Automating CIS Benchmark Reporting and Remediation

JAMF NATION LIVE

Agenda

1 | macOS Security

Have a look what Apple has been doing on the security stack and build into the system.

2 | Security Benchmarks

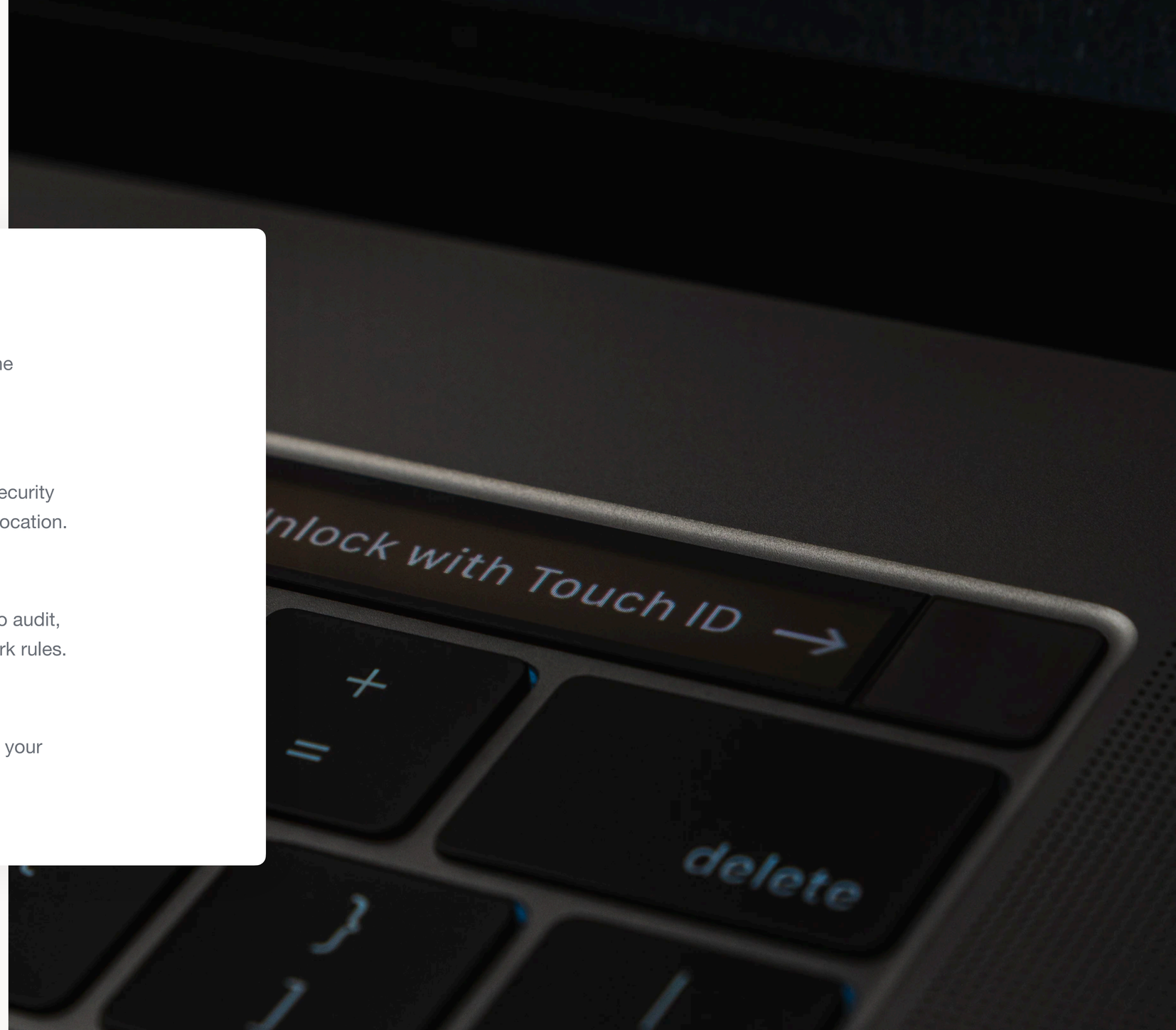
Organisations that provide guidance of the Security standard depending on industry and/or geo-location.

3 | Scripts

How we can use the CIS-Script to help you to audit, remediate and report based on the Benchmark rules.

4 | Implementation

See how easy it is to deploy the CIS script in your environment.



Business is **changing**

JAMF NATION LIVE

Employee mobility
Work **anywhere**

JAMF NATION LIVE

Protecting Corporate & Customer **Data**

JAMF NATION LIVE

Security & Compliance

JAMF NATION LIVE

AEM **Platform**

Manage your Devices

Apple Ecosystem Management

ENTERPRISE

Jamf Pro

SMB

Jamf Now

EDUCATION

Jamf School

DATA POLICY

Jamf Data Policy

Connect your Users

Identity & Access Control

MAC ACCOUNT & SECURE AUTHENTICATION

Jamf Connect

ZTNA NETWORK ACCESS

Jamf Private Access

Protect your Data

Endpoint Security

macOS THREAT DETECT & PREVENTION

Jamf Protect

iOS DEVICE THREAT DETECT & PREVENTION

Jamf Threat Defence

Complete your Solution

Value-Added Workflows

EDUCATION

- Teacher
- Student
- Parent

HEALTHCARE

- Patient Experience
- Clinical Communication
- Virtual Visits

X-INDUSTRY

- Set-up and Reset for Shared Devices and workflow

Connect your Users

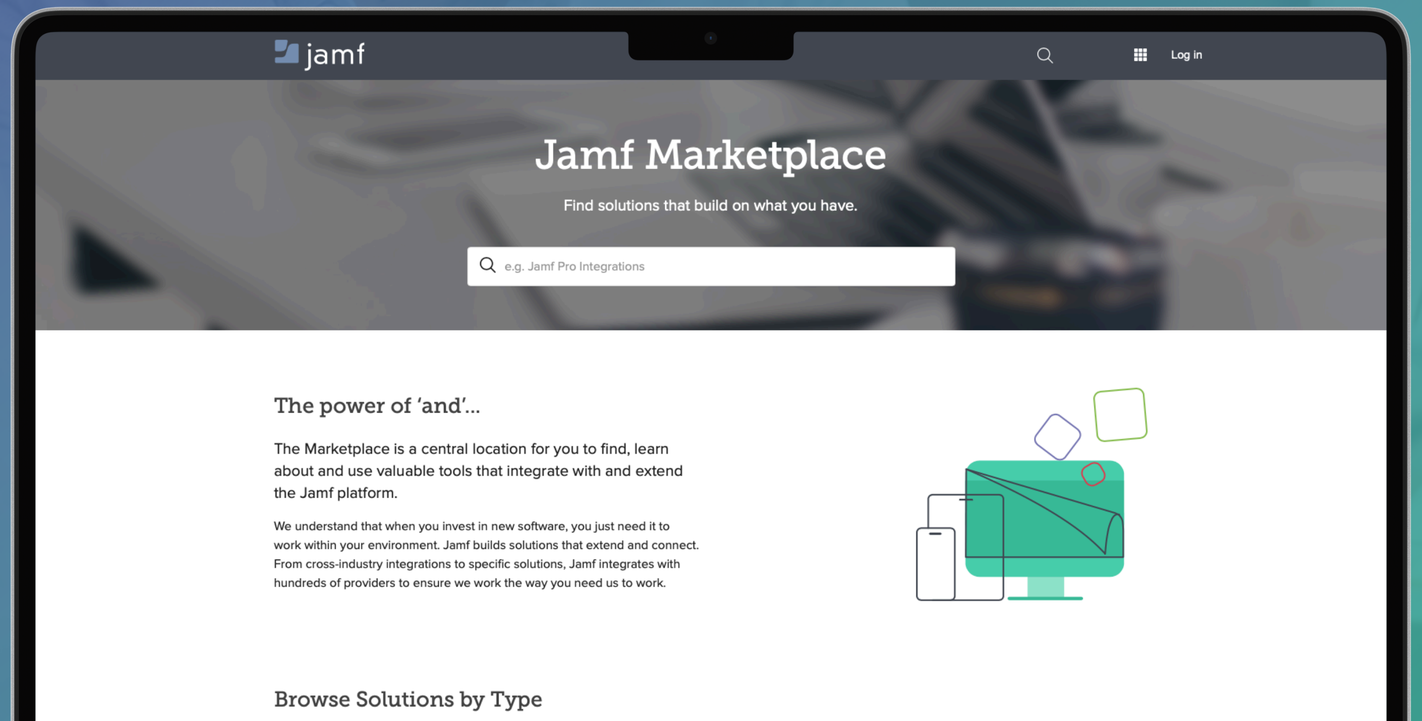
Manage your Devices

Protect your Data

Amplify the power of Jamf with integrations, apps and open-source tools

Jamf Marketplace

Expanded Ecosystem and Support Strengthen the Jamf Platform and Improve Jamf Efficiency



JAMF NATION LIVE

macOS Security

JAMF NATION LIVE

Enterprise-grade security
that’s built right in.

JAMF NATION LIVE

UNIX

Apple File System

Mobile Device Management

Password Protection

Secure Enclave

Malware Removal Tool

Secure Authentication

Runtime Protection

FileVault

Access Rights

Configuration Enforcement

Mandatory Access Controls

Encrypted Disk Images

Touch ID

System Integrity Protection

Keychains

XProtect

Automatic Security Updates

Cryptographic Validation

Gatekeeper

Firewall

App Transport Security

ISO Certification

System Extensions

VPN On-Demand

Smart Cards

Digital Signing and Encryption

VPN

Secure Boot

Restrictions

Firmware Password

Per-app VPN

Remote Wipe

Single Sign-On

Per-message S/MIME

App Code Signing

Sandboxing

Internet Recovery

AirDrop Security

Remote Lock

JAMF NATION LIVE

Security Benchmarks

Center for Internet Security

Defense Information Security Agency (US)

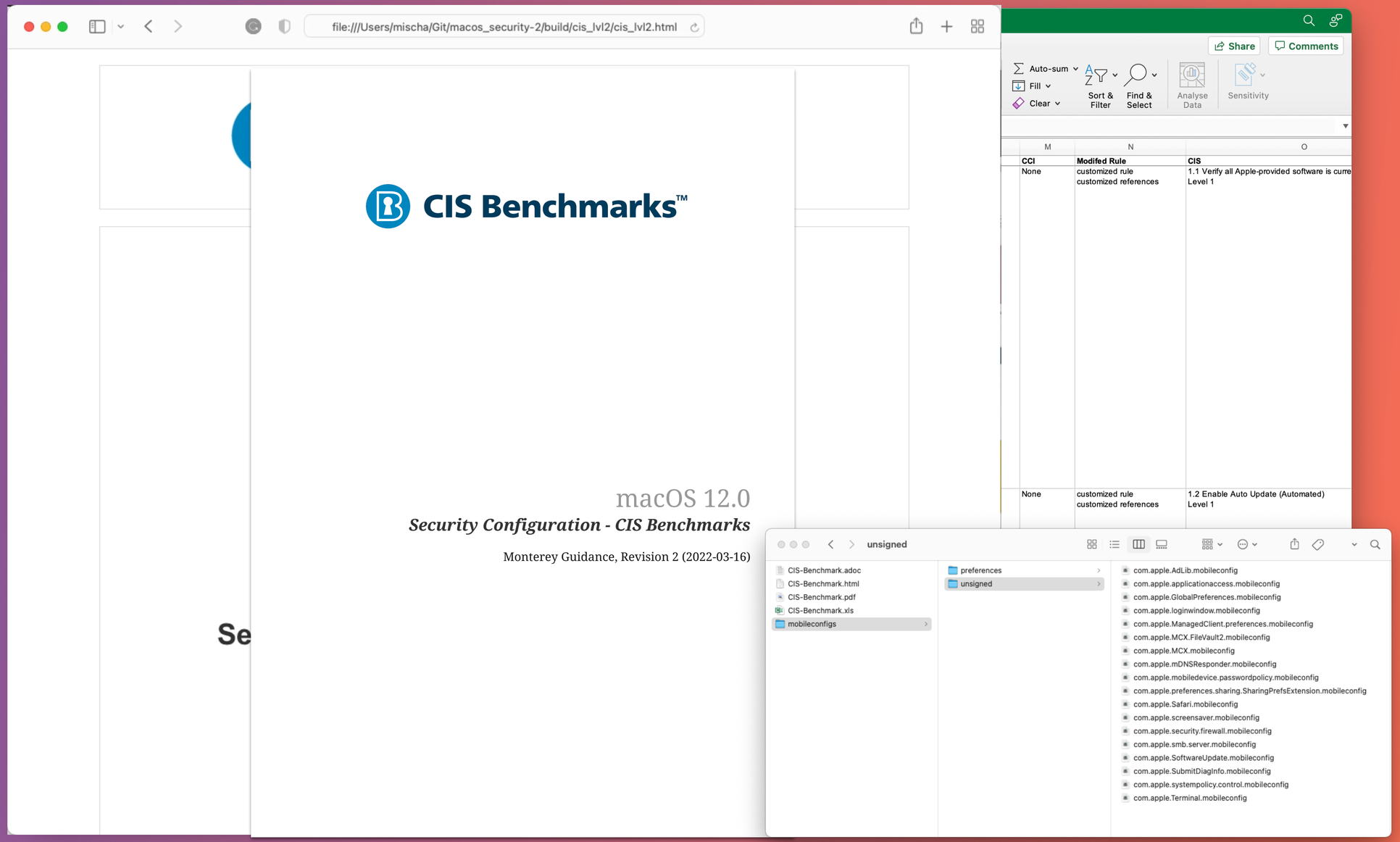
National Institute of Standards and Technology (US)

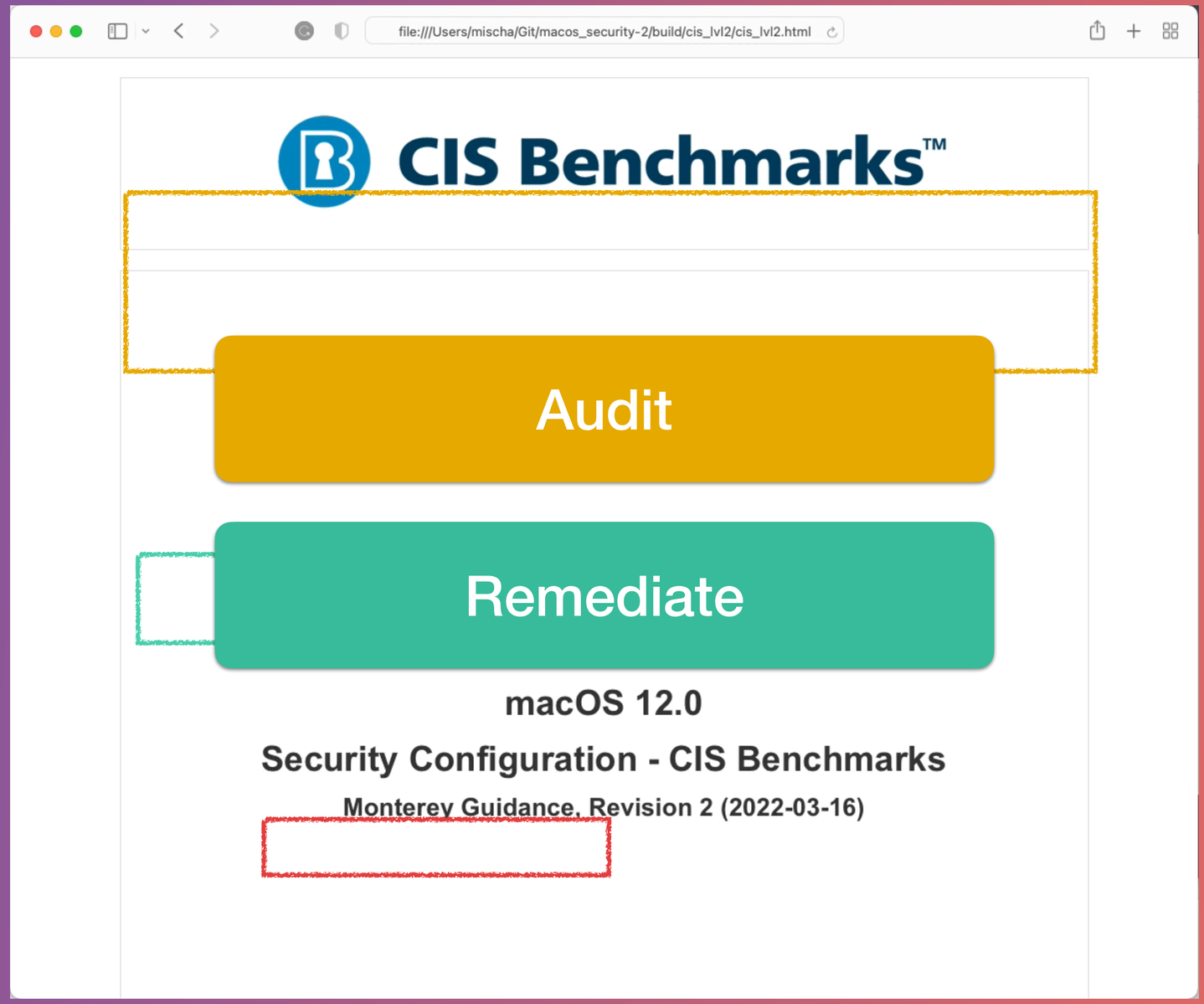
National Cyber Security Centre (UK)

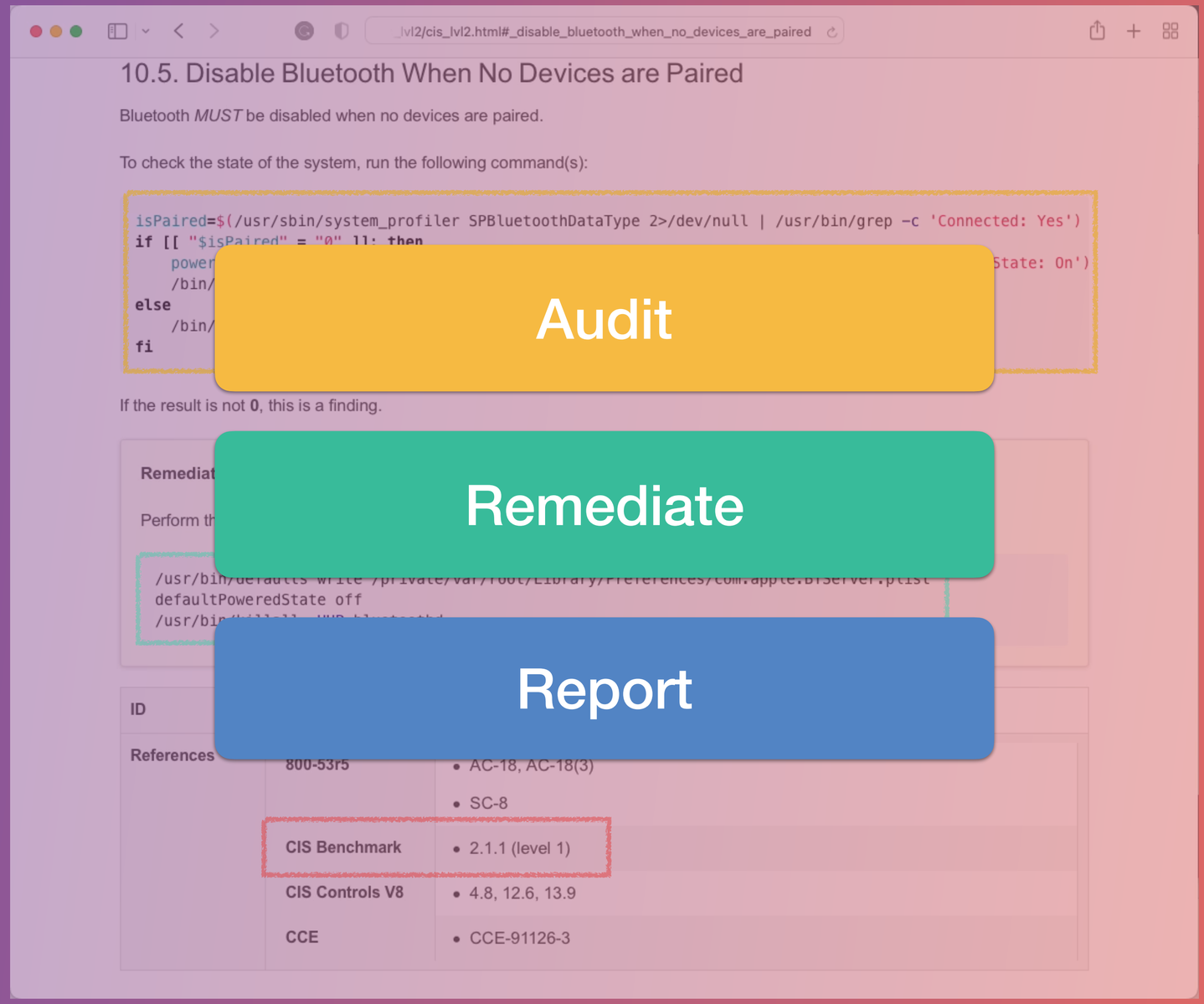
macOS Security Compliance

github.com/usnistgov/macos_security

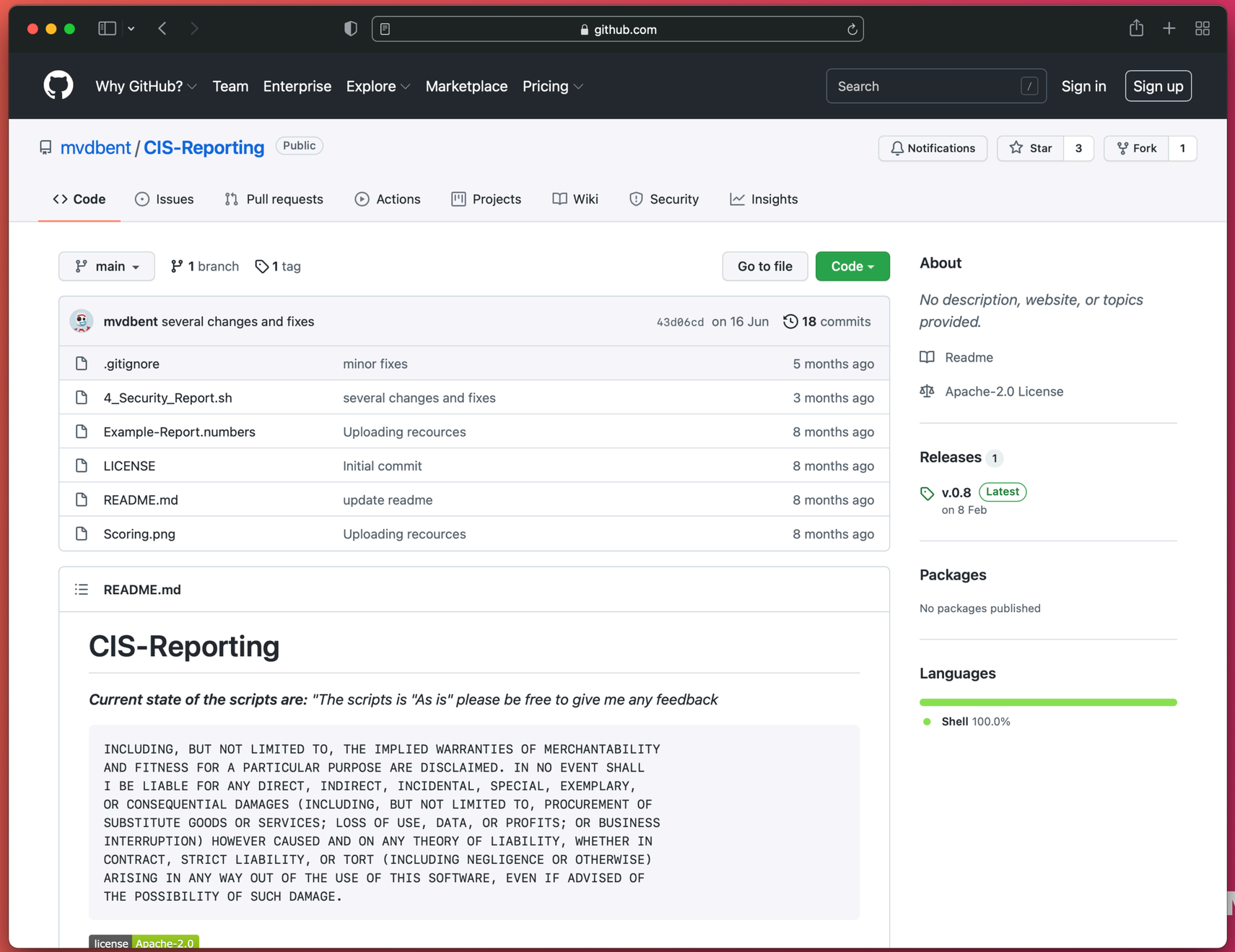
JAMF NATION LIVE


file:///Users/mischa/Git/macos_security-2/build/cis_lvl2/cis_lvl2.html
CIS Benchmarks™
macOS 12.0
Security Configuration - CIS Benchmarks
Monterey Guidance, Revision 2 (2022-03-16)
Share
Comments
Auto-sum
Fill
Clear
Sort & Filter
Find & Select
Analyse Data
Sensitivity
M
N
O
CCI
Modifed Rule
CIS
None
customized rule
customized references
1.1 Verify all Apple-provided software is curre
Level 1
None
customized rule
customized references
1.2 Enable Auto Update (Automated)
Level 1
unsigned
CIS-Benchmark.adoc
CIS-Benchmark.html
CIS-Benchmark.pdf
CIS-Benchmark.xls
mobileconfigs
preferences
unsigned
com.apple.AdLib.mobileconfig
com.apple.applicationaccess.mobileconfig
com.apple.GlobalPreferences.mobileconfig
com.apple.loginwindow.mobileconfig
com.apple.ManagedClient.preferences.mobileconfig
com.apple.MCX.FileVault2.mobileconfig
com.apple.MCX.mobileconfig
com.apple.mDNSResponder.mobileconfig
com.apple.mobiledevice.passwordpolicy.mobileconfig
com.apple.preferences.sharing.SharingPrefsExtension.mobileconfig
com.apple.Safari.mobileconfig
com.apple.screensaver.mobileconfig
com.apple.security.firewall.mobileconfig
com.apple.smb.server.mobileconfig
com.apple.SoftwareUpdate.mobileconfig
com.apple.SubmitDiagInfo.mobileconfig
com.apple.systempolicy.control.mobileconfig
com.apple.Terminal.mobileconfig


file:///Users/mischa/Git/macos_security-2/build/cis_lvl2/cis_lvl2.html
CIS Benchmarks™
Audit
Remediate
macOS 12.0
Security Configuration - CIS Benchmarks
Monterey Guidance, Revision 2 (2022-03-16)


10.5. Disable Bluetooth When No Devices are Paired
Bluetooth *MUST* be disabled when no devices are paired.
To check the state of the system, run the following command(s):
isPaired=$(/usr/sbin/system_profiler SPBluetoothDataType 2>/dev/null | /usr/bin/grep -c 'Connected: Yes')
if [["$isPaired" = "0"]]; then
else
fi
If the result is not **0**, this is a finding.
Audit
Remediate
Report
ID
References
800-53r5
• AC-18, AC-18(3)
• SC-8
CIS Benchmark
• 2.1.1 (level 1)
CIS Controls V8
• 4.8, 12.6, 13.9
CCE
• CCE-91126-3

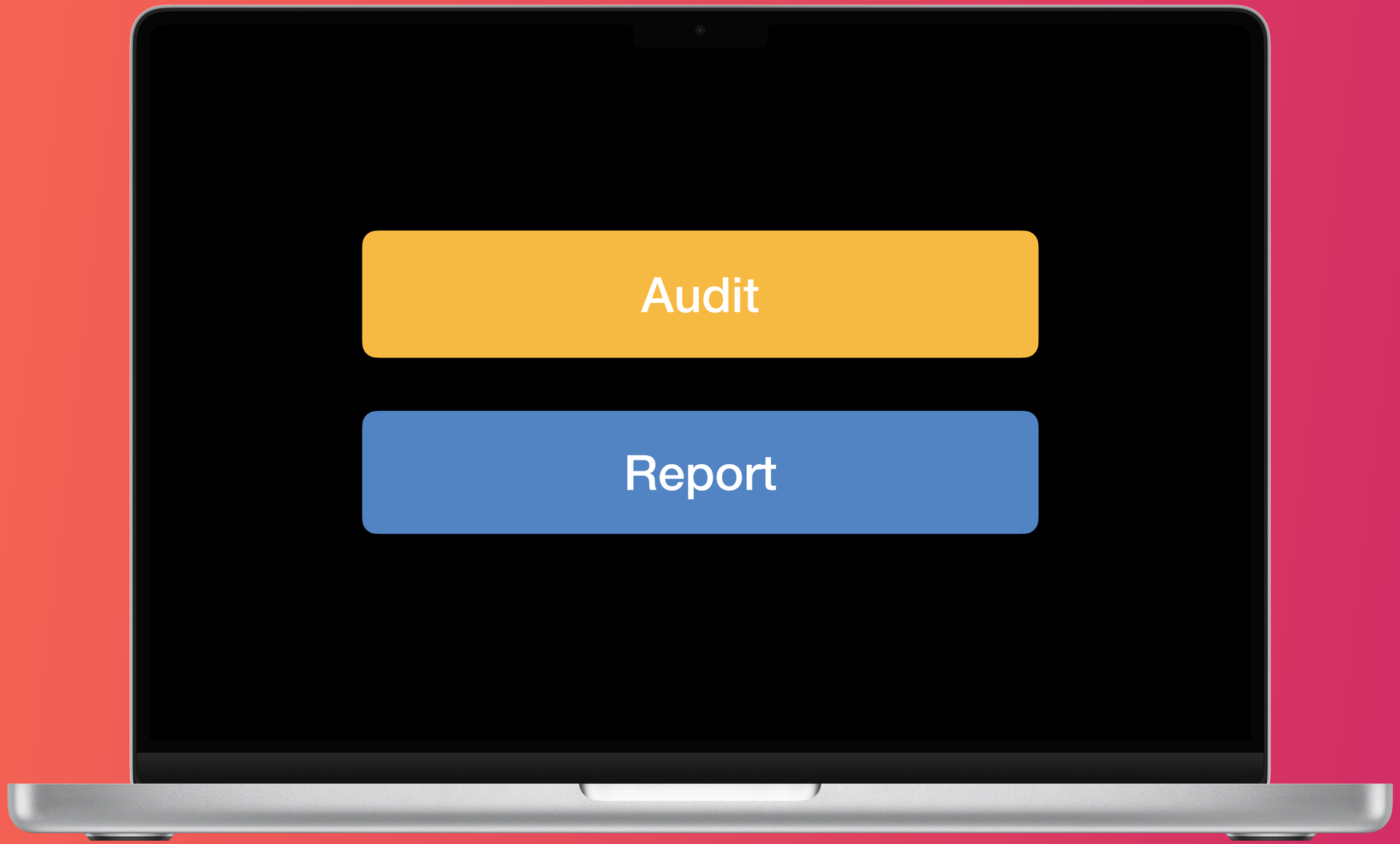
Scripts



CIS Script

github.com/mvdbent/CIS-Script

JAMF NATION LIVE


Audit
Report

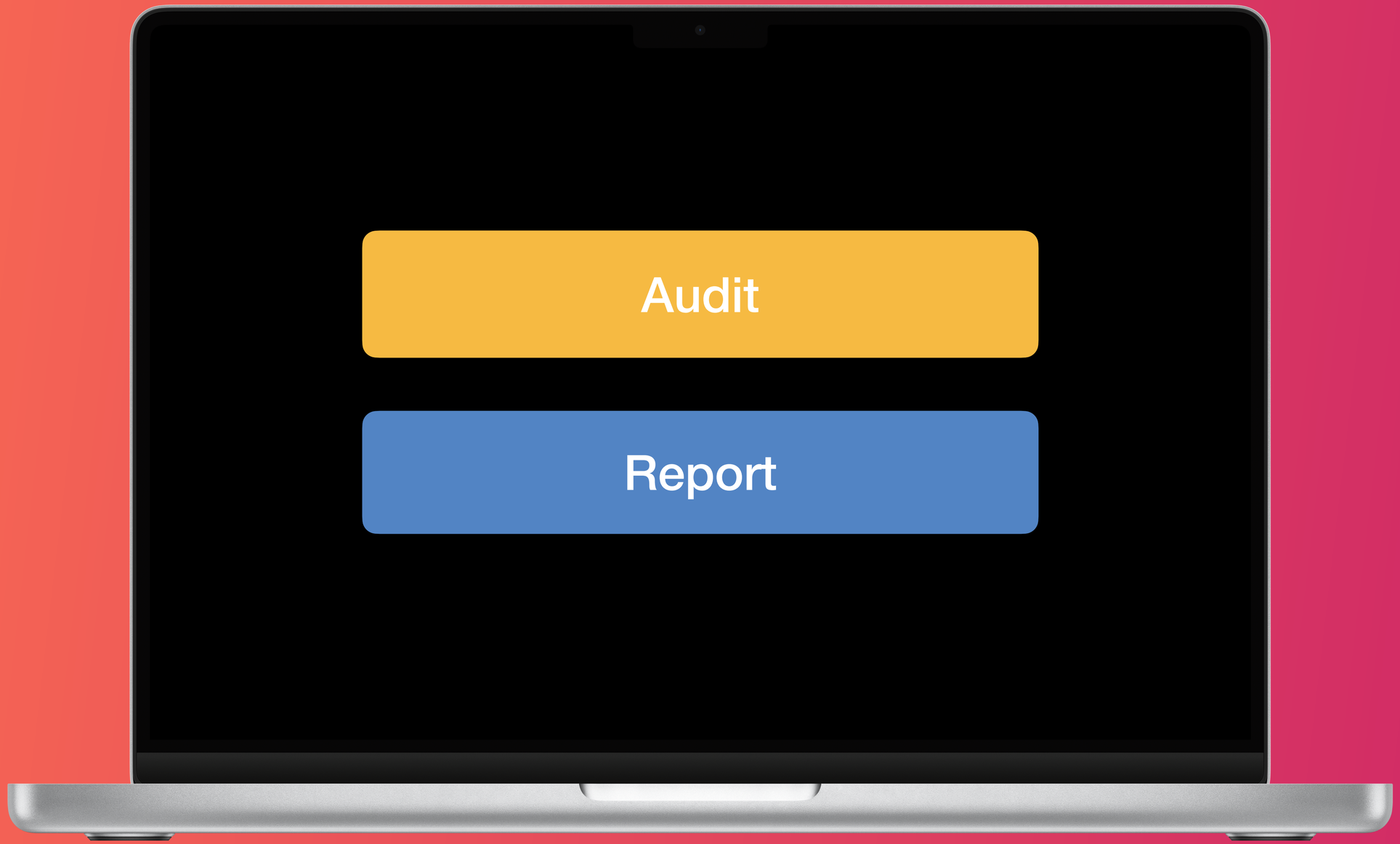

Finder
File
Edit
View
Go
Window
Help
Wed 8 Jun 14:22

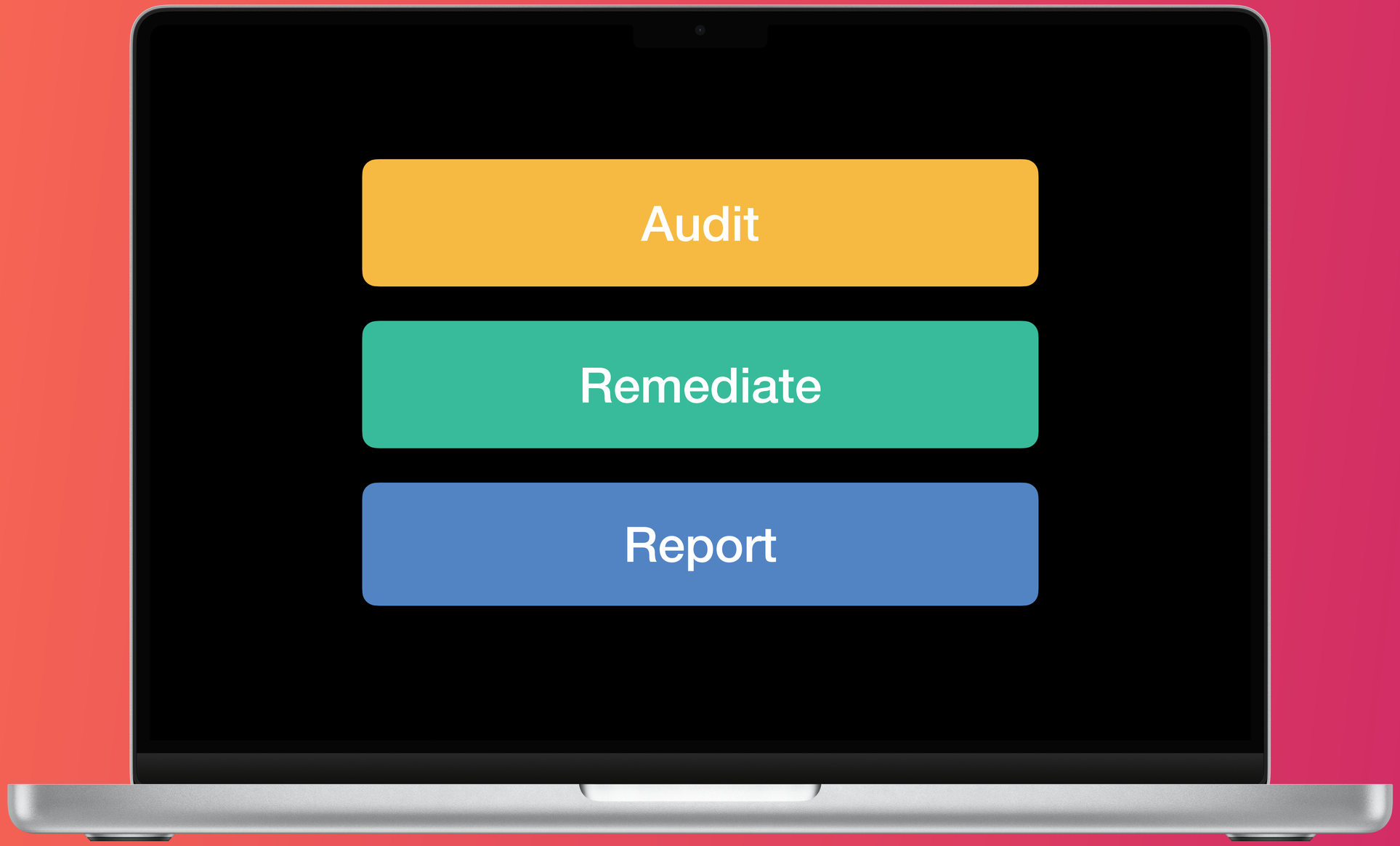
CISBenchmarkReport-Full

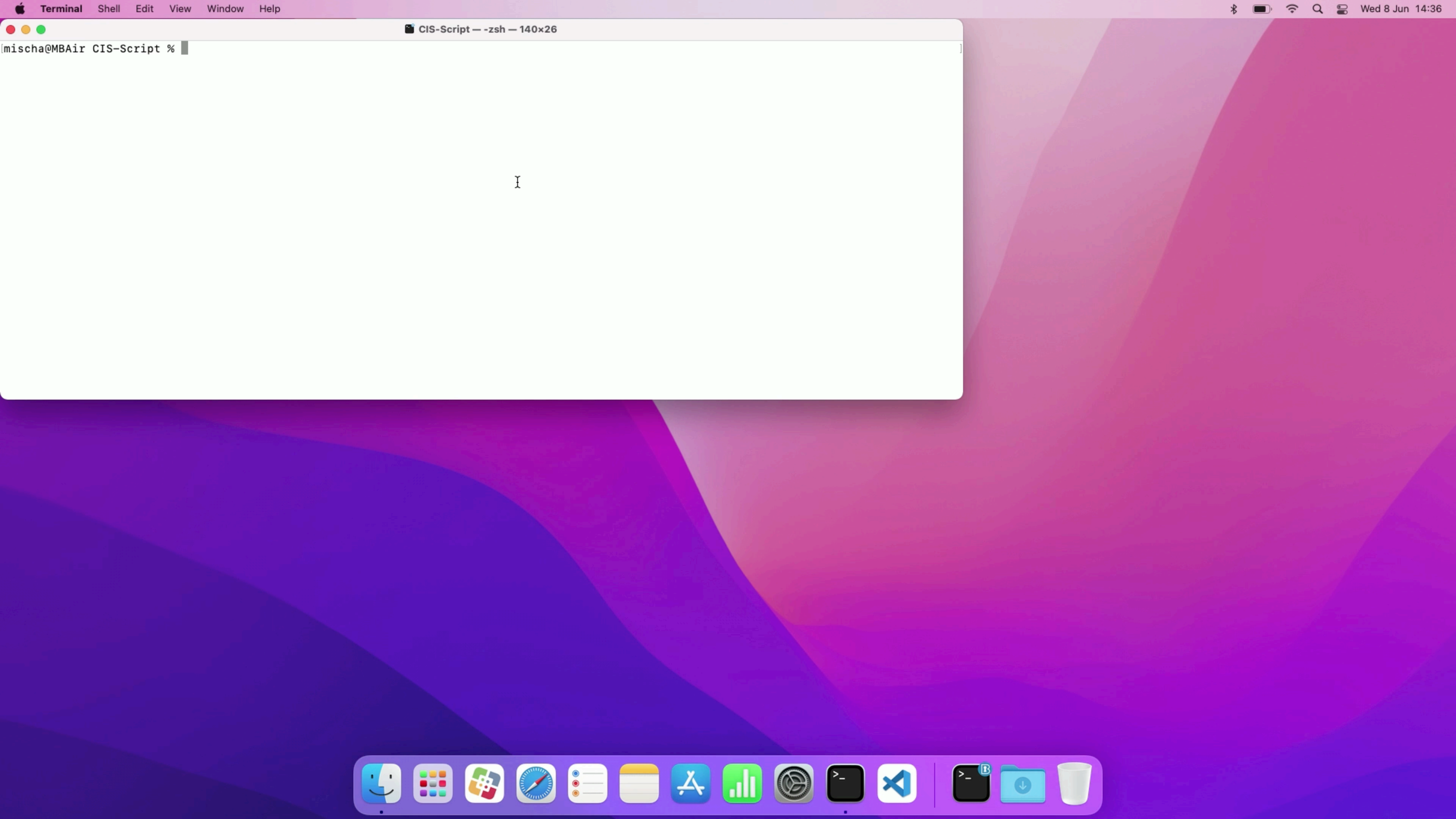
Audit Number	Level	Scoring	Result	Managed	Preference domain	Option	Value	Method	Comments	Remediate
1.1 Verify all Apple-provided software is current (Automated)	1		Passed					Script	Apple Software is Current	Script > sudo /usr/sbin/softwareupdate --install --restart --recommended
1.2 Enable Auto Update (Automated)	1		Passed	FALSE	com.apple.SoftwareUpdate	AutomaticCheckEnabled	TRUE	Profile	Auto Update: Enabled	Configuration profile - payload > com.apple.SoftwareUpdate > AutomaticCheckEnabled=true
1.3 Enable Download new updates when available (Automated)	1		Passed	FALSE	com.apple.SoftwareUpdate	AutomaticDownload	TRUE	Profile	Download new updates when available: Enabled	Configuration profile - payload > com.apple.SoftwareUpdate > AutomaticDownload=true
1.4 Enable app update installs (Automated)	1		Passed	FALSE	com.apple.commerce	AutoUpdate	TRUE	Profile	App updates: Enabled	Configuration profile - payload > com.apple.SoftwareUpdate > AutomaticallyInstallAppUpdates=true
1.5 Enable system data files and security updates install (Automated)	1		Failed	FALSE	com.apple.SoftwareUpdate	ConfigDataInstall	None	Profile	System data files and security update installs: Disabled	Configuration profile - payload > com.apple.SoftwareUpdate > ConfigDataInstall=true - CriticalUpdateInstall=true
1.6 Enable macOS update installs (Automated)	1		Passed	FALSE	com.apple.SoftwareUpdate	AutomaticallyInstallMacOSUpdates	TRUE	Profile	macOS update installs: Enabled	Configuration profile - payload > com.apple.SoftwareUpdate > AutomaticallyInstallMacOSUpdates=true)
2.1.1 Turn off Bluetooth, if no paired devices exist (Automated)	1		Failed					Script	No Paired Devices	Script - defaults write /Library/Preferences/com.apple.Bluetooth ControllerPowerState -bool false
2.1.2 Show Bluetooth status in menu bar (Automated)	1		Passed	FALSE	com.apple.controlcenter	NSStatusItem Visible Bluetooth		Script	Show Bluetooth status in menu bar: Enabled	Script > sudo -u firstuser defaults -currentHost write com.apple.controlcenter.plist Bluetooth -int 18
2.2.1 "Enable Set time and date automatically" (Automated)	1		Failed	FALSE	com.apple.timed	TMAutomaticTimeOnlyEnabled	None	Profile	Time and date automatically: Disabled	Configuration profile - payload > com.apple.timed > TMAutomaticTimeOnlyEnabled=true
2.2.2 Ensure time set is within appropriate limits (Automated)	1		Passed					Script	Network Time Server: time.euro.apple.com	Script > sudo /usr/sbin/systemsetup -setusingnetworktime on && sudo /usr/sbin/systemsetup -setnetworktimeserver time.euro.apple.com
2.3.1 Set an inactivity interval of 20 minutes or less for the screen saver (Automated)	1		Passed	FALSE	com.apple.screensaver	idleTime		Profile	Inactivity interval for the screen saver: 1200	Configuration profile - payload > com.apple.screensaver > idleTime=1200
2.3.2 Secure screen saver corners (Automated)	2		Failed	FALSE	com.apple.dock	wvous-bl-corner, wvous-tl-corner, wvous-tr-corner, wvous-br-corner	None, None, None, None	Profile	Secure screen saver corners: Disabled	Configuration profile - payload > com.apple.dock > wvous-tl-corner=5, wvous-br-corner=10, wvous-bl-corner=13, wvous-tr-corner=0 - 5=Start Screen Saver, 10=Put Display to Sleep, 13=Lock Screen
2.3.3 Familiarize users with screen lock tools or corner to Start Screen Saver (Manual)	1		Passed	FALSE	com.apple.dock			Manual	End-users are familiar with screen lock tools or Hot Corners	Familiarise users with screen lock tools or corner to Start Screen Saver
2.4.1 Disable Remote Apple Events (Automated)	1		Passed					Script	Remote Apple Events: Disabled	Script > sudo /usr/sbin/systemsetup -setremoteappleevents off && sudo launchctl disable system/com.apple.AEServer
2.4.2 Disable Internet Sharing (Automated)	1		Passed					Profile	Internet Sharing: Disabled	Configuration profile - payload > com.apple.MCX > forceInternetSharingOff=true
2.4.3 Disable Screen Sharing (Automated)	1		Passed					Script	Screen Sharing: Disabled	Script > sudo launchctl disable system/com.apple.screensharing
2.4.4 Disable Printer Sharing (Automated)	1		Passed					Script	Printer Sharing: Disabled	Script > sudo /usr/sbin/cupsctl --no-share-printers
2.4.5 Disable Remote Login (Automated)	1		Passed					Script	Remote Login: Disabled	Script > sudo /usr/sbin/systemsetup -setremotelogin off
2.4.6 Disable DVD or CD Sharing (Automated)	1		Passed					Script	DVD or CD Sharing: Disabled	Script > sudo launchctl unload -w /System/Library/LaunchDaemons/com.apple.ODSAgent.plist
2.4.7 Disable Bluetooth Sharing (Automated)	1		Passed	FALSE	com.apple.Bluetooth	PrefKeyServicesEnabled		Script	Bluetooth Sharing: Disabled	Script > sudo -u 'CURRENT_USER' defaults -currentHost write com.apple.Bluetooth PrefKeyServicesEnabled -bool false
2.4.8 Disable File Sharing (Automated)	1		Passed					Script	File Sharing: Disabled	Script > sudo launchctl disable system/com.apple.smbd
2.4.9 Disable Remote Management (Automated)	1		Passed					Script	Remote Management: Disabled	Script > sudo /System/Library/CoreServices/RemoteManagement/ARDAgent.app/Contents/Resources/kickstart -deactivate -stop
2.4.10 Disable Content Caching (Automated)	2		Passed	FALSE	com.apple.applicationaccess	allowContentCaching	None	Profile	Content Caching: Disabled	Configuration profile - payload > com.apple.applicationaccess > allowContentCaching=false
2.4.11 Disable Media Sharing (Automated)	1		Failed	FALSE	com.apple.preferences.sharing.SharingPrefsExtension	homeSharingUIStatus, legacySharingUIStatus, mediaSharingUIStatus	None, None, None	Profile	Media Sharing: Enabled	Configuration profile - payload > com.apple.preferences.sharing.SharingPrefsExtension > homeSharingUIStatus=0 > legacySharingUIStatus=0 > mediaSharingUIStatus=0
2.5.1.1 Enable FileVault (Automated)	1		Passed	FALSE	com.apple.MCX.FileVault2	Enable	None	Profile	FileVault: Enabled	Configuration profile - payload > com.apple.MCX.FileVault2 > Enable=On
2.5.1.2 Ensure all user storage APFS volumes are encrypted (Manual)	1		Passed					Manual	Startup Volume: Encrypted	Manual - Ensure all user storage APFS Volumes are encrypted
2.5.1.3 Ensure all user storage CoreStorage volumes are encrypted (Manual)	1		Not applicable					Manual	Volumes: APFS	Manual - Ensure all user CoreStorage volumes encrypted
2.5.2.1 Enable Gatekeeper (Automated)	1		Passed	FALSE	com.apple.systempolicy.control	EnableAssessment	None	Profile	Gatekeeper: Enabled	Configuration profile - payload > com.apple.systempolicy.control > EnableAssessment=true
2.5.2.2 Enable Firewall (Automated)	1		Failed	FALSE	com.apple.security.firewall	EnableFirewall	None	Profile	Firewall: Disabled	Configuration profile - payload > com.apple.security.firewall > EnableFirewall=true
2.5.2.3 Enable Firewall Stealth Mode (Automated)	1		Passed	FALSE	com.apple.security.Firewall	EnableStealthMode	None	Profile	Firewall Stealth Mode: Enabled	Configuration profile - payload > com.apple.security.firewall > EnableStealthMode=true
2.5.3 Review Application Firewall Rules (Manual)	1		Passed					Profile	Application Firewall Rules: Application Managed	Configuration profile - payload > com.apple.security.firewall > Applications > Array > BundleID=com.apple.app > Allowed=false
2.5.4 Enable Location Services (Automated)	2		Passed					Script	Location Services: Enabled	Script > sudo /usr/bin/defaults write /var/db/locationd/Library/Preferences/ByHost/com.apple.locationd LocationServicesEnabled -bool true && sudo /bin/launchctl kickstart -k system/com.apple.locationd
2.5.5 Monitor Location Services Access (Manual)	2		Notice					Manual	3 applications can accessing location services	Manual - Disable unnecessary applications from accessing location services
2.5.6 Disable sending diagnostic and usage data to Apple (Automated)	2		Passed	FALSE	com.apple.SubmitDiagInfo	AutoSubmit	None	Profile	Sending diagnostic and usage data to Apple: Disabled	Configuration profile - payload > com.apple.SubmitDiagInfo > AutoSubmit=false - payload > com.apple.applicationaccess > allowDiagnosticSubmission=false
2.5.7 Limit Ad tracking and personalized Ads (Automated)	1		Passed	FALSE	com.apple.AdLib	allowApplePersonalizedAdvertising		Profile	Limited Ad Tracking: Disabled	Configuration profile - payload > com.apple.AdLib > allowApplePersonalizedAdvertising=false
2.6.1 iCloud configuration (Manual)	2		Passed					Manual	no iCloud account(s) configured	Manual - Use a profile to disable services where organizationally required
2.6.2 iCloud keychain (Manual)	2		Failed	FALSE	com.apple.applicationaccess	allowCloudKeychainSync	None	Profile	iCloud keychain: Enabled	Configuration profile - payload > com.apple.applicationaccess) allowCloudKeychainSync=false
2.6.3 iCloud Drive (Manual)	2		Failed	FALSE	com.apple.applicationaccess	allowCloudDocumentSync	None	Profile	iCloud Drive: Enabled	Configuration profile - payload > com.apple.applicationaccess > allowCloudDocumentSync=false
2.6.4 iCloud Drive Document and Desktop sync (Manual)	2		Failed	FALSE	com.apple.applicationaccess	allowCloudDesktopAndDocuments	None	Profile	iCloud Drive Document and Desktop sync: Enabled	Configuration profile - payload > com.apple.applicationaccess > allowCloudDesktopAndDocuments=false
2.7.1 Time Machine Auto-Backup (Automated)	2		Passed					Script	Time Machine Auto-Backup: Enabled	Script > sudo defaults write /Library/Preferences/com.apple.TimeMachine.plist AutoBackup 1
2.7.2 Time Machine Volumes Are Encrypted (Automated)	1		Passed					Manual	No Time Machine Volumes available	Manual > Set encryption through Disk Utility or diskutil in terminal
2.8 Disable Wake for network access (Automated)	1		Passed					Script	Wake for network access: Disabled	Script > sudo /usr/bin/pmset -a womp 0
2.9 Disable Power Nap (Automated)	1		Passed					Script	Power Nap: Enabled	Script > sudo /usr/bin/pmset -a powernap 0
2.10 Enable Secure Keyboard Entry in terminal.app (Automated)	1		Failed	FALSE	com.apple.Terminal	SecureKeyboardEntry	None	Profile	Secure Keyboard Entry in terminal.app: Disabled	Configuration profile - payload > com.apple.Terminal > SecureKeyboardEntry=true
2.11 Ensure EFI version is valid and being regularly checked (Automated)	1		Not applicable						EFI Firmware Integrity is not supported by this Mac. T2 Chip found.	
3.1 Enable security auditing (Automated)	1		Passed					Script	Security auditing: Enabled	Script > sudo launchctl load -w /System/Library/LaunchDaemons/com.apple.auditd.plist
3.2 Configure Security Auditing Flags per local organizational requirements (Manual)	2		Passed					Script	Security Auditing Flags: Enabled	Script > sudo /usr/bin/sed -i.bak '/^flags/ s/$/,ad/' /etc/security/audit_control /usr/sbin/audit -s
3.3 Retain install.log for 365 or more days with no maximum size (Automated)	1		Failed					Script	Retain install.log: Less than 365 days	Script > add 'ttl=365' to /etc/asl/com.apple.install
3.4 Ensure security auditing retention (Automated)	1		Failed					Script	Security auditing retention: Unconfigured	Script > add 'expire-after:60d OR 1G' to /etc/security/audit_control
3.5 Control access to audit records (Automated)	1		Passed					Script	Control access to audit records: Correct ownership	Script > sudo chown -R root /var/audit
3.6 Ensure Firewall is configured to log (Automated)	1		Passed					Script	Firewall logging: Enabled	Script > sudo /usr/libexec/ApplicationFirewall/socketfilterfw --setloggingmode on
4.1 Disable Bonjour advertising service (Automated)	2		Failed	FALSE	com.apple.mDNSResponder	NoMulticastAdvertisements	None	Profile	Bonjour advertising service: Enabled	Configuration profile - payload > com.apple.mDNSResponder > NoMulticastAdvertisements=true
4.2 Enable "Show Wi-Fi status in menu bar" (Automated)	1		Passed		com.apple.controlcenter	NSStatusItem Visible WiFi	TRUE	Script	Wi-Fi status in menu bar: Enabled	Script > sudo -u <username> defaults -currentHost write com.apple.controlcenter.plist WiFi -int 18
4.4 Ensure http server is not running (Automated)	1		Passed					Script	HTTP server service: Disabled	Script > sudo launchctl disable system/org.apache.httpd
4.5 Ensure nfs server is not running. (Automated)	1		Passed					Script	NFS server service: Disabled	Script > sudo launchctl disable system/com.apple.nfsd && sudo rm /etc/exports
5.1.1 Secure Home Folders (Automated)	1		Passed					Script	Home Folders: Secure	Script > sudo chmod og-rwx 'HomeFolders'
5.1.2 Check System Wide Applications for appropriate permissions (Automated)	1		Passed					Script	All System Wide Applications have appropriate permissions	Script > sudo chmod -R o-w /Applications/<applicationname>
5.1.3 Check System folder for world writable files (Automated)	1		Passed					Script	All System folder for world are not writable files	Script > sudo chmod -R o-w /Path/<baddirectory>
5.1.4 Check Library folder for world writable files (Automated)	2		Passed					Script	All Library folder for world are not writable files	Script > sudo chmod -R o-w /System/Volumes/Data/Library/<baddirectory>
5.3 Reduce the sudo timeout period (Automated)	1		Passed					Script	The sudo timeout period is reduced	Script > echo "Defaults timestamp_timeout=0" >> /etc/sudoers
5.4 Automatically lock the login keychain for inactivity (Manual)	2		Passed					Script	Automatically lock the login keychain for inactivity: Enabled	Script > sudo -u <username> security set-keychain-settings -t 21600 /Users/<username>/Library/Keychains/login.keychain

Audit Number	Level	Scoring	Result	Managed	Preference domain	Option
1.1 Verify all Apple-provided software is current (Automated)	1		Passed			
1.2 Enable Auto Update (Automated)	1		Passed	FALSE	com.apple.SoftwareUpdate	AutomaticCheckEnable
1.3 Enable Download new updates when available (Automated)	1		Passed	FALSE	com.apple.SoftwareUpdate	AutomaticDownload
1.4 Enable app update installs (Automated)	1		Passed	FALSE	com.apple.commerce	AutoUpdate
1.5 Enable system data files and security updates install (Automated)	1		Failed	FALSE	com.apple.SoftwareUpdate	ConfigDataInstall
1.6 Enable macOS update installs (Automated)	1		Passed	FALSE	com.apple.SoftwareUpdate	AutomaticallyInstallMac
2.1.1 Turn off Bluetooth, if no paired devices exist (Automated)	1		Failed			
2.1.2 Show Bluetooth status in menu bar (Automated)	1		Passed	FALSE	com.apple.controlcenter	NSStatusItem Visible Bl
2.2.1 "Enable Set time and date automatically" (Automated)	1		Failed	FALSE	com.apple.timed	TMAutomaticTimeOnlyE
2.2.2 Ensure time set is within appropriate limits (Automated)	1		Passed			
2.3.1 Set an inactivity interval of 20 minutes or less for the screen saver (Automated)	1		Passed	FALSE	com.apple.screensaver	idleTime
2.3.2 Secure screen saver corners (Automated)	2		Failed	FALSE	com.apple.dock	wvous-bl-corner, wvous
2.3.3 Familiarize users with screen lock tools or corner to Start Screen Saver (Manual)	1		Passed	FALSE	com.apple.dock	
2.4.1 Disable Remote Apple Events (Automated)	1		Passed			
2.4.2 Disable Internet Sharing (Automated)	1		Passed			
2.4.3 Disable Screen Sharing (Automated)	1		Passed			
2.4.4 Disable Printer Sharing (Automated)	1		Passed			
2.4.5 Disable Remote Login (Automated)	1		Passed			
2.4.6 Disable DVD or CD Sharing (Automated)	1		Passed			
2.4.7 Disable Bluetooth Sharing (Automated)	1		Passed	FALSE	com.apple.Bluetooth	PrefKeyServicesEnable
2.4.8 Disable File Sharing (Automated)	1		Passed			

	Remediate
	Script > sudo /usr/sbin/softwareupdate --install --restart --recommended
	Configuration profile - payload > com.apple.SoftwareUpdate > AutomaticCheckEnabled=true
	Configuration profile - payload > com.apple.SoftwareUpdate > AutomaticDownload=true
	Configuration profile - payload > com.apple.SoftwareUpdate > AutomaticallyInstallAppUpdates=true
bled	Configuration profile - payload > com.apple.SoftwareUpdate > ConfigDataInstall=true - CriticalUpdateInstall=true
	Configuration profile - payload > com.apple.SoftwareUpdate > AutomaticallyInstallMacOSUpdates=true)
	Script - defaults write /Library/Preferences/com.apple.Bluetooth ControllerPowerState -bool false
	Script > sudo -u firstuser defaults -currentHost write com.apple.controlcenter.plist Bluetooth -int 18
	Configuration profile - payload > com.apple.timed > TMAutomaticTimeOnlyEnabled=true
	Script > sudo /usr/sbin/systemsetup -setusingnetworktime on && sudo /usr/sbin/systemsetup -setnetworktimeserver time.euro.apple.com
	Configuration profile - payload > com.apple.screensaver > idleTime=1200
	Configuration profile - payload > com.apple.dock > wvous-tl-corner=5, wvous-br-corner=10, wvous-bl-corner=13, wvous-tr-corner=0 - 5=Start Screen Saver, 10=Put Display to Sleep, 13=Lock Screen
Corners	Familiarise users with screen lock tools or corner to Start Screen Saver
	Script > sudo /usr/sbin/systemsetup -setremoteappleevents off && sudo launchctl disable system/com.apple.AEServer
	Configuration profile - payload > com.apple.MCX > forceInternetSharingOff=true
	Script > sudo launchctl disable system/com.apple.screensharing
	Script > sudo /usr/sbin/cupsctl --no-share-printers
	Script > sudo /usr/sbin/systemsetup -setremotelogin off
	Script > sudo launchctl unload -w /System/Library/LaunchDaemons/com.apple.ODSAgent.plist
	Script > sudo -u 'CURRENT_USER' defaults -currentHost write com.apple.Bluetooth PrefKeyServicesEnabled -bool false
	Script > sudo launchctl disable system/com.apple.smbd


Audit
Report


Audit
Remediate
Report


Terminal Shell Edit View Window Help
Wed 8 Jun 14:36
CIS-Script — -zsh — 140×26
mischa@MBAir CIS-Script %

CISBenchmarkReport

Audit Number	Level	Scoring	Result	Managed	Method	Comments
1.1 Verify all Apple-provided software is current (Automated)	1		Passed		Script	Apple Software is Current
1.2 Enable Auto Update (Automated)	1		Passed	FALSE	Profile	Auto Update: Enabled
1.3 Enable Download new updates when available (Automated)	1		Passed	FALSE	Profile	Download new updates when available: Enabled
1.4 Enable app update installs (Automated)	1		Passed	FALSE	Profile	App updates: Enabled
1.5 Enable system data files and security updates install (Automated)	1		Failed	FALSE	Profile	System data files and security update installs: Disabled
1.6 Enable macOS update installs (Automated)	1		Passed	FALSE	Profile	macOS update installs: Enabled
2.1.1 Turn off Bluetooth, if no paired devices exist (Automated)	1		Passed After Remediation		Script	No Paired Devices
2.1.2 Show Bluetooth status in menu bar (Automated)	1		Passed	FALSE	Script	Show Bluetooth status in menu bar: Enabled
2.2.1 "Enable Set time and date automatically" (Automated)	1		Failed	FALSE	Profile	Time and date automatically: Disabled
2.2.2 Ensure time set is within appropriate limits (Automated)	1		Passed		Script	Network Time Server: time.euro.apple.com
2.3.1 Set an inactivity interval of 20 minutes or less for the screen saver (Automated)	1		Passed	FALSE	Profile	Inactivity interval for the screen saver: 1200
2.3.2 Secure screen saver corners (Automated)	2		Failed	FALSE	Profile	Secure screen saver corners: Disabled
2.3.3 Familiarize users with screen lock tools or corner to Start Screen Saver (Manual)	1		Passed	FALSE	Manual	End-users are familiar with screen lock tools or Hot Corners
2.4.1 Disable Remote Apple Events (Automated)	1		Passed		Script	Remote Apple Events: Disabled
2.4.2 Disable Internet Sharing (Automated)	1		Passed		Profile	Internet Sharing: Disabled
2.4.3 Disable Screen Sharing (Automated)	1		Passed		Script	Screen Sharing: Disabled
2.4.4 Disable Printer Sharing (Automated)	1		Passed		Script	Printer Sharing: Disabled
2.4.5 Disable Remote Login (Automated)	1		Passed		Script	Remote Login: Disabled
2.4.6 Disable DVD or CD Sharing (Automated)	1		Passed		Script	DVD or CD Sharing: Disabled
2.4.7 Disable Bluetooth Sharing (Automated)	1		Passed	FALSE	Script	Bluetooth Sharing: Disabled
2.4.8 Disable File Sharing (Automated)	1		Passed		Script	File Sharing: Disabled
2.4.9 Disable Remote Management (Automated)	1		Passed		Script	Remote Management: Disabled
2.4.10 Disable Content Caching (Automated)	2		Passed	FALSE	Profile	Content Caching: Disabled
2.4.11 Disable Media Sharing (Automated)	1		Failed	FALSE	Profile	Media Sharing: Enabled

❯ ./CISBenchmarkScript.sh --help

```
The following options are available:

        -f      --fullreport    Print Full Report
        -h      --help          Displays this message or details on a specific verb
        -r      --remediate     Enable Remediation

EXAMPLES
    ./CISBenchmarkScript.sh
            Run script to print Short Report

    ./CISBenchmarkScript.sh -f
            Run script to print Full Report

    ./CISBenchmarkScript.sh -r
            Run script with Remediation enabled

    ./CISBenchmarkScript.sh -rf
            Run script with Remediation enabled and print Full Report
```

How the script is built

CIS Script

- Assemble.sh
- Build
- Fragments
- Jamf
- LICENSE
- README.md
- Utils

CIS Script

- Assemble.sh
- Build
- Fragments
- Jamf
- LICENSE
- README.md
- Utils

- Footer.sh
- Header.json
- Header.sh
- OrgScores
- Version.sh

```
#!/bin/zsh

script_dir=$(dirname ${0:A})
projectfolder=$(dirname $script_dir)

source ${projectfolder}/Header.sh

CISLevel="1"
audit="2.1.1 Turn off Bluetooth, if no paired devices exist (Automated)"
orgScore="OrgScore2_1_1"
emptyVariables

# Verify organizational score
runAudit
# If organizational score is 1 or tr
if [[ "${auditResult}" == "1" ]]; th
    method="Script"
    remediate="Script - defaults wri                                    -bool false"

    connectable=$(system_profiler SPBluetoothDataType 2>&1 | grep -c "Connected: Yes")
    bluetoothEnabled=$(system_profiler SPBluetoothDataType 2>&1 | grep -c "State: On")
    comment="Paired Devices: ${conne
    # if [[ "$connectable" == 0 ]] &
    if [[ "$connectable" -gt 0 ]] &&                                    [[ "$bluetoothEnabled" == 0 ]]; then
        result="Passed"
    else
        result="Failed"
        comment="No Paired Devices"

        # Remediation
        if [[ "${remediateResult}" =
            /usr/bin/defaults write                                     efaultPoweredState off
            killall -HUP bluetoothd

            # re-check
            bluetoothEnabled=$(system_profiler SPBluetoothDataType 2>&1 | grep -c "State: On")
            if [[ "$bluetoothEnabled" == 0 ]]; then
                result="Passed After Remediation"
            else
                result="Failed After Remediation"
            fi
        fi
    fi
fi
printReport
```

Audit

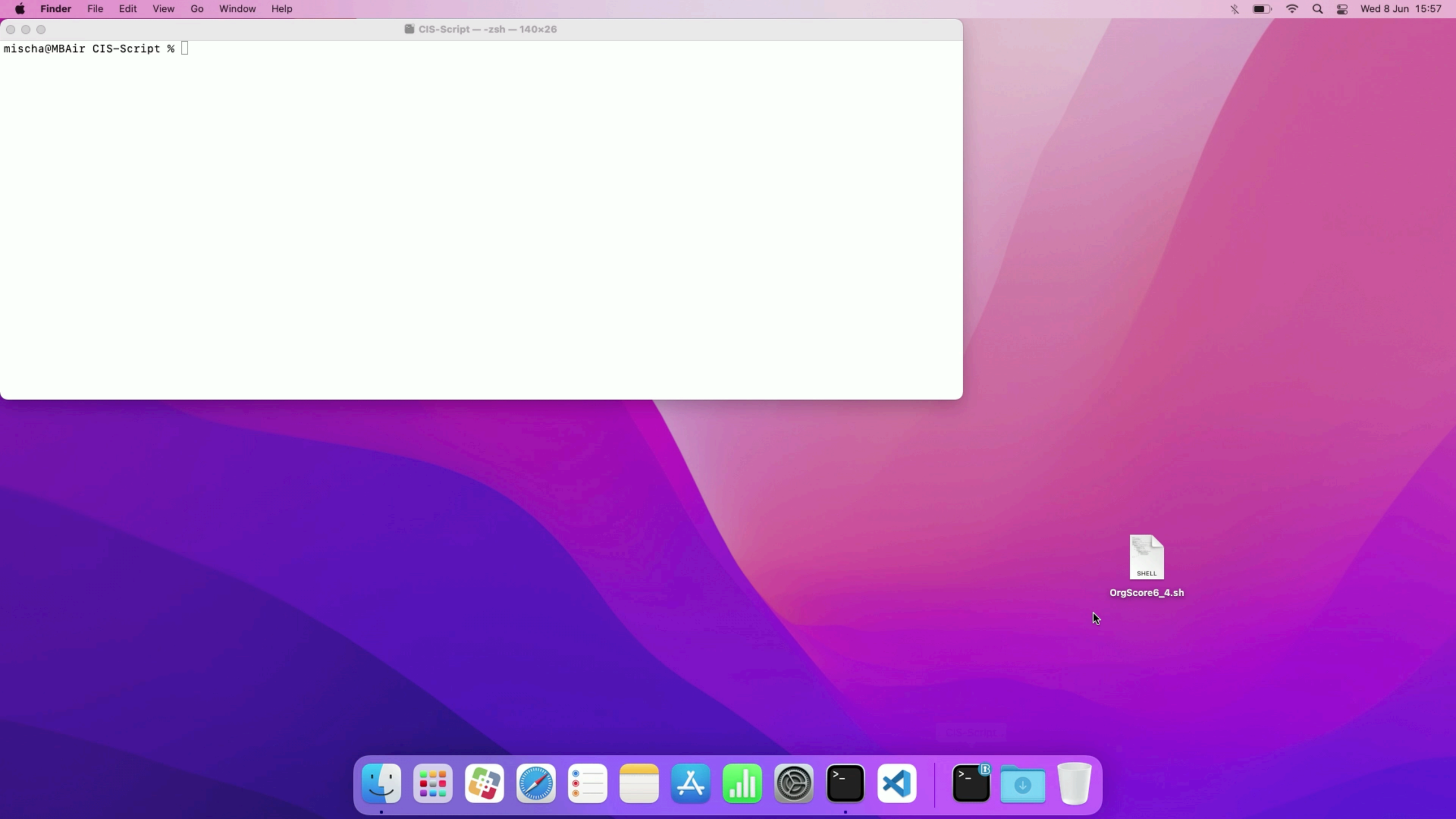
Remediate

Report

Custom rules

CIS-Script/Fragments/OrgScores


Demo


Finder File Edit View Go Window Help
Wed 8 Jun 15:57
CIS-Script — -zsh — 140×26
mischa@MBAir CIS-Script %
SHELL
OrgScore6_4.sh

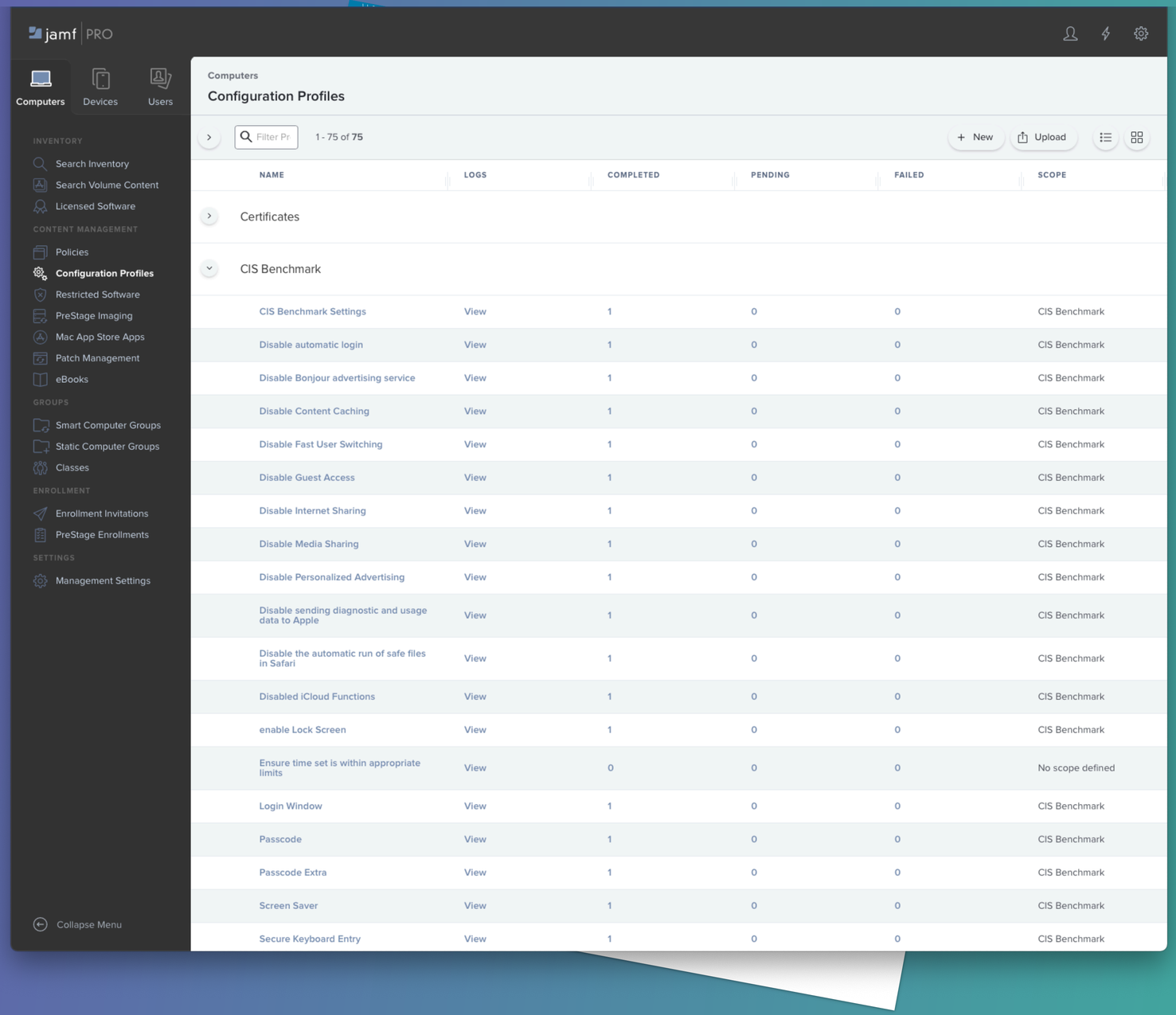
❯ ./Assemble.sh --help

```
The following options are available:

        -h      --help      Displays this message or details on a specific verb
        -j      --json      Builds Jamf Pro Custom Schema.json file
        -s      --separate  Builds separate CIS Benchmark Script from the fragments

EXAMPLES
    ./Assemble.sh
            Builds CIS Benchmark Script from the fragments

    ./Assemble.sh -j
            Builds Jamf Pro Custom Schema.json file

    ./Assemble.sh -s
            Builds separate CIS Benchmark Script from the fragments
```

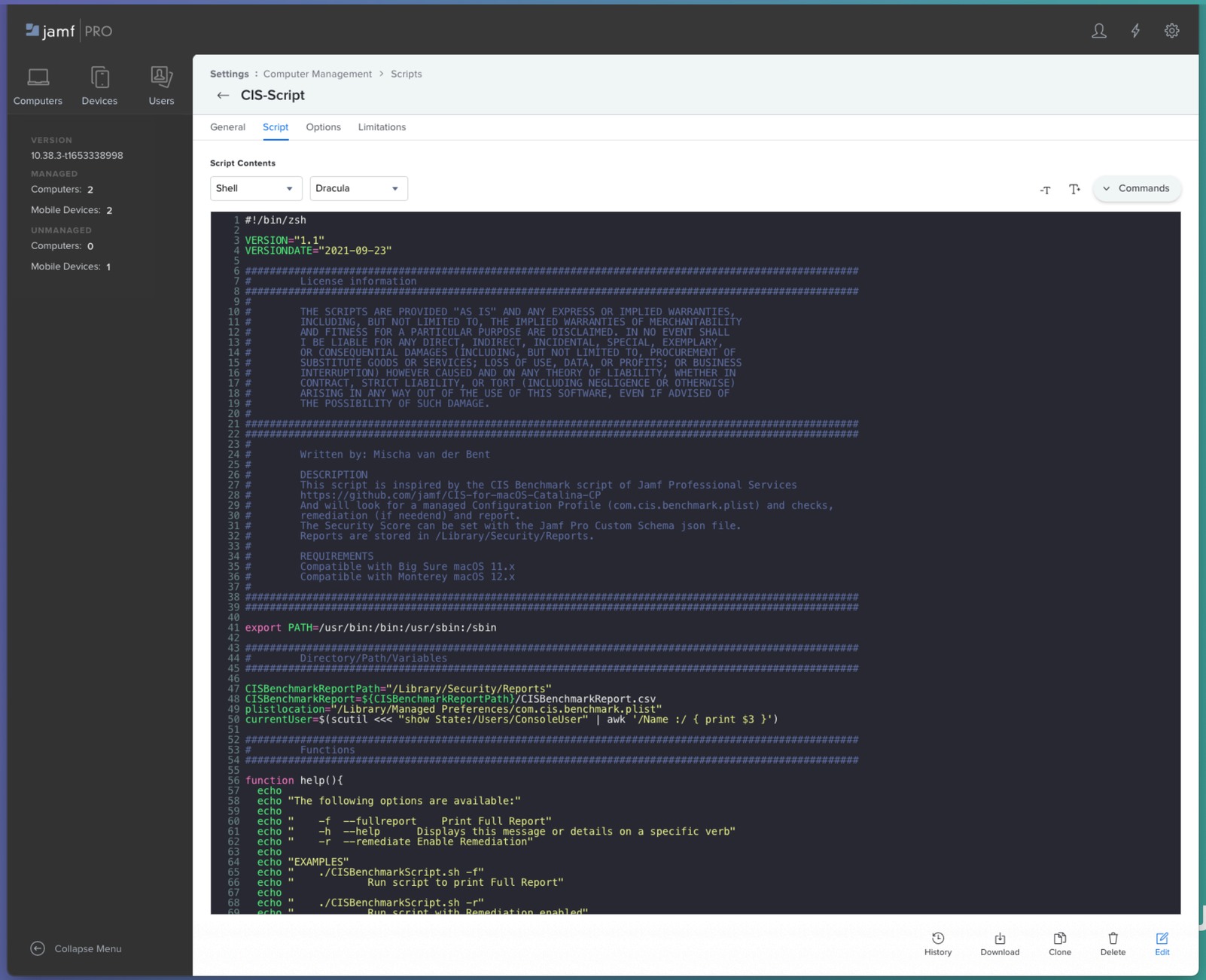
macOS
Big Sur

macOS
Monterey

Implementation



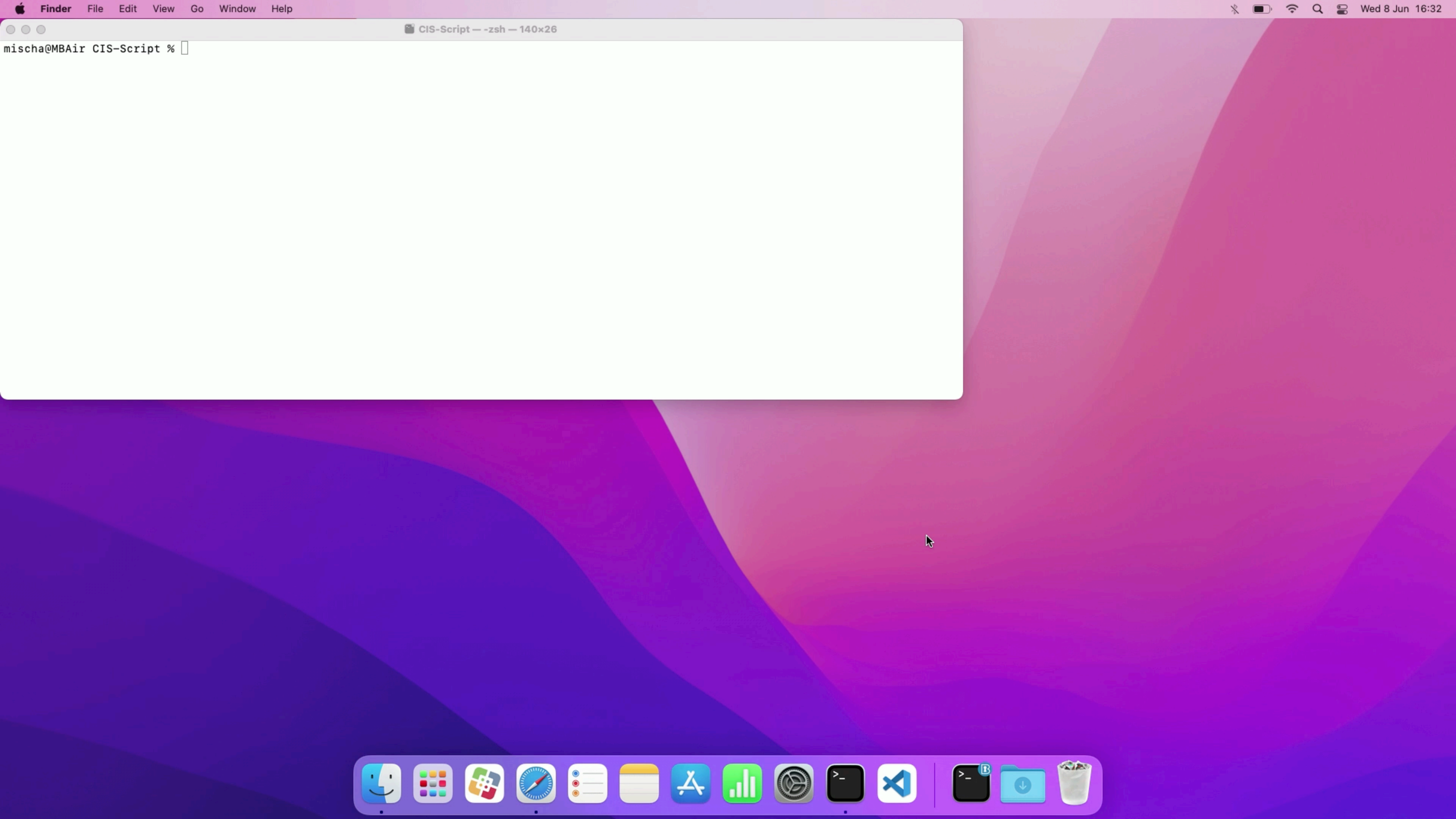
JAMF NATION LIVE

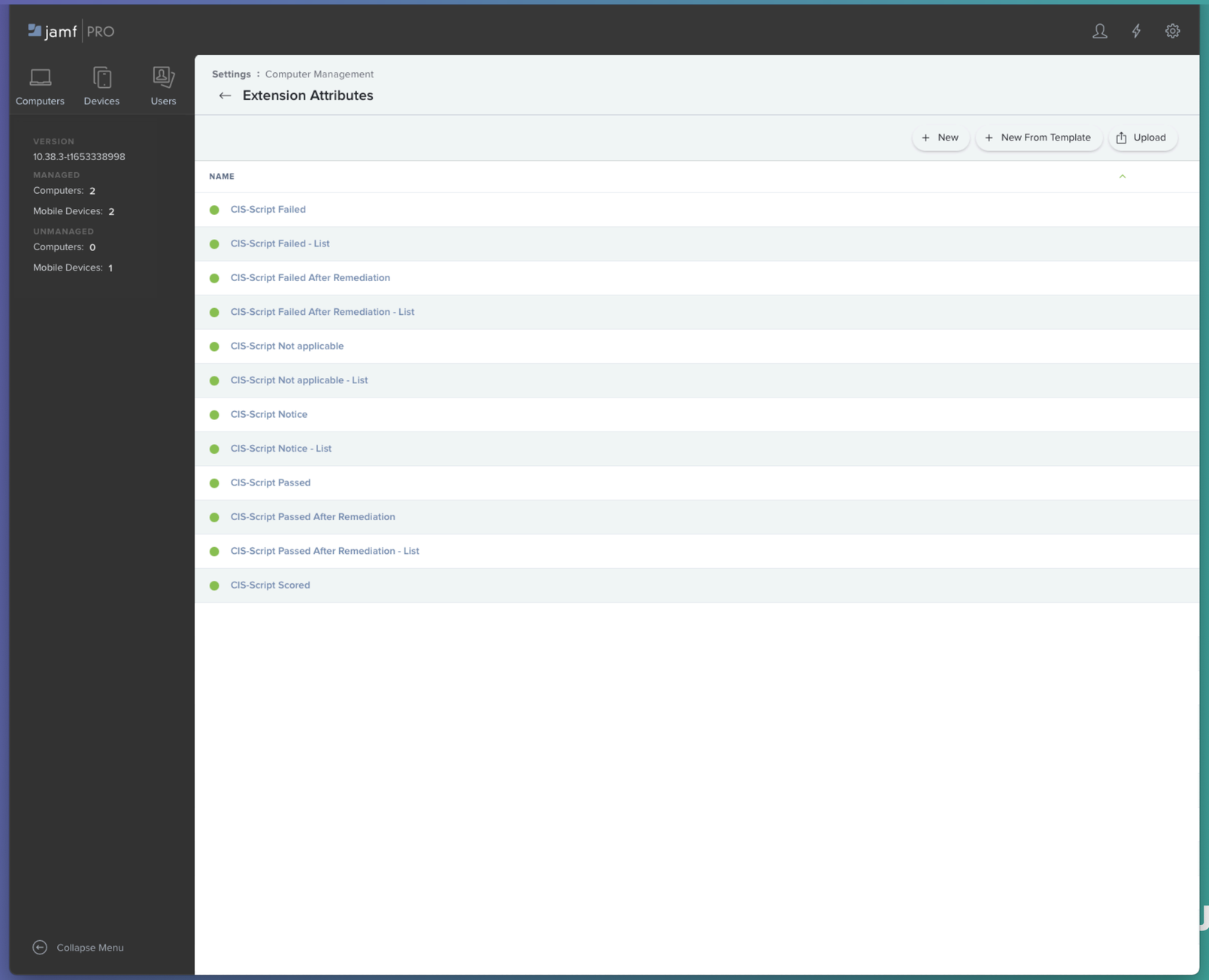


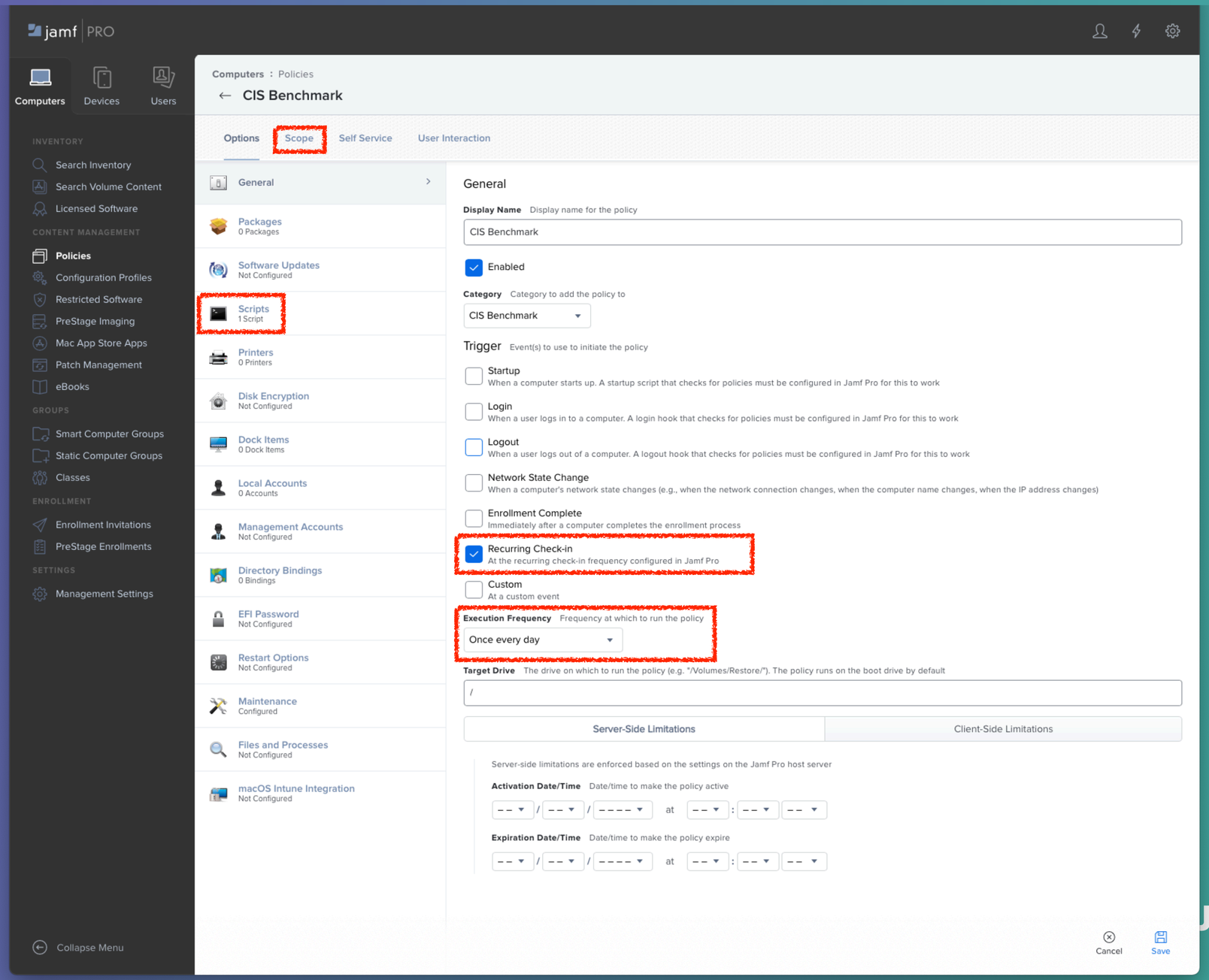
Configure

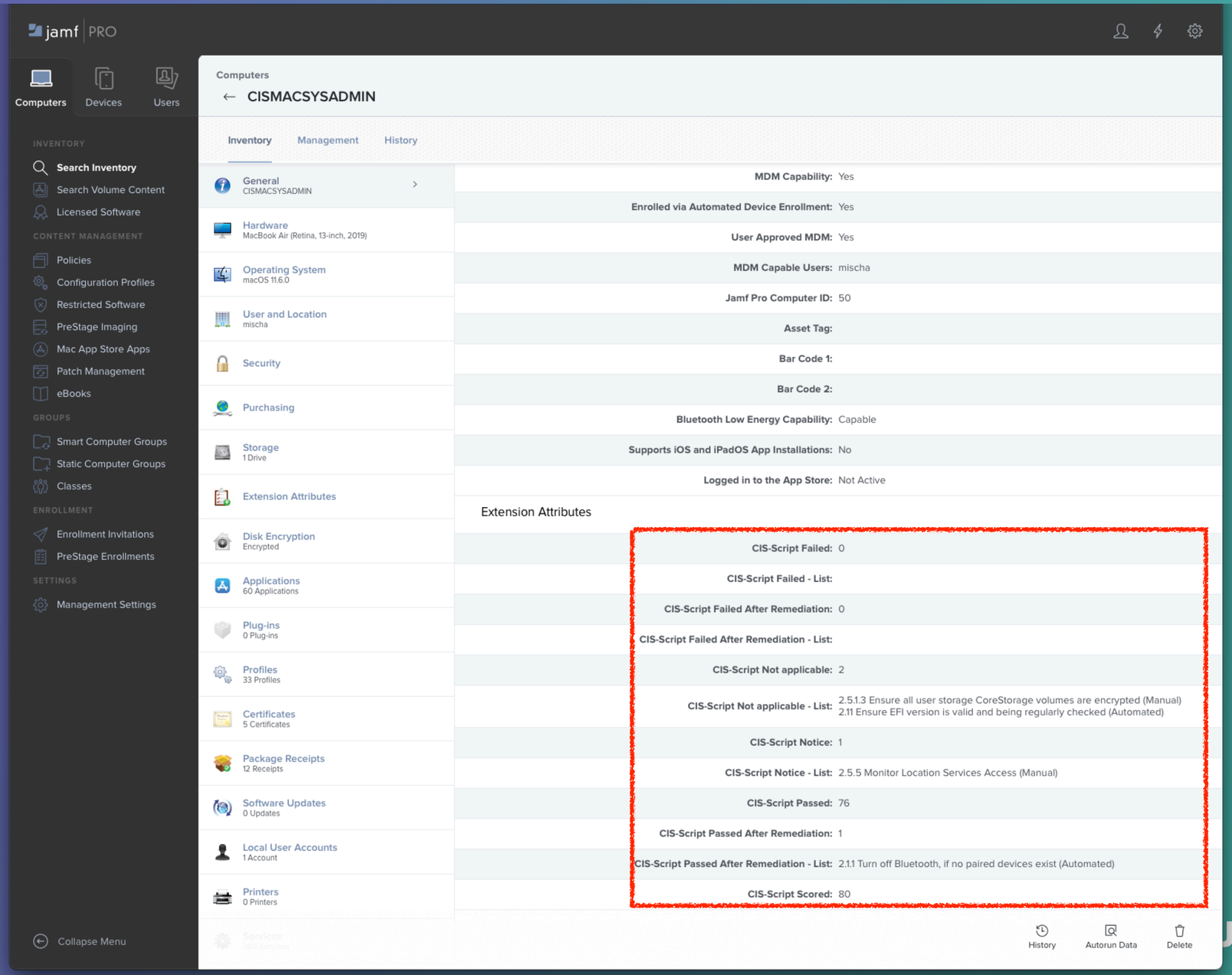
Jamf Pro Custom Schema.json

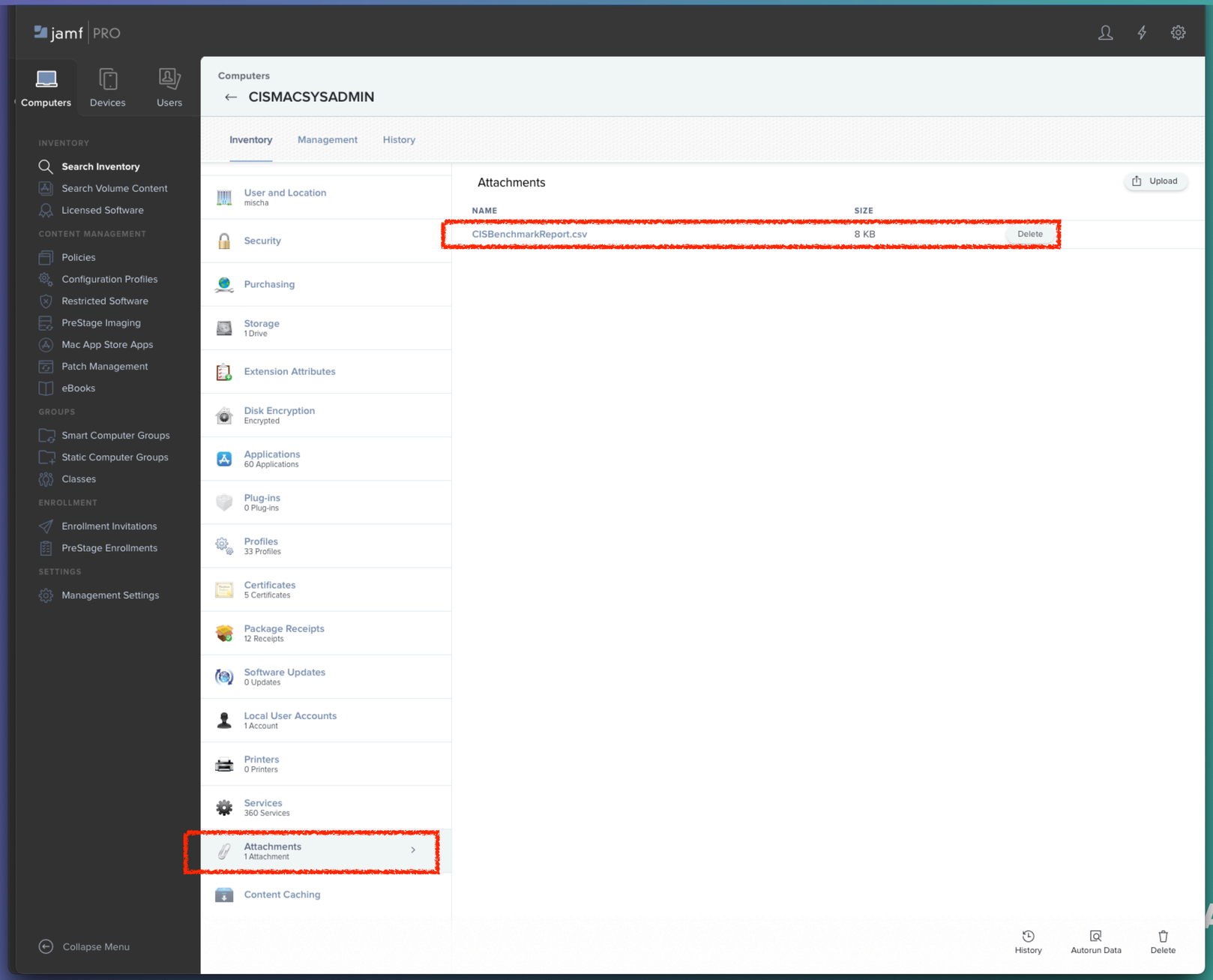

Demo


Finder File Edit View Go Window Help
Wed 8 Jun 16:32
CIS-Script — -zsh — 140×26
mischa@MBAir CIS-Script %









Apple Security Certifications and Compliance Centre

support.apple.com/en-gb/guide/sccc/

macOS Security Compliance

github.com/usnistgov/macos_security

CIS Script

github.com/mvdbent/CIS-Script

@mvdbent

#macos_security_compliance #security

Recap

1 | macOS Security

Have a look what Apple has been doing on the security stack and build into the system.

2 | Security Benchmarks

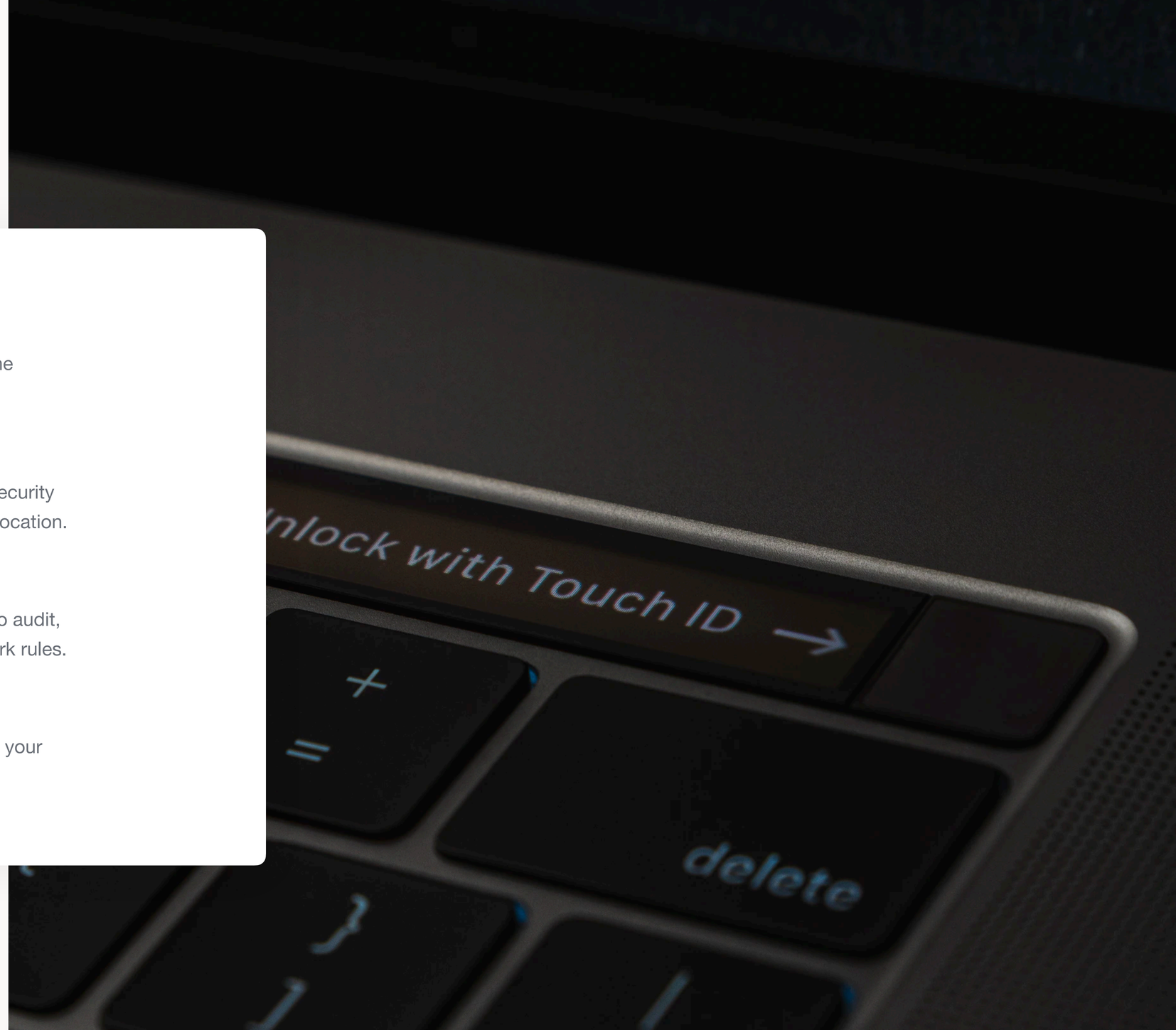
Organisations that provide guidance of the Security standard depending on industry and/or geo-location.

3 | Scripts

How we can use the CIS-Script to help you to audit, remediate and report based on the Benchmark rules.

4 | Implementation

See how easy it is to deploy the CIS script in your environment.




Thank You!
JAMF NATION LIVE

Questions?