

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**"

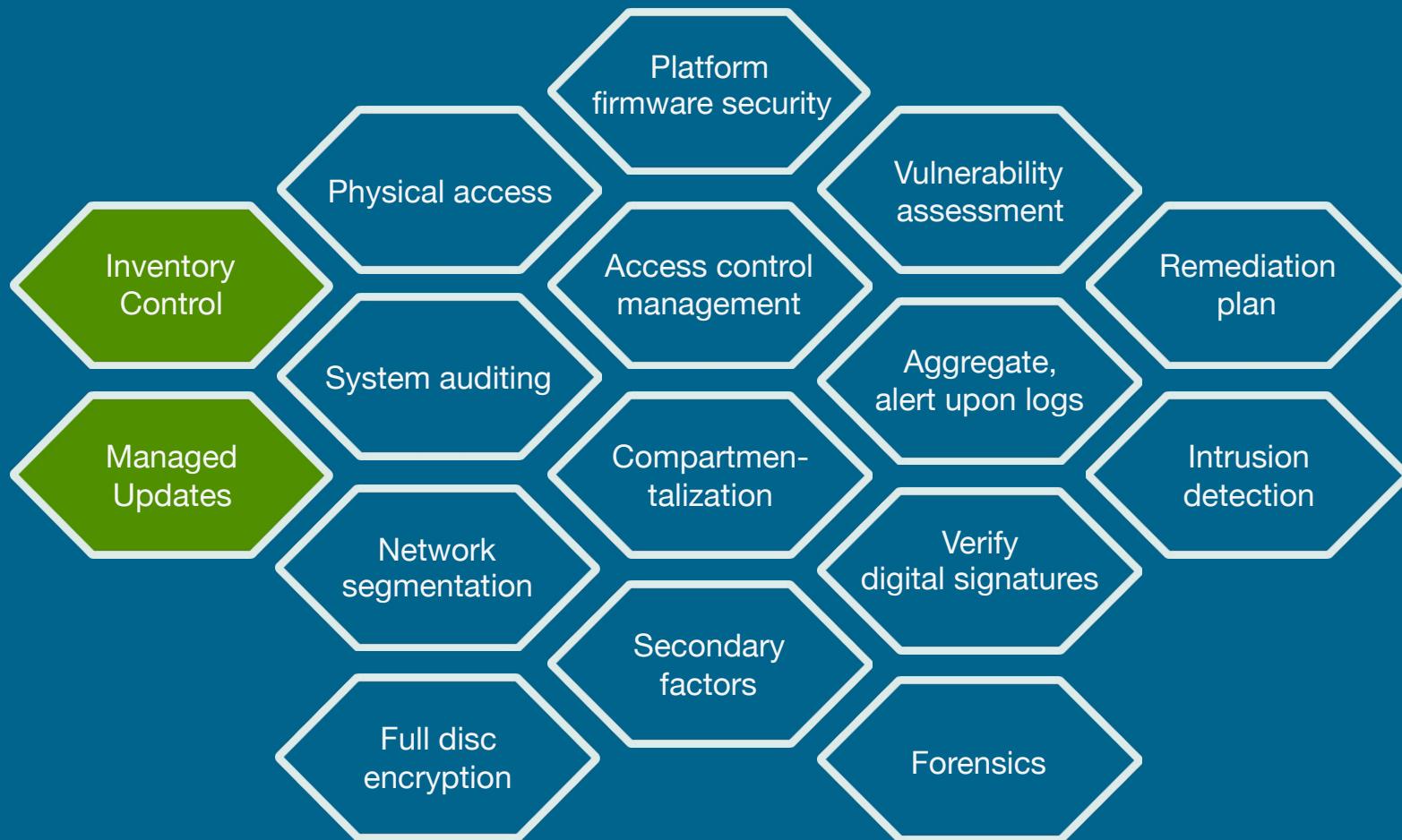
Security TL;DR:

**Make yourself expensive
to attack so that they just
target someone else.**

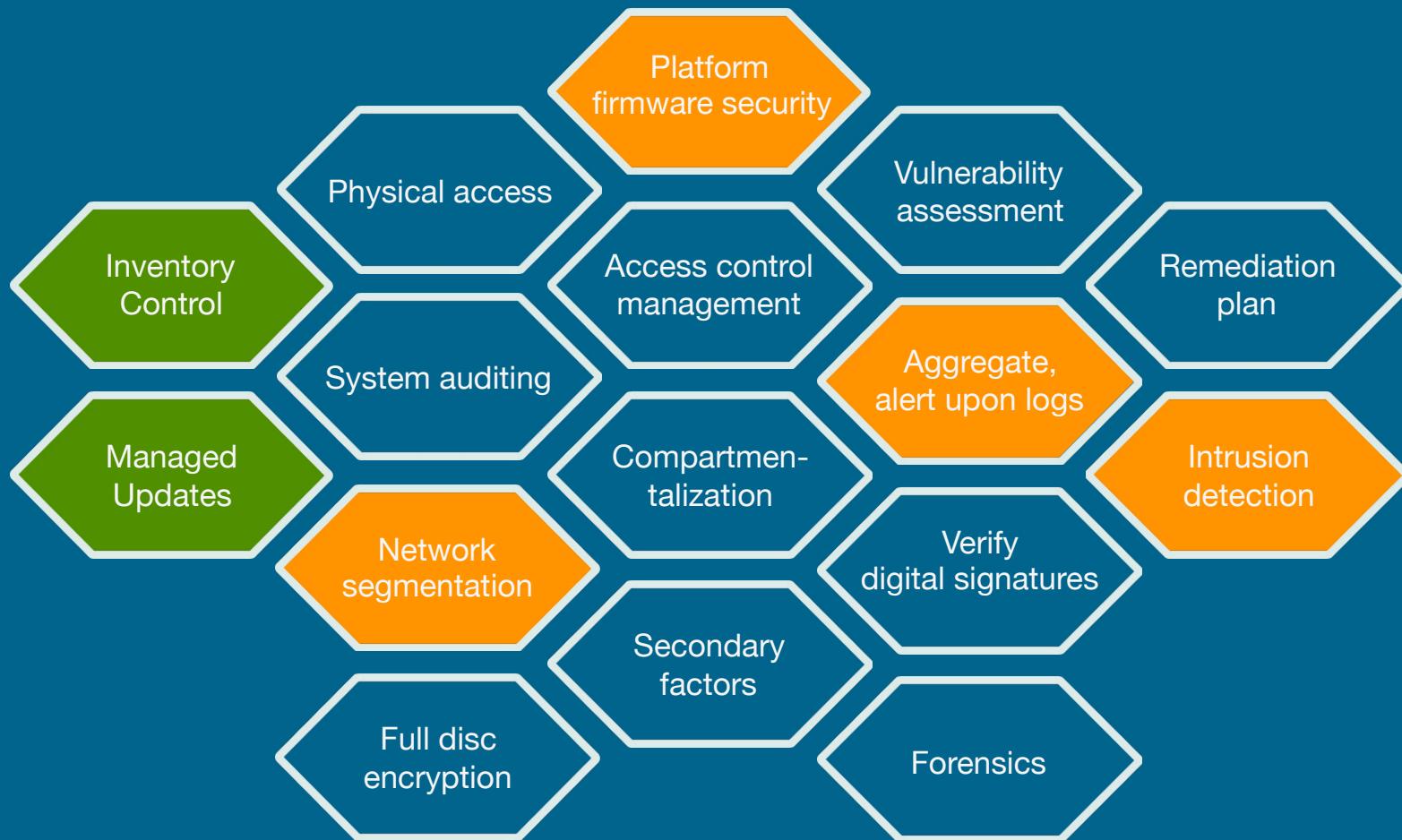


Security Baseline

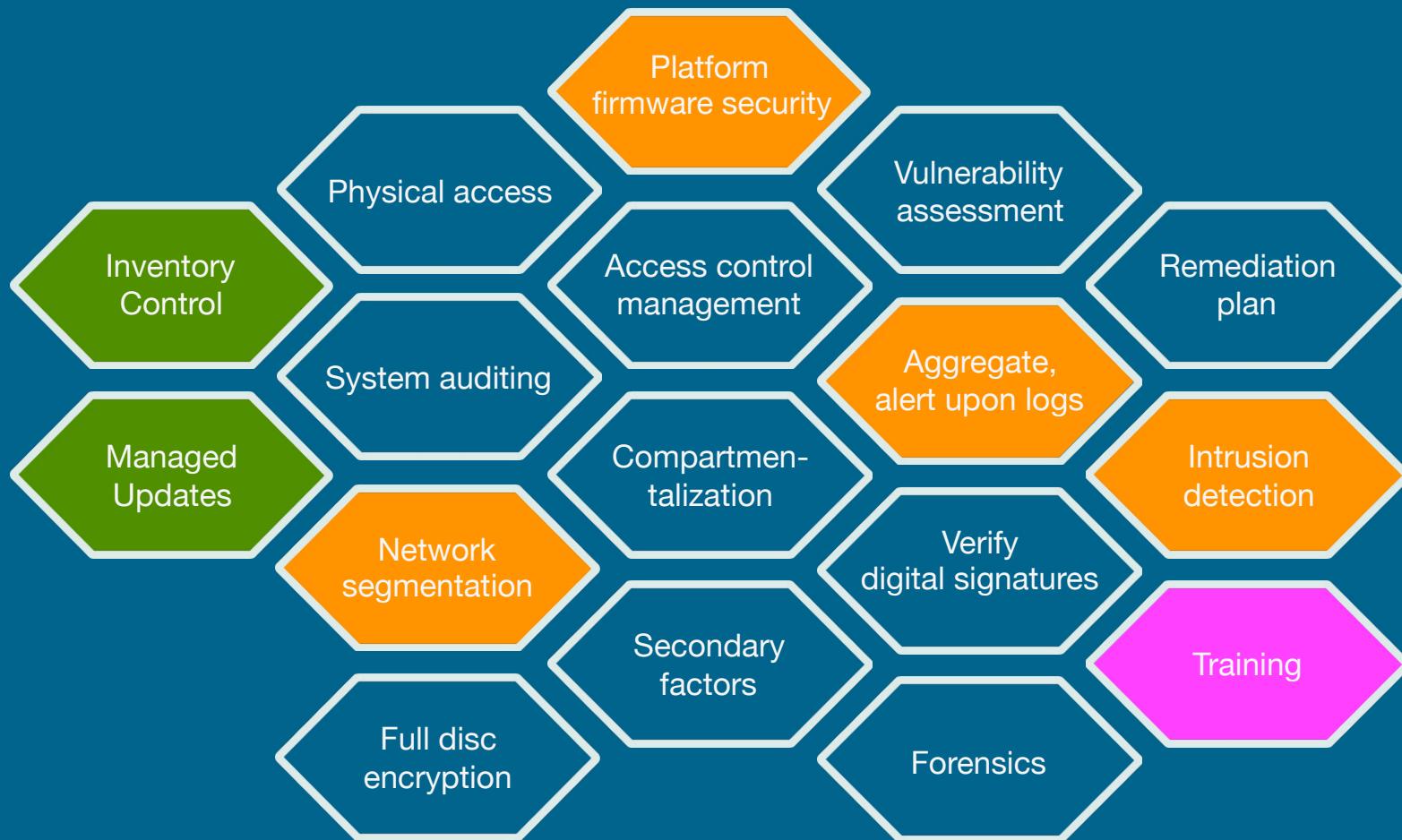
Components



Components



Components



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



The screenshot shows a PDF document titled "Security_Baseline_for_Hardened_PCs_and_Laptops.pdf" (page 1 of 6) open in a Mac OS X window. The left sidebar contains a table of contents:

- History of Changes
- ▼ 1. Security Baseline Requirements
 - 1.1 Access Control & Accounts
 - 1.2 (Network) Interfaces
 - 1.3 Physical Security
 - 1.4 Procedures
 - 1.5 Software & Applications
 - 1.6 Training
 - 1.7 Additional Security Baselines
- 2. References

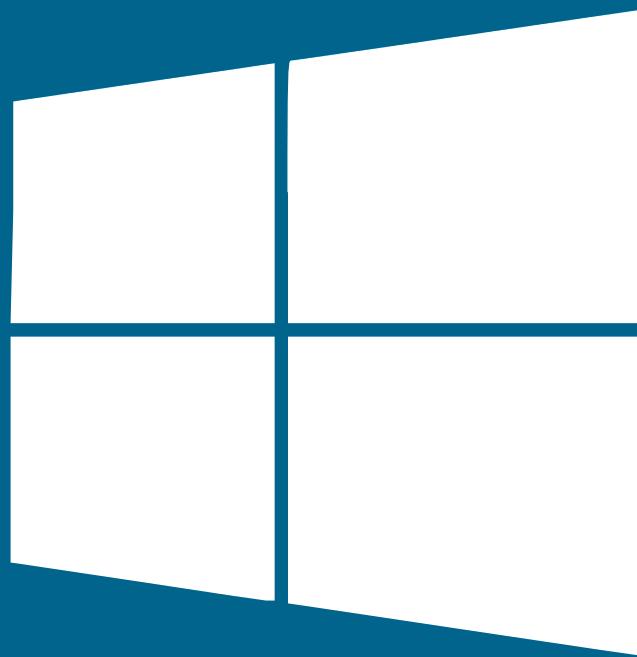
The main content area features a large title:

SECURITY BASELINE FOR HARDEDNED PCS AND LAPTOPS

ABSTRACT A "Security Baseline" defines a set of basic security objectives which must be met by any given service or system. The objectives are chosen to be pragmatic and complete, and do not impose technical means. Therefore, details on how these security objectives are fulfilled by a particular service/system must be documented in a separate "Security Implementation Document" [1]. These details depend on the operational environment a service/system is deployed into, and might, thus, creatively use and apply any relevant security measure. Derogations from the baseline are possible and expected, and must be explicitly marked.

At CERN, for each service/system used in production, such a Security Implementation Document must be produced by its system/service owner, and be accepted and approved by the Computer Security Officer. All systems/services must be implemented and deployed in compliance with their corresponding Security Implementation Document. Non-compliance will ultimately lead to reduced network connectivity for the affected services and systems (i.e. closure of CERN firewall openings, access blocked to other network domains, and/or disconnection from the CERN network).

While also relevant for the "Linux" operating system, this Security Baseline is mainly focussed on PCs and laptops running the "Windows" or "MacOS" operating systems and which are regularly used for accessing unsolicited PDF documents or with frequent professional access to random web sites: used for critical operations in the accelerator



Windows 10 RS2 Security Baseline.xlsx

Open with Microsoft Excel

Policy Path	Policy Setting Name	MDM Area	MDM Policy	MS Baseline	Help Text
Account: Lockout	Account lockout duration			15	<p>Account lockout duration</p> <p>This security setting determines the number of minutes a locked-out account remains locked out.</p> <p>If an account lockout threshold is defined, the account lockout duration must be greater than or equal to the account lockout threshold.</p> <p>Default: None, because this policy setting only has meaning when an Account lockout threshold is defined.</p>
Account: Lockout	Account lockout threshold			10	<p>Account lockout threshold</p> <p>This security setting determines the number of failed logon attempts that causes a user account to be locked out.</p> <p>Failed password attempts against workstations or member servers that have been locked out by this policy setting.</p> <p>Default: 0.</p>
Account: Lockout	Reset account lockout counter after			15	<p>Reset account lockout counter after</p> <p>This security setting determines the number of minutes that must elapse after a failed logon attempt before the account lockout counter is reset.</p> <p>If an account lockout threshold is defined, this reset time must be less than or equal to the account lockout threshold.</p> <p>Default: None, because this policy setting only has meaning when an Account lockout threshold is defined.</p>
Audit Policy	Audit account logon events				<p>Audit account logon events</p> <p>This security setting determines whether the OS audits each time this computer validates credentials.</p> <p>Account logon events are generated whenever a computer validates the credentials.</p> <p>If this policy setting is defined, the administrator can specify whether to audit only successes or both successes and failures.</p> <p>Default: Success.</p>
Audit Policy	Audit account management				<p>Audit account management</p> <p>This security setting determines whether to audit each event of account management.</p> <p>A user account or group is created, changed, or deleted.</p> <p>A user account is renamed, disabled, or enabled.</p> <p>A password is set or changed.</p> <p>If you define this policy setting, you can specify whether to audit successes, audit failures, or both.</p> <p>Default:</p> <p>Success on domain controllers.</p> <p>No auditing on member servers.</p>
Audit Policy	Audit directory service access				<p>Audit directory service access</p> <p>This security setting determines whether the OS audits user attempts to access Active Directory.</p> <p>The administrator can specify whether to audit only successes, only failures, both successes and failures, or both successes and failures.</p> <p>If Success auditing is enabled, an audit entry is generated each time any account succeeds in its attempt to access Active Directory.</p> <p>If Failure auditing is enabled, an audit entry is generated each time any user unsuccessfully attempts to access Active Directory.</p> <p>Default:</p> <p>Success on domain controllers.</p> <p>Undefined for a member computer.</p>
Audit Policy	Audit logon events				<p>Audit logon events</p> <p>This security setting determines whether the OS audits each instance of a user attempting to log on to the system.</p> <p>Log off events are generated whenever a logged on user account's logon session is terminated.</p> <p>Default: Success.</p>
					<p>Audit object access</p> <p>This security setting determines whether the OS audits user attempts to access non-computer objects.</p>

Microsoft Security Compliance Toolkit



CIS_Apple OSX_10.12_Benchmark_v1.0.0.pdf (page 36 of 197)

2.3.3 Verify Display Sleep is set to a value larger than the Screen Saver
(Not Scored)

Profile Applicability:

- Level 1

Description:

If the Screen Saver is used to lock the screen, verify the Display Sleep settings are longer than the Screen Saver setting. If the display goes to sleep before the screen saver activates, the computer will appear to be off, but will be unprotected.

Rationale:

Users of the system can easily assume that the computer is protected when the display goes to sleep. The computer should be configured so that the screen is locked whenever the display turns off automatically.

Audit:

In System Preferences: Energy Saver, verify the slider for "Put the display(s) to sleep..." to a reasonable number, but longer than the screen saver setting. The Mac will display a warning if the number is too short.

Alternatively, use the following command:

```
pmset -g | grep displaysleep
```

and verify the value returned is longer than the Screen Saver, if the Screen Saver is used to lock the screen.

Remediation:

In System Preferences: Energy Saver, drag the slider for "Put the display(s) to sleep..." to a reasonable number, but longer than the screen saver setting. The Mac will display a warning if the number is too short.

Alternatively, use the following command:

```
sudo pmset -c displaysleep 0
```

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

The screenshot shows a GitHub repository page for 'drduh / macOS-Security-and-Privacy-Guide'. The repository has 12,745 stars and 844 forks. It contains 431 commits, 1 branch, and 0 releases. There are 53 contributors. The repository uses the MIT license. The last commit was 20 days ago. The repository includes files like 14F27_launchd.csv, 15B42_launchd.csv, 16A323_launchd.csv, CNAME, InstallESD_Hashes.csv, LICENSE, README-cn.md, README.md, and _config.yml.

A practical guide to securing macOS.

apple macos security privacy osx disk-encryption macos-setup macos-security macbook-security dnsrypt-proxy
macbook-configuration

431 commits 1 branch 0 releases 53 contributors MIT

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

File	Description	Last Commit
14F27_launchd.csv	Describe a few more services, and suggest 'Yosemite-Stop-Launch'. Fix #...	2 years ago
15B42_launchd.csv	Add 10.11.1 services csv.	2 years ago
16A323_launchd.csv	Remove broken line	a year ago
CNAME	Create CNAME	9 months ago
InstallESD_Hashes.csv	Add 10.13.2 (17C88) hashes	a month ago
LICENSE	Initial commit	3 years ago
README-cn.md	Track upstream updates	9 months ago
README.md	Update flash instructions, fix #247	20 days ago
_config.yml	Set theme jekyll-theme-minimal	9 months ago



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 reimagine 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

The screenshot shows a GitHub repository page for 'osx-config-check' by 'kristovatlas'. The repository has 265 commits, 4 branches, 3 releases, 5 contributors, and follows the MIT license. It has 52 watchers, 961 stars, and 93 forks. The repository description is 'Verify the configuration of your OS X machine.' The commit list includes changes for hooks, scripts, .gitignore, CONTRIBUTING.md, LICENSE, README.md, app.py, const.py, dns_helper.sh, hjson_to_json.py, and osx-config.hjson.

Verify the configuration of your OS X machine.

File / Commit	Description	Time Ago
kristovatlas Merge pull request #168 from kristovatlas/v1.1.0-rc1 ...	Latest commit 7ab816d on Oct 6, 2016	
hooks	add pre-commit to convert HJSON to JSON	2 years ago
scripts	fix the disabling of AirDrop	2 years ago
.gitignore	add write functionality to Chrome defaults script	2 years ago
CONTRIBUTING.md	add details about versioning	2 years ago
LICENSE	#151 use MIT license	a year ago
README.md	update sample output in README	a year ago
app.py	bump app version	a year ago
const.py	initial commit	2 years ago
dns_helper.sh	add dns_helper script	2 years ago
hjson_to_json.py	Non-developer users can use JSON instead of HJson	2 years ago
osx-config.hjson	fix config check: chrome pop-ups	2 years ago

#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,..)



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.

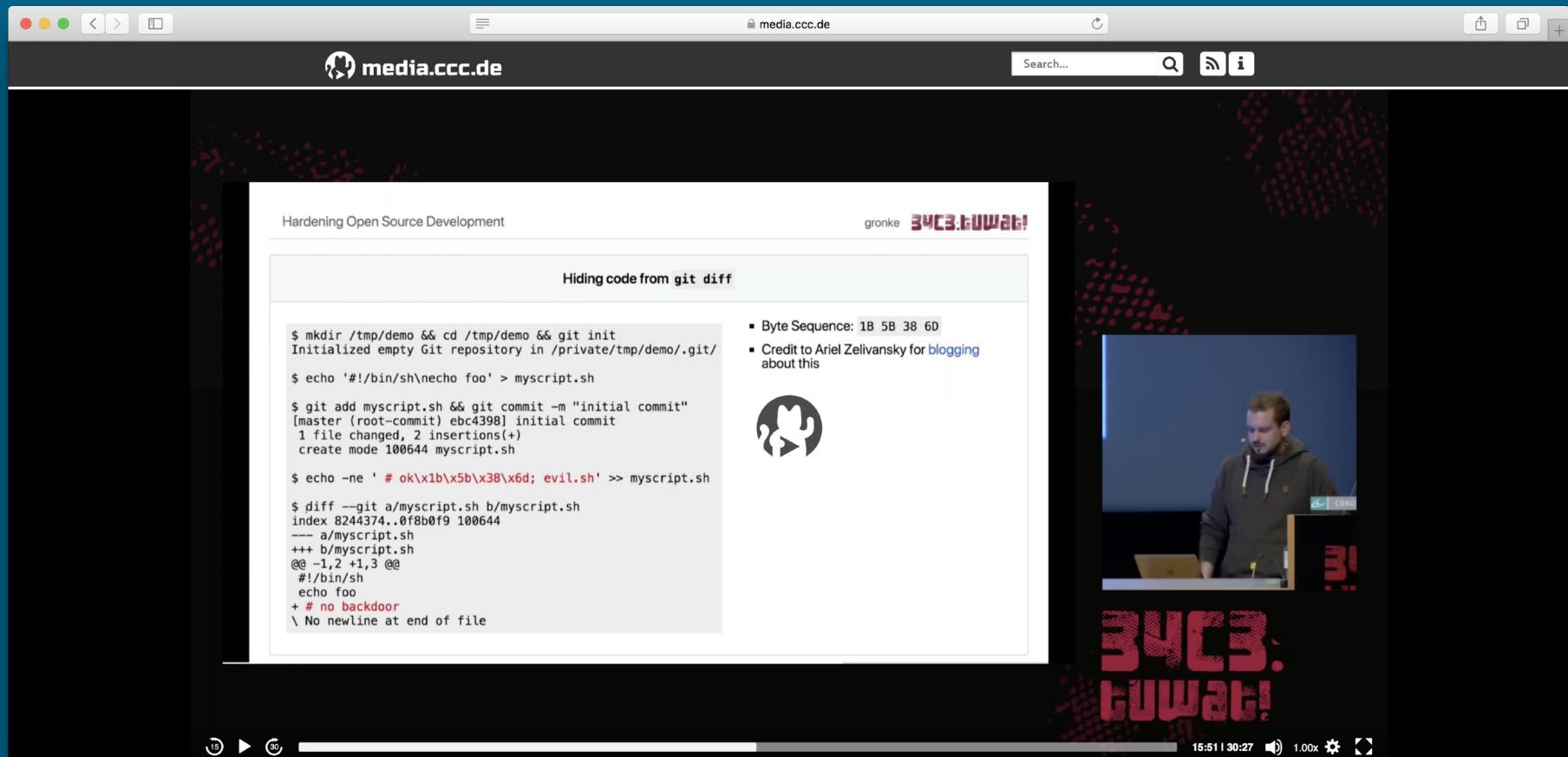
CVE-2017-1000117

Repercussions

Acknowledge risk of executing malicious binaries

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

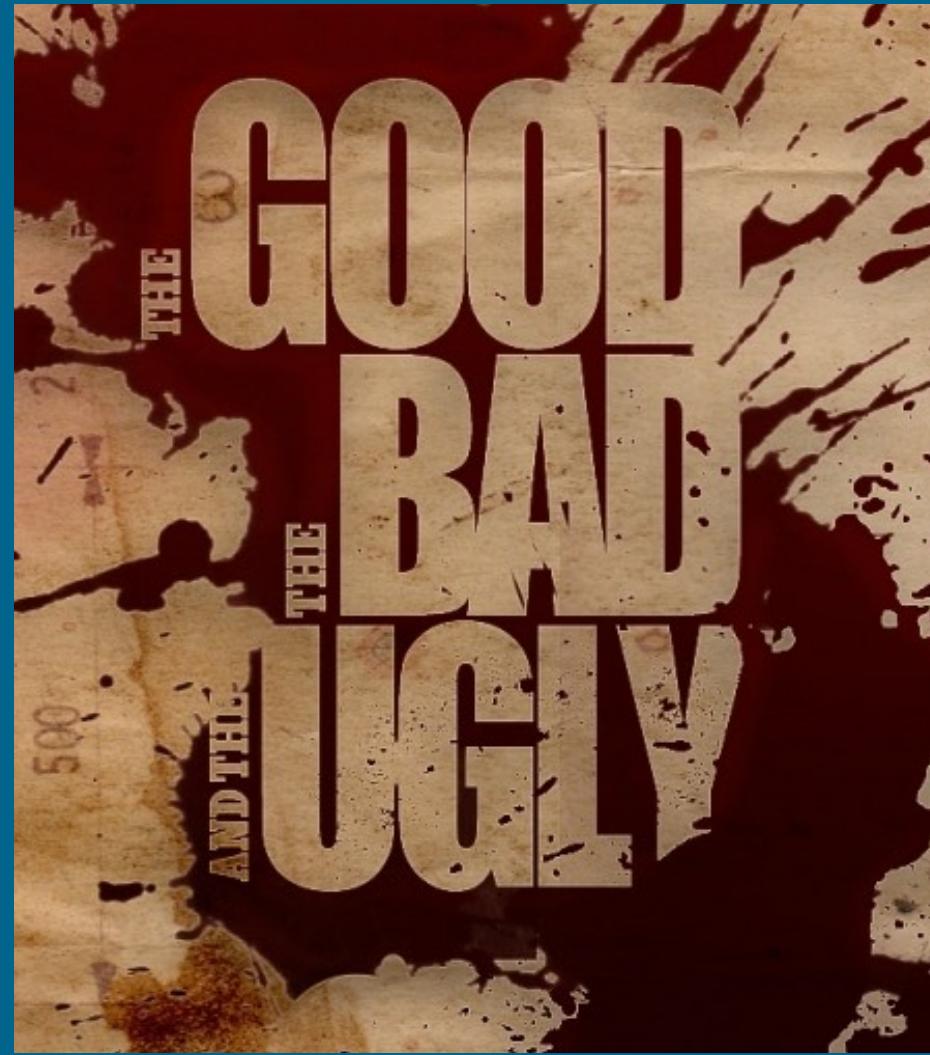
media.ccc.de/v/34c3-9249-hardening_open_source_development



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





www.tenable.com

Support Community Downloads Documentation Education Login

Nessus

Binary download files for Nessus Professional, Nessus Manager, and connecting Nessus Scanners to Tenable.io & SecurityCenter.

Nessus - 7.0.2

Release Date
02/13/2018
Release Notes:
[Nessus 7.0.2](#)

Name	Description	Details
Nessus-7.0.2-es5.x86_64.rpm	Red Hat ES 5 (64-bit) / CentOS 5 / Oracle Linux 5 (including Unbreakable Enterprise Kernel)	Checksum
Nessus-7.0.2-x64.msi	Windows Server 2008, Server 2008 R2*, Server 2012, Server 2012 R2, 7, 8, 10, Server 2016 (64-bit)	Checksum
Nessus-7.0.2-fc20.x86_64.rpm	Fedora 20, 21, 25, 26, 27 (64-bit)	Checksum
Nessus-7.0.2.dmg	macOS (10.8 – 10.13)	Checksum
Nessus-7.0.2-suse11.x86_64.rpm	SUSE 11 Enterprise (64-bit)	Checksum
Nessus-7.0.2-es5.i386.rpm	Red Hat ES 5 i386(32-bit) / CentOS 5 / Oracle Linux 5 (including Unbreakable Enterprise Kernel)	Checksum
Nessus-7.0.2-debian6_i386.deb	Debian 6, 7, 8, 9 / Kali Linux 1, 2017.3 i386(32-bit)	Checksum
Nessus-7.0.2-es7.x86_64.rpm	Red Hat ES 7 (64-bit) / CentOS 7 / Oracle Linux 7 (including Unbreakable Enterprise Kernel)	Checksum

https://www.inspec.io

The screenshot shows the InSpec website homepage. At the top, there's a search bar with a magnifying glass icon. Below it is a navigation bar with links for Tutorials, Docs, Community, Github, Try the Demo, and Download. The main header features the InSPEC logo and the tagline "InSpec is compliance as code". A large, semi-transparent circular overlay on the left contains a small purple triangle icon. The central content area has a blue gradient background with a network graph graphic. Below the tagline, there's a section titled "Automated testing, codified" with a detailed description of what InSpec is. At the bottom, there's a footer with a "FEATURES OF INSPEC" section and a "Get started" button.

InSPEC

inspec.io

Tutorials Docs Community Github Try the Demo Download

InSpec is compliance as code

Automated testing, codified

InSpec is an open-source testing framework for infrastructure with a human-readable language for specifying compliance, security and other policy requirements. Easily integrate automated tests that check for adherence to policy into any stage of your deployment pipeline.

FEATURES OF INSPEC

Get started

```
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 — 109x25
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 — 109x25
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



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.

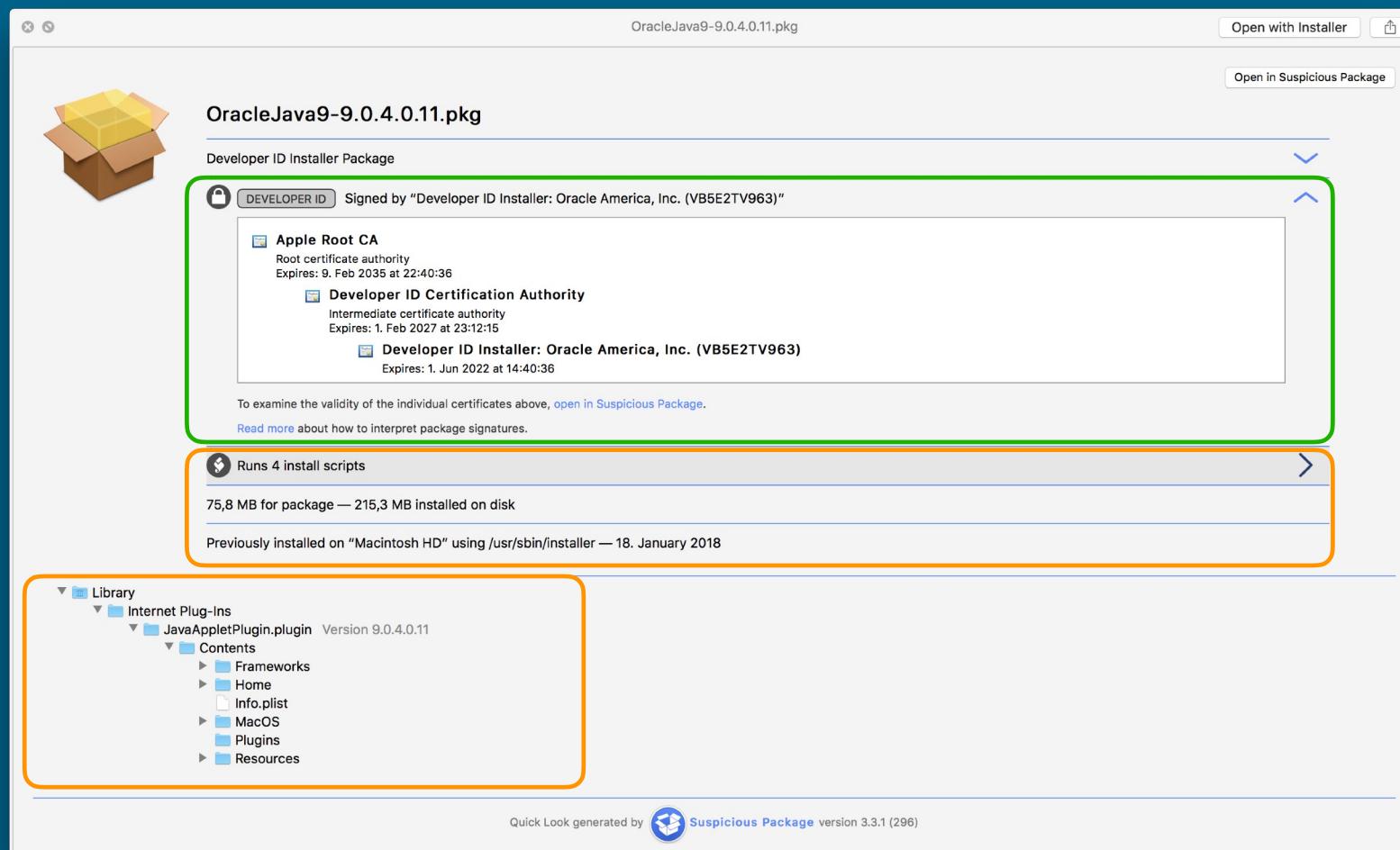
```
$ brew install wget
```

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

name	path	interprete	sha256	main_bundle_exec
unpack200	/Library/Internet Plug-Ins/JavaAppletPlugin.plugin/Contents/Home/bin		cdc164f6ea631d6f8548c3271297e4b8fcf1997b5bee3d47f6f83f7645df3c20d	1
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		940e4a0a3c16d0e0a4cd826f958a26bc7b85611d13804ecc8bc640a65d2b5f	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		d473aef5690447149de80e40e29ee1325c092160a8555a44562807a9c52a935	0
servertool	/Library/Internet Plug-Ins/JavaAppletPlugin.plugin/Contents/Home/bin		6ee25d34b365b42b13364c5e4fa56bc42ca75c07dbe145d76b90668f0959f844	0
orbd	/Library/Internet Plug-Ins/JavaAppletPlugin.plugin/Contents/Home/bin		2655a6f979e2dc0a5bd3931cab9291015d7a4d0661505cb2ffff88bf306b52a4	0
keytool	/Library/Internet Plug-Ins/JavaAppletPlugin.plugin/Contents/Home/bin		84b706d85182024dbf5105f39f2e7c6591cbcd88c8609837e85171be931971b1	0
pack200	/Library/Internet Plug-Ins/JavaAppletPlugin.plugin/Contents/Home/bin		3b6874748fe0a593de93a63cc8e4ce14a1356e26574cf010574b1601b043ecfb	0
jjs	/Library/Internet Plug-Ins/JavaAppletPlugin.plugin/Contents/Home/bin		7d298591edf77b6f3ee7d81549b494f3f61b9f6b4b3fa9b907aa97d043310c9f	0
tnameserv	/Library/Internet Plug-Ins/JavaAppletPlugin.plugin/Contents/Home/bin		d2ec61d606044f6c7313852f4d87ff007b20de2bc823f2e6a4ad83547d39bee	0
jcontrol	/Library/Internet Plug-Ins/JavaAppletPlugin.plugin/Contents/Home/bin		ba5212c07edc29a377068022236fa0820863b09874e0ffd93b43acee306cc8f6	0
JavaWSApplicationStub	/Library/Internet Plug-Ins/JavaAppletPlugin.plugin/Contents/Home/lib/shortcuts		64a414ff9f3699fca07c8b8b77852a892d8890f6ba9a1eb6f8158ff7bbba1b6c	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		3f9229c15dcca316594c1e62eef36aa643533daaa1d91da1b9fa5d61975d0668	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		f9eff9d098debfc65e81216d14ac5a09d8366e2fa18d0a400f72fb9133cb3eb	0

Fingerprint binaries

OracleJava9-9.0.4.0.11.pkg

name	path	interprete	sha256	main_bundle_exec
unpack200	/Library/Internet Plug-Ins/JavaAppletPlugin.plugin/Contents/Home/bin		e74c0d918b09aef73d5439ff1782f2758713266ec7157ac52d234d44da508dc	1
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		0b3a412e5c9f25d5a32ef23b09d6c7b16d9a306d3d1aa7d822fcf98dd35b9dfa	0
rmiregistry	/Library/Internet Plug-Ins/JavaAppletPlugin.plugin/Contents/Home/bin		aa6effdd405f6d1dd6961ba8cb37c46151e4b878c75cc25fe16ceac61af1588ba	0
jrunscript	/Library/Internet Plug-Ins/JavaAppletPlugin.plugin/Contents/Home/bin		5e08613e91b61c566e2db9f9ad47bbfb297b0105f1225b02910e164b051a1985	0
java	/Library/Internet Plug-Ins/JavaAppletPlugin.plugin/Contents/Home/bin		55bb6a3085ef5cfa486b5a3957e6cc018065324a8d99b61bf0cc060a29fc7746	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		6a096375f30f37a9af5d846e8cef45ef259456d52a62c627bbaa167eff64de3	0
orbd	/Library/Internet Plug-Ins/JavaAppletPlugin.plugin/Contents/Home/bin		329761ec52c699d8fc6ef2e11e87c8ae7b0ba99d12ff9b6a2a1b6a71b1b5	0
keytool	/Library/Internet Plug-Ins/JavaAppletPlugin.plugin/Contents/Home/bin		15f40bb7682a066c98d1fa146fb29d203abea525d9e029cae5832a3e93e8148	0
pack200	/Library/Internet Plug-Ins/JavaAppletPlugin.plugin/Contents/Home/bin		483936605e4760b5bc8fc9ed7526b513569e6fb0828e0249560006fd9f10bf	0
jjs	/Library/Internet Plug-Ins/JavaAppletPlugin.plugin/Contents/Home/bin		799c9d86f921250c3d43862c228cb5a974411051c4daf0418570cf52626f9e36	0
tnameserv	/Library/Internet Plug-Ins/JavaAppletPlugin.plugin/Contents/Home/bin		1f9bb289bdc5af5421903f97d03cd9788280b82b0fab28f2a94b16d9deba6	0
jcontrol	/Library/Internet Plug-Ins/JavaAppletPlugin.plugin/Contents/Home/bin		60bb74c8421ce536bbc49efdf8a4741d70d8e4a06a61ce4f5f618e5682c5010	0
JavaWSApplicationStub	/Library/Internet Plug-Ins/JavaAppletPlugin.plugin/Contents/Home/lib/shortcuts		d7e571479afada2425a95ac3b924353dedf8e5ce04fc80bc4ae4039743eb20f	0
jspawnhelper	/Library/Internet Plug-Ins/JavaAppletPlugin.plugin/Contents/Home/lib		c62fe99bffff383e4e828a14a5e86d5211b2b9f478c9e60439b833b634f779f	0
JavaUpdater	/Library/Internet Plug-Ins/JavaAppletPlugin.plugin/Contents/Resources/JavaUpdater.app/Contents/MacOS		ef505ea841e83befc963e33ada4cee0fa3b10c0c0f2823d7e49446b91901317a	0
Helper-Tool	/Library/Internet Plug-Ins/JavaAppletPlugin.plugin/Contents/Resources	/bin/bash	7a2c6e84bb1ff121196777056c1504d31a8348d70acb3f0d67334c9fe4f2a20	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		dc722a5fef1fa460221e2874c418b4389aa6a98935995ebef5c9086e674dc45	0

Inspect for difference in detail

The screenshot shows two windows of the Kaleidoscope application side-by-side, comparing two CSV files: `java-9.0.1.0.11.csv` and `java-9.0.4.0.11.csv`. The left window (A) corresponds to `java-9.0.1.0.11.csv` and the right window (B) corresponds to `java-9.0.4.0.11.csv`. Both windows have a header row and several data rows. The data rows are color-coded in pairs, indicating they are identical between the two versions. The first few rows are as follows:

	A: java-9.0.1.0.11.csv	B: java-9.0.4.0.11.csv
19	Oracle America, Inc. (VB5E2TV963)", "Oracle America, Inc.", VB5E2TV963, 2017-06-03 09:19:36 +0000, 2022-06-04 09:19:36 +0000 ~	Oracle America, Inc. (VB5E2TV963)", "Oracle America, Inc.", VB5E2TV963, 2017-06-03 09:19:36 +0000, 2022-06-04 09:19:36 +0000 ~
20	JavaWSApplicationStub,/Library/Internet Plug-Ins/JavaAppletPlugin.plugin/Contents/Home/lib/shortcuts,,64a414ff9f3699fc07c8d8b77852a892d8890f6ba9a1eb6f8158ff7bba1b6c,0,..... jspawnhelper,/Library/Internet Plug-Ins/JavaAppletPlugin.plugin/Contents/Home/lib,,ef683342502005f896c3c377fb76aba360129e0b16f3835bd8ed39cd1ca052f,0,.....	JavaWSApplicationStub,/Library/Internet Plug-Ins/JavaAppletPlugin.plugin/Contents/Home/lib/shortcuts,,d7e571479afada2425af95ac3b924353dedf8e5ce04fc80bc4ae4039743eb20f,0,..... jspawnhelper,/Library/Internet Plug-Ins/JavaAppletPlugin.plugin/Contents/Home/lib,,c62fe99b8fffff383e4e828a14a5e86d5211b2b9f478c9e60439b833b634f779f,0,.....
21	JavaUpdater,/Library/Internet Plug-Ins/JavaAppletPlugin.plugin/Contents/Resources/JavaUpdater.app/Contents/MacOS,,f51f084d8c15b18070ab5a17b33e3ec589c8298c67dc291d194ec974314c62f3,0,.....	JavaUpdater,/Library/Internet Plug-Ins/JavaAppletPlugin.plugin/Contents/Resources/JavaUpdater.app/Contents/MacOS,,ef505ea841e83befc963e33ada4cee0fa3b10c0c0f2823d7e49446b91901317a,0,.....
22	Helper-Tool,/Library/Internet Plug-Ins/JavaAppletPlugin.plugin/Contents/Resources,/bin/bash,,7a2c6e84bb1ff21196777056c1504d31a8348d70acb3f0d67334c9fe4f2a2a0,0,.....	Helper-Tool,/Library/Internet Plug-Ins/JavaAppletPlugin.plugin/Contents/Resources,/bin/bash,,7a2c6e84bb1ff21196777056c1504d31a8348d70acb3f0d67334c9fe4f2a2a0,0,.....
23	JavawsLauncher,/Library/Internet Plug-Ins/JavaAppletPlugin.plugin/Contents/Resources/JavawsLauncher.app/Contents/MacOS,,7f723fd0926746800d17183859346ce5f47719753e099d126f02737e94bc8ea7,0,.....,359222 959dbdf6454687f66b49cc4d46d8d9d605c144901a6ae6e7807aba7a7d,"Developer ID Application: Oracle America, Inc. (VB5E2TV963)", "Oracle America, Inc.", VB5E2TV963, 2017-06-03 09:19:36 +0000, 2022-06-04 09:19:36 +0000 ~	JavawsLauncher,/Library/Internet Plug-Ins/JavaAppletPlugin.plugin/Contents/Resources/JavawsLauncher.app/Contents/MacOS,,abb44820d934a07b98a151e6d44f0dea2b4f0e3f319caa70b899460ad8c842b,0,.....,359222959dbdf6454687f66b49cc4d46d8d9d605c144901a6ae6e7807aba7a7d,"Developer ID Application: Oracle America, Inc. (VB5E2TV963)", "Oracle America, Inc.", VB5E2TV963, 2017-06-03 09:19:36 +0000, 2022-06-04 09:19:36 +0000 ~
24	JavaControlPanelHelper,/Library/Internet Plug-Ins/JavaAppletPlugin.plugin/Contents/Resources,,3f9229c15dcca316594c1e62eeb36aa643533daaa1d91da1b9fa5d61975d0668,0,.....	JavaControlPanelHelper,/Library/Internet Plug-Ins/JavaAppletPlugin.plugin/Contents/Resources,,2f8103250b892be88f0fc395005a86ac1573f33606dc8ff1834911b3488377c7,0,.....
25	finish_installation,/Library/Internet Plug-Ins/JavaAppletPlugin.plugin/Contents/Frameworks/Sparkle.framework/Versions/A/Resources/finish_installation.app/Contents/MacOS,,38e3063bb8a45ca07ec3d1b69fd8c3d643a8e6039dc2c4a4ac989e4c8567b3,0,.....,359222 959dbdf6454687f66b49cc4d46d8d9d605c144901a6ae6e7807aba7a7d,"Developer ID Application: Oracle America, Inc. (VB5E2TV963)", "Oracle America, Inc.", VB5E2TV963, 2017-06-03 09:19:36 +0000, 2022-06-04 09:19:36 +0000 ~	finish_installation,/Library/Internet Plug-Ins/JavaAppletPlugin.plugin/Contents/Frameworks/Sparkle.framework/Versions/A/Resources/finish_installation.app/Contents/MacOS,,d9834a578556ec7e4d1ae751c20255bca91357c6fd54b4bc7a0705c0d00bef8f,0,.....,359222959dbdf6454687f66b49cc4d46d8d9d605c144901a6ae6e7807aba7a7d,"Developer ID Application: Oracle America, Inc. (VB5E2TV963)", "Oracle America, Inc.", VB5E2TV963, 2017-06-03 09:19:36 +0000, 2022-06-04 09:19:36 +0000 ~
26	com.oracle.java.JavaUpdateHelper,/Library/Internet Plug-Ins/JavaAppletPlugin.plugin/Contents/Frameworks/Sparkle.framework/Versions/A/Resources/finish_installation.app/Contents/Library/,LaunchServices,,f9eff9d098debfcfd65e81216d14ac5a09d8366e2fa18d0a400f72fb9133bc3eb,0,.....,Install new Java Update,com.oracle.java.JavaUpdateHelper,,359222959dbdf6454687f66b49cc4d46d8d9d605c144901a6ae6e7807aba7a7d,"Developer ID Application: Oracle America, Inc. (VB5E2TV963)", "Oracle America, Inc.", VB5E2TV963, 2017-06-03 09:19:36 +0000, 2022-06-04 09:19:36 +0000 ~	com.oracle.java.JavaUpdateHelper,/Library/Internet Plug-Ins/JavaAppletPlugin.plugin/Contents/Frameworks/Sparkle.framework/Versions/A/Resources/finish_installation.app/Contents/Library/,dc722a5fef1fa460221e2874c418b4389aa6a98935995ebef5c9086e674dc45,0,.....,Install new Java Update,com.oracle.java.JavaUpdateHelper,,359222959dbdf6454687f66b49cc4d46d8d9d605c144901a6ae6e7807aba7a7d,"Developer ID Application: Oracle America, Inc. (VB5E2TV963)", "Oracle America, Inc.", VB5E2TV963, 2017-06-03 09:19:36 +0000, 2022-06-04 09:19:36 +0000 ~

Discuss responsibly

macaduk
macdevopsyvr
osquery
santa
security
zentral

Channels 

active directory
adobe
airwatch
announcements

 **apettinen** 12:01 PM
is this new on 10.12.4 /usr/libexec/firmwarecheckers/ethcheck/ethcheck ?
launchdaemon in /S/L/LD/com.apple.driver.ethcheck.plist

 **Daz_Wallace** m 12:03 PM
I don't have it on 10.12.3 MacBook Pro (Retina, 15-Inch, Mid 2014)

 **bbass** 12:03 PM
Not on a 10.12.3 retina iMac, either.

 **apettinen** 12:03 PM
yep, I did not see it in 10.12.3 either
the creation date is 9th of feb

 **Daz_Wallace** m 12:04 PM
No pending firmware updates?

 **apettinen** 12:04 PM
nope
also eficheck
in /usr/libexec/firmwarecheckers/eficheck/eficheck

 **Daz_Wallace** m 12:05 PM
I have no `/usr/libexec/firmwarecheckers` directory

 **apettinen** 12:05 PM
added this Shell snippet: `/usr/libexec/firmwarecheckers/eficheck/eficheck -h` ▾

```
1 usage: eficheck: [ --save -b <EFI bin output file> ]  
2 [ --cleanup -b <EFI bin input/output file> ]  
3 [ --generate-hashes [ -b <EFI bin input file> ] [ -p <Output folder path> ] ]  
4 [ --integrity-check [ -h <EFI hash input file> [ -b <EFI bin input file> ] ] ]  
5 [ --show-hashes [ -h <EFI hash input file> ] | [ -b <EFI bin input file> ] ]
```



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

The screenshot shows the Jamf Pro web interface with the following details:

Left Sidebar:

- jamf PRO
- Computers
- Devices
- Users

Middle Section:

- VERSION: 10.2.0-t1518103206
- MANAGED Computers: 13
- Mobile Devices: 11

Current View: Settings > System Settings > Change Management Logs

Table Headers: DATE/TIME, USERNAME

Table Data:

DATE/TIME	USERNAME
02/11/2018 at 1:23 PM	MaxMustermann
02/11/2018 at 1:22 PM	MaxMustermann
02/11/2018 at 1:12 PM	MaxMustermann
02/11/2018 at 1:12 PM	hs
02/11/2018 at 1:09 PM	hs
02/11/2018 at 1:09 PM	hs
02/11/2018 at 1:08 PM	hs
02/11/2018 at 12:46 PM	hs

Details Dialog: A modal window titled "Details" displays configuration settings for a specific log entry (ID: 109). The settings include:

Setting	Value
ID	109
Name
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 per day
Available Offline	false
Scope	No scope
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

Buttons: OK (blue)

```
# 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

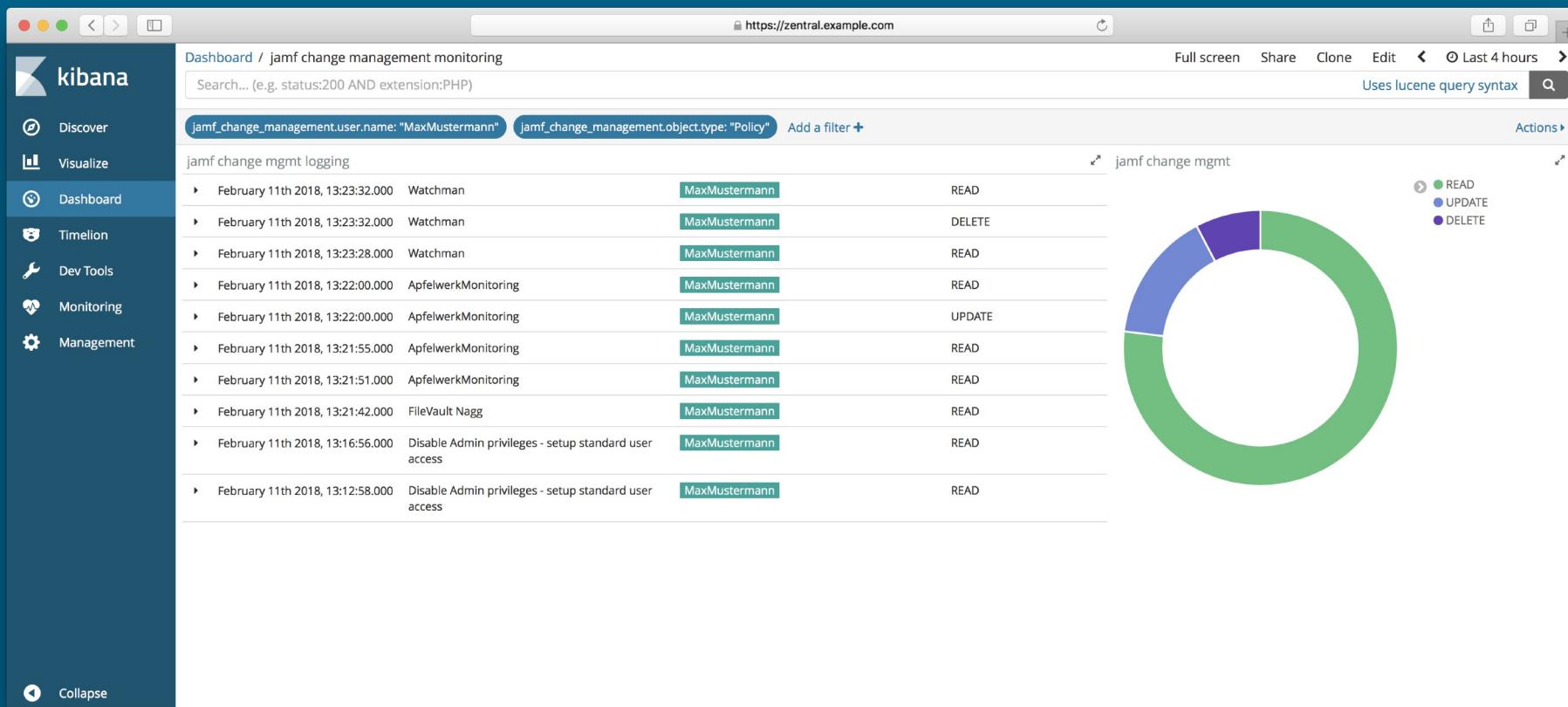
The screenshot shows a Kibana dashboard titled "jamf change management monitoring". The left sidebar includes links for Discover, Visualize, Dashboard (which is selected), Timelion, Dev Tools, Monitoring, and Management. The main area displays a table of log entries under the heading "jamf change mgmt logging". The table has columns for Time, jamf_change_management.object.name, jamf_change_management.user.name, and jamf_change_management.action. Two entries are listed:

Time	jamf_change_management.object.name	jamf_change_management.user.name	jamf_change_management.action
February 11th 2018, 13:22:00.000	ApfelwerkMonitoring	MaxMustermann	UPDATE
February 11th 2018, 13:12:57.000	Disable Admin privileges - setup standard user access	MaxMustermann	UPDATE

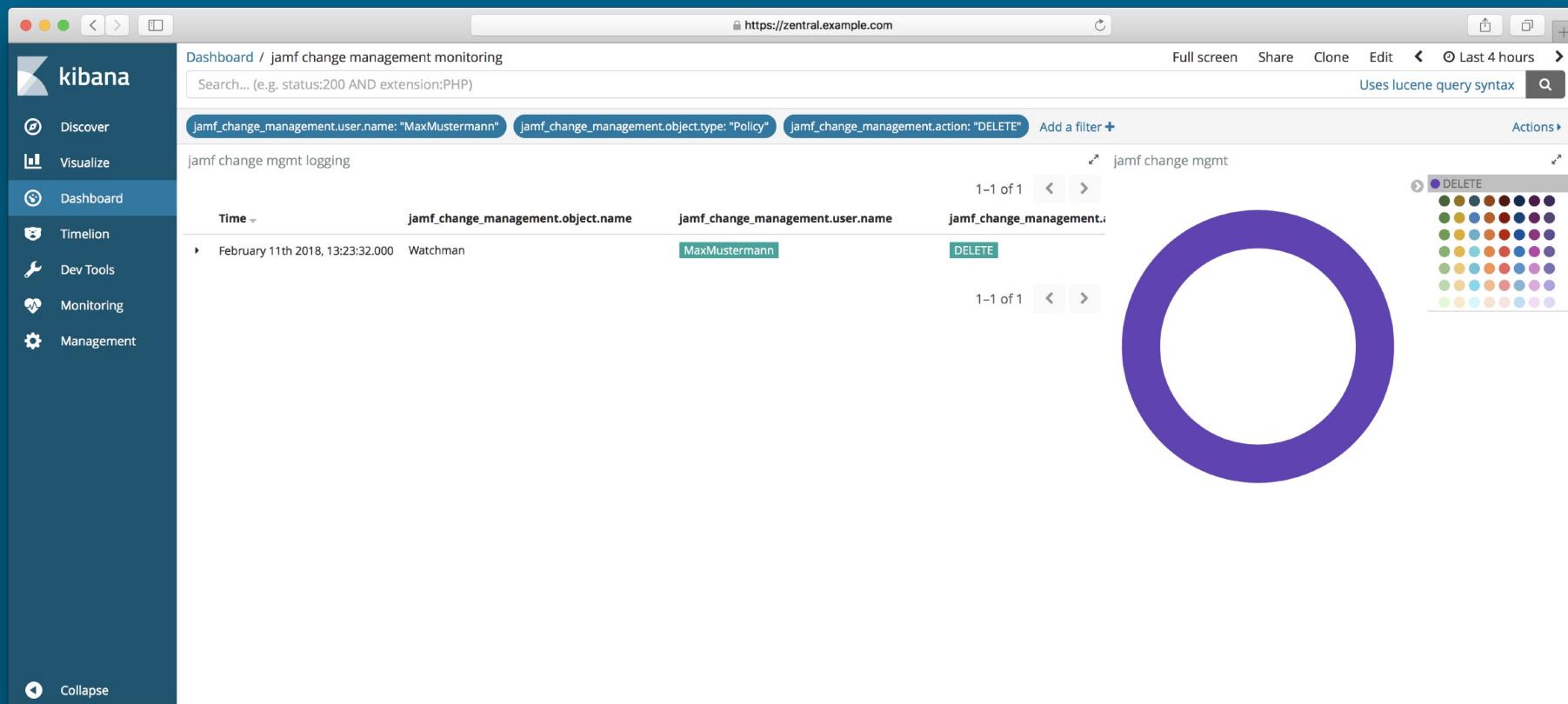
Below the table, there are two tabs: "Table" (selected) and "JSON". The "JSON" tab displays the raw log data as follows:

```
1 {  
2   "_index": "zentral-events-2018-02-08",  
3   "_type": "doc",  
4   "_id": "U1_IhGEDIUhG5NgXaKO",  
5   "_version": 1,  
6   "_score": null,  
7   "_source": {  
8     "created_at": "2018-02-11T12:12:57+00:00",  
9     "id": "aba46f7a-b92d-4ec6-b1e8-562cae4304fb",  
10    "index": 0,  
11    "type": "jamf_change_management",  
12    "tags": [  
13      "jamf",  
14      "jamf_beat"  
15    ],  
16    "jamf_change_management": {  
17      "action": "UPDATE",  
18      "object": {  
19        "type": "Policy",  
20        "id": 109,  
21        "name": "Disable Admin privileges - setup standard user access",  
22        "enabled": false,  
23        "triggered_by_check-in": false,  
24      }  
25    }  
26  }  
27 }  
28 }
```

Log aggregation



Log aggregation



A screenshot of a Kibana dashboard titled "jamf change management monitoring". The dashboard is filtered by "jamf_change_management.user.name: 'MaxMustermann'", "jamf_change_management.object.type: 'Policy'", and "jamf_change_management.action: 'DELETE'". The results show a single log entry from February 11th, 2018, at 13:23:32.000, which details a "Watchman" object being deleted by "MaxMustermann". A large purple circle is overlaid on the right side of the dashboard.

Dashboard / jamf change management monitoring

Search... (e.g. status:200 AND extension:PHP)

jamf_change_management.user.name: "MaxMustermann" jamf_change_management.object.type: "Policy" jamf_change_management.action: "DELETE" Add a filter +

Full screen Share Clone Edit Last 4 hours Actions > Uses lucene query syntax

jamf change mgmt logging

jamf change mgmt

Time jamf_change_management.object.name jamf_change_management.user.name jamf_change_management.i

February 11th 2018, 13:23:32.000 Watchman MaxMustermann DELETE

1-1 of 1

1-1 of 1

DELETE

Collapse

http://dev-sec.io

Hardening Framework

dev-sec.io

Features Articles Docs Team Community

Overview

Hardening Framework Components

	Applications	Operations	OS	Network
✓ Applications	MySQL PostgreSQL	Apache Nginx	Logging / Monitoring User Management Patch-management	SSH Hardening Operating System Hardening
✗ Operations				Intrusion Detection Firewall
✓ OS				
✗ Network				

✓ included ✗ not in scope

The screenshot shows a web browser window with the URL <http://dev-sec.io> in the address bar. The page content is divided into two main sections: "OS Hardening" and "SSH Hardening".

OS Hardening

Secure the base operating system

PAM Configures pam and pam_limits	Permissions Restrict the permissions by setting SUID bits and configuring system paths.	Verified Packages Verifies only signed packages are installed.	Sysctl Set secure kernel parameters
---	---	--	---

[Chef GitHub](#) [Chef Supermarket](#) [Puppet GitHub](#) [Puppet Forge](#) [Ansible GitHub](#) [Ansible Galaxy](#)

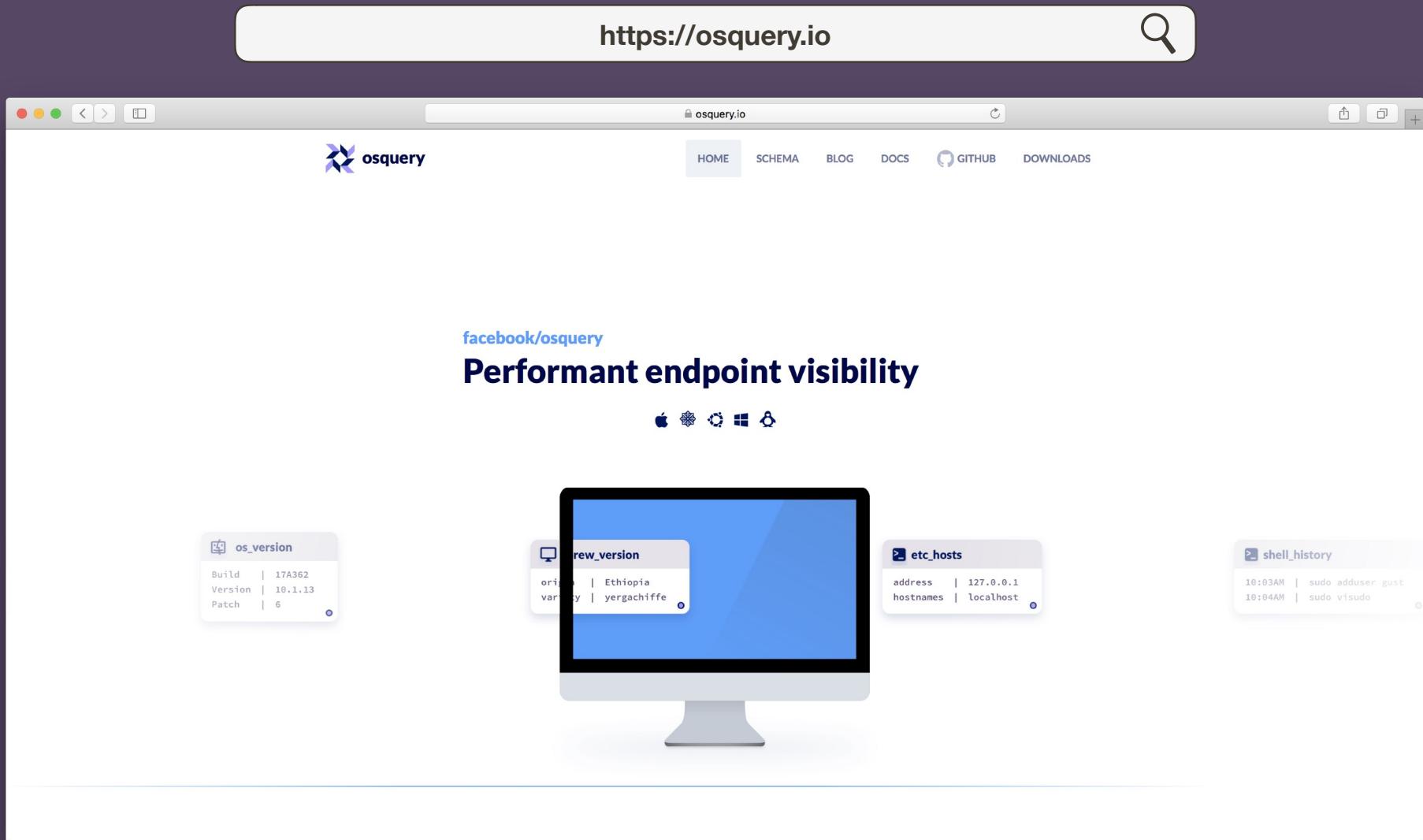
SSH Hardening

Secure configuration of SSH

Secure Ciphers Configures SSH with secure ciphers.	Configuration Configures the ssh client and server with industry best-practices.	Certificate Authentication Deactivates password authentication and enables the secure certificate authentication.	User Management Leave the user management with their authorization to you, thus enabling a smooth integration without changing existing infrastructure.
--	--	---	---

OSQuery

(Change detection)





194 Tables

- plist
- portage_keywords
- portage_packages
- portage_use
- power_sensors
- preferences
- process_envs
- process_events
- process_file_events
- process_memory_map
- process_open_files
- process_open_sockets
- processes
- programs
- prometheus_metrics
- python_packages
- quicklook_cache
- registry
- routes
- rpm_package_files
- rpm_packages
- safari_extensions
- sandboxes

platform_info
Information about EFI/UEFI/ROM and platform/boot.

[Improve this Description on Github](#)

COLUMN	TYPE	DESCRIPTION
vendor	TEXT	Platform code vendor
version	TEXT	Platform code version
date	TEXT	Self-reported platform code update date
revision	TEXT	BIOS major and minor revision
address	TEXT	Relative address of firmware mapping
size	TEXT	Size in bytes of firmware
volume_size	INTEGER	(Optional) size of firmware volume
extra	TEXT	Platform-specific additional information

plist
Read and parse a plist file.

[Improve this Description on Github](#)

COLUMN	TYPE	DESCRIPTION
key	TEXT	Preference top-level key
subkey	TEXT	Intermediate key path, includes lists/dicts
value	TEXT	String value of most CF types
path	TEXT	(optional) read preferences from a plist

<https://osquery.io>



A curated list of community projects to help you use and extend osquery.

The screenshot shows a grid of nine community projects, each with a GitHub link. The projects are:

- airbnb / streamalert** ★ 1100
StreamAlert is a serverless, realtime data analysis framework which empowers you to ingest, analyze, and
- mwielgoszewski / doorman** ★ 337
an osquery fleet manager
- zentralopensource / zentral** ★ 248
Zentral is a framework to gather, process, and monitor system events and link them to an inventory.
- kolide / fleet** ★ 207
A flexible control server for osquery fleets
- palantir / osquery-configuration** ★ 126
A repository for using osquery for incident detection and response
- kolide / launcher** ★ 91
Osquery launcher, autoupdater, and packager
- osquery / osquery-python** ★ 86
python bindings for osquery
- heroku / windmill** ★ 78
A TLS endpoint for serving osquery configuration
- kolide / osquery-go** ★ 77
Go bindings for Osquery

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>



Screenshot of the GitHub repository page for `google / santa`.

The repository summary shows:

- Code: 741 commits
- Branches: 3 branches
- Releases: 35 releases
- Contributors: 12 contributors
- Licence: Apache-2.0

Recent commits:

File	Message	Time Ago
config	tburgin config: use KVO (#234)	Latest commit fc87cde 2 days ago
Conf	project/config: Move /var/log/santa.log to /var/db/santa/santa.log (#173)	9 months ago
Docs	docs: updated configuration details (#232)	16 days ago
Santa.xcodeproj	config: use KVO (#234)	2 days ago
Santa.xcworkspace	Check in xcworkspace	3 years ago
Source	config: use KVO (#234)	2 days ago
Tests	santa-driver: add an acknowledge feature to allow timeouts (#220)	14 days ago
.clang-format	Project: Add clang-format file, apply most of the fixes it suggested	2 years ago
.gitignore	Update .gitignore (#211)	4 months ago
.travis.yml	Project: Add bundler caching to travis build (#95)	a year ago
CONTRIBUTING.md	Update style guide links	2 years ago
LICENSE	Initial commit	3 years ago

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



The screenshot shows a macOS-style browser window with a red header bar containing the URL. The main content area displays the Santa documentation on [santa.readthedocs.io](https://santa.readthedocs.io/en/latest/). The page title is "Welcome to the Santa Docs". The left sidebar has a red header "Santa" and a search bar. It lists several sections: "Introduction", "Welcome to Santa", "Binary Whitelisting Overview", "Syncing Overview", "Deployment", "Configuration", "Development", "Building", "Details", "santa-driver", "santad", "santactl", "santabs", "santa-gui", "mode", "events", "rules", "scopes", and "syncing". The "Binary Whitelisting Overview" section is currently selected and highlighted in dark grey. The main content area starts with a heading "Welcome to Santa Docs" and a paragraph about Santa being a binary whitelisting/blacklisting system for macOS. It then lists sections for "Introduction", "Deployment", "Development", and "Details". Under "Details", there is a "Binaries" section which describes the five main components of Santa.

Docs » Introduction » Welcome to Santa

Welcome to the Santa Docs

Santa is a binary whitelisting / blacklisting system for macOS. Here you will find the documentation for understanding how Santa works, how to deploy it and how to contribute.

Introduction

The following documents give an overview of how Santa accomplishes binary whitelisting / blacklisting at the enterprise scale.

- [Binary Whitelisting](#): How Santa makes allow or deny decisions for any `execve()` taking place.
- [Syncing](#): How configuration and whitelist / blacklist rules are applied from a sync server.

Deployment

- [Configuration](#): The local and sync server configuration options.

Development

- [Building Santa](#): How to build and load Santa for testing on a development machine.
- [Contributing](#): How to contribute a bug fix or new feature to Santa.

Details

For those who want even more details on how Santa works under the hood, this section is for you.

Binaries

There are five main components that make up Santa whose core functionality is described in snippets below. For additional detail on each component, visit their respective pages. These quick descriptions do not encompass all the jobs performed by each component, but do provide a quick look at the basic

```
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 — 108x32
→ ~ 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 — 108x32
Code-signed          : No
Rule                 : Whitelisted (Scope)

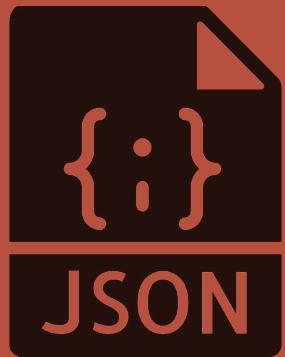
Path                : /usr/local/Cellar/openssl/1.0.2n/share/man/man3/SSL_want.3ssl
SHA-256             : 431169ef71eef6bafb60b6cc2e9668df3e626d1e20d1cd703678e2046fbb82f
SHA-1               : f2155a75244f9c38598d47064263c3844e45a782
Type                : Unknown
Code-signed          : No
Rule                 : Whitelisted (Scope)

Path                : /usr/local/Cellar/openssl/1.0.2n/share/man/man3/ripemd.3ssl
SHA-256             : fb0830337e463212baff3e3826539c76d3e573e4c207dd2efb58d2e97b0cce90e
SHA-1               : b8cb2d3534519c9d7f0bf874b1cc171143776bfc
Type                : Unknown
Code-signed          : No
Rule                 : Whitelisted (Scope)

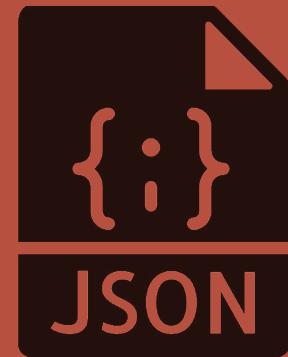
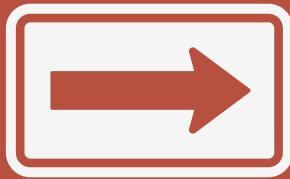
Path                : /usr/local/Cellar/openssl/1.0.2n/share/man/man3/d2i_SSL_SESSION.3ssl
SHA-256             : d476b930334787ebc5b2afd9328338275d9de77c5628479d29598deb2cdcd5cd
SHA-1               : c9a6333829cc7ec3cc7d910487fee59ca3152add
Type                : Unknown
Code-signed          : No
Rule                 : 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

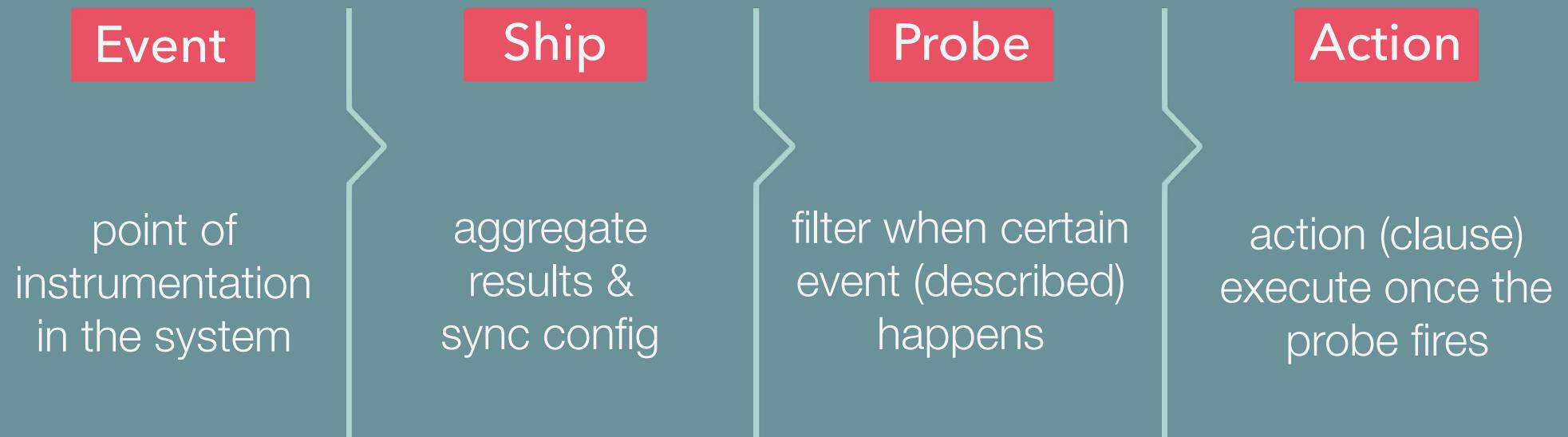


brew-openssl-1.0.2h.json



brew-openssl-1.0.2n.json

Event streams



>>> Event stream data is stored for historic inspection

<https://zentral.io>



The screenshot shows a web browser window for the URL <https://zentral.io>. The page title is "ZENTRAL Osquery". On the left, there are two bar charts: one for "osquery events" (green bars) and one for "osquery machines" (red bars). The main headline reads "OPEN HUB FOR MONITORING". Below the headline, a paragraph describes Zentral as a framework for monitoring system events and linking them to an inventory, mentioning its integration with Osquery and Santa. The background of the page features a close-up image of a dark computer keyboard.

ZENTRAL Osquery

CONTACT

OPEN HUB FOR MONITORING

Zentral is a framework to gather, process, and monitor system events and link them to an inventory. It integrates Osquery's performant endpoint visibility and Google's Santa binary whitelisting/blacklisting system to your client management solution. Simply identify and react to changes on macOS and Linux clients.

github.com/zentralopensource/zentral

The screenshot shows a GitHub repository page for the 'zentral' project. The repository has 496 commits, 1 branch, 2 releases, and 10 contributors. The latest commit was b12de53, made 3 days ago. The repository is licensed under Apache-2.0. The page includes tabs for Code, Issues (16), Pull requests (3), Projects (1), Wiki, Insights, and Settings. It also features a search bar and navigation icons.

Zentral is a framework to gather, process, and monitor system events and link them to an inventory.

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

File	Description	Time Ago
conf	Revert to intermediate TLS configuration	2 months ago
docs	Update the README and point the doc to the Wiki	a year ago
server	Add delete empty MUBs functionality	2 months ago
tests	Fix probe event type aggregation	3 days ago
zentral	Merge pull request #58 from devx/add-docker-machine-id-support	3 days ago
.dockerignore	Build product archives for easier enrollment	10 months ago
.gitignore	MDM OTA Enrollment	3 months ago
.travis.yml	Add TravisCI	10 months ago
Dockerfile	Add U2F verification devices support	4 months ago
LICENSE	first commit	2 years ago

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:wAji0DIHR8XzAaYMzw71URpSWFLP4U3KjpGI0ijUKo.
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

The screenshot shows a web browser window for the zentral platform at <https://zentral.example.com>. The page displays an audit event from a probe named "COMPLIANCE - _jamfmgmt ssh break-in attempt".

Probe COMPLIANCE - *_jamfmgmt ssh break-in attempt* events

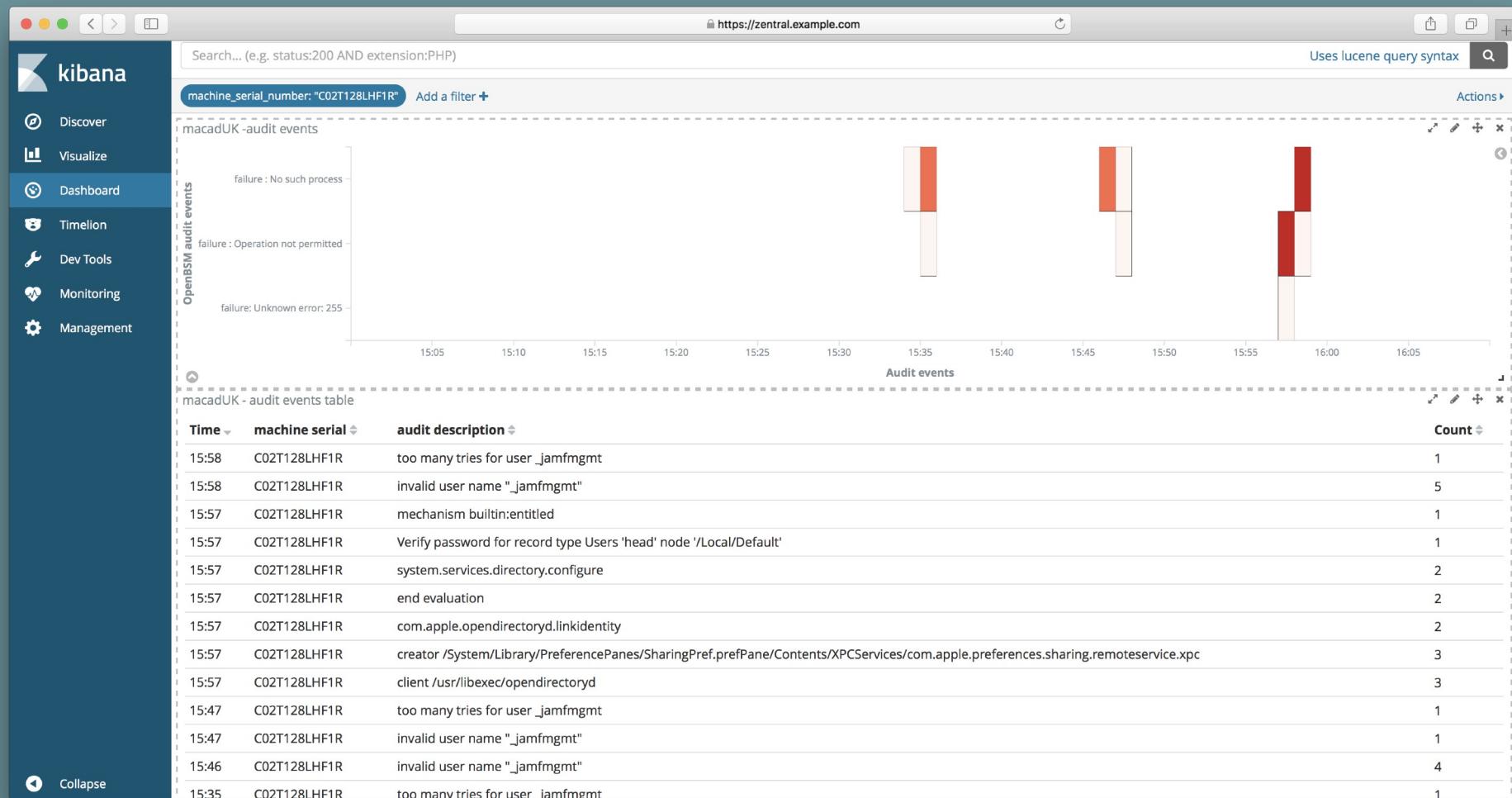
Metadata

C02T128LHF1R
audit
Feb. 9, 2018, 2:58 p.m.

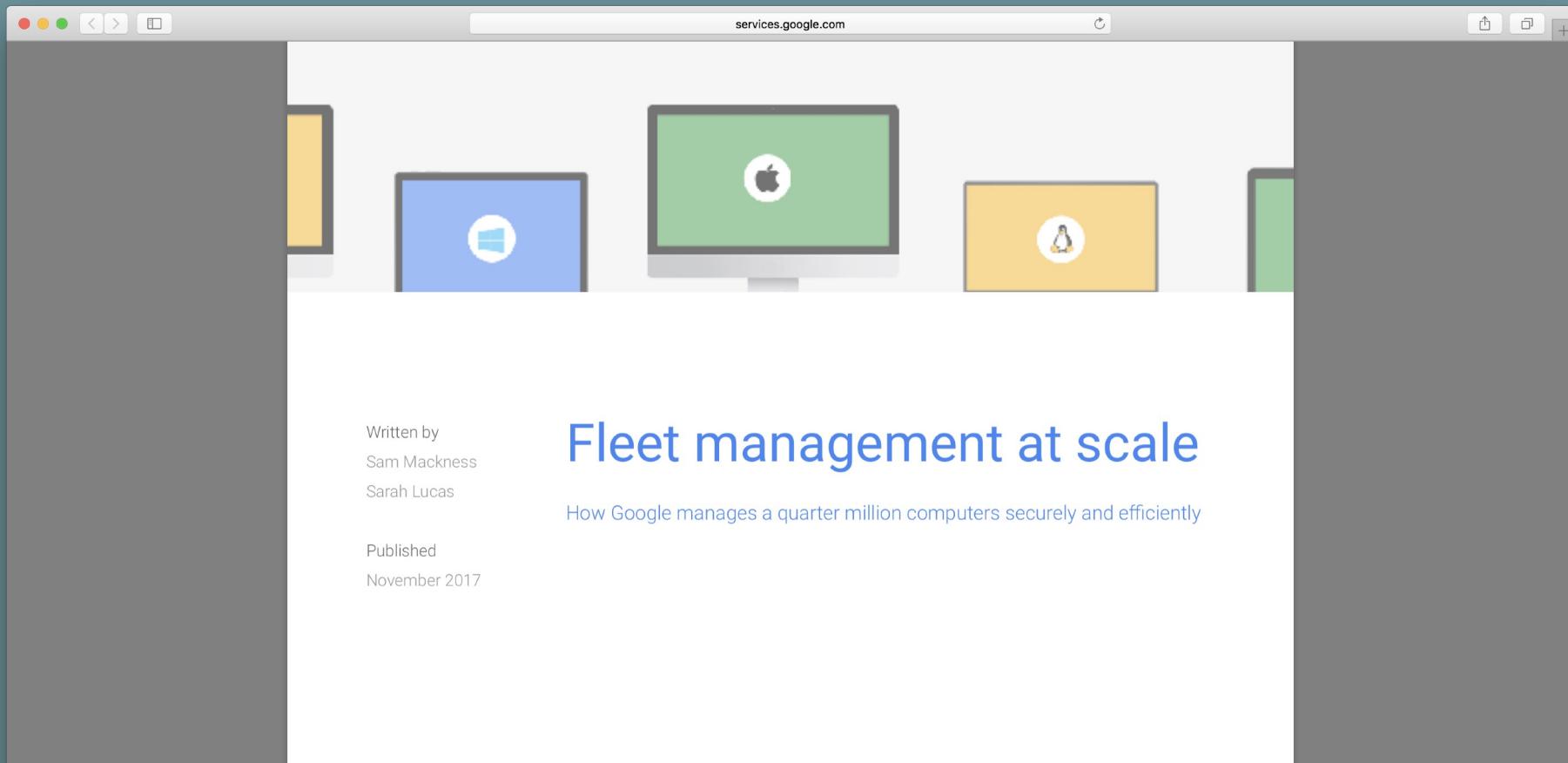
Data

```
{'event_id': 'OpenSSH login',
 'event_id_modifier': '0',
 'length': 109,
 'return': {'status': 'failure : Operation not permitted',
            'value': '4294967295'},
 'subject_ex': {'audit_uid': '-1',
                'gid': 'nogroup',
                'process_id': 20525,
                'real_gid': 'nogroup',
                'real_uid': '-1',
                'session_id': 20525,
                'terminal_ip_address': '192.168.84.134',
                'terminal_port': 59105,
                'uid': '-1'},
 'text': ['too many tries for user _jamfmgmt'],
 'version': 11}
```

Open BSM audit



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



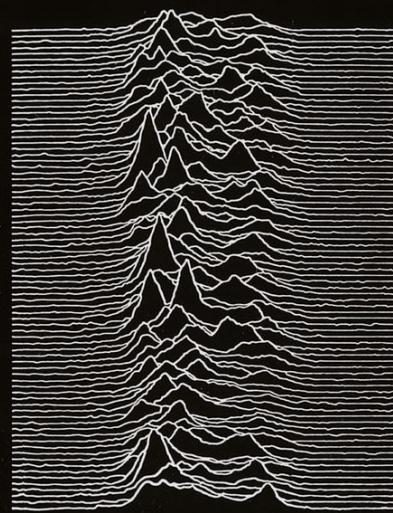
Rebuild your
Security Baseline

Data Protection & Regulation

TY!



Q & A



Links



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