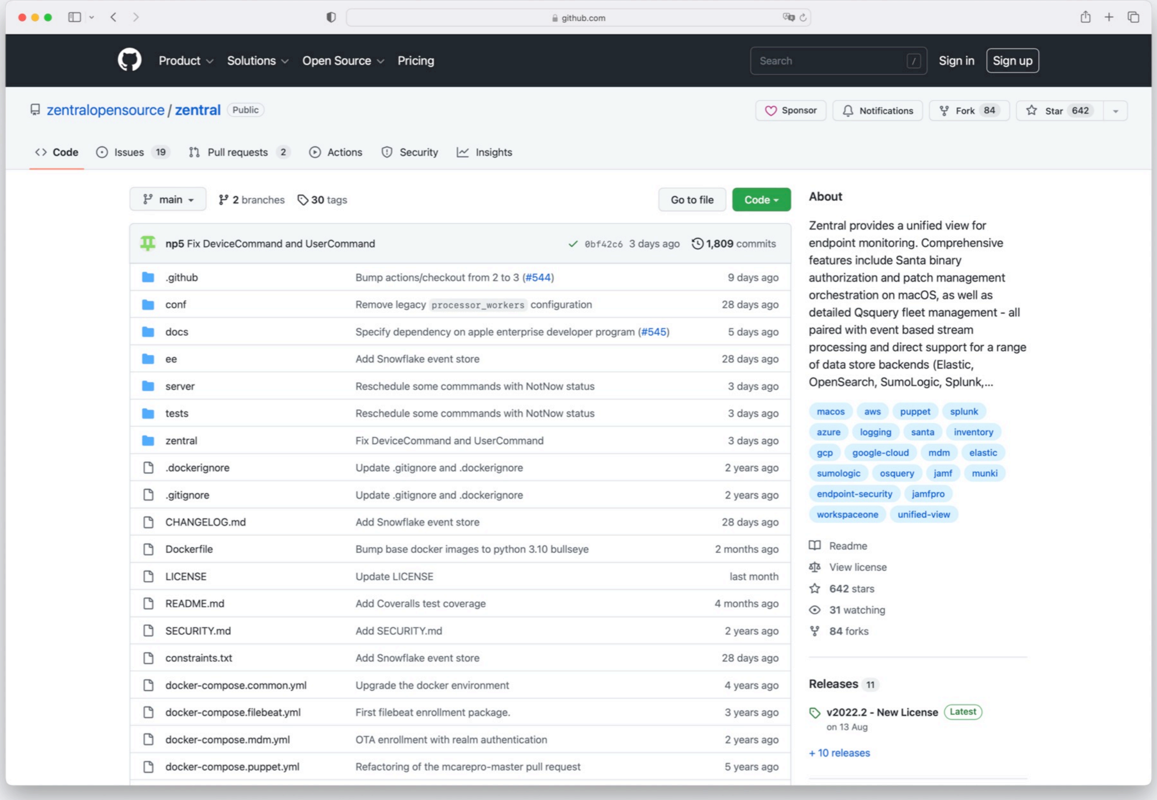
MacSysAdmin 2022

Henry Stamerjohann, October 4-7 2022

https://zentral.io

MacSysAdmin 2022



zentralopensource / zentral Public

np5 Fix DeviceCommand and UserCommand ✓ 0bf42c6 3 days ago 1,809 commits

.github	Bump actions/checkout from 2 to 3 (#544)	9 days ago
conf	Remove legacy `processor_workers` configuration	28 days ago
docs	Specify dependency on apple enterprise developer program (#545)	5 days ago
ee	Add Snowflake event store	28 days ago
server	Reschedule some commands with NotNow status	3 days ago
tests	Reschedule some commands with NotNow status	3 days ago
zentral	Fix DeviceCommand and UserCommand	3 days ago
.dockerignore	Update .gitignore and .dockerignore	2 years ago
.gitignore	Update .gitignore and .dockerignore	2 years ago
CHANGELOG.md	Add Snowflake event store	28 days ago
Dockerfile	Bump base docker images to python 3.10 bullseye	2 months ago
LICENSE	Update LICENSE	last month
README.md	Add Coveralls test coverage	4 months ago
SECURITY.md	Add SECURITY.md	2 years ago
constraints.txt	Add Snowflake event store	28 days ago
docker-compose.common.yml	Upgrade the docker environment	4 years ago
docker-compose.filebeat.yml	First filebeat enrollment package.	3 years ago
docker-compose.mdm.yml	OTA enrollment with realm authentication	2 years ago
docker-compose.puppet.yml	Refactoring of the mcarepro-master pull request	5 years ago

About

Zentral provides a unified view for endpoint monitoring. Comprehensive features include Santa binary authorization and patch management orchestration on macOS, as well as detailed Qsquery fleet management - all paired with event based stream processing and direct support for a range of data store backends (Elastic, OpenSearch, SumoLogic, Splunk,...

Readme

View license

642 stars

31 watching

84 forks

Releases 11

v2022.2 - New License Latest
on 13 Aug

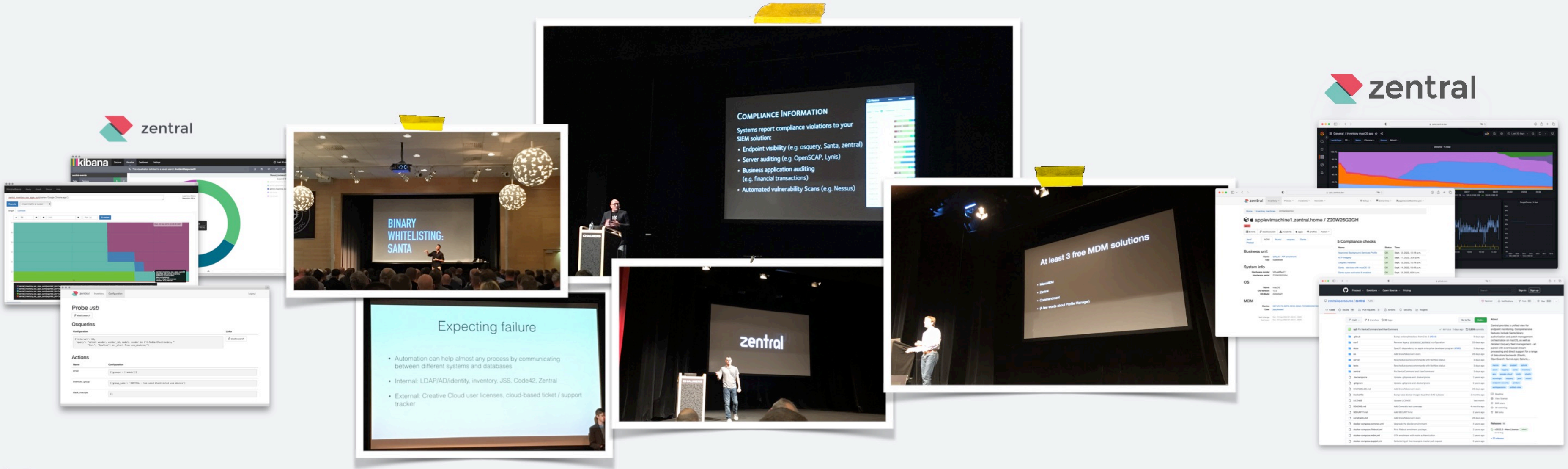
+ 10 releases

Henry Stamerjohann, October 4-7 2022

zentral

https://zentral.io

MacSysAdmin 2022



BINARY WHITELISTING: SANTA

COMPLIANCE INFORMATION

Systems report compliance violations to your SIEM solution:

- Endpoint visibility (e.g. osquery, Santa, zentral)
- Server auditing (e.g. OpenSCAP, Lynis)
- Business application auditing (e.g. financial transactions)
- Automated vulnerability Scans (e.g. Nessus)

Expecting failure

- Automation can help almost any process by communicating between different systems and databases
- Internal: LDAP/AD/identity, inventory, JSS, Code42, Zentral
- External: Creative Cloud user licenses, cloud-based ticket / support tracker

zentral

At least 3 free MDM solutions

- MicroMDM
- Zentral
- Commandment
- (A few words about Profile Manager)

zentral

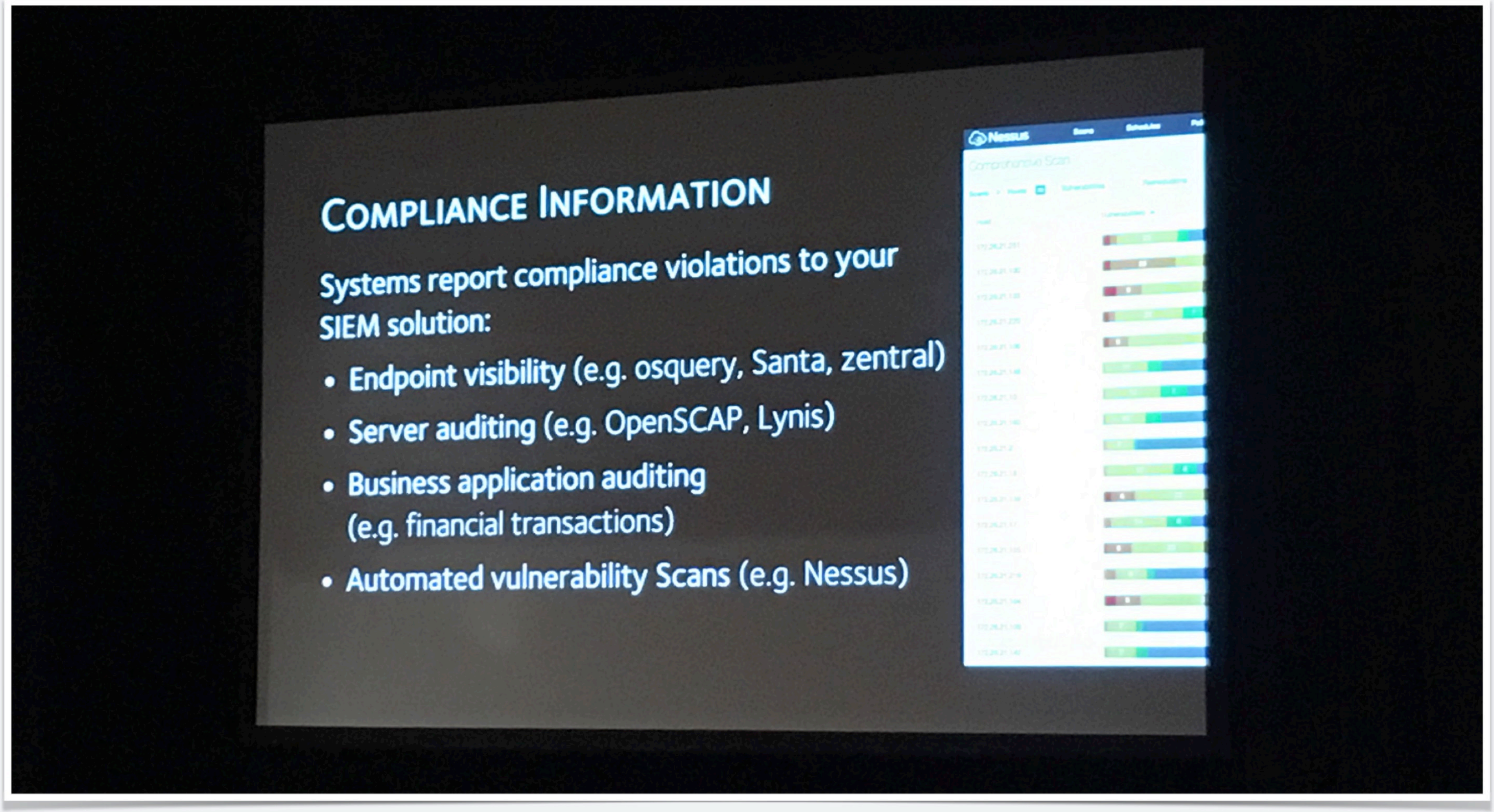
Henry Stamerjohann, October 4-7 2022

https://zentral.io

Compliance ☑

Proof of a compliant state - where's the benefit for macadmins?

Henry Stamerjohann, October 4-7 2022

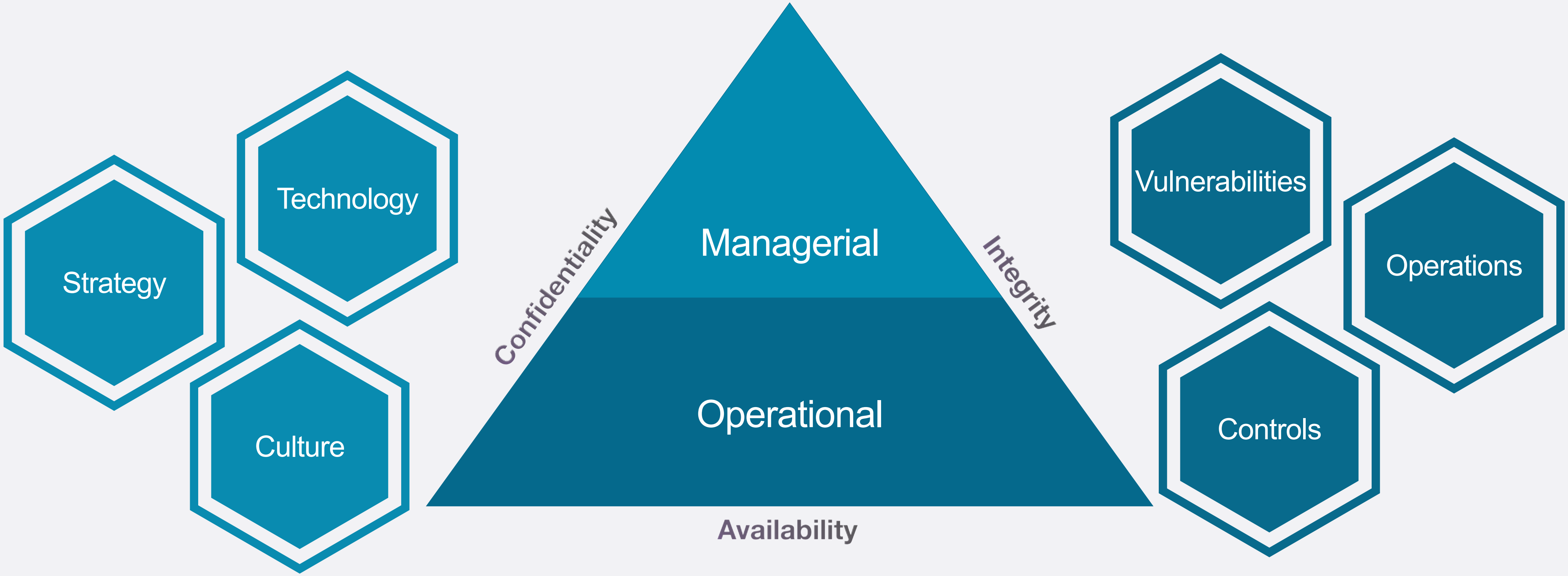


Compliance Information

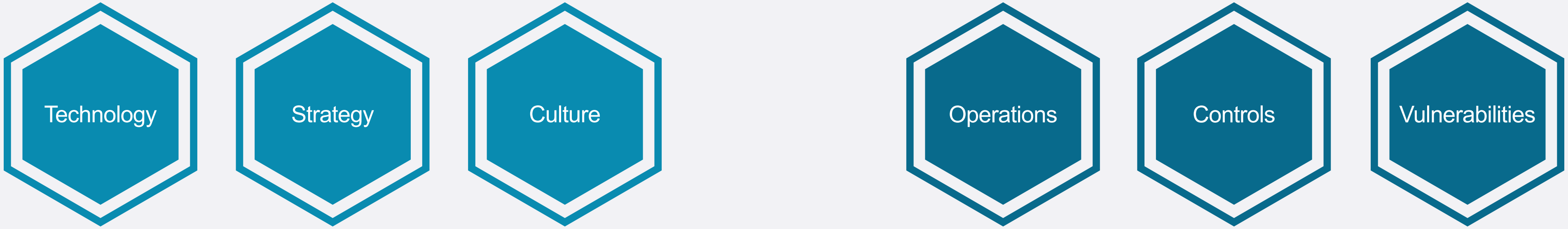
Systems report compliance violations to your SIEM solution:

- Endpoint visibility (e.g. osquery, Santa, zentral)
- Server auditing (e.g. OpenSCAP, Lynis)
- Business application auditing (e.g. financial transactions)
- Automated vulnerability Scans (e.g. Nessus)

Perspectives



Perspectives



Technology

Strategy

Culture

Operations

Controls

Vulnerabilities

- Strategize and apply concepts
- Implement management tools and methodologies
- Critically analyze the current business situation
- Identify target state
- Perform a gap analysis
- Develop a comprehensive cybersecurity roadmap
- Includes employees at all levels in the organization in every type of job role

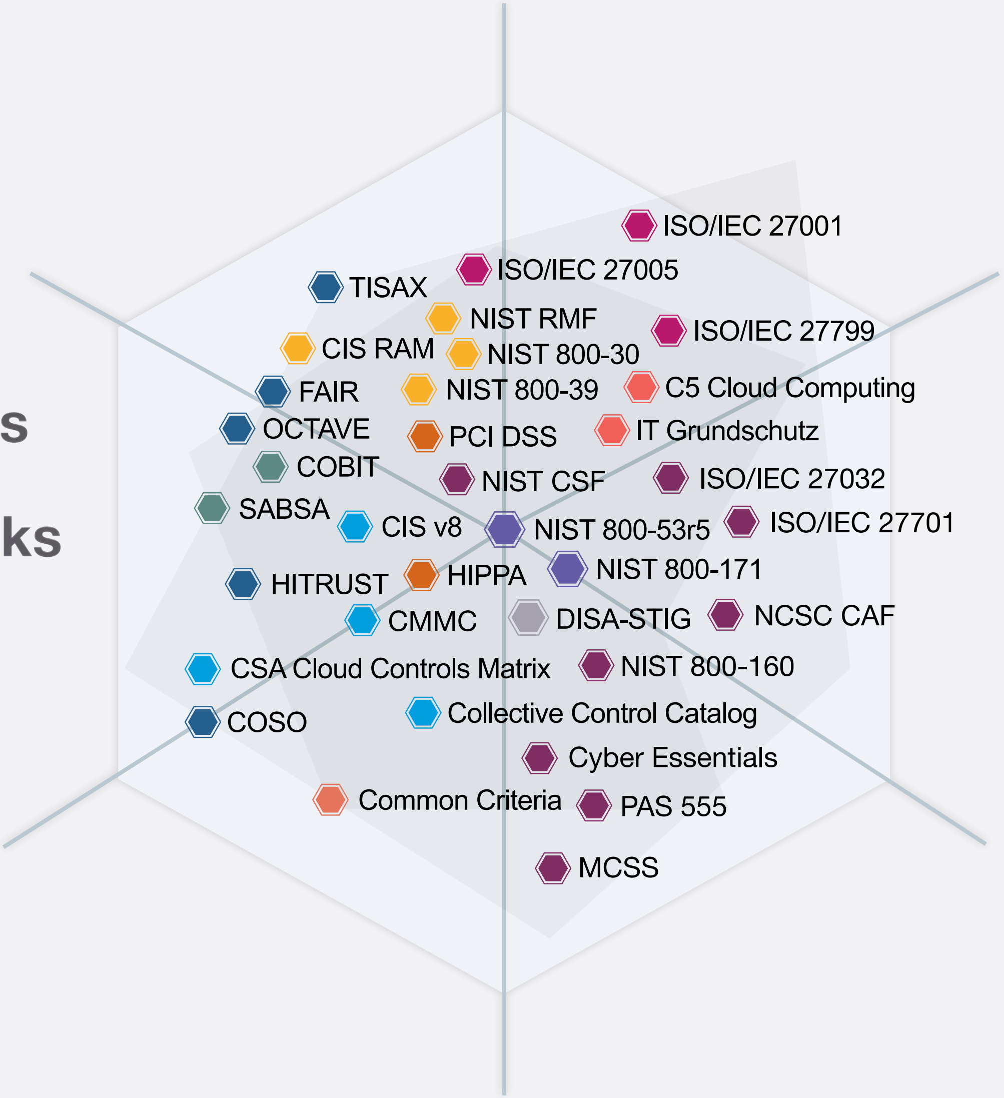
- Understand security controls
- Implement security controls
- Audit security controls
- Create an effective, comprehensive vulnerability management model
- Guide which threats need attention
- Continually mature your security operations, in turn saving time, money, and hours of frustration.

Source: SANS, 2020 I ALL RIGHTS RESERVED

Control frameworks

Program frameworks

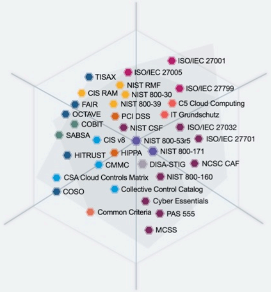
Risk frameworks



Control frameworks

Program frameworks

Risk frameworks

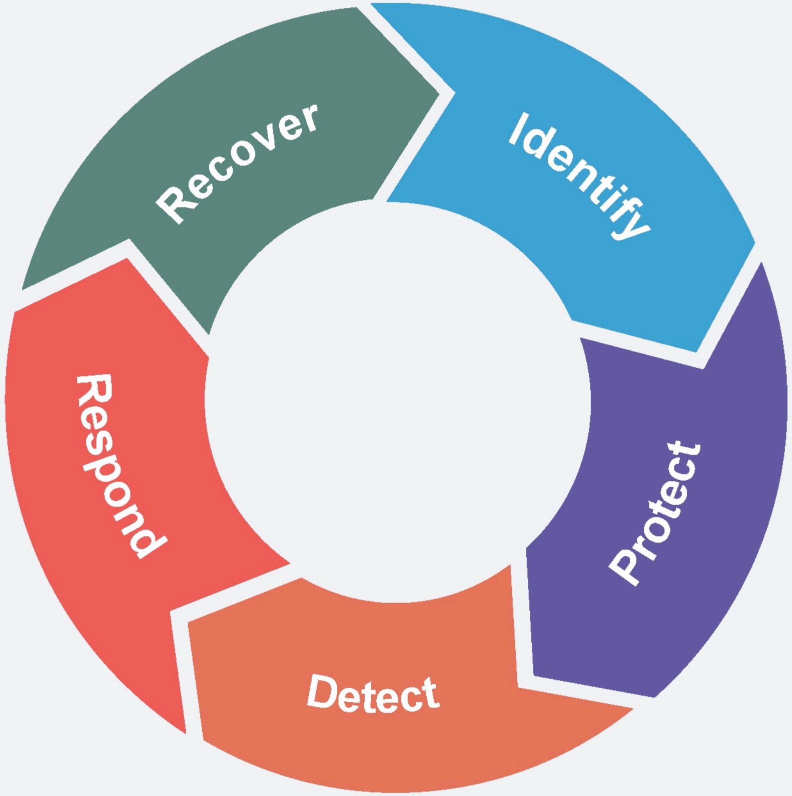


Cyber Security Framework

NIST CSF v1.1

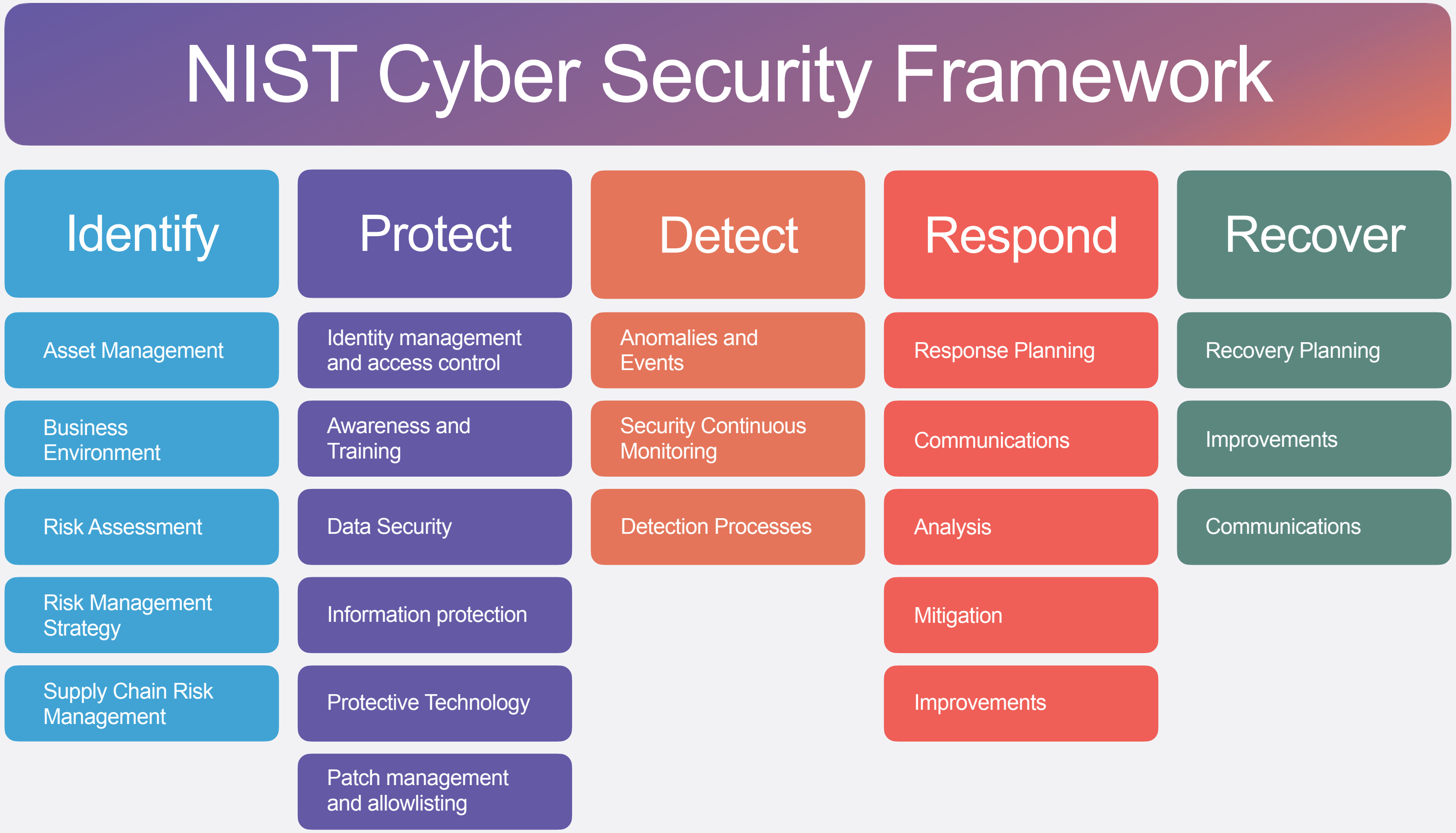
NIST CSF v1.1

Framework Core



NIST CSF v1.1

Profiles

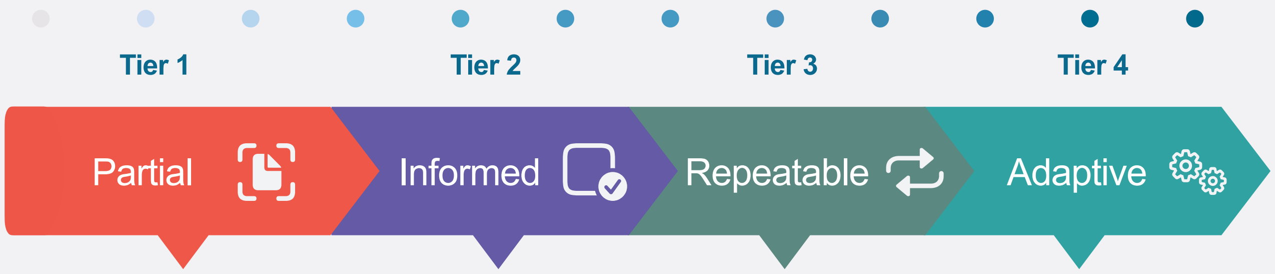


NIST Cyber Security Framework

Identify	Protect	Detect	Respond	Recover
Asset Management	Identity management and access control	Anomalies and Events	Response Planning	Recovery Planning
Business Environment	Awareness and Training	Security Continuous Monitoring	Communications	Improvements
Risk Assessment	Data Security	Detection Processes	Analysis	Communications
Risk Management Strategy	Information protection		Mitigation	
Supply Chain Risk Management	Protective Technology		Improvements	
	Patch management and allowlisting			

NIST CSF v1.1

Tiers



Tier 1

Partial

- Sparse defined processes and procedures
- No or incomplete documentation
- Ad-hoc decisions and reactive processes
- Basic IT security measures and tools

Tier 2

Informed

- Largely defined processes and procedures
- Documentation in place, manual maintenance
- Focus on prevention and response
- Integration of IT security measures and tools

Tier 3

Repeatable

- Processes well defined and implemented
- Consistent security architecture
- Formal and standardized approach
- Functional IT risk management, basis for strategy

Tier 4

Adaptive

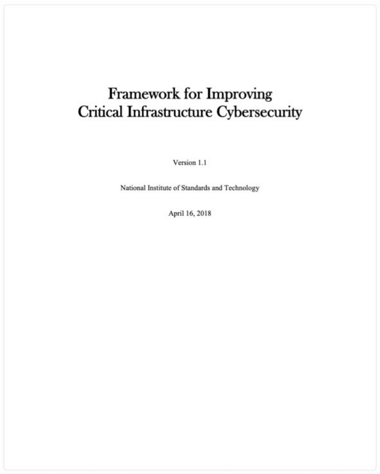
- Processes largely automated, KPIs in place
- Security is corporate culture, security awareness, security by design
- Business process risk understanding
- Integrated Risk Management Process and enhanced Security Monitoring

NIST Cyber Security Framework

Identify	Protect	Detect	Respond	Recover
Asset Management	Identity management and access control	Anomalies and Events	Response Planning	Recovery Planning
Business Environment	Awareness and Training	Security Continuous Monitoring	Communications	Improvements
Risk Assessment	Data Security	Detection Processes	Analysis	Communications
Risk Management Strategy	Information protection		Mitigation	
Supply Chain Risk Management	Protective Technology		Improvements	
	Patch management and allowlisting			

Guiding principles

Guardrails in achieving the goal



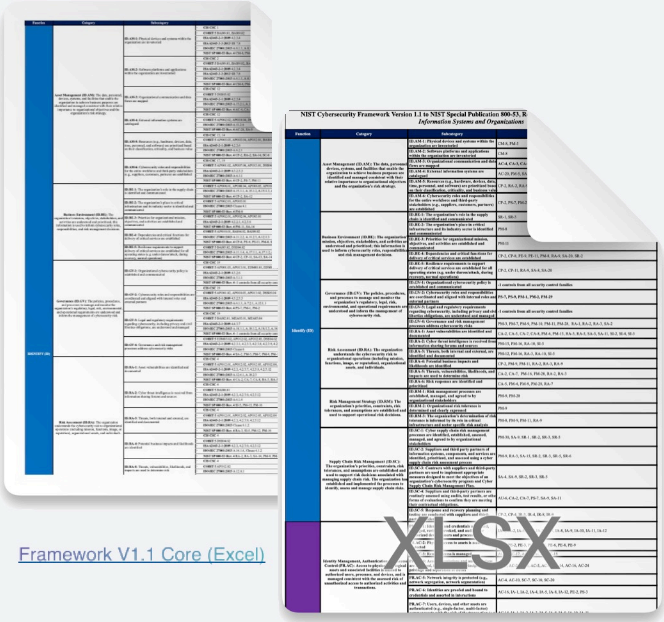
Framework for Improving
Critical Infrastructure Cybersecurity

Version 1.1

National Institute of Standards and Technology

April 16, 2018

Framework V1.1 (PDF)



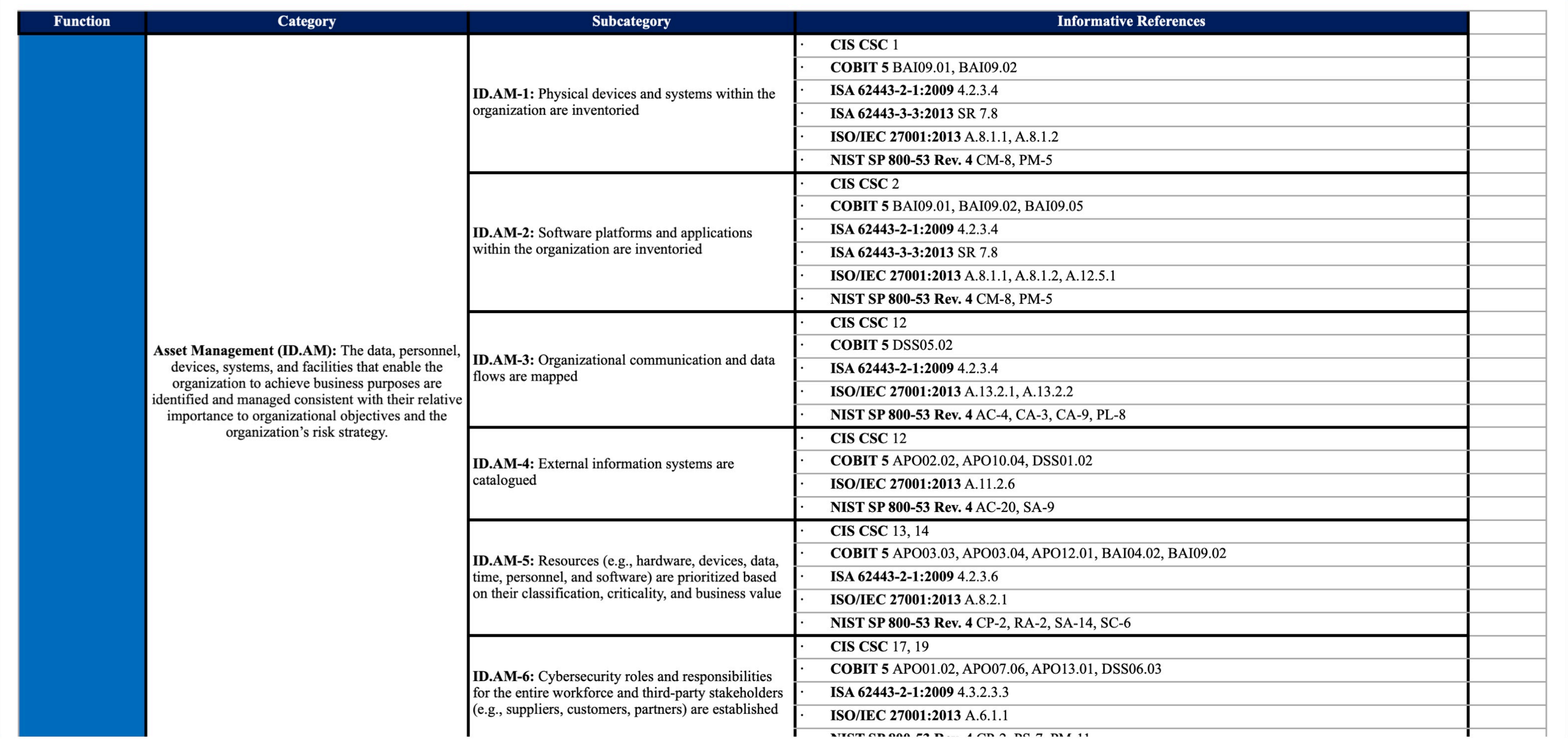
NIST Cybersecurity Framework Version 1.1 to NIST Special Publication 800-53, R
Information Systems and Organizations

Function	Category	Subcategory

Framework V1.1 Core (Excel)

https://www.nist.gov/cyberframework/framework

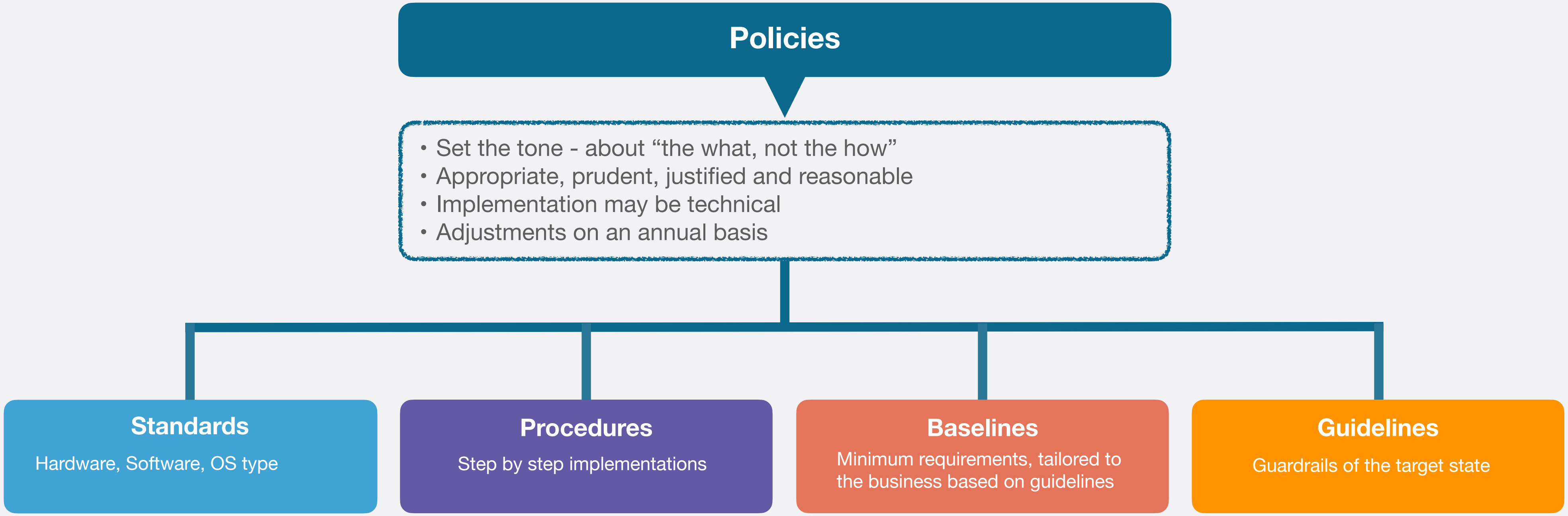
Guiding principles



Function	Category	Subcategory	Informative References
	Asset Management (ID.AM): The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to organizational objectives and the organization's risk strategy.	**ID.AM-1:** Physical devices and systems within the organization are inventoried	· **CIS CSC** 1
			· **COBIT 5** BAI09.01, BAI09.02
			· **ISA 62443-2-1:2009** 4.2.3.4
			· **ISA 62443-3-3:2013** SR 7.8
			· **ISO/IEC 27001:2013** A.8.1.1, A.8.1.2
			· **NIST SP 800-53 Rev. 4** CM-8, PM-5
		ID.AM-2: Software platforms and applications within the organization are inventoried	· **CIS CSC** 2
			· **COBIT 5** BAI09.01, BAI09.02, BAI09.05
			· **ISA 62443-2-1:2009** 4.2.3.4
			· **ISA 62443-3-3:2013** SR 7.8
			· **ISO/IEC 27001:2013** A.8.1.1, A.8.1.2, A.12.5.1
			· **NIST SP 800-53 Rev. 4** CM-8, PM-5
		ID.AM-3: Organizational communication and data flows are mapped	· **CIS CSC** 12
			· **COBIT 5** DSS05.02
			· **ISA 62443-2-1:2009** 4.2.3.4
			· **ISO/IEC 27001:2013** A.13.2.1, A.13.2.2
			· **NIST SP 800-53 Rev. 4** AC-4, CA-3, CA-9, PL-8
		ID.AM-4: External information systems are catalogued	· **CIS CSC** 12
			· **COBIT 5** APO02.02, APO10.04, DSS01.02
			· **ISO/IEC 27001:2013** A.11.2.6
			· **NIST SP 800-53 Rev. 4** AC-20, SA-9
		ID.AM-5: Resources (e.g., hardware, devices, data, time, personnel, and software) are prioritized based on their classification, criticality, and business value	· **CIS CSC** 13, 14
			· **COBIT 5** APO03.03, APO03.04, APO12.01, BAI04.02, BAI09.02
			· **ISA 62443-2-1:2009** 4.2.3.6
			· **ISO/IEC 27001:2013** A.8.2.1
			· **NIST SP 800-53 Rev. 4** CP-2, RA-2, SA-14, SC-6
		ID.AM-6: Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established	· **CIS CSC** 17, 19
			· **COBIT 5** APO01.02, APO07.06, APO13.01, DSS06.03
			· **ISA 62443-2-1:2009** 4.3.2.3.3
			· **ISO/IEC 27001:2013** A.6.1.1
			· **NIST SP 800-53 Rev. 4** CP-2, PS-7, PM-11

Policies

Aligned with the business



Policies

- Set the tone - about “the what, not the how”
- Appropriate, prudent, justified and reasonable
- Implementation may be technical
- Adjustments on an annual basis

Standards

Hardware, Software, OS type

Procedures

Step by step implementations

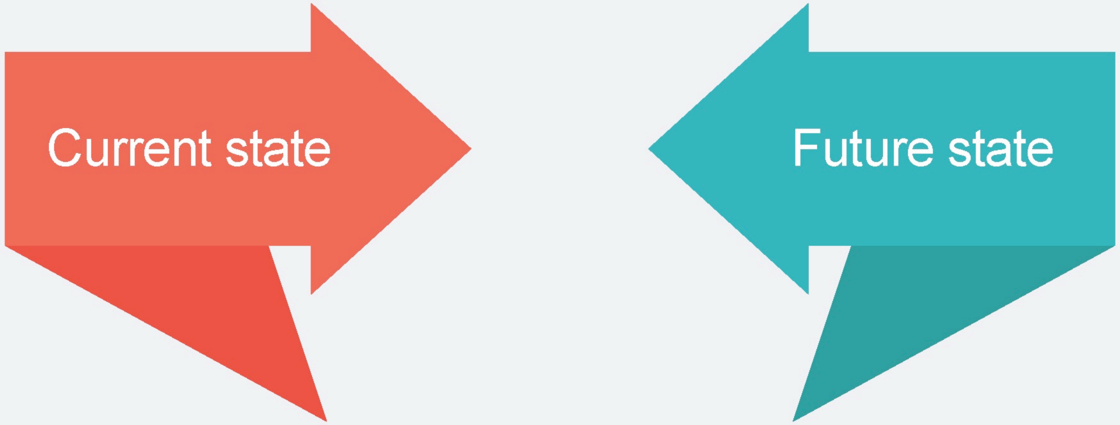
Baselines

Minimum requirements, tailored to the business based on guidelines

Guidelines

Guardrails of the target state

Gap analysis

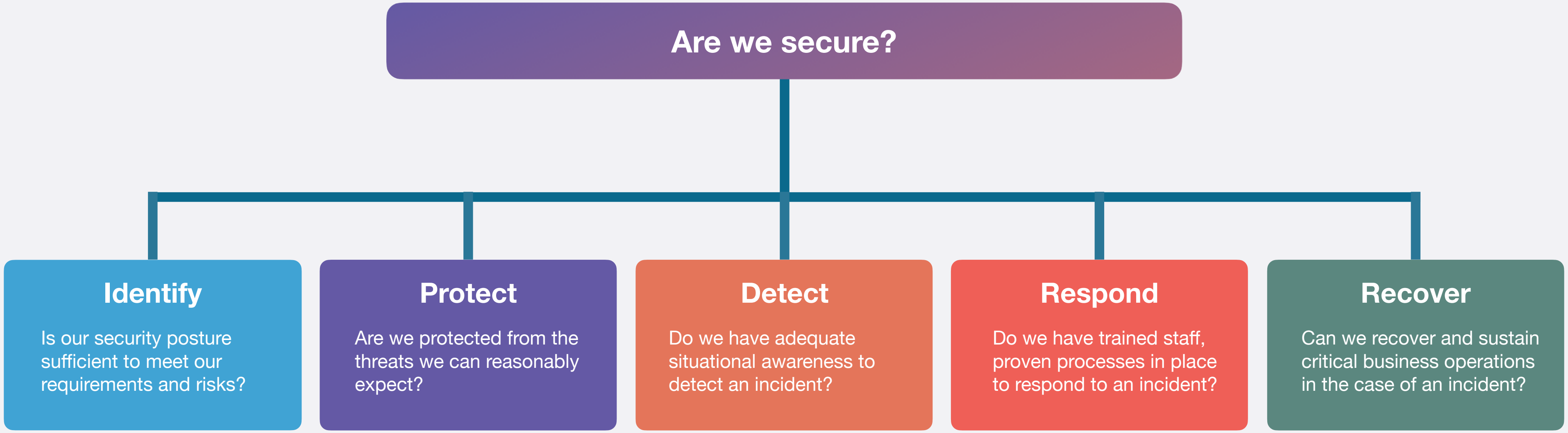


Current state

Future state

Continuous improvement

Built a risk register



Are we secure?

Identify

Is our security posture sufficient to meet our requirements and risks?

Protect

Are we protected from the threats we can reasonably expect?

Detect

Do we have adequate situational awareness to detect an incident?

Respond

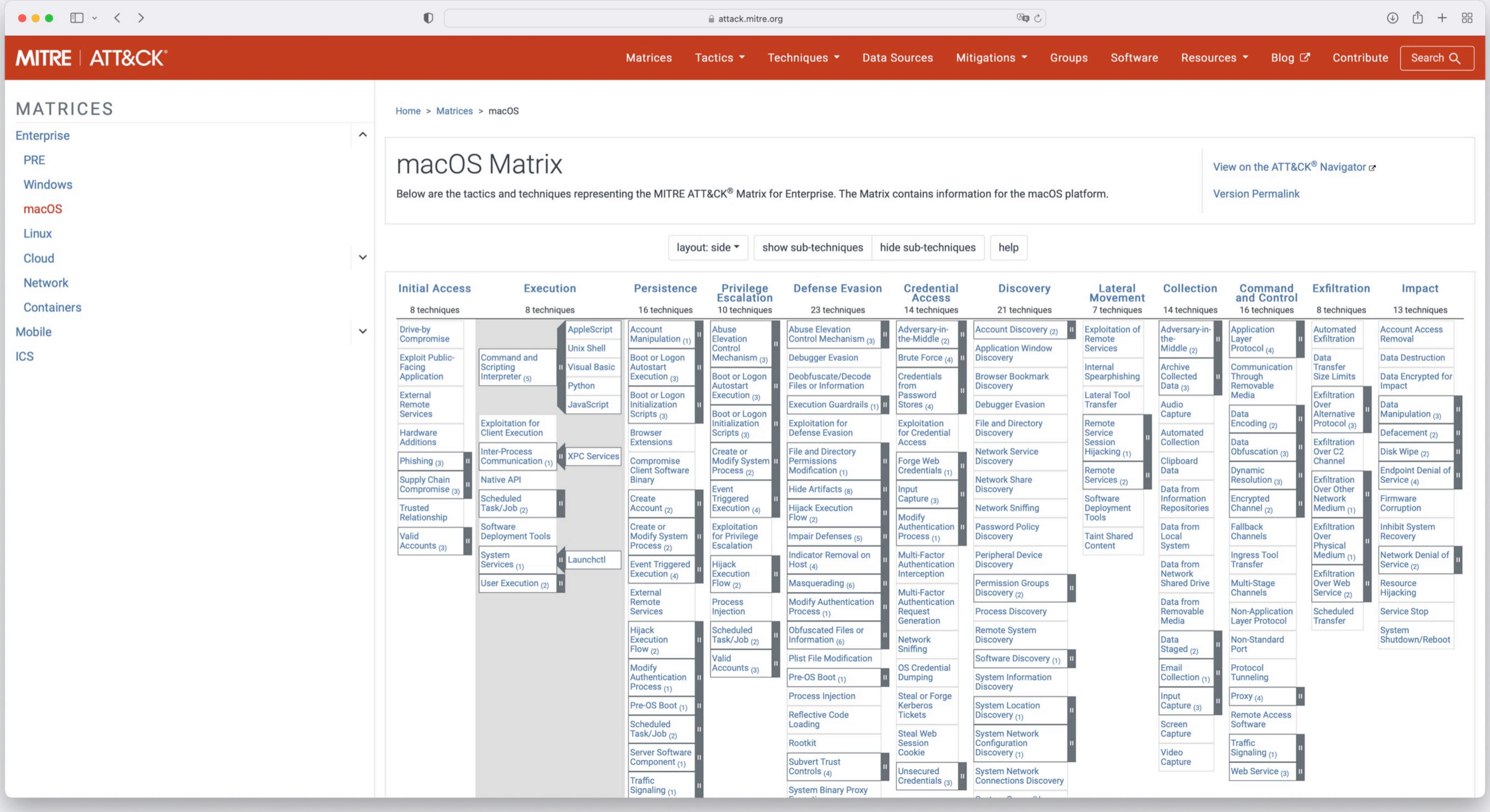
Do we have trained staff, proven processes in place to respond to an incident?

Recover

Can we recover and sustain critical business operations in the case of an incident?

Adversarial Tactics, Techniques, & Common Knowledge

MITRE ATT&CK



Home > Matrices > macOS

macOS Matrix

Below are the tactics and techniques representing the MITRE ATT&CK® Matrix for Enterprise. The Matrix contains information for the macOS platform.

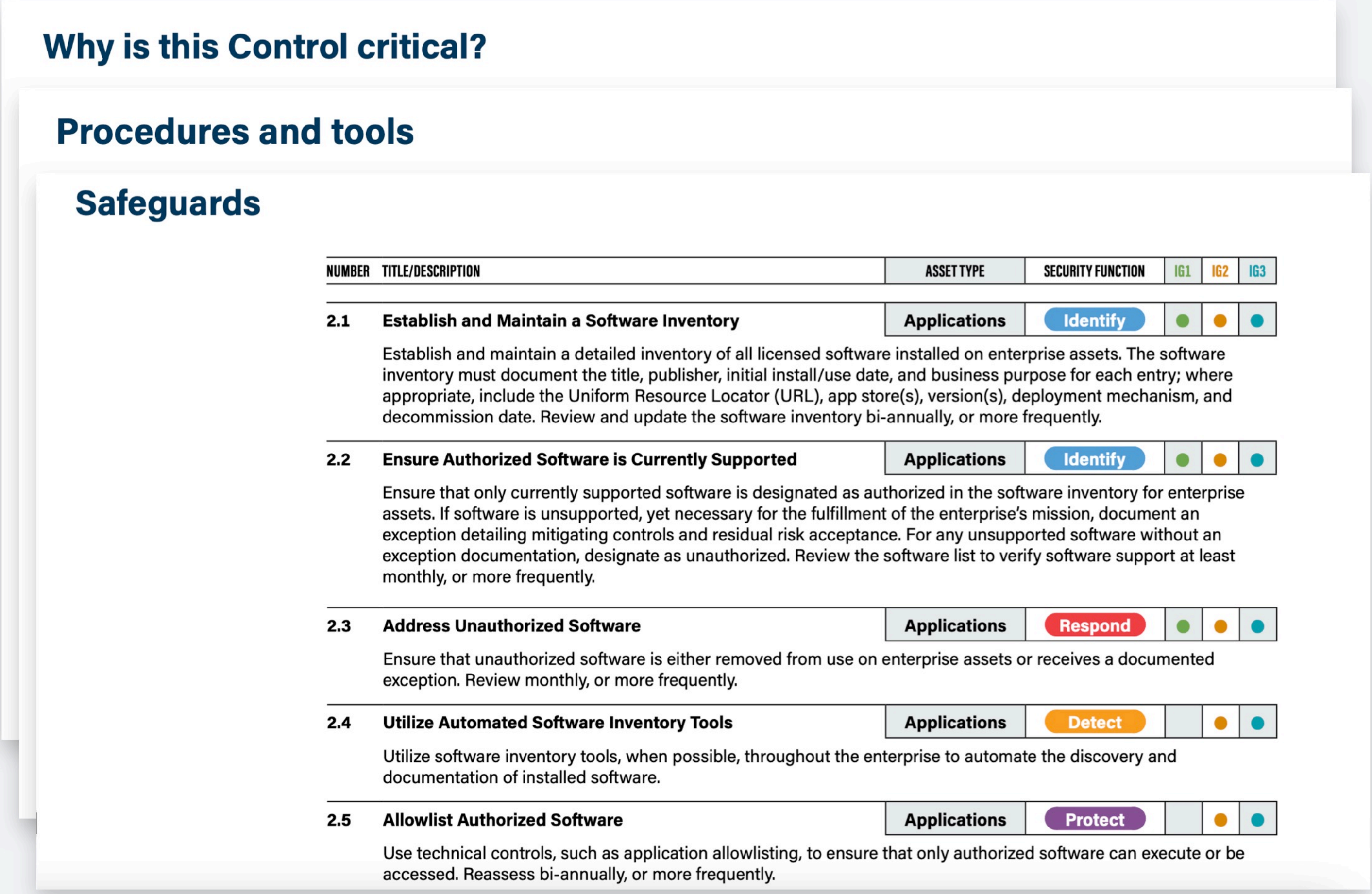
View on the ATT&CK® Navigator

Version Permalink

Initial Access 8 techniques	Execution 8 techniques	Persistence 16 techniques	Privilege Escalation 10 techniques	Defense Evasion 23 techniques	Credential Access 14 techniques	Discovery 21 techniques	Lateral Movement 7 techniques	Collection 14 techniques	Command and Control 16 techniques	Exfiltration 8 techniques	Impact 13 techniques
Drive-by Compromise	Command and Scripting Interpreter (5) AppleScript Unix Shell Visual Basic Python JavaScript	Account Manipulation (1)	Abuse Elevation Control Mechanism (3)	Abuse Elevation Control Mechanism (3)	Adversary-in-the-Middle (2)	Account Discovery (2)	Exploitation of Remote Services	Adversary-in-the-Middle (2)	Application Layer Protocol (4)	Automated Exfiltration	Account Access Removal
Exploit Public-Facing Application	Exploitation for Client Execution	Boot or Logon Autostart Execution (3)	Boot or Logon Autostart Execution (3)	Debugger Evasion	Brute Force (4)	Application Window Discovery	Internal Spearphishing	Archive Collected Data (3)	Communication Through Removable Media	Data Transfer Size Limits	Data Destruction
External Remote Services	Inter-Process Communication (1) XPC Services	Boot or Logon Initialization Scripts (3)	Boot or Logon Initialization Scripts (3)	Deobfuscate/Decode Files or Information	Credentials from Password Stores (4)	Browser Bookmark Discovery	Lateral Tool Transfer	Audio Capture	Data Encoding (2)	Exfiltration Over Alternative Protocol (3)	Data Encrypted for Impact
Hardware Additions	Native API	Browser Extensions	Create or Modify System Process (2)	Execution Guardrails (1)	Exploitation for Credential Access	Debugger Evasion	Remote Service Session Hijacking (1)	Automated Collection	Data Obfuscation (3)	Exfiltration Over C2 Channel	Data Manipulation (3)
Phishing (3)	Scheduled Task/Job (2)	Compromise Client Software Binary	Event Triggered Execution (4)	Exploitation for Defense Evasion	Forge Web Credentials (1)	File and Directory Discovery	Remote Services (2)	Clipboard Data	Dynamic Resolution (3)	Exfiltration Over Other Network Medium (1)	Defacement (2)
Supply Chain Compromise (3)	Software Deployment Tools	Create Account (2)	Exploitation for Privilege Escalation	File and Directory Permissions Modification (1)	Input Capture (3)	Network Service Discovery	Software Deployment Tools	Data from Information Repositories	Encrypted Channel (2)	Exfiltration Over Physical Medium (1)	Disk Wipe (2)
Trusted Relationship	System Services (1) Launchctl	Create or Modify System Process (2)	Hijack Execution Flow (2)	Hide Artifacts (8)	Modify Authentication Process (1)	Network Share Discovery	Taint Shared Content	Data from Local System	Fallback Channels	Exfiltration Over Web Service (2)	Endpoint Denial of Service (4)
Valid Accounts (3)	User Execution (2)	Event Triggered Execution (4)	Process Injection	Hijack Execution Flow (2)	Multi-Factor Authentication Interception	Network Sniffing		Data from Network Shared Drive	Ingress Tool Transfer	Scheduled Transfer	Firmware Corruption
		External Remote Services	Scheduled Task/Job (2)	Impair Defenses (5)	Multi-Factor Authentication Request Generation	Password Policy Discovery		Data from Removable Media	Multi-Stage Channels		Inhibit System Recovery
		Hijack Execution Flow (2)	Valid Accounts (3)	Indicator Removal on Host (4)	Network Sniffing	Peripheral Device Discovery		Data Staged (2)	Non-Application Layer Protocol		Network Denial of Service (2)
		Modify Authentication Process (1)		Masquerading (6)	OS Credential Dumping	Permission Groups Discovery (2)		Email Collection (1)	Non-Standard Port		Resource Hijacking
		Pre-OS Boot (1)		Modify Authentication Process (1)	Steal or Forge Kerberos Tickets	Process Discovery		Input Capture (3)	Protocol Tunneling		Service Stop
		Scheduled Task/Job (2)		Obfuscated Files or Information (6)	Steal Web Session Cookie	Remote System Discovery		Screen Capture	Proxy (4)		System Shutdown/Reboot
		Server Software Component (1)		Plist File Modification	Unsecured Credentials (3)	Software Discovery (1)		Video Capture	Remote Access Software		
		Traffic Signaling (1)		Pre-OS Boot (1)		System Information Discovery			Traffic Signaling (1)		
				Process Injection		System Location Discovery (1)			Web Service (3)		
				Reflective Code Loading		System Network Configuration Discovery (1)					
				Rootkit		System Network Connections Discovery					
				Subvert Trust Controls (4)							
				System Binary Proxy							

CIS
Critical Security Controls v8

CIS
Critical Security Controls v8

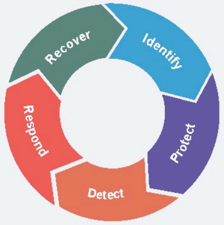


Why is this Control critical?

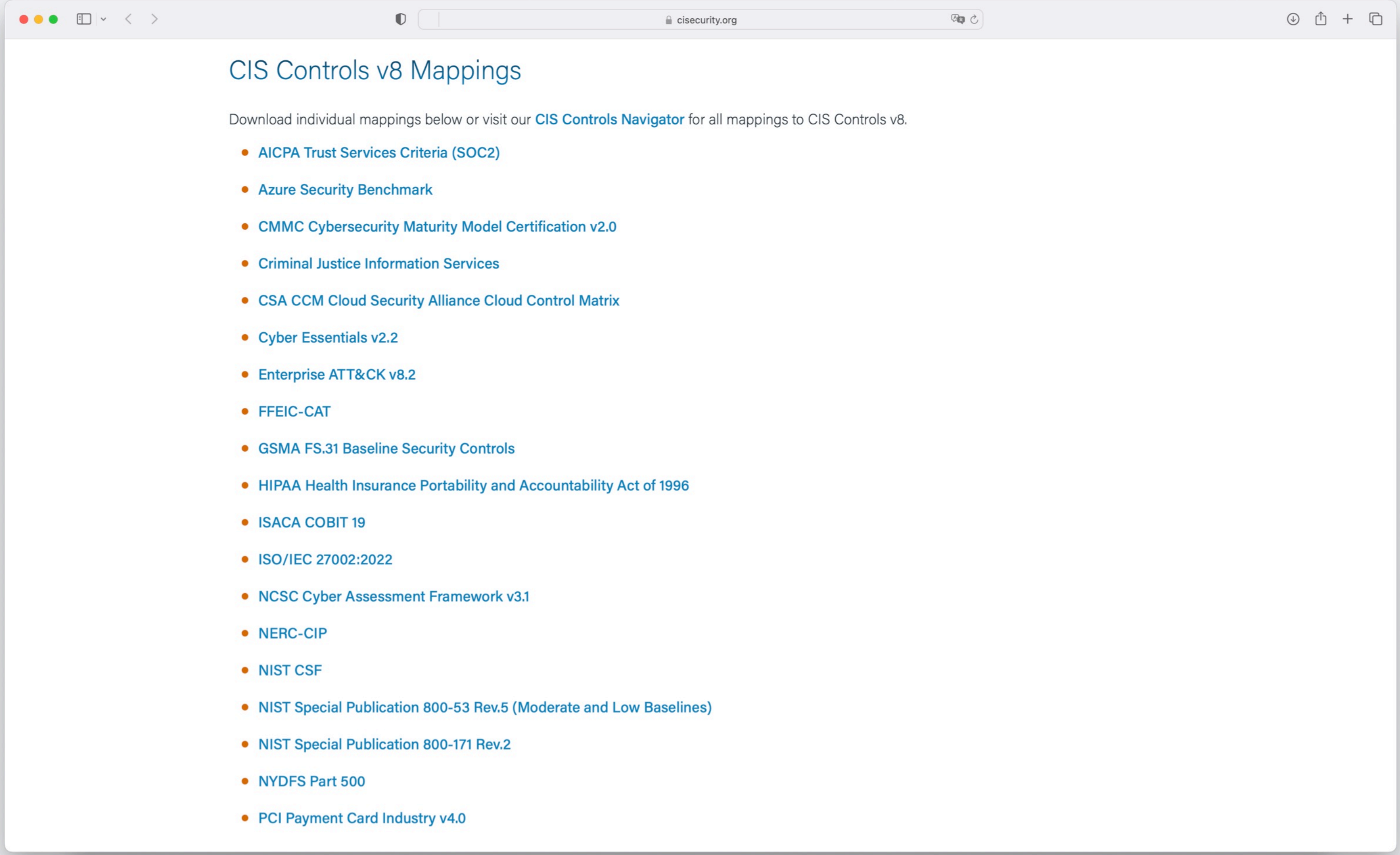
Procedures and tools

Safeguards

NUMBER	TITLE/DESCRIPTION	ASSET TYPE	SECURITY FUNCTION	IG1	IG2	IG3
2.1	**Establish and Maintain a Software Inventory** Establish and maintain a detailed inventory of all licensed software installed on enterprise assets. The software inventory must document the title, publisher, initial install/use date, and business purpose for each entry; where appropriate, include the Uniform Resource Locator (URL), app store(s), version(s), deployment mechanism, and decommission date. Review and update the software inventory bi-annually, or more frequently.	Applications	Identify	●	●	●
2.2	**Ensure Authorized Software is Currently Supported** Ensure that only currently supported software is designated as authorized in the software inventory for enterprise assets. If software is unsupported, yet necessary for the fulfillment of the enterprise's mission, document an exception detailing mitigating controls and residual risk acceptance. For any unsupported software without an exception documentation, designate as unauthorized. Review the software list to verify software support at least monthly, or more frequently.	Applications	Identify	●	●	●
2.3	**Address Unauthorized Software** Ensure that unauthorized software is either removed from use on enterprise assets or receives a documented exception. Review monthly, or more frequently.	Applications	Respond	●	●	●
2.4	**Utilize Automated Software Inventory Tools** Utilize software inventory tools, when possible, throughout the enterprise to automate the discovery and documentation of installed software.	Applications	Detect		●	●
2.5	**Allowlist Authorized Software** Use technical controls, such as application allowlisting, to ensure that only authorized software can execute or be accessed. Reassess bi-annually, or more frequently.	Applications	Protect		●	●



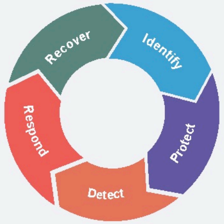
CIS
Critical Security Controls v8



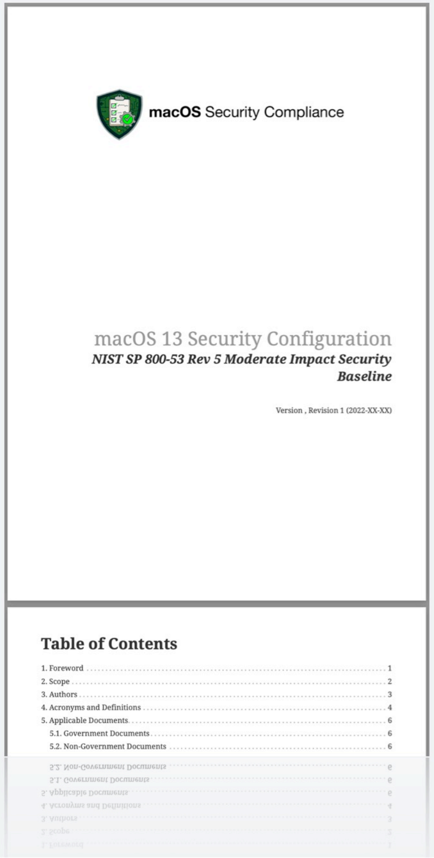
CIS Controls v8 Mappings

Download individual mappings below or visit our CIS Controls Navigator for all mappings to CIS Controls v8.

- AICPA Trust Services Criteria (SOC2)
- Azure Security Benchmark
- CMMC Cybersecurity Maturity Model Certification v2.0
- Criminal Justice Information Services
- CSA CCM Cloud Security Alliance Cloud Control Matrix
- Cyber Essentials v2.2
- Enterprise ATT&CK v8.2
- FFEIC-CAT
- GSMA FS.31 Baseline Security Controls
- HIPAA Health Insurance Portability and Accountability Act of 1996
- ISACA COBIT 19
- ISO/IEC 27002:2022
- NCSC Cyber Assessment Framework v3.1
- NERC-CIP
- NIST CSF
- NIST Special Publication 800-53 Rev.5 (Moderate and Low Baselines)
- NIST Special Publication 800-171 Rev.2
- NYDFS Part 500
- PCI Payment Card Industry v4.0



macOS Security Compliance Project
NIST 800-53 and CIS critical controls v8

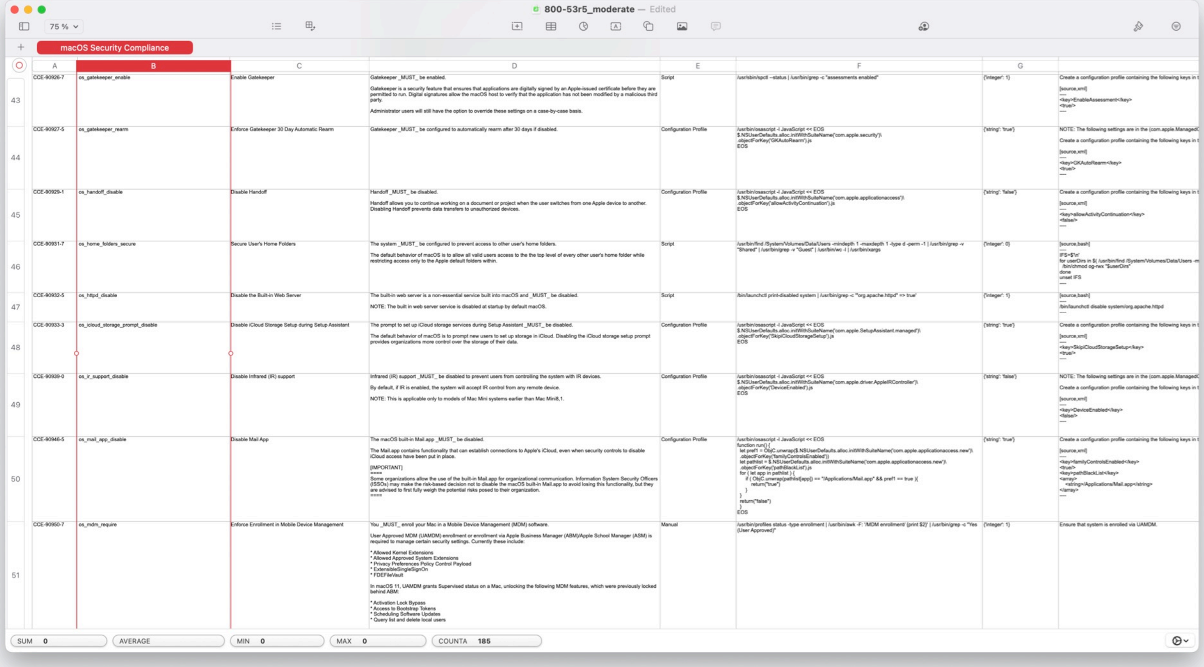


macOS Security Compliance

macOS 13 Security Configuration
NIST SP 800-53 Rev 5 Moderate Impact Security Baseline

Version , Revision 1 (2022-XX-XX)

Table of Contents



	A	B	C	D	E	F	G	
43	CCE-90926-7	os_gatekeeper_enable	Enable Gatekeeper	Gatekeeper _MUST_ be enabled. Gatekeeper is a security feature that ensures that applications are digitally signed by an Apple-issued certificate before they are permitted to run. Digital signatures allow the macOS host to verify that the application has not been modified by a malicious third party. Administrator users will still have the option to override these settings on a case-by-case basis.	Script	/usr/sbin/spctl --status | /usr/bin/grep -c "assessments enabled"	{'integer': 1}	Create a configuration profile containing the following keys in t [source,xml] ---- <key>EnableAssessment</key> <true/> ----
44	CCE-90927-5	os_gatekeeper_rearm	Enforce Gatekeeper 30 Day Automatic Rearm	Gatekeeper _MUST_ be configured to automatically rearm after 30 days if disabled.	Configuration Profile	/usr/bin/osascript -l JavaScript << EOS $.NSUserDefaults.alloc.initWithSuiteName('com.apple.security')\ .objectForKey('GKAutoRearm').js EOS	{'string': 'true'}	NOTE: The following settings are in the (com.apple.ManagedC Create a configuration profile containing the following keys in t [source,xml] ---- <key>GKAutoRearm</key> <true/> ----
45	CCE-90929-1	os_handoff_disable	Disable Handoff	Handoff _MUST_ be disabled. Handoff allows you to continue working on a document or project when the user switches from one Apple device to another. Disabling Handoff prevents data transfers to unauthorized devices.	Configuration Profile	/usr/bin/osascript -l JavaScript << EOS $.NSUserDefaults.alloc.initWithSuiteName('com.apple.applicationaccess')\ .objectForKey('allowActivityContinuation').js EOS	{'string': 'false'}	Create a configuration profile containing the following keys in t [source,xml] ---- <key>allowActivityContinuation</key> <false/> ----
46	CCE-90931-7	os_home_folders_secure	Secure User's Home Folders	The system _MUST_ be configured to prevent access to other user's home folders. The default behavior of macOS is to allow all valid users access to the the top level of every other user's home folder while restricting access only to the Apple default folders within.	Script	/usr/bin/find /System/Volumes/Data/Users -mindepth 1 -maxdepth 1 -type d -perm -1 | /usr/bin/grep -v "Shared" | /usr/bin/grep -v "Guest" | /usr/bin/wc -l | /usr/bin/xargs	{'integer': 0}	[source,bash] ---- IFS=$'\n' for userDirs in $(/usr/bin/find /System/Volumes/Data/Users -m /bin/chmod og-rwx "$userDirs" done unset IFS ----
47	CCE-90932-5	os_httpd_disable	Disable the Built-in Web Server	The built-in web server is a non-essential service built into macOS and _MUST_ be disabled. NOTE: The built in web server service is disabled at startup by default macOS.	Script	/bin/launchctl print-disabled system | /usr/bin/grep -c '"org.apache.httpd" => true'	{'integer': 1}	[source,bash] ---- /bin/launchctl disable system/org.apache.httpd ----
48	CCE-90933-3	os_icloud_storage_prompt_disable	Disable iCloud Storage Setup during Setup Assistant	The prompt to set up iCloud storage services during Setup Assistant _MUST_ be disabled. The default behavior of macOS is to prompt new users to set up storage in iCloud. Disabling the iCloud storage setup prompt provides organizations more control over the storage of their data.	Configuration Profile	/usr/bin/osascript -l JavaScript << EOS $.NSUserDefaults.alloc.initWithSuiteName('com.apple.SetupAssistant.managed')\ .objectForKey('SkipiCloudStorageSetup').js EOS	{'string': 'true'}	Create a configuration profile containing the following keys in t [source,xml] ---- <key>SkipiCloudStorageSetup</key> <true/> ----
49	CCE-90939-0	os_ir_support_disable	Disable Infrared (IR) support	Infrared (IR) support _MUST_ be disabled to prevent users from controlling the system with IR devices. By default, if IR is enabled, the system will accept IR control from any remote device. NOTE: This is applicable only to models of Mac Mini systems earlier than Mac Mini8,1.	Configuration Profile	/usr/bin/osascript -l JavaScript << EOS $.NSUserDefaults.alloc.initWithSuiteName('com.apple.driver.AppleIRController')\ .objectForKey('DeviceEnabled').js EOS	{'string': 'false'}	NOTE: The following settings are in the (com.apple.ManagedC Create a configuration profile containing the following keys in t [source,xml] ---- <key>DeviceEnabled</key> <false/> ----

50	CCE-90946-5	os_mail_app_disable	Disable Mail App	The macOS built-in Mail.app _MUST_ be disabled.
				The Mail.app contains functionality that can establish connections to Apple's iCloud, even when security controls to disable iCloud access have been put in place.
				[IMPORTANT]
				====
				Some organizations allow the use of the built-in Mail.app for organizational communication. Information System Security Officers (ISSOs) may make the risk-based decision not to disable the macOS built-in Mail.app to avoid losing this functionality, but they are advised to first fully weigh the potential risks posed to their organization.
				====
					Configuration Profile	/usr/bin/osascript -l JavaScript << EOS
						function run() {
						let pref1 = ObjC.unwrap($.NSUserDefaults.alloc.initWithSuiteName('com.apple.applicationaccess.new')\
						.objectForKey('familyControlsEnabled'))
						let pathlist = $.NSUserDefaults.alloc.initWithSuiteName('com.apple.applicationaccess.new')\
						.objectForKey('pathBlackList').js
						for (let app in pathlist) {
						if (ObjC.unwrap(pathlist[app]) == "/Applications/Mail.app" && pref1 == true){
						return("true")
						}
						}
						return("false")
						}
						EOS
							{'string': 'true'}	Create a configuration profile containing the following keys in t
								[source,xml]
								---- 	
								<key>familyControlsEnabled</key>
								<true/>
								<key>pathBlackList</key>
								<array>
								<string>/Applications/Mail.app</string>
								</array>
								---- 	

51	CCE-90950-7	os_mdm_require	Enforce Enrollment in Mobile Device Management	You _MUST_ enroll your Mac in a Mobile Device Management (MDM) software. User Approved MDM (UAMDM) enrollment or enrollment via Apple Business Manager (ABM)/Apple School Manager (ASM) is required to manage certain security settings. Currently these include: * Allowed Kernel Extensions * Allowed Approved System Extensions * Privacy Preferences Policy Control Payload * ExtensibleSingleSignOn * FDEFileVault In macOS 11, UAMDM grants Supervised status on a Mac, unlocking the following MDM features, which were previously locked behind ABM: * Activation Lock Bypass * Access to Bootstrap Tokens * Scheduling Software Updates * Query list and delete local users	Manual	/usr/bin/profiles status -type enrollment | /usr/bin/awk -F: '/MDM enrollment/ {print $2}' | /usr/bin/grep -c "Yes (User Approved)"	{'integer': 1}	Ensure that system is enrolled via UAMDM.

https://github.com/usnistgov/macos_security

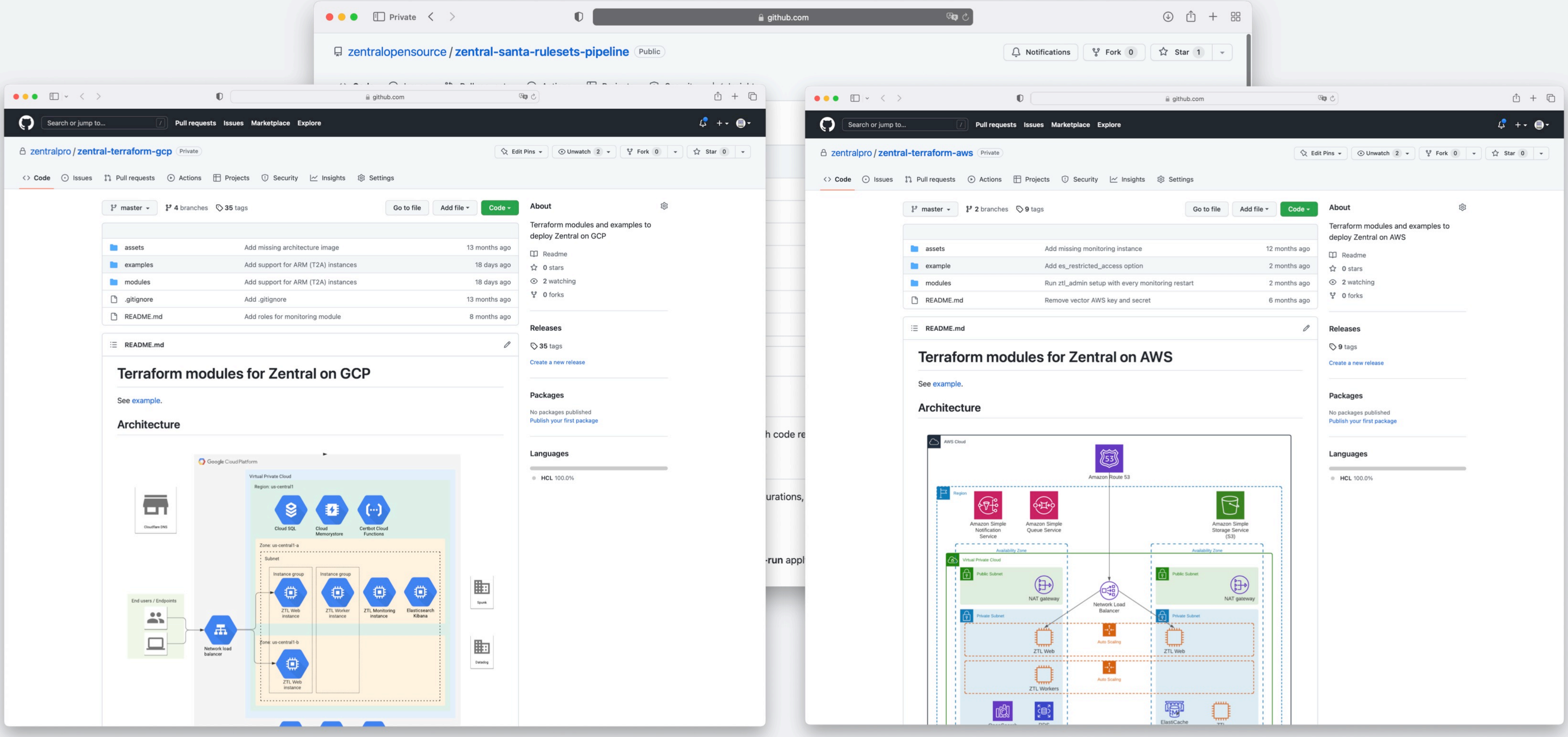
https://support.apple.com/en-gb/guide/sccc/sccc22685bb2/web

Security is not a task,
it's a culture.

GitOps

Built-in change management

GitOps



zentralopensource / zentral-santa-rulesets-pipeline Public

Notifications | Fork 0 | Star 1

h code re

urations,

-run appl

github.com

zentralpro / zentral-terraform-gcp Private

Edit Pins | Unwatch 2 | Fork 0 | Star 0

Code | Issues | Pull requests | Actions | Projects | Security | Insights | Settings

master | 4 branches | 35 tags | Go to file | Add file | Code

assets	Add missing architecture image	13 months ago
examples	Add support for ARM (T2A) instances	18 days ago
modules	Add support for ARM (T2A) instances	18 days ago
.gitignore	Add .gitignore	13 months ago
README.md	Add roles for monitoring module	8 months ago

README.md

Terraform modules for Zentral on GCP

See example.

Architecture

About

Terraform modules and examples to deploy Zentral on GCP

Readme

0 stars

2 watching

0 forks

Releases

35 tags

Create a new release

Packages

No packages published

Publish your first package

Languages

HCL 100.0%

github.com

zentralpro / zentral-terraform-aws Private

Edit Pins | Unwatch 2 | Fork 0 | Star 0

Code | Issues | Pull requests | Actions | Projects | Security | Insights | Settings

master | 2 branches | 9 tags | Go to file | Add file | Code

assets	Add missing monitoring instance	12 months ago
example	Add es_restricted_access option	2 months ago
modules	Run ztl_admin setup with every monitoring restart	2 months ago
README.md	Remove vector AWS key and secret	6 months ago

README.md

Terraform modules for Zentral on AWS

See example.

Architecture

About

Terraform modules and examples to deploy Zentral on AWS

Readme

0 stars

2 watching

0 forks

Releases

9 tags

Create a new release

Packages

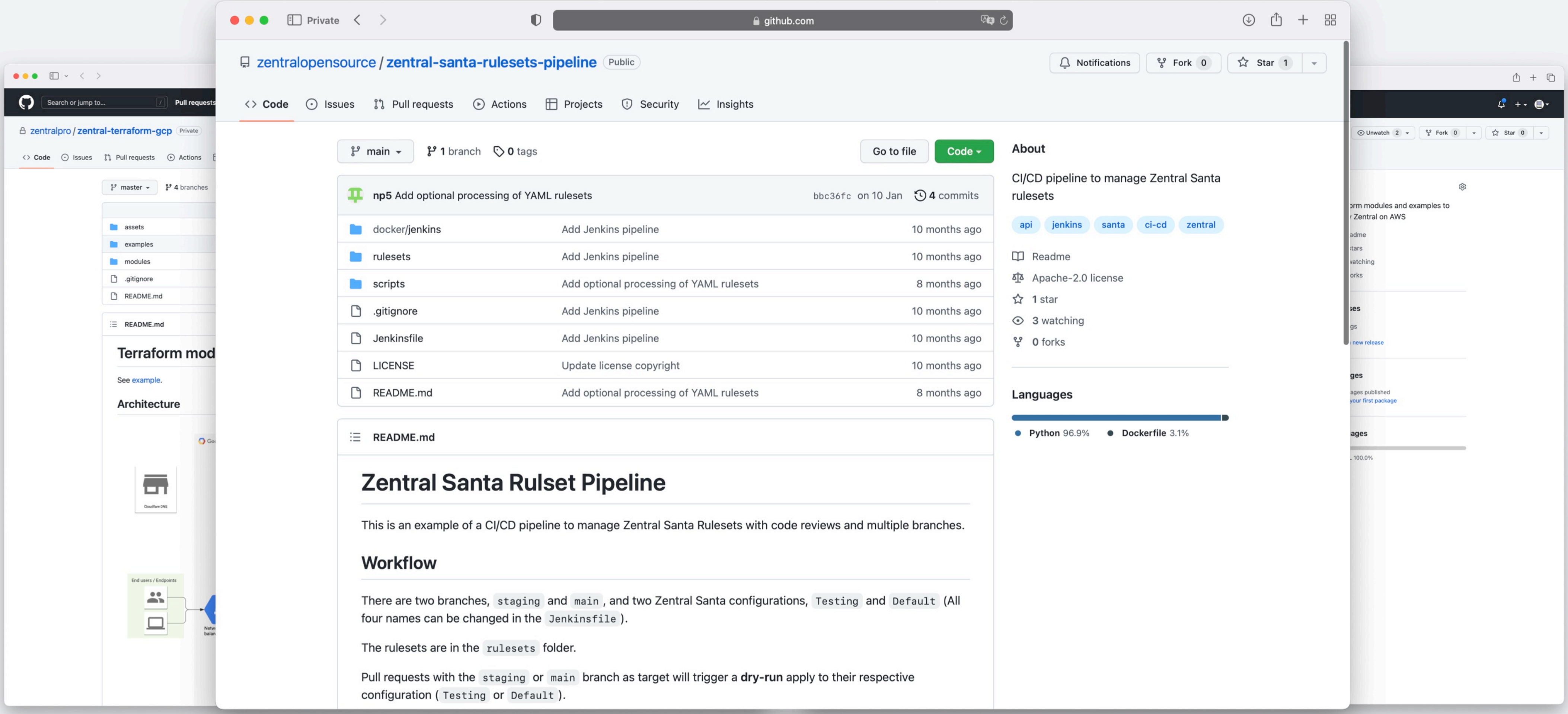
No packages published

Publish your first package

Languages

HCL 100.0%

GitOps



np5 Add optional processing of YAML rulesets bbc36fc on 10 Jan 4 commits

docker/jenkins	Add Jenkins pipeline	10 months ago
rulesets	Add Jenkins pipeline	10 months ago
scripts	Add optional processing of YAML rulesets	8 months ago
.gitignore	Add Jenkins pipeline	10 months ago
Jenkinsfile	Add Jenkins pipeline	10 months ago
LICENSE	Update license copyright	10 months ago
README.md	Add optional processing of YAML rulesets	8 months ago

README.md

Zentral Santa Rulset Pipeline

This is an example of a CI/CD pipeline to manage Zentral Santa Rulesets with code reviews and multiple branches.

Workflow

There are two branches, `staging` and `main`, and two Zentral Santa configurations, `Testing` and `Default` (All four names can be changed in the `Jenkinsfile`).

The rulesets are in the `rulesets` folder.

Pull requests with the `staging` or `main` branch as target will trigger a **dry-run** apply to their respective configuration (`Testing` or `Default`).

About

CI/CD pipeline to manage Zentral Santa rulesets

GitOps

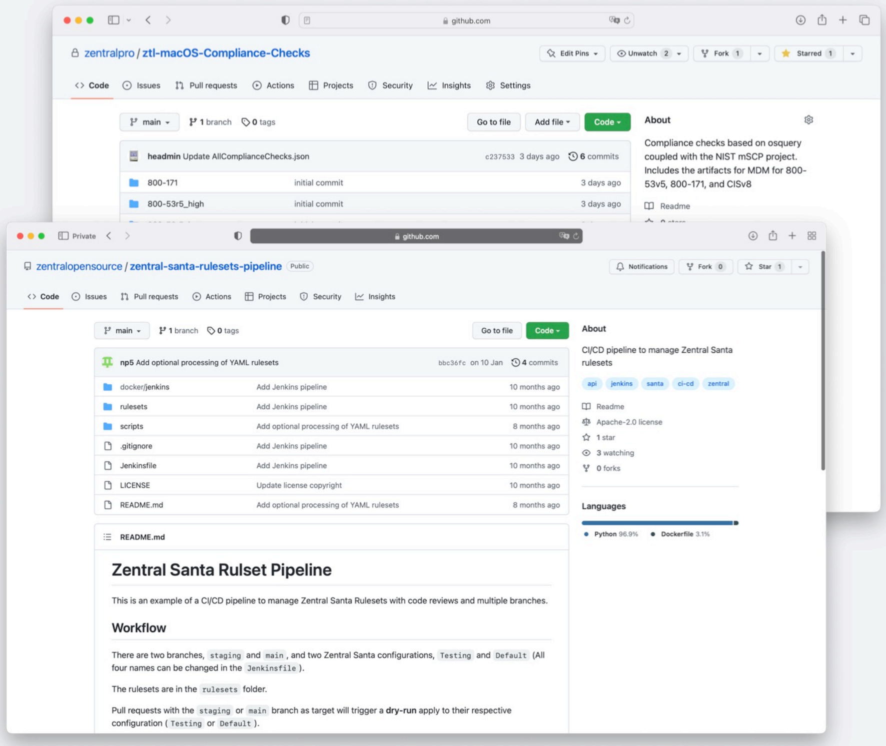
Free GUI with GitHub (or equivalent)

Authentication and authorization

Peer review

Branches

Auditing



headmin Update AllComplianceChecks.json	c237533 3 days ago	6 commits
800-171	initial commit	3 days ago
800-53r5_high	initial commit	3 days ago

Compliance checks based on osquery coupled with the NIST mSCP project. Includes the artifacts for MDM for 800-53v5, 800-171, and CISv8

CI/CD pipeline to manage Zentral Santa rulesets

np5 Add optional processing of YAML rulesets	bbc36fc on 10 Jan	4 commits
docker/jenkins	Add Jenkins pipeline	10 months ago
rulesets	Add Jenkins pipeline	10 months ago
scripts	Add optional processing of YAML rulesets	8 months ago
.gitignore	Add Jenkins pipeline	10 months ago
Jenkinsfile	Add Jenkins pipeline	10 months ago
LICENSE	Update license copyright	10 months ago
README.md	Add optional processing of YAML rulesets	8 months ago

Zentral Santa Rulset Pipeline

This is an example of a CI/CD pipeline to manage Zentral Santa Rulesets with code reviews and multiple branches.

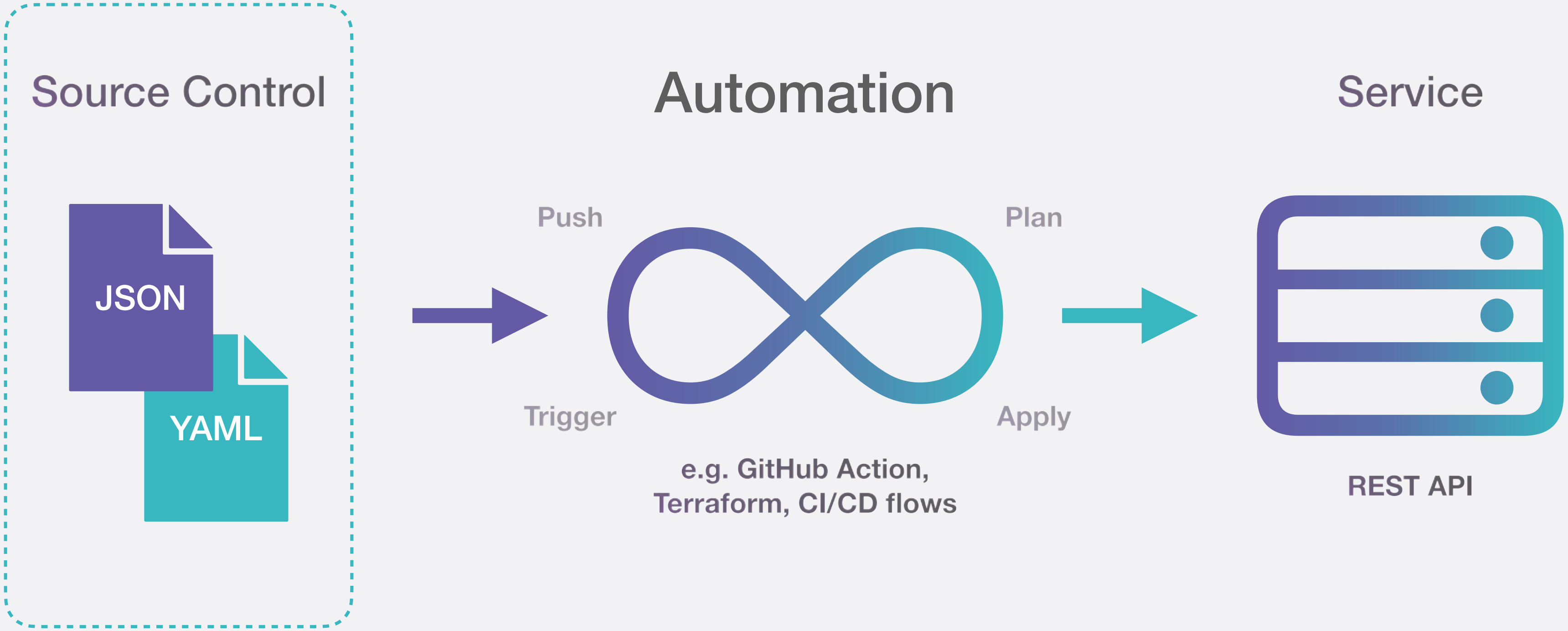
Workflow

There are two branches, `staging` and `main`, and two Zentral Santa configurations, `Testing` and `Default` (All four names can be changed in the `Jenkinsfile`).

The rulesets are in the `rulesets` folder.

Pull requests with the `staging` or `main` branch as target will trigger a **dry-run** apply to their respective configuration (`Testing` or `Default`).

GIT + HTTP API



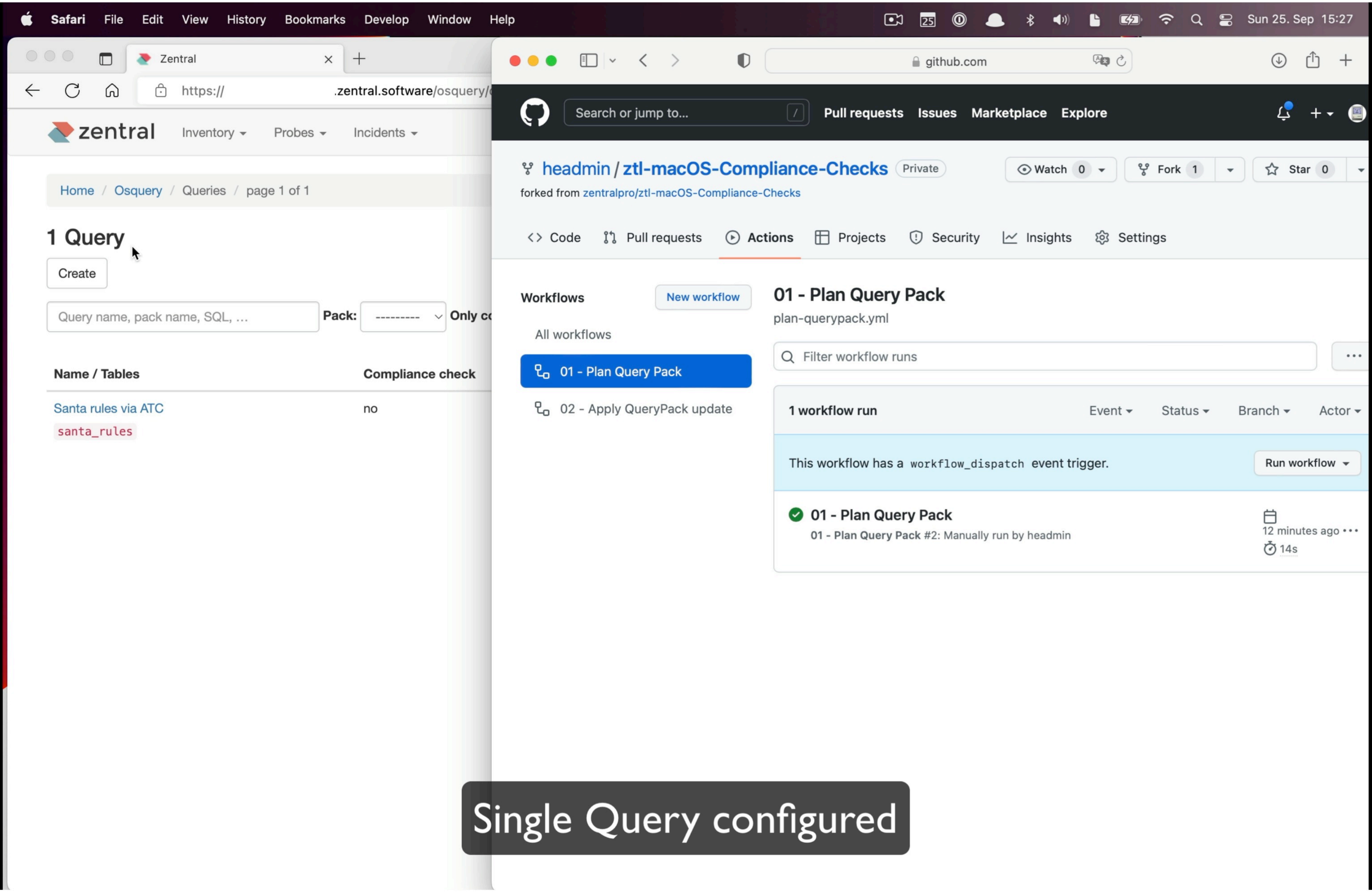
Source Control

Automation

Service

e.g. GitHub Action, Terraform, CI/CD flows

REST API



Safari File Edit View History Bookmarks Develop Window Help
Sun 25. Sep 15:27
Zentral
https:// .zentral.software/osquery/
zentral
Inventory
Probes
Incidents
Home / Osquery / Queries / page 1 of 1

1 Query

Name / Tables	Compliance check
Santa rules via ATC `santa_rules`	no

headmin / ztl-macOS-Compliance-Checks Private

forked from zentralpro/ztl-macOS-Compliance-Checks

01 - Plan Query Pack

plan-querypack.yml

This workflow has a `workflow_dispatch` event trigger.

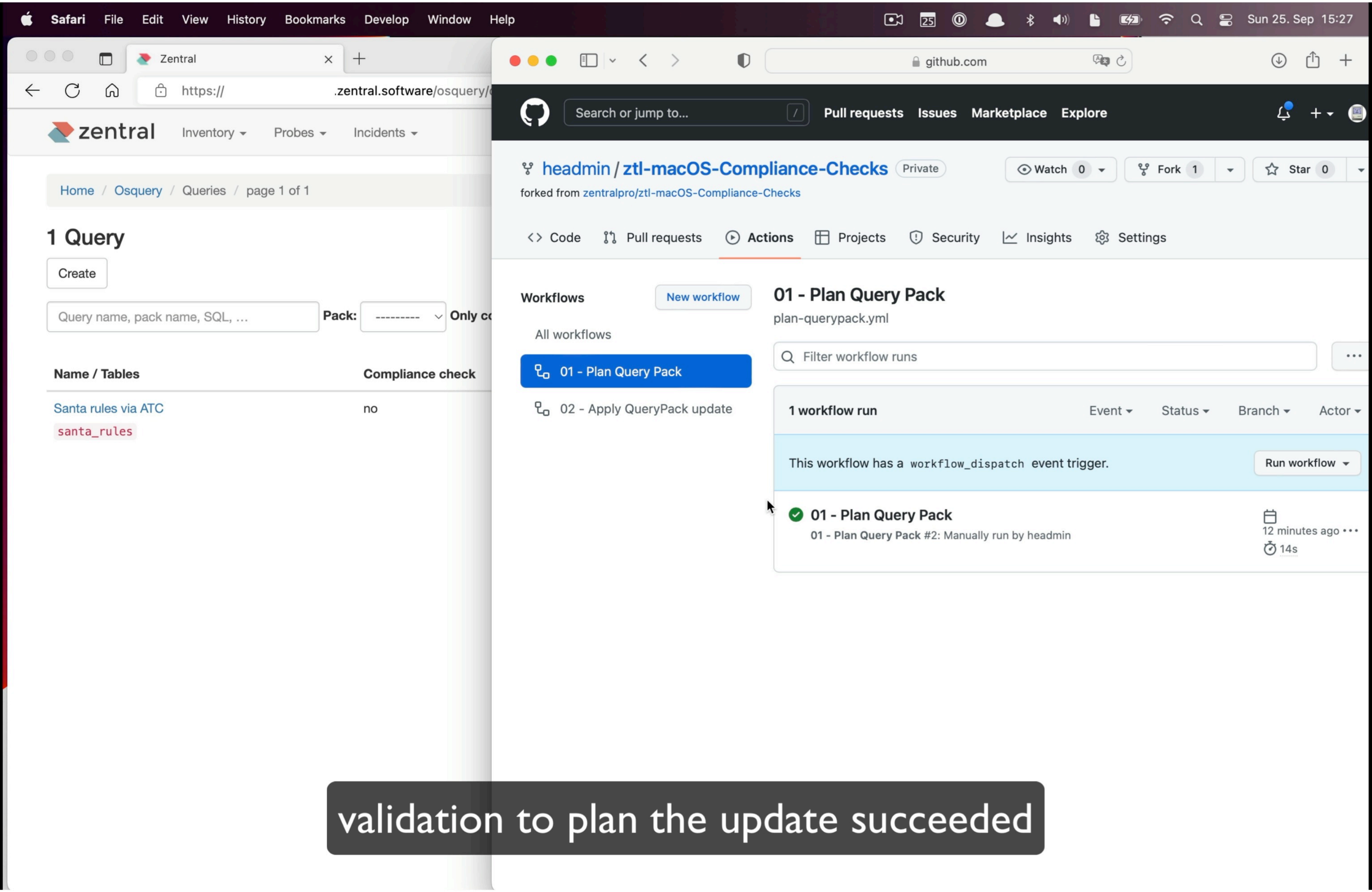
✓ 01 - Plan Query Pack

01 - Plan Query Pack #2: Manually run by headmin

12 minutes ago

14s

Single Query configured



Home / Osquery / Queries / page 1 of 1

1 Query

Create

Query name, pack name, SQL, ... Pack: ---------- Only c

Name / Tables	Compliance check
Santa rules via ATC santa_rules	no

headmin / ztl-macOS-Compliance-Checks Private

forked from zentralpro/ztl-macOS-Compliance-Checks

Workflows

All workflows

01 - Plan Query Pack

02 - Apply QueryPack update

01 - Plan Query Pack

plan-querypack.yml

1 workflow run

This workflow has a `workflow_dispatch` event trigger.

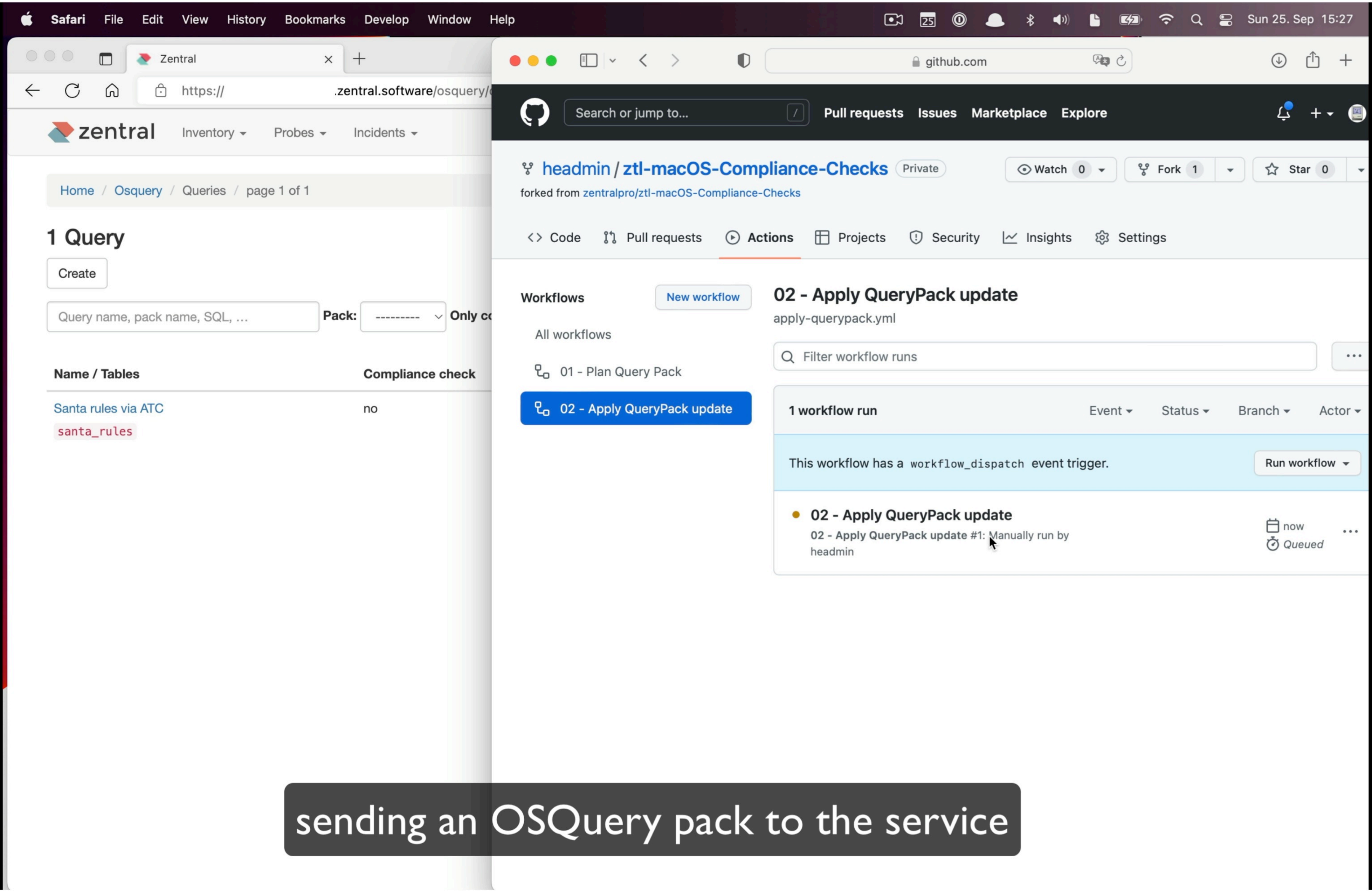
01 - Plan Query Pack

01 - Plan Query Pack #2: Manually run by headmin

12 minutes ago

14s

validation to plan the update succeeded



Safari File Edit View History Bookmarks Develop Window Help
Sun 25. Sep 15:27
Zentral
https:// .zentral.software/osquery/
zentral
Inventory
Probes
Incidents
github.com
Search or jump to...
Pull requests Issues Marketplace Explore
Code Pull requests Actions Projects Security Insights Settings

Home / Osquery / Queries / page 1 of 1

1 Query

Create

Query name, pack name, SQL, ...

Pack: ---------- Only c

Name / Tables	Compliance check
Santa rules via ATC santa_rules	no

headmin / ztl-macOS-Compliance-Checks Private

forked from zentralpro/ztl-macOS-Compliance-Checks

Watch 0 · Fork 1 · Star 0

Workflows — New workflow

- All workflows
- 01 - Plan Query Pack
- 02 - Apply QueryPack update

02 - Apply QueryPack update

apply-querypack.yml

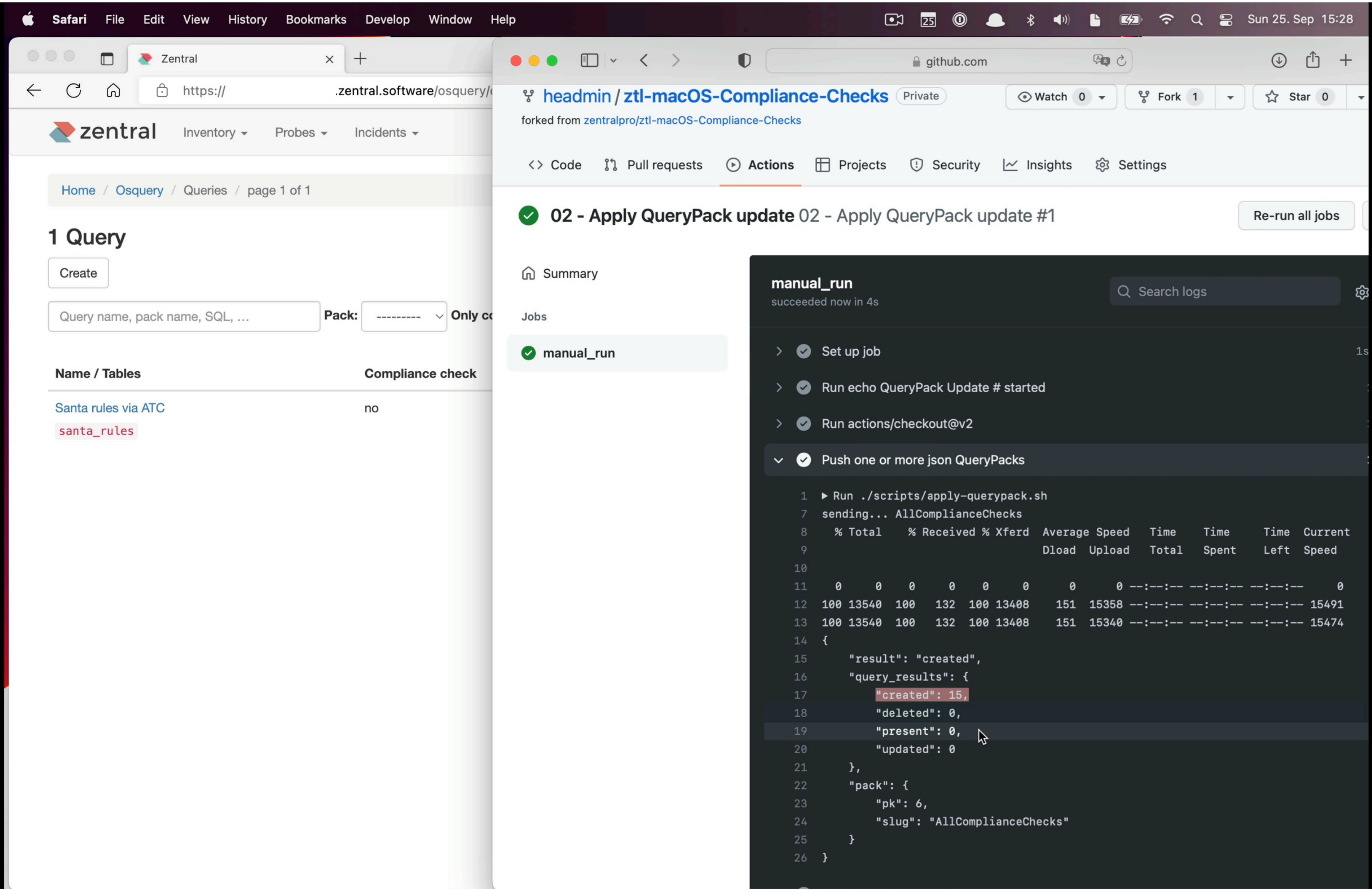
Filter workflow runs

1 workflow run — Event · Status · Branch · Actor

This workflow has a `workflow_dispatch` event trigger. Run workflow

● **02 - Apply QueryPack update**
02 - Apply QueryPack update #1: Manually run by headmin
now
Queued

sending an OSQuery pack to the service



Home / Osquery / Queries / page 1 of 1

1 Query

Query name, pack name, SQL, ...

Name / Tables	Compliance check
Santa rules via ATC santa_rules	no

headmin / ztl-macOS-Compliance-Checks Private

forked from zentralpro/ztl-macOS-Compliance-Checks

02 - Apply QueryPack update 02 - Apply QueryPack update #1

manual_run

manual_run
succeeded now in 4s

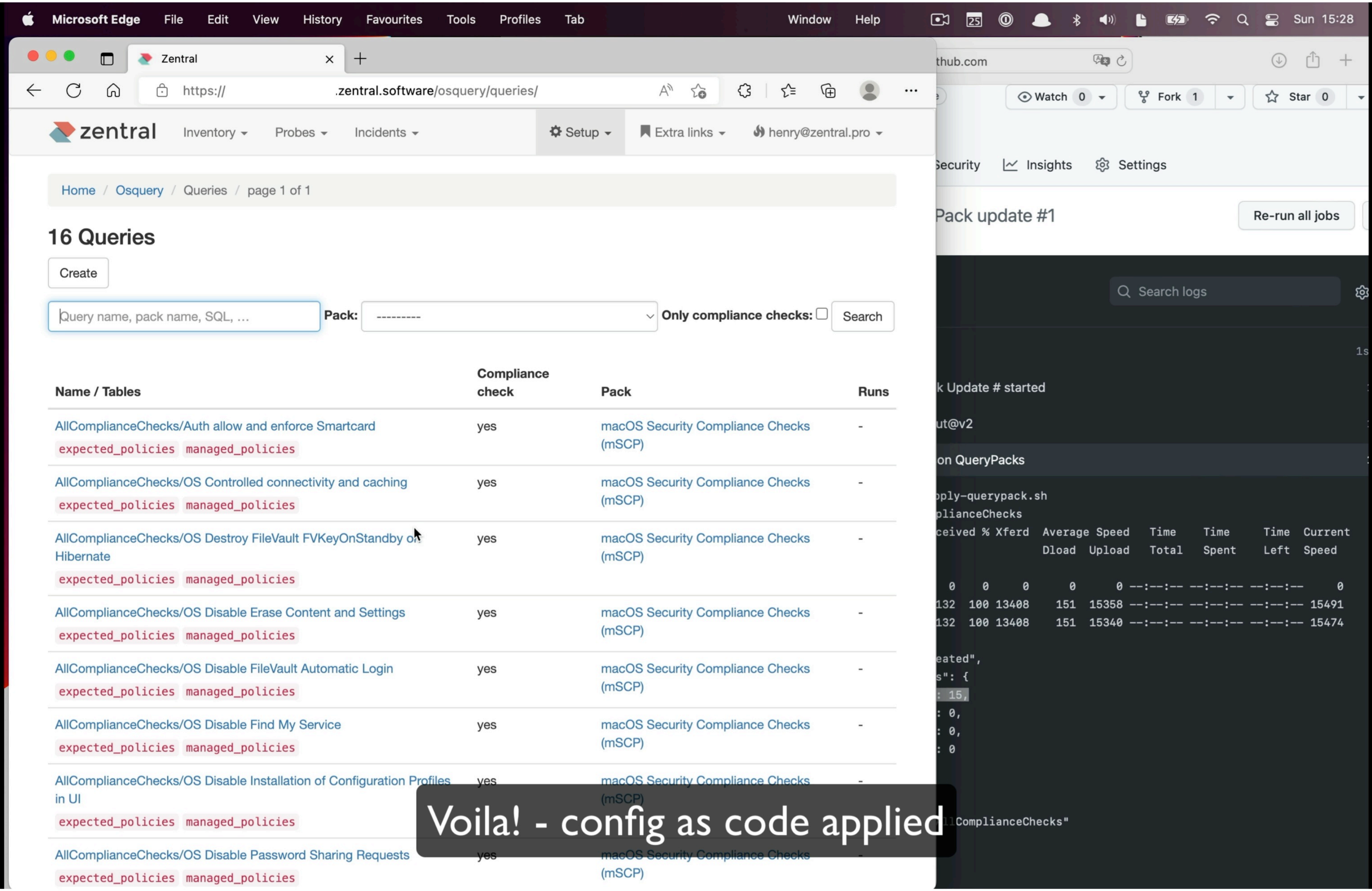
Set up job 1s

Run echo QueryPack Update # started

Run actions/checkout@v2

Push one or more json QueryPacks

```
▶ Run ./scripts/apply-querypack.sh
sending... AllComplianceChecks
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed

  0     0    0     0    0     0      0      0 --:--:-- --:--:-- --:--:--     0
100 13540  100   132  100 13408    151  15358 --:--:-- --:--:-- --:--:-- 15491
100 13540  100   132  100 13408    151  15340 --:--:-- --:--:-- --:--:-- 15474
{
    "result": "created",
    "query_results": {
        "created": 15,
        "deleted": 0,
        "present": 0,
        "updated": 0
    },
    "pack": {
        "pk": 6,
        "slug": "AllComplianceChecks"
    }
}
```



Home / Osquery / Queries / page 1 of 1

16 Queries

Query name, pack name, SQL, ... Pack: ---------- Only compliance checks: □

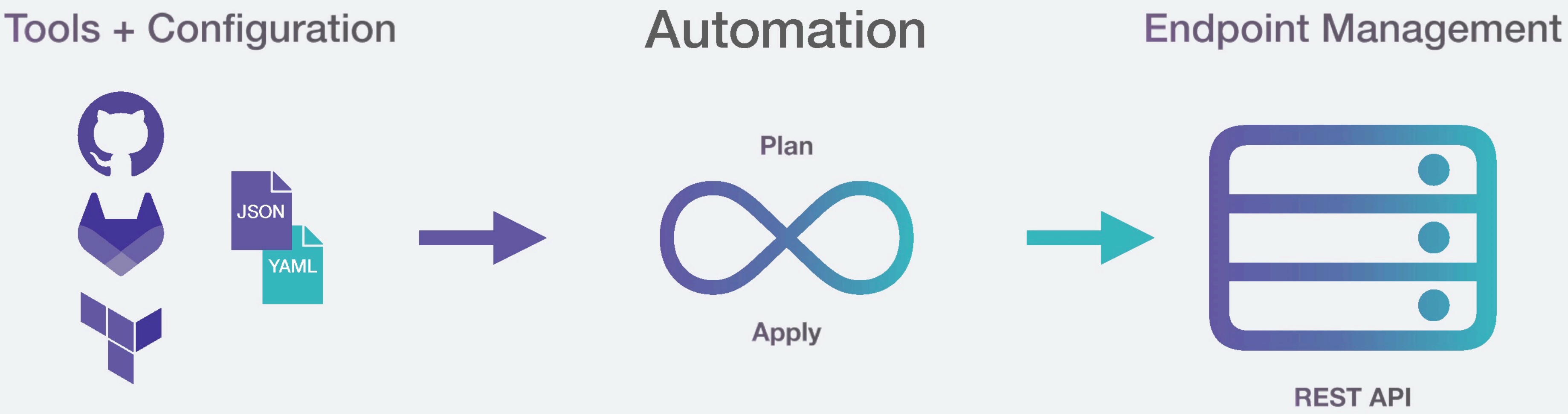
Name / Tables	Compliance check	Pack	Runs
AllComplianceChecks/Auth allow and enforce Smartcard `expected_policies` `managed_policies`	yes	macOS Security Compliance Checks (mSCP)	-
AllComplianceChecks/OS Controlled connectivity and caching `expected_policies` `managed_policies`	yes	macOS Security Compliance Checks (mSCP)	-
AllComplianceChecks/OS Destroy FileVault FVKeyOnStandby on Hibernate `expected_policies` `managed_policies`	yes	macOS Security Compliance Checks (mSCP)	-
AllComplianceChecks/OS Disable Erase Content and Settings `expected_policies` `managed_policies`	yes	macOS Security Compliance Checks (mSCP)	-
AllComplianceChecks/OS Disable FileVault Automatic Login `expected_policies` `managed_policies`	yes	macOS Security Compliance Checks (mSCP)	-
AllComplianceChecks/OS Disable Find My Service `expected_policies` `managed_policies`	yes	macOS Security Compliance Checks (mSCP)	-
AllComplianceChecks/OS Disable Installation of Configuration Profiles in UI `expected_policies` `managed_policies`	yes	macOS Security Compliance Checks (mSCP)	-
AllComplianceChecks/OS Disable Password Sharing Requests `expected_policies` `managed_policies`	yes	macOS Security Compliance Checks (mSCP)	-

Pack update #1

```
                                                                 1s
k Update # started
ut@v2
on QueryPacks
pply-querypack.sh
pliianceChecks
ceived % Xferd  Average Speed   Time    Time     Time  Current
                Dload  Upload   Total   Spent    Left  Speed

  0    0     0      0      0 --:--:-- --:--:-- --:--:--     0
132  100 13408    151  15358 --:--:-- --:--:-- --:--:-- 15491
132  100 13408    151  15340 --:--:-- --:--:-- --:--:-- 15474

eated",
s": {
: 15,
: 0,
: 0,
: 0

llComplianceChecks"
```

Voila! - config as code applied

Configuration in Code



Tools + Configuration

Automation

Endpoint Management

Plan

Apply

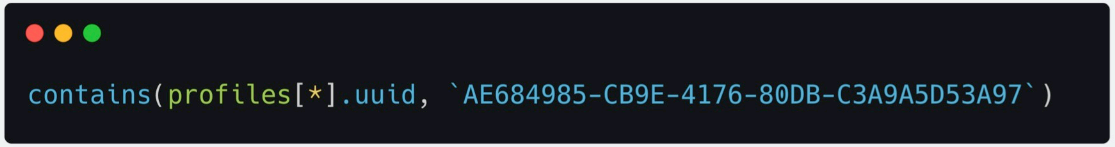
REST API

Compliance Checks

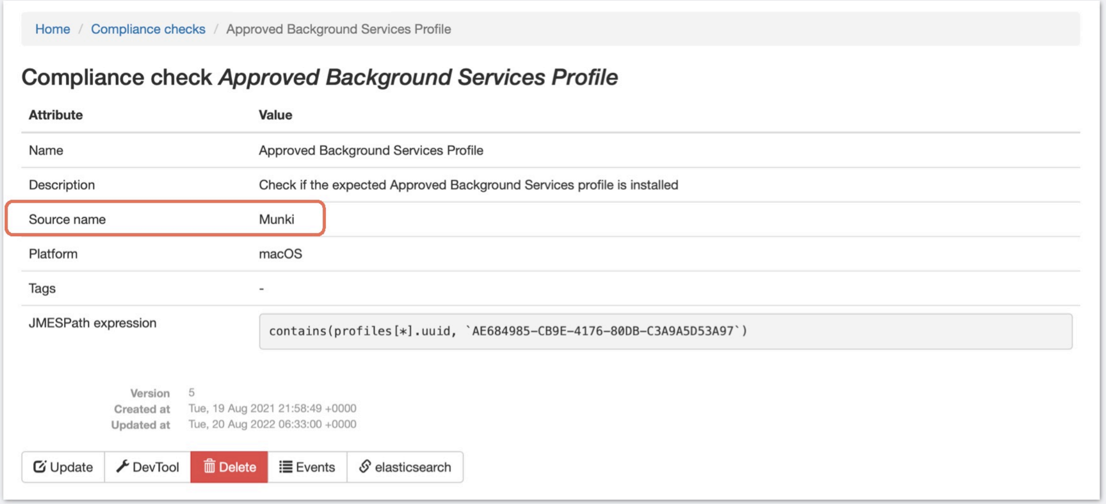
Integrated pass/fail data

Compliance Checks

Search for Configuration profile present



```
contains(profiles[*].uuid, `AE684985-CB9E-4176-80DB-C3A9A5D53A97`)
```

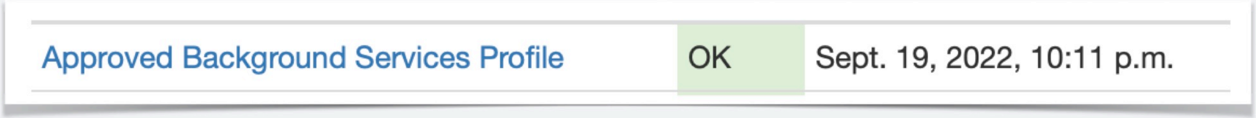


Home / Compliance checks / Approved Background Services Profile

Compliance check *Approved Background Services Profile*

Attribute	Value
Name	Approved Background Services Profile
Description	Check if the expected Approved Background Services profile is installed
Source name	Munki
Platform	macOS
Tags	-
JMESPath expression	`contains(profiles[*].uuid, `AE684985-CB9E-4176-80DB-C3A9A5D53A97`)`

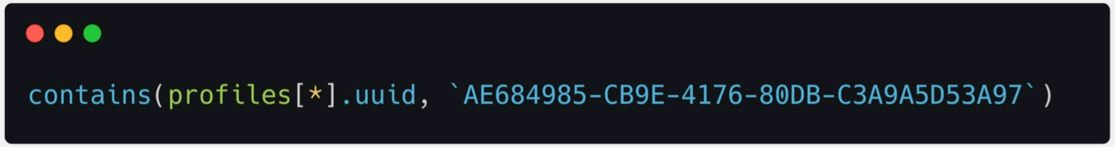
Version	5
Created at	Tue, 19 Aug 2021 21:58:49 +0000
Updated at	Tue, 20 Aug 2022 06:33:00 +0000



Approved Background Services Profile	OK	Sept. 19, 2022, 10:11 p.m.

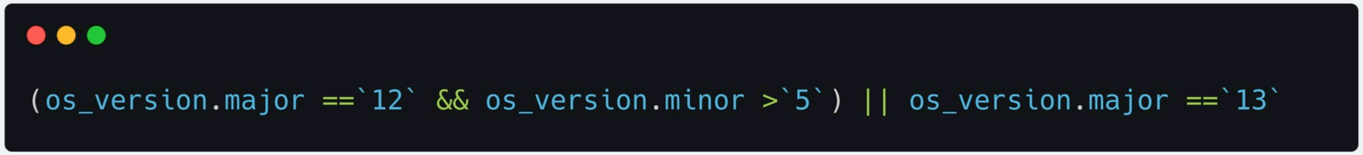
Compliance Checks

Search for Configuration profile present



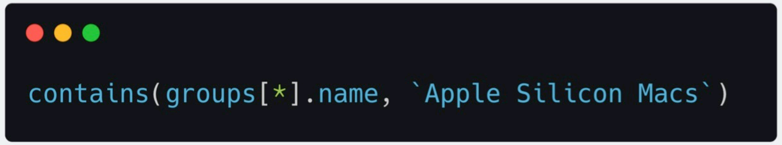
```
contains(profiles[*].uuid, `AE684985-CB9E-4176-80DB-C3A9A5D53A97`)
```

Search for OS Versions



```
(os_version.major ==`12` && os_version.minor >`5`) || os_version.major ==`13`
```

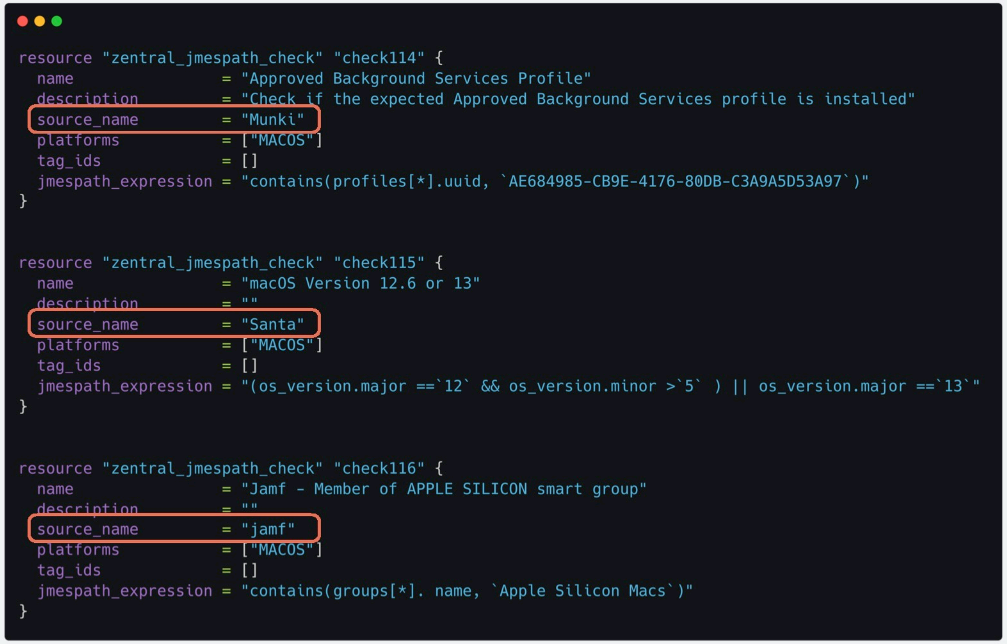
Search for Group Membership



```
contains(groups[*].name, `Apple Silicon Macs`)
```

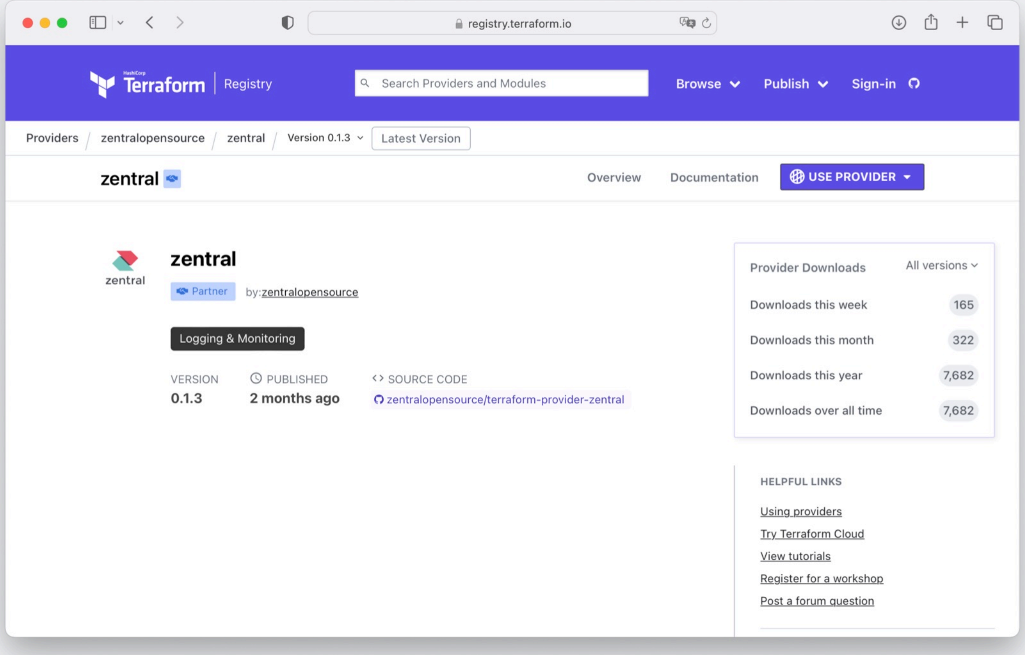
Compliance Checks

..as code with Terraform



```
resource "zentral_jmespath_check" "check114" {
  name                = "Approved Background Services Profile"
  description         = "Check if the expected Approved Background Services profile is installed"
  source_name         = "Munki"
  platforms           = ["MACOS"]
  tag_ids             = []
  jmespath_expression = "contains(profiles[*].uuid, `AE684985-CB9E-4176-80DB-C3A9A5D53A97`)"
}

resource "zentral_jmespath_check" "check115" {
  name                = "macOS Version 12.6 or 13"
  description         = ""
  source_name         = "Santa"
  platforms           = ["MACOS"]
  tag_ids             = []
  jmespath_expression = "(os_version.major ==`12` && os_version.minor >`5` ) || os_version.major ==`13`"
}

resource "zentral_jmespath_check" "check116" {
  name                = "Jamf - Member of APPLE SILICON smart group"
  description         = ""
  source_name         = "jamf"
  platforms           = ["MACOS"]
  tag_ids             = []
  jmespath_expression = "contains(groups[*]. name, `Apple Silicon Macs`)"
}
```

Compliance testing across multiple sources



registry.terraform.io

Terraform | Registry

Search Providers and Modules

Browse · Publish · Sign-in

Providers / zentralopensource / zentral / Version 0.1.3 · Latest Version

zentral

Overview · Documentation · USE PROVIDER

zentral

Partner · by:zentralopensource

Logging & Monitoring

VERSION 0.1.3

PUBLISHED 2 months ago

SOURCE CODE zentralopensource/terraform-provider-zentral

Provider Downloads · All versions

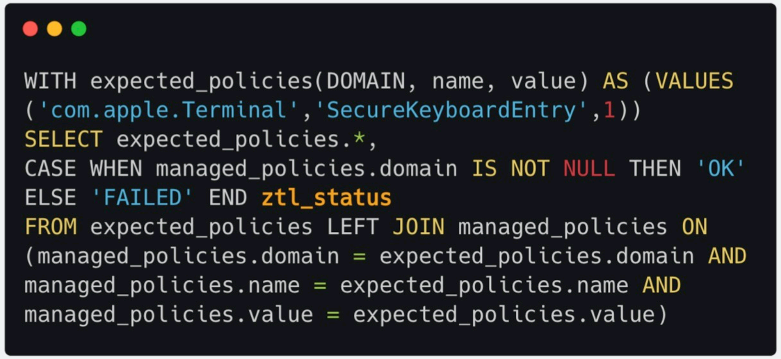
Downloads this week	165
Downloads this month	322
Downloads this year	7,682
Downloads over all time	7,682

HELPFUL LINKS

- Using providers
- Try Terraform Cloud
- View tutorials
- Register for a workshop
- Post a forum question

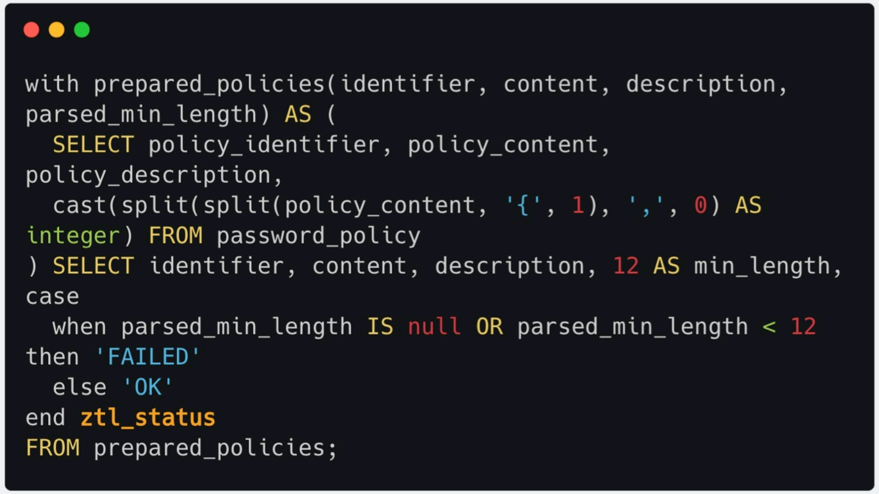
Compliance Checks

Osquery based checks*



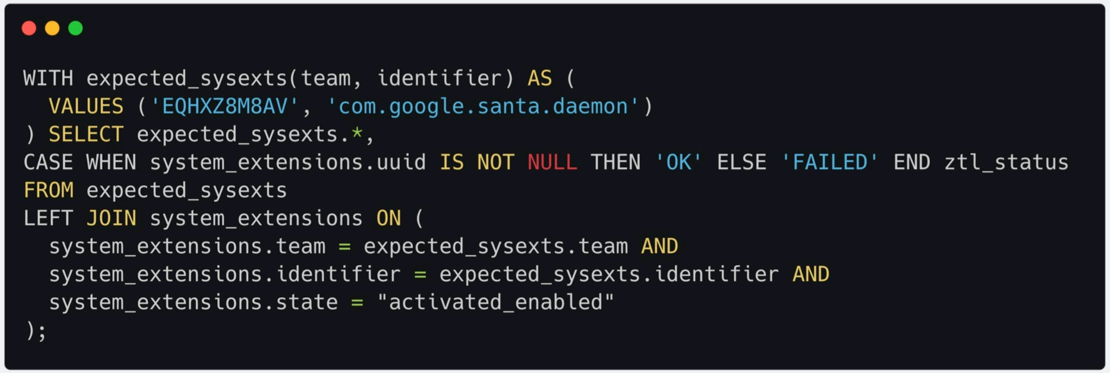
```
WITH expected_policies(DOMAIN, name, value) AS (VALUES
('com.apple.Terminal','SecureKeyboardEntry',1))
SELECT expected_policies.*,
CASE WHEN managed_policies.domain IS NOT NULL THEN 'OK'
ELSE 'FAILED' END ztl_status
FROM expected_policies LEFT JOIN managed_policies ON
(managed_policies.domain = expected_policies.domain AND
managed_policies.name = expected_policies.name AND
managed_policies.value = expected_policies.value)
```

Validate Terminal Secure Keyboard Entry



```
with prepared_policies(identifier, content, description,
parsed_min_length) AS (
  SELECT policy_identifier, policy_content,
policy_description,
  cast(split(split(policy_content, '{', 1), ',', 0) AS
integer) FROM password_policy
) SELECT identifier, content, description, 12 AS min_length,
case
  when parsed_min_length IS null OR parsed_min_length < 12
then 'FAILED'
  else 'OK'
end ztl_status
FROM prepared_policies;
```

Validate Password Policy

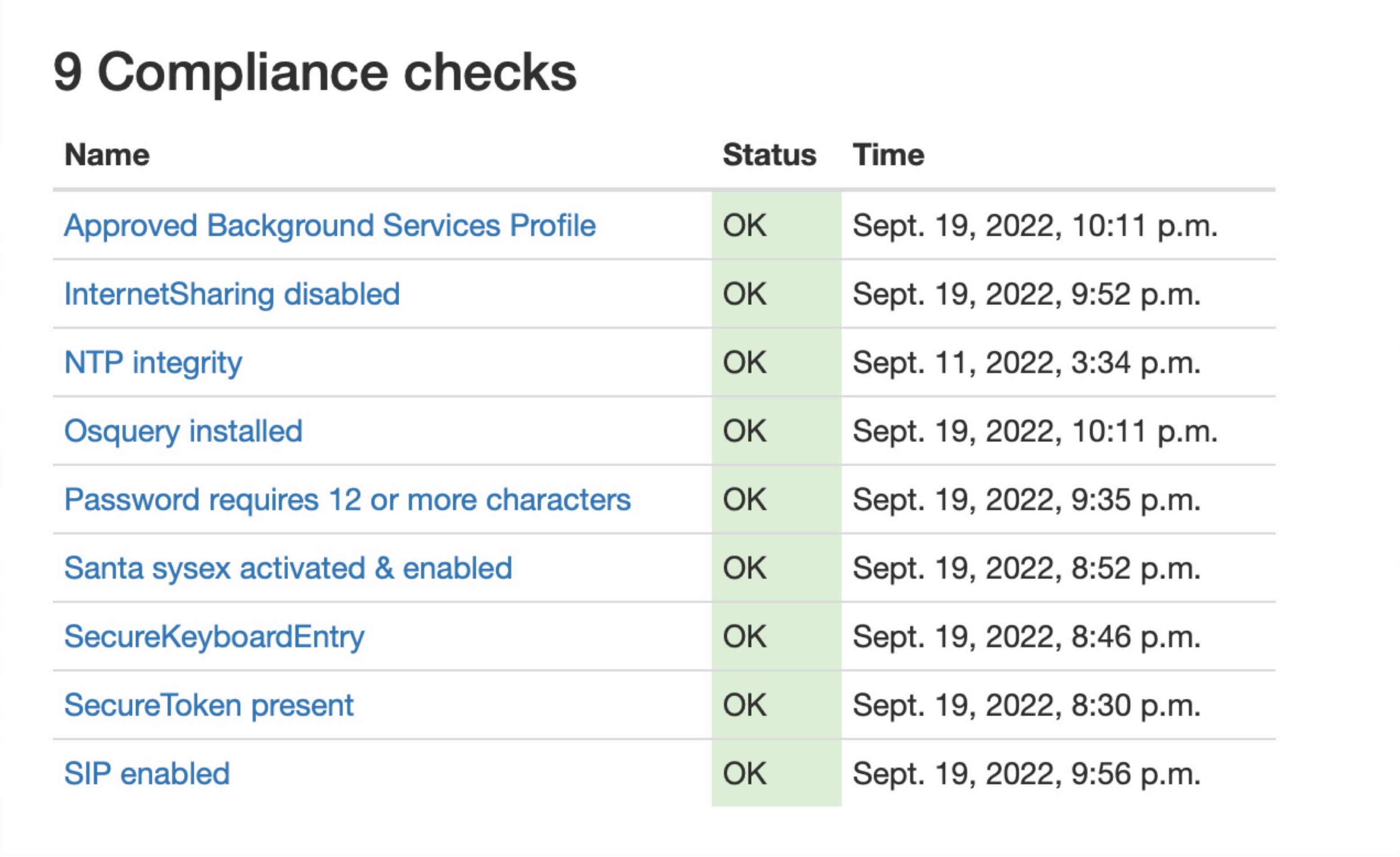


```
WITH expected_sysexts(team, identifier) AS (
  VALUES ('EQHXZ8M8AV', 'com.google.santa.daemon')
) SELECT expected_sysexts.*,
CASE WHEN system_extensions.uuid IS NOT NULL THEN 'OK' ELSE 'FAILED' END ztl_status
FROM expected_sysexts
LEFT JOIN system_extensions ON (
  system_extensions.team = expected_sysexts.team AND
  system_extensions.identifier = expected_sysexts.identifier AND
  system_extensions.state = "activated_enabled"
);
```

Validate Security Extension activated

*managed as OsqueryPack

Compliance Checks



9 Compliance checks

Name	Status	Time
Approved Background Services Profile	OK	Sept. 19, 2022, 10:11 p.m.
InternetSharing disabled	OK	Sept. 19, 2022, 9:52 p.m.
NTP integrity	OK	Sept. 11, 2022, 3:34 p.m.
Osquery installed	OK	Sept. 19, 2022, 10:11 p.m.
Password requires 12 or more characters	OK	Sept. 19, 2022, 9:35 p.m.
Santa sysex activated & enabled	OK	Sept. 19, 2022, 8:52 p.m.
SecureKeyboardEntry	OK	Sept. 19, 2022, 8:46 p.m.
SecureToken present	OK	Sept. 19, 2022, 8:30 p.m.
SIP enabled	OK	Sept. 19, 2022, 9:56 p.m.

Compliance ☑

Summary & Conclusion

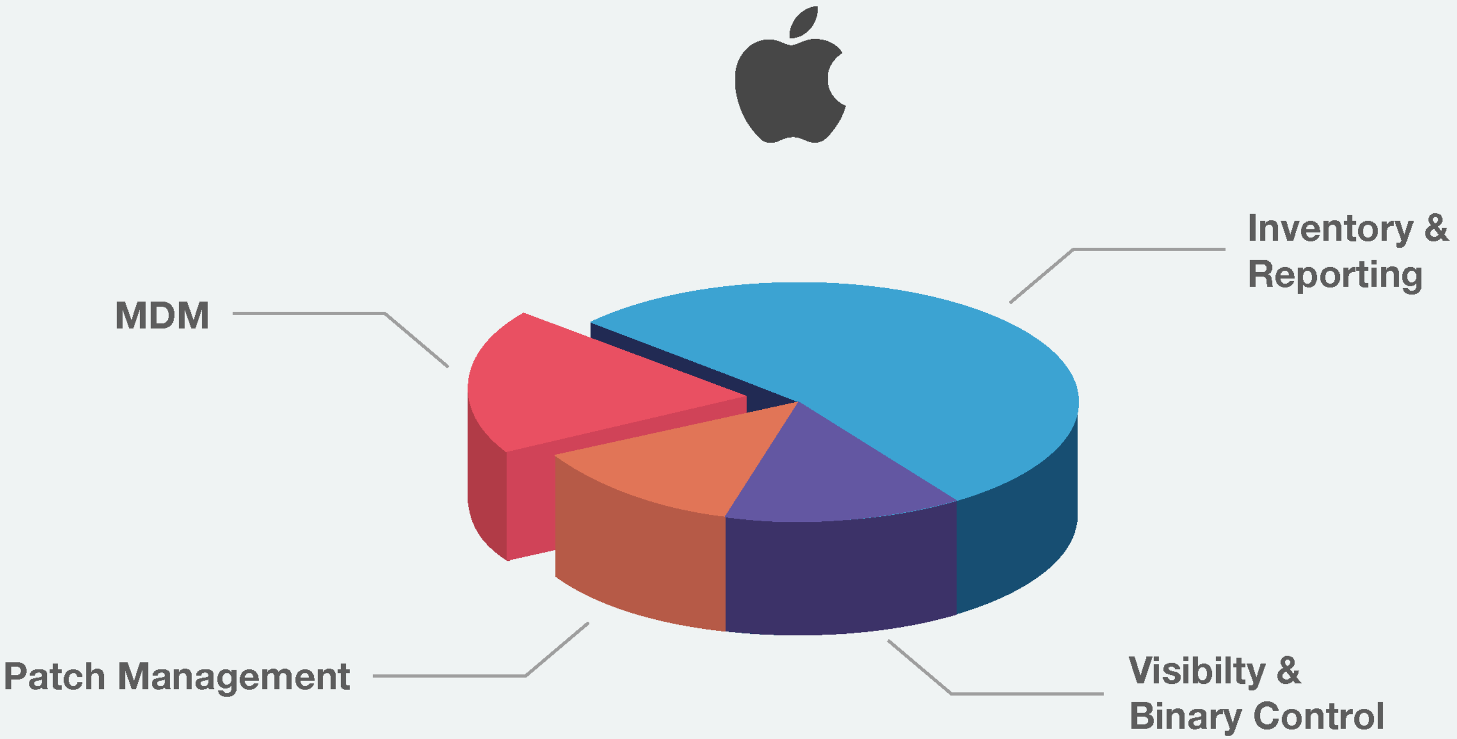
Compliance pathways

- Mindset
- Review regulatory requirements
- Conduct a risk assessment
- Close gaps / missing controls
- Set up overlapping security controls
- Automate compliance reporting activities
- Security awareness training

Compliance pathways

- NIST Cybersecurity Framework
- MITRE ATT&CK
- CIS Critical Security Controls
- macOS Security Compliance Project
- Open source solutions
- Vendor-based solutions
- Measure your effectiveness

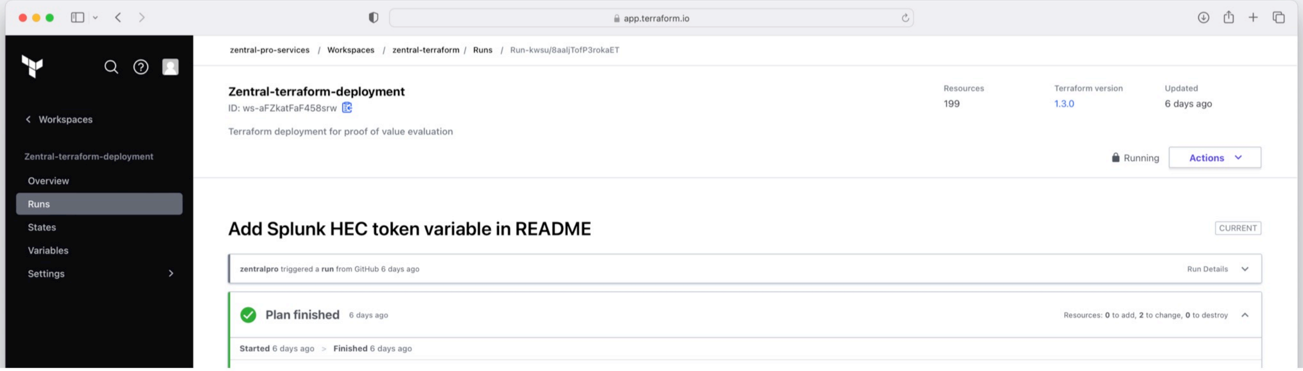
Common needs



zentral.io

A SOURCE AVAILABLE (ZPEL-1.0) AND APACHE 2.0 LICENSE SOFTWARE PROJECT

device management



zentral-pro-services / Workspaces / zentral-terraform / Runs / Run-kwsu/8aaljTofP3rokaET

Zentral-terraform-deployment

ID: ws-aFZkatFaF458srw

Terraform deployment for proof of value evaluation

Resources	Terraform version	Updated
199	1.3.0	6 days ago

Running

Add Splunk HEC token variable in README

CURRENT

zentralpro triggered a **run** from GitHub 6 days ago

✓ Plan finished 6 days ago

Resources: **0** to add, **2** to change, **0** to destroy

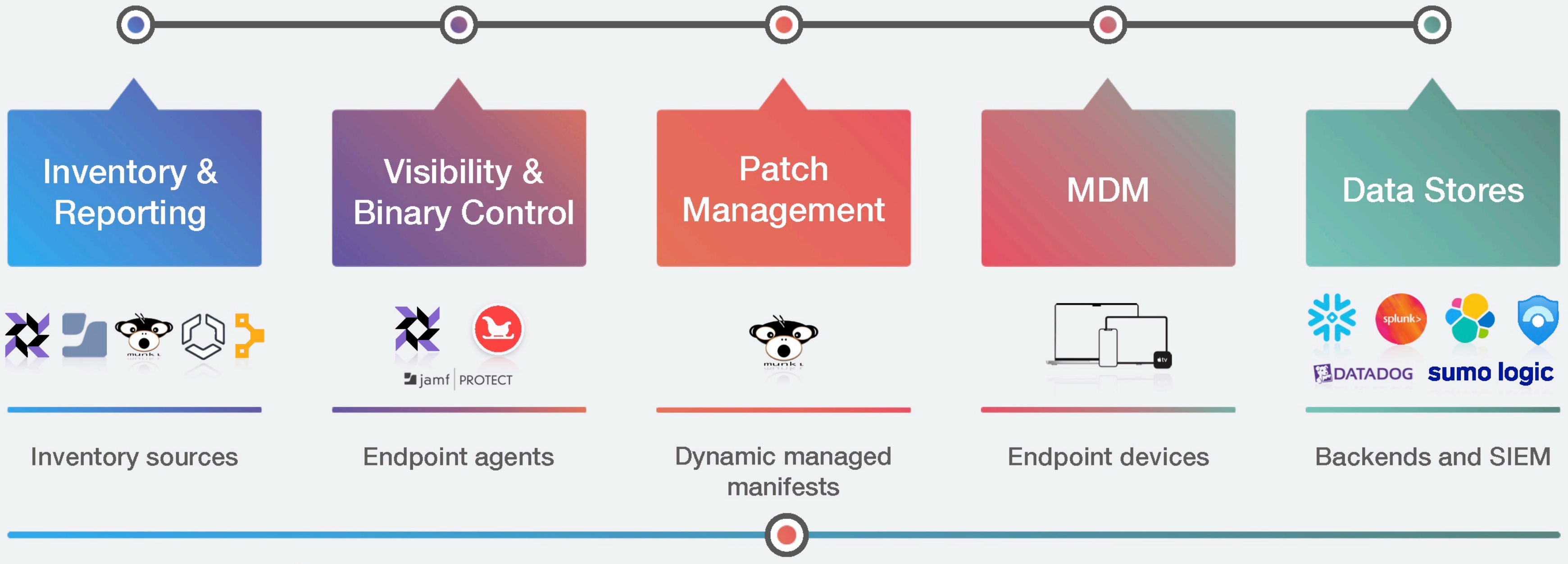
Started 6 days ago > **Finished** 6 days ago

Enterprise Support

License with SLA

zentral

device management



Inventory & Reporting

Visibility & Binary Control

Patch Management

MDM

Data Stores

Inventory sources

Endpoint agents

Dynamic managed manifests

Endpoint devices

Backends and SIEM

GUI

APIs

Terraform

CI/CD

GitOps

https://zentral.io

Enterprise Support

License with SLA

Thank you!

You’re awesome

@henry

@head_min

· MAC · SYS · ADMIN ·

GOTHENBURG

https://zentral.io

Further resources

https://blog.macadmin.me/tags/macsysadmin/

@henry

@head_min

MAC · SYS · ADMIN ·
GOTHENBURG

https://zentral.io