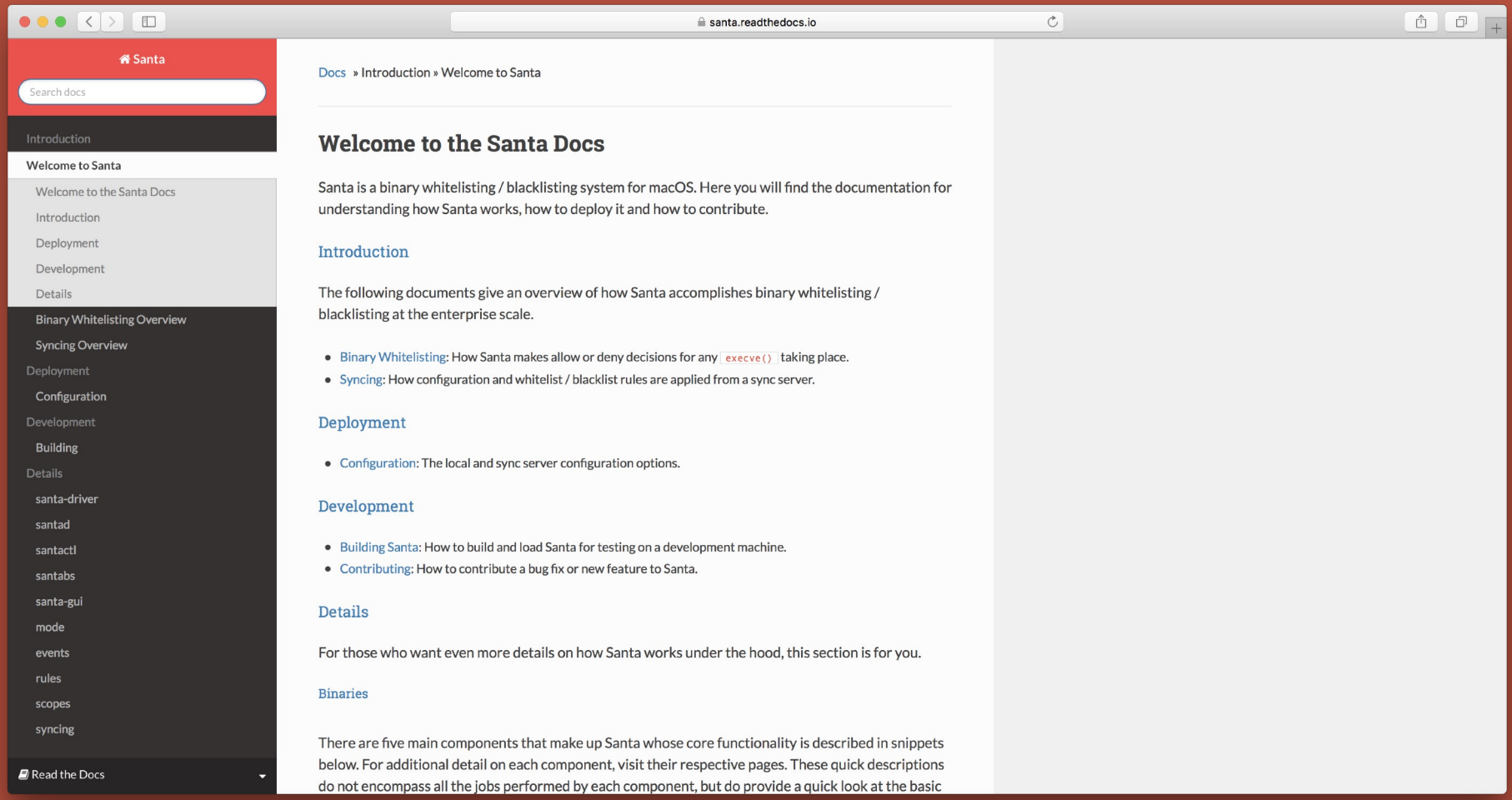
Google Santa

(Binary control)

https://github.com/google/santa



https://santa.readthedocs.io/en/latest/



```
Usage: santactl fileinfo [options] [file-paths]
    --recursive (-r): Search directories recursively.
    --json: Output in JSON format.
    --key: Search and return this one piece of information.
           You may specify multiple keys by repeating this flag.
           Valid Keys:
                       "Path"
                       "SHA-256"
...
                       "Bundle Name"
                       "Bundle Version Str"
...
                       "Signing Chain"

    --cert-index: Supply an integer corresponding to a certificate of the
                  signing chain to show info only for that certificate.

    --filter: Use predicates of the form 'key=regex' to filter out which files
              are displayed. Valid keys are the same as for --key.

Examples: santactl fileinfo --cert-index 1 --key SHA-256 --json /usr/bin/yes
          santactl fileinfo --key SHA-256 --json /usr/bin/yes
          santactl fileinfo /usr/bin/yes /bin/*
          santactl fileinfo /usr/bin -r --key Path --key SHA-256 --key Rule
          santactl fileinfo /usr/bin/* --filter Type=Script --filter Path=zip
```

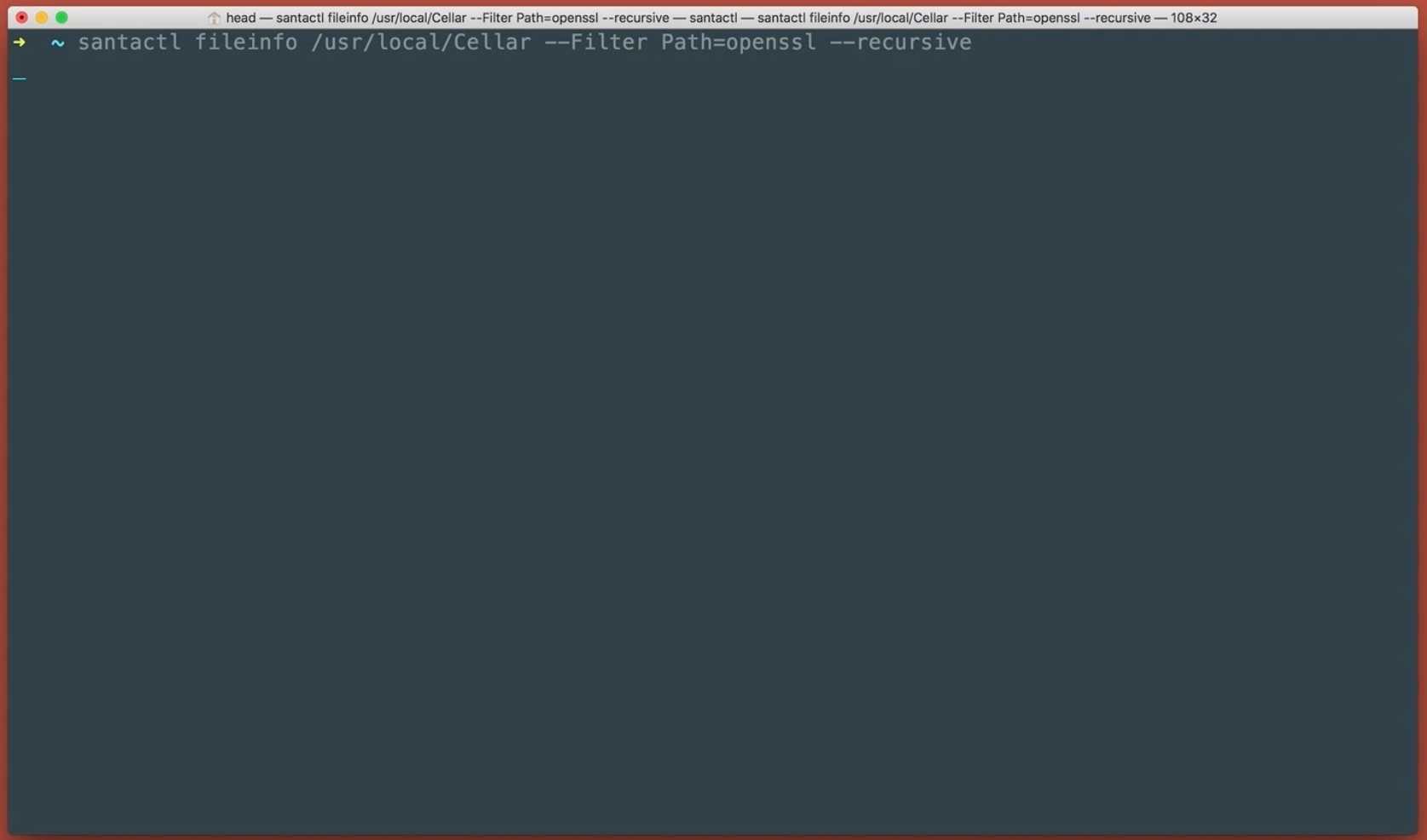
Scan executable content

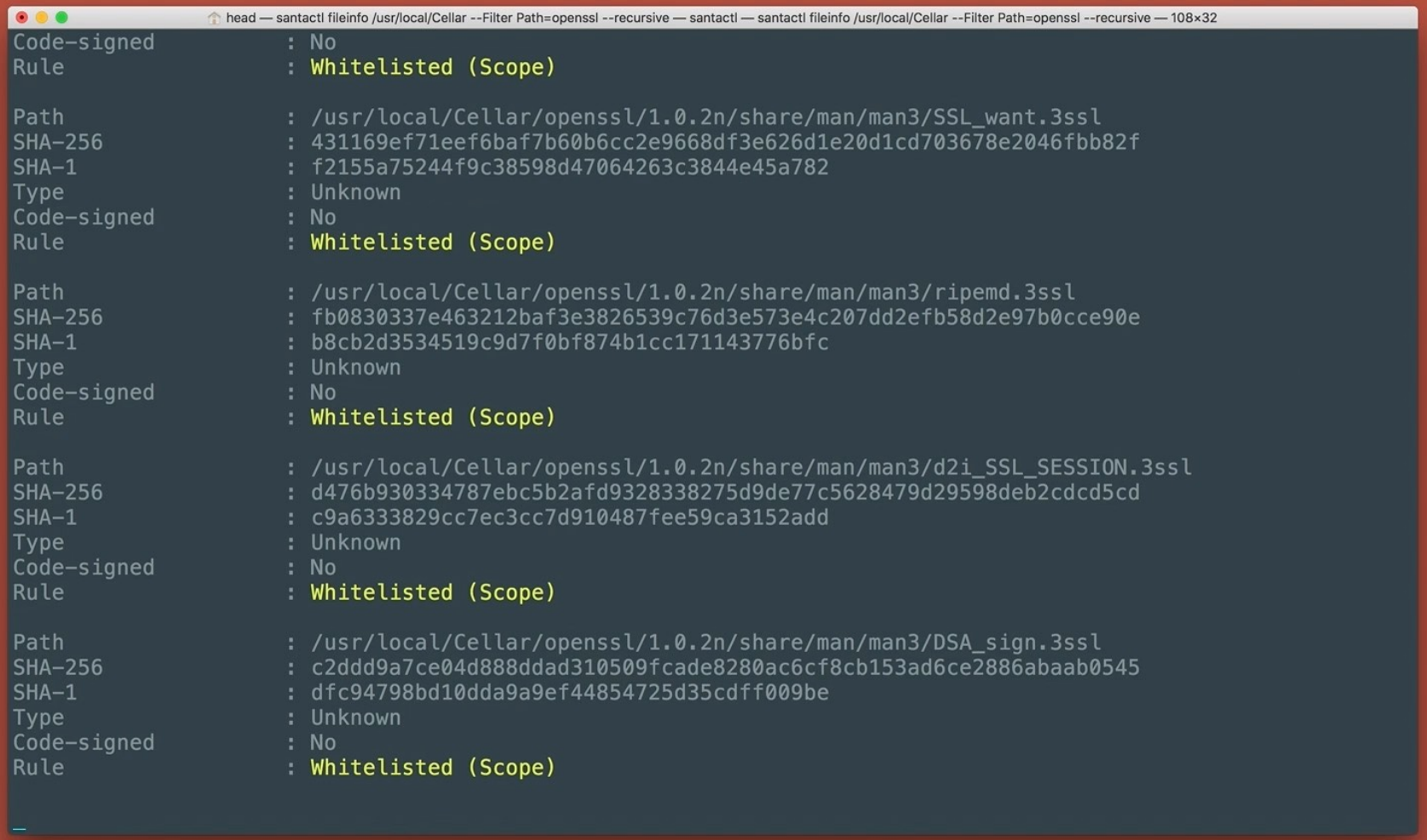
```
## Here we recursively scan Google Chrome.app for Paths, Fingerprints of embedded scripts

santactl fileinfo /Applications/Google\ Chrome.app --filter Type=Script --recursive --json
```

```
santactl fileinfo /Applications/Google\ Chrome.app --filter Type=Script --recursive --json
[
{
  "Bundle Version" : "3282.119",
  "SHA-256" : "78e304c7078062f3b20da41a18404f747e776f55bb4f94e6f944c99fce8703d9",
  "SHA-1" : "c7a80ccba988df9a6289add0d2fee5617cf88443",
  "Type" : "Script",
  "Path" : "\/Applications\/Google Chrome.app\/Contents\/Versions\/64.0.3282.119\/Google Chrome
Framework.framework\/Versions\/A\/Resources\/keystone_promote_postflight.sh",
  "Rule" : "Whitelisted (Scope)",
  "Code-signed" : "No",
  "Bundle Version Str" : "64.0.3282.119"
},
{
  "Bundle Version" : "3282.119",
  "SHA-256" : "7e9425061f96114ff9075268063aa92b48846d89f476eeda5cd0dd106538a2c0",
  "SHA-1" : "14fba10907ccdc9392ae941f40703d0a732c9595",
  "Type" : "Script",
  "Path" : "\/Applications\/Google Chrome.app\/Contents\/Versions\/64.0.3282.119\/Google Chrome
Framework.framework\/Versions\/A\/Resources\/install.sh",
  "Rule" : "Whitelisted (Scope)",
  "Code-signed" : "No",
  "Bundle Version Str" : "64.0.3282.119"
},
{
  "Bundle Version" : "3282.119",
  "SHA-256" : "19de5dd790efe55479c2b7bfc179efc4c8faeb5022ca7bd99384e5fa6f1bc399",
  "SHA-1" : "9667ed8a2376a944586436f2179d37dbccd3cb03",
  "Type" : "Script",
  "Path" : "\/Applications\/Google Chrome.app\/Contents\/Versions\/64.0.3282.119\/Google Chrome
Framework.framework\/Versions\/A\/Resources\/keystone_promote_preflight.sh",
  "Rule" : "Whitelisted (Scope)",
  "Code-signed" : "No",
  "Bundle Version Str" : "64.0.3282.119"
}
]
```

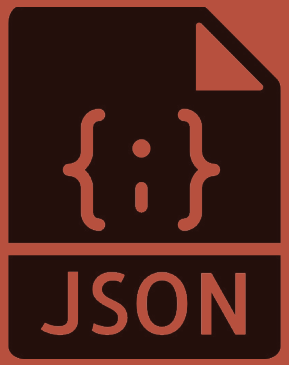
Scan executable content

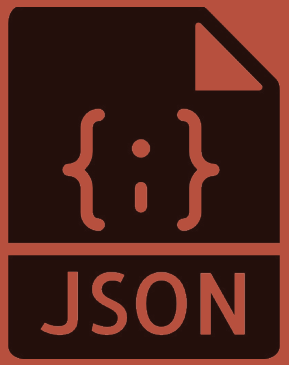
```
## Here we recursively scan a Homebrew installed openssl library to get Paths, Fingerprints

santactl fileinfo /usr/local/Cellar --Filter Path=openssl --recursive
```


head — santactl fileinfo /usr/local/Cellar --Filter Path=openssl --recursive — santactl — santactl fileinfo /usr/local/Cellar --Filter Path=openssl --recursive — 108×32
➜ ~ santactl fileinfo /usr/local/Cellar --Filter Path=openssl --recursive


head — santactl fileinfo /usr/local/Cellar --Filter Path=openssl --recursive — santactl — santactl fileinfo /usr/local/Cellar --Filter Path=openssl --recursive — 108×32
Code-signed : No
Rule : Whitelisted (Scope)
Path : /usr/local/Cellar/openssl/1.0.2n/share/man/man3/SSL_want.3ssl
SHA-256 : 431169ef71eef6baf7b60b6cc2e9668df3e626d1e20d1cd703678e2046fbb82f
SHA-1 : f2155a75244f9c38598d47064263c3844e45a782
Type : Unknown
Code-signed : No
Rule : Whitelisted (Scope)
Path : /usr/local/Cellar/openssl/1.0.2n/share/man/man3/ripemd.3ssl
SHA-256 : fb0830337e463212baf3e3826539c76d3e573e4c207dd2efb58d2e97b0cce90e
SHA-1 : b8cb2d3534519c9d7f0bf874b1cc171143776bfc
Type : Unknown
Code-signed : No
Rule : Whitelisted (Scope)
Path : /usr/local/Cellar/openssl/1.0.2n/share/man/man3/d2i_SSL_SESSION.3ssl
SHA-256 : d476b930334787ebc5b2afd9328338275d9de77c5628479d29598deb2cdcd5cd
SHA-1 : c9a6333829cc7ec3cc7d910487fee59ca3152add
Type : Unknown
Code-signed : No
Rule : Whitelisted (Scope)
Path : /usr/local/Cellar/openssl/1.0.2n/share/man/man3/DSA_sign.3ssl
SHA-256 : c2ddd9a7ce04d888ddad310509fcade8280ac6cf8cb153ad6ce2886abaab0545
SHA-1 : dfc94798bd10dda9a9ef44854725d35cdff009be
Type : Unknown
Code-signed : No
Rule : Whitelisted (Scope)

Diff for analyze





brew-openssl-1.0.2h.json

brew-openssl-1.0.2n.json

Event streams

Event

point of instrumentation in the system

Ship

aggregate results & sync config

Probe

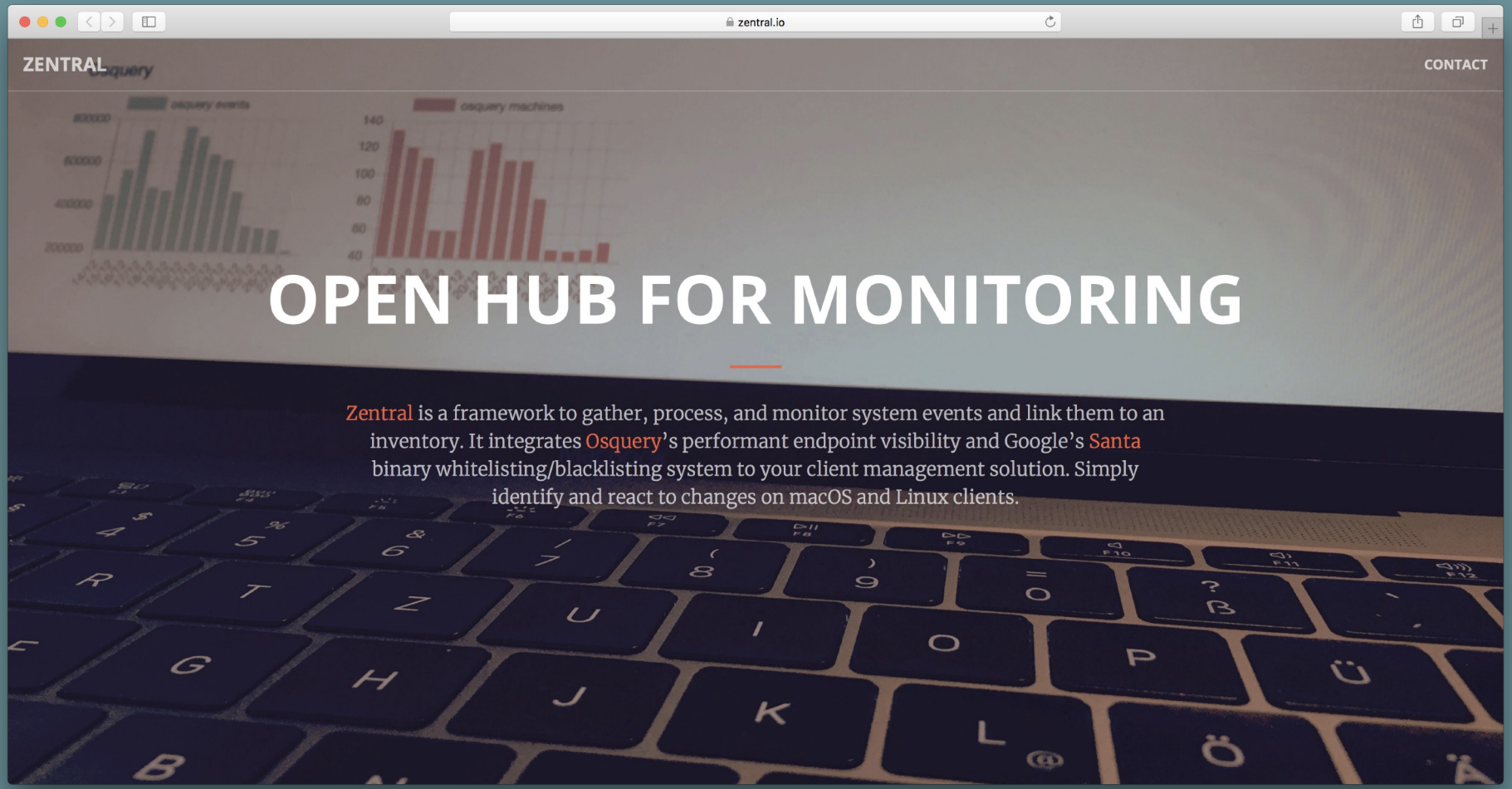
filter when certain event (described) happens

Action

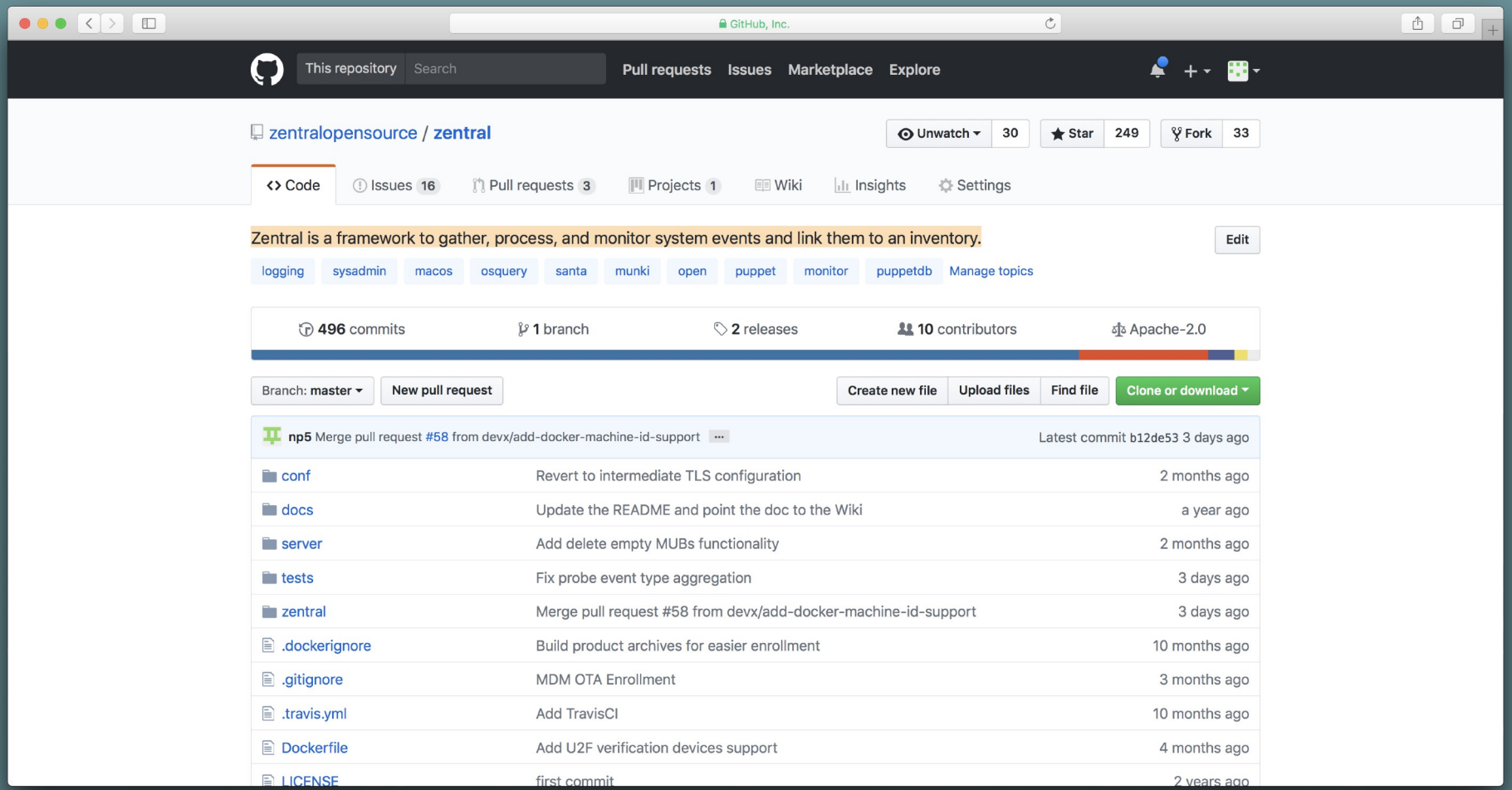
action (clause) execute once the probe fires

>>> Event stream data is stored for historic inspection

https://zentral.io



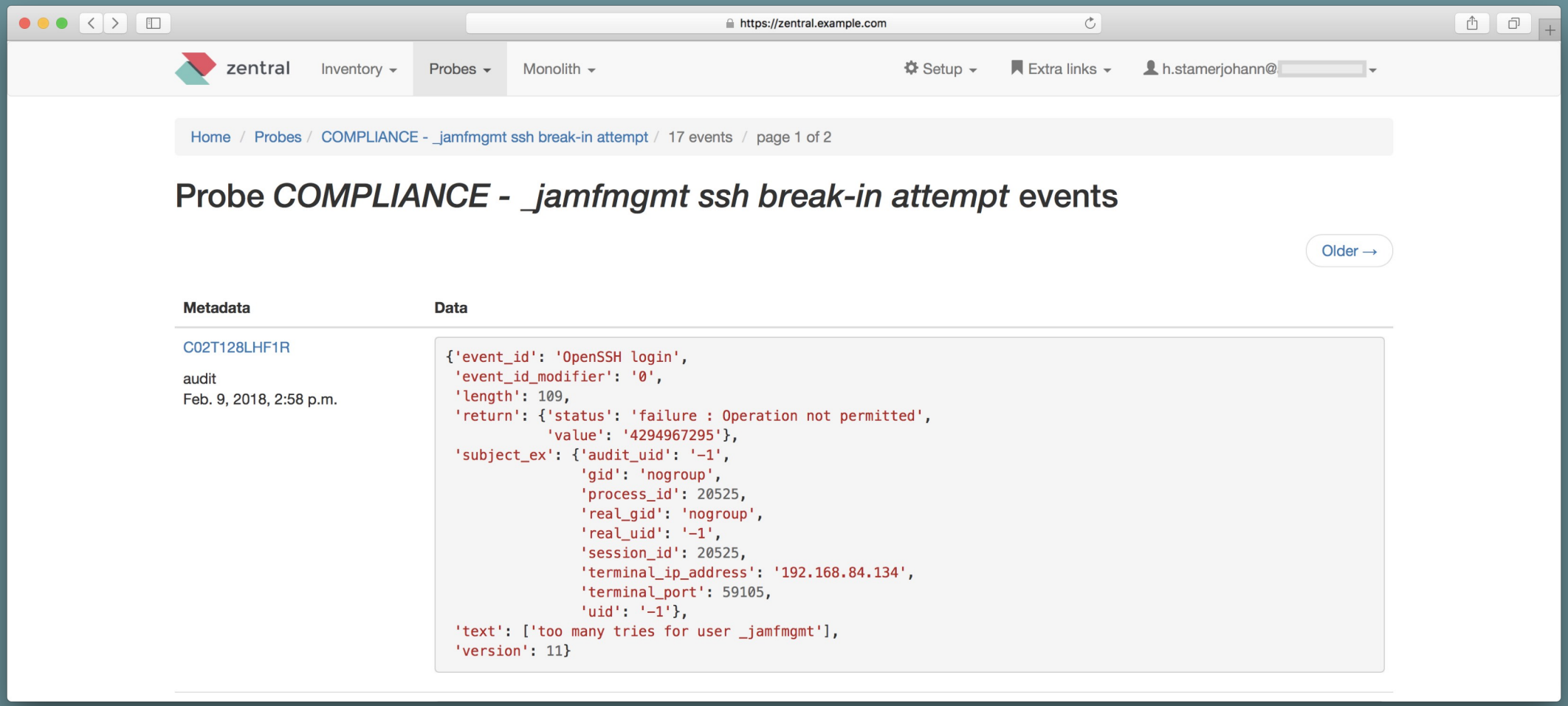
github.com/zentralopensource/zentral



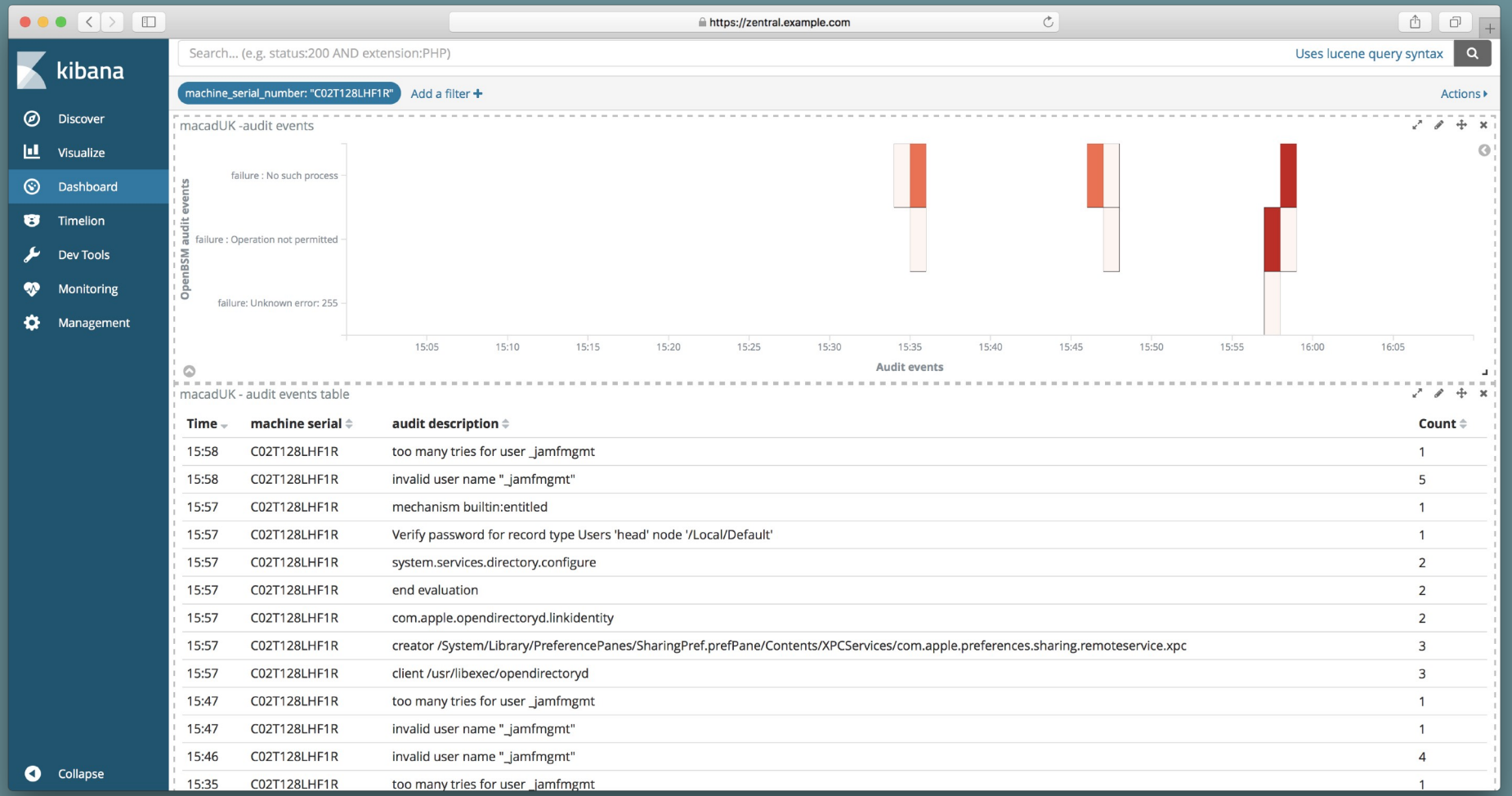
Open BSM audit

```
ssh _jamfmgmt@007-admin-mac
The authenticity of host '007-admin-mac (192.168.84.71)' can't be established.
ECDSA key fingerprint is SHA256:wAjioDIHR8XzAaYMzw71URpSWFLP4U3KjpGIOijUKo.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '007-admin-mac' (ECDSA) to the list of known hosts.
Password:
Password:
Password:
_jamfmgmt@007-admin-mac's password:
Received disconnect from 192.168.84.71 port 22:2: Too many authentication failures
Disconnected from 192.168.84.71 port 22
```

Open BSM audit

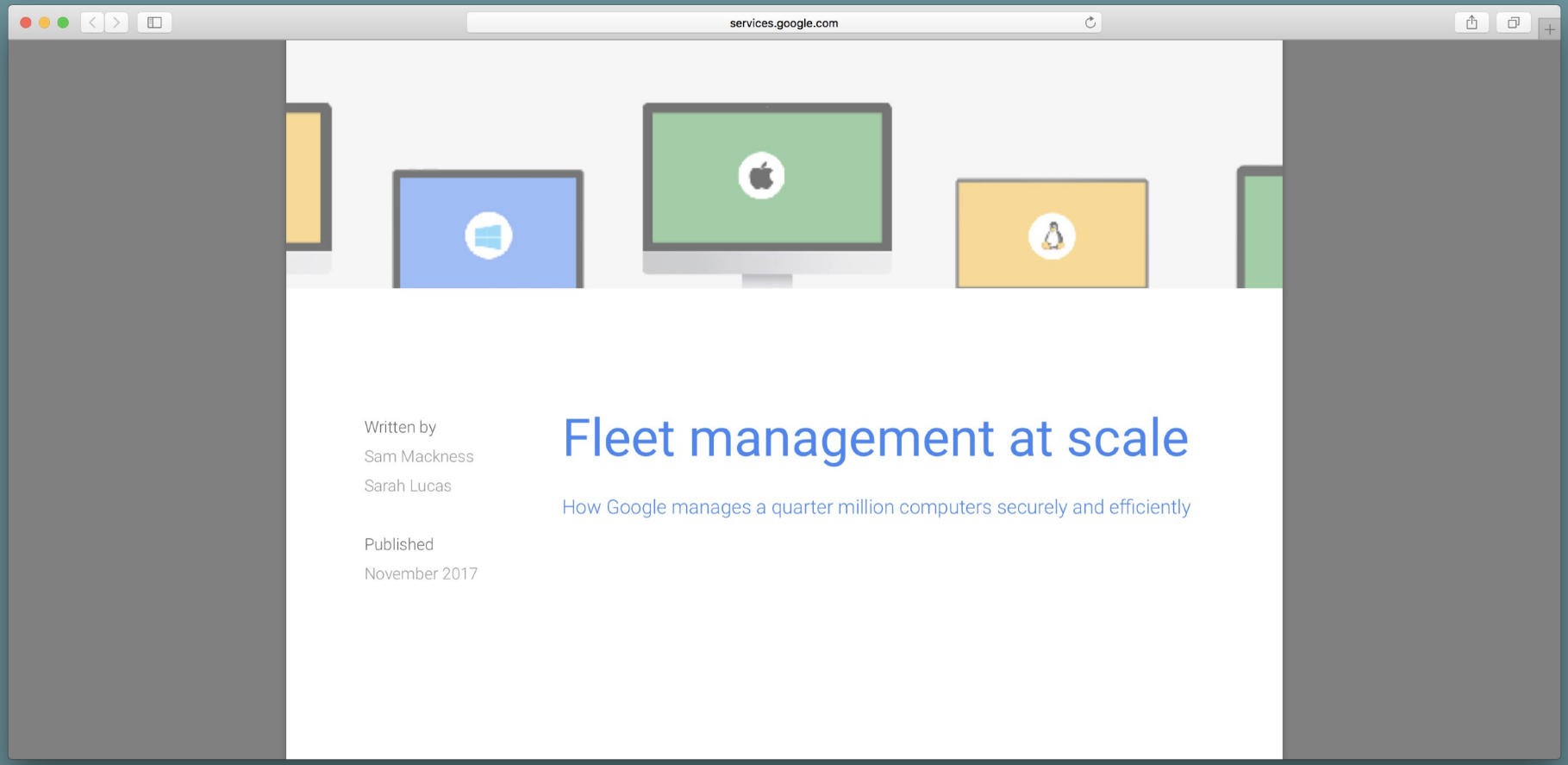


Open BSM audit



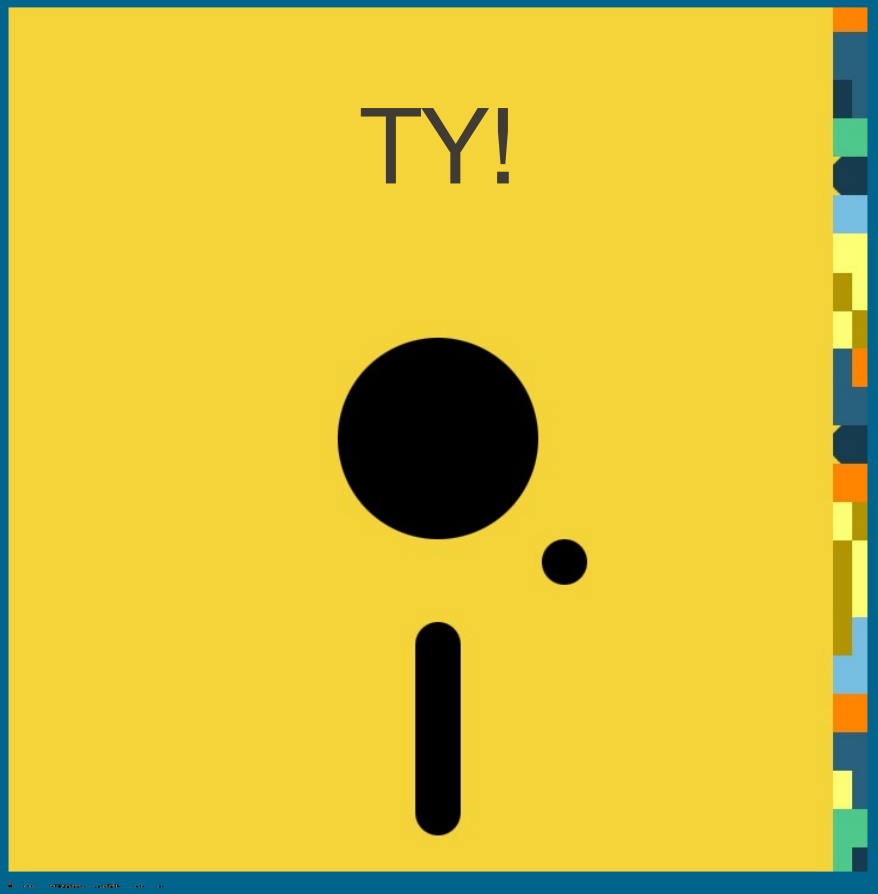
Time	machine serial	audit description	Count
15:58	C02T128LHF1R	too many tries for user _jamfmgmt	1
15:58	C02T128LHF1R	invalid user name "_jamfmgmt"	5
15:57	C02T128LHF1R	mechanism builtin:entitled	1
15:57	C02T128LHF1R	Verify password for record type Users 'head' node '/Local/Default'	1
15:57	C02T128LHF1R	system.services.directory.configure	2
15:57	C02T128LHF1R	end evaluation	2
15:57	C02T128LHF1R	com.apple.opendirectoryd.linkidentity	2
15:57	C02T128LHF1R	creator /System/Library/PreferencePanes/SharingPref.prefPane/Contents/XPCServices/com.apple.preferences.sharing.remoteservice.xpc	3
15:57	C02T128LHF1R	client /usr/libexec/opendirectoryd	3
15:47	C02T128LHF1R	too many tries for user _jamfmgmt	1
15:47	C02T128LHF1R	invalid user name "_jamfmgmt"	1
15:46	C02T128LHF1R	invalid user name "_jamfmgmt"	4
15:35	C02T128LHF1R	too many tries for user _jamfmgmt	1

http://services.google.com/fh/files/misc/fleet_management_at_scale_white_paper.pdf



Rebuild your Security Baseline

Data Protection & Regulation


TY!

Q & A

Links

https://github.com/apfelwerk/macadUK2018-baseline-requirements