

# DataGuardian Pro

## SOC2 Compliance Report

Generated on: May 03, 2025 11:15

Scan ID: SOC-20250503-0805a1

## Executive Summary

This report presents the findings of a SOC2 compliance analysis conducted on <https://github.com/vishaal314/terrascan> (branch: **master**) on **2025-05-03 11:15:17**. The scan identified a total of **161** compliance issues with **129** high-risk items. The overall compliance score is **1/100**. **Technologies Detected:** terraform, cloudformation, ansible, javascript, docker, kubernetes, pulumi. Each finding in this report is mapped to specific SOC2 Trust Services Criteria (TSC) to help you understand how it impacts your compliance posture. The TSC categories include:

- CC: Common Criteria (Security)
- A: Availability
- PI: Processing Integrity
- C: Confidentiality
- P: Privacy

Scan Type	soc2
Repository URL	<a href="https://github.com/vishaal314/terrascan">https://github.com/vishaal314/terrascan</a>
Branch	master
Date & Time	2025-05-03 11:15:17
Technologies	terraform, cloudformation, ansible, javascript, docker, kubernetes, pulumi
Compliance Score	1/100
IaC Files Found	1662
Total Files Scanned	2202
High Risk Issues	129
Medium Risk Issues	32
Low Risk Issues	0
Security Issues	146
Availability Issues	10
Confidentiality Issues	5

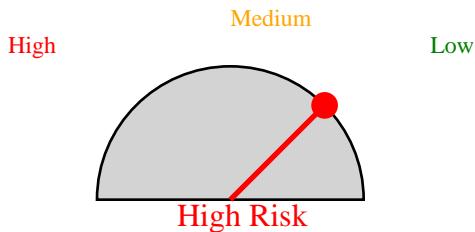
# Risk Assessment



## GDPR Compliance Protection

High risk of potential GDPR fines - immediate action required

Potential fines up to €20 million or 4% of global revenue



This scan has identified a high number of high-risk PII items. Immediate action is recommended to ensure GDPR compliance and protect sensitive data.

# Data Sustainability Compliance

Data sustainability measures how efficiently your organization manages personal data in compliance with GDPR principles of data minimization, storage limitation, and purpose limitation. A higher score indicates better long-term data governance practices.



Measures resource optimization, code efficiency, and energy consumption

## Detailed Findings

### SOC2 Compliance Summary

This SOC2 compliance scan resulted in a score of 1/100, which is considered **Critical**. The findings are categorized below based on Trust Services Criteria (TSC) categories to help with prioritization and remediation.

Repository	<a href="https://github.com/vishaal314/terrascan">https://github.com/vishaal314/terrascan</a>
Branch	master
Scan Date	2025-05-03 11:15:17
Total Findings	161
High Risk Findings	129
Medium Risk Findings	32
Low Risk Findings	0

### Findings by SOC2 TSC Category



# SOC2 Detailed Findings

File	Line	Description	Risk	Category	SOC2 TSC
deploy/helm/templates/12_main_tf	32	Container not running as non-root user	MEDIUM	Security	CC1.1, CC1.2, CC1.3, CC1.4, CC2.1
pkg/cli/testdata/run-test/main_tf	2	AWS provider without version constraint	MEDIUM	Security	CC1.1, CC1.2, CC1.3, CC1.4, CC2.1
pkg/cli/testdata/run-test/19_pod.yaml	19	Container allowed to escalate privileges	HIGH	Security	CC1.1, CC1.2, CC1.3, CC1.4, CC2.1
pkg/cli/testdata/run-test/48_pod.yaml	48	Container allowed to escalate privileges	HIGH	Security	CC1.1, CC1.2, CC1.3, CC1.4, CC2.1
pkg/cli/testdata/run-test/14_web.tf	14	Security group with unrestricted ingress	HIGH	Security	CC6.6, CC6.7
pkg/cli/testdata/run-test/29_web.tf	29	Security group with unrestricted ingress	HIGH	Security	CC6.6, CC6.7
pkg/downloader/module/57_downloader	57	Hard-coded credentials or secrets	HIGH	Security	CC6.1, CC6.6, CC6.7
pkg/http-server/file-scan/107	107	Hard-coded credentials or secrets	HIGH	Security	CC6.1, CC6.6, CC6.7
pkg/http-server/file-scan/395	395	Hard-coded credentials or secrets	HIGH	Security	CC6.1, CC6.6, CC6.7
pkg/http-server/start.g65	65	Hard-coded credentials or secrets	HIGH	Security	CC6.1, CC6.6, CC6.7
pkg/http-server/start.g96	96	Hard-coded credentials or secrets	HIGH	Security	CC6.1, CC6.6, CC6.7
pkg/http-server/webhook/84-scan	84	Hard-coded credentials or secrets	HIGH	Security	CC6.1, CC6.6, CC6.7
pkg/http-server/webhook/38-scan	38	Hard-coded credentials or secrets	HIGH	Security	CC6.1, CC6.6, CC6.7
pkg/http-server/webhook/44-scan	44	Hard-coded credentials or secrets	HIGH	Security	CC6.1, CC6.6, CC6.7
pkg/http-server/webhook/24-scan	24	Hard-coded credentials or secrets	HIGH	Security	CC6.1, CC6.6, CC6.7
pkg/http-server/assets/5_bootstrap	5	Hard-coded credentials or secrets	HIGH	Security	CC6.1, CC6.6, CC6.7
pkg/http-server/testdata/1/testconfig	11	AWS provider without version constraint	MEDIUM	Security	CC1.1, CC1.2, CC1.3, CC1.4, CC2.1
pkg/http-server/testdata/50_testconfig	50	Security group with unrestricted ingress	HIGH	Security	CC6.6, CC6.7
pkg/http-server/testdata/58_testconfig	58	Security group with unrestricted ingress	HIGH	Security	CC6.6, CC6.7
.../v1/testdata/template/243/deploy	243	Amazon S3 policy with unrestricted access	HIGH	Security	CC6.1, CC6.3
.../v1/testdata/template/783/deploy	783	S3 bucket with public read access	HIGH	Confidentiality	C1.1
...testdata/templates/s3/24_deploy	24	Template with unrestricted access	HIGH	Security	CC6.1, CC6.3
...testdata/templates/s3/77_deploy	77	Template with public read access	HIGH	Confidentiality	C1.1
...ac-providers/docker/40_parse	40	Hard-coded credentials or secrets	HIGH	Security	CC6.1, CC6.6, CC6.7
...bernetes/v1/testdata/k84_temp	184	Parsing hostPath volume	HIGH	Security	CC6.1, CC6.8
...bernetes/v1/testdata/k87_temp	187	Parsing hostPath volume	HIGH	Security	CC6.1, CC6.8
...data/file-test-data/test/5bad_k8n	5	Kubernetes container allowed to escalate privileges	HIGH	Security	CC1.1, CC1.2, CC1.3, CC1.4, CC2.1
...data/file-test-data/test/33bad_k8n	33	Kubernetes container allowed to escalate privileges	HIGH	Security	CC1.1, CC1.2, CC1.3, CC1.4, CC2.1
.../file-test-data/test/bat/5_meta	5	Container allowed to escalate privileges	HIGH	Security	CC1.1, CC1.2, CC1.3, CC1.4, CC2.1

.../file-test-data/test_bad_28_metadataContainer allowed to escalate privileges	HIGH	Security	CC1.1, CC1.2, CC1.3, CC1.4, CC2.1
...-test-data/test_bad_15_metadataContainer allowed to escalate privileges	HIGH	Security	CC1.1, CC1.2, CC1.3, CC1.4, CC2.1
...-test-data/test_bad_20_metadataContainer allowed to escalate privileges	HIGH	Security	CC1.1, CC1.2, CC1.3, CC1.4, CC2.1
...file-test-data/test_bad_5_namespacesContainer allowed to escalate privileges	HIGH	Security	CC1.1, CC1.2, CC1.3, CC1.4, CC2.1
...file-test-data/test_bad_33_namespacesContainer allowed to escalate privileges	HIGH	Security	CC1.1, CC1.2, CC1.3, CC1.4, CC2.1
...tdata/file-test-data/test_14_no_kubernetesContainer allowed to escalate privileges	HIGH	Security	CC1.1, CC1.2, CC1.3, CC1.4, CC2.1
...tdata/file-test-data/test_32_no_kubernetesContainer allowed to escalate privileges	HIGH	Security	CC1.1, CC1.2, CC1.3, CC1.4, CC2.1
...a/file-test-data/test_n14_metadataContainer allowed to escalate privileges	HIGH	Security	CC1.1, CC1.2, CC1.3, CC1.4, CC2.1
...a/file-test-data/test_n32_metadataContainer allowed to escalate privileges	HIGH	Security	CC1.1, CC1.2, CC1.3, CC1.4, CC2.1
...e-test-data/test_no_16_metadataContainer allowed to escalate privileges	HIGH	Security	CC1.1, CC1.2, CC1.3, CC1.4, CC2.1
...e-test-data/test_no_182_metadataContainer allowed to escalate privileges	HIGH	Security	CC1.1, CC1.2, CC1.3, CC1.4, CC2.1
...testdata/file-test-data/test_15_no_podContainer allowed to escalate privileges	HIGH	Security	CC1.1, CC1.2, CC1.3, CC1.4, CC2.1
...testdata/file-test-data/test_20_no_podContainer allowed to escalate privileges	HIGH	Security	CC1.1, CC1.2, CC1.3, CC1.4, CC2.1
...le-test-data/test_pod19_skip_16_gentainer allowed to escalate privileges	HIGH	Security	CC1.1, CC1.2, CC1.3, CC1.4, CC2.1
...le-test-data/test_pod48_skip_16_gentainer allowed to escalate privileges	HIGH	Security	CC1.1, CC1.2, CC1.3, CC1.4, CC2.1
...testdata/yaml-extension15/testContainer allowed to escalate privileges	HIGH	Security	CC1.1, CC1.2, CC1.3, CC1.4, CC2.1
...testdata/yaml-extension39/testContainer allowed to escalate privileges	HIGH	Security	CC1.1, CC1.2, CC1.3, CC1.4, CC2.1
...with-multiple-documents11/testContainer allowed to escalate privileges	HIGH	Security	CC1.1, CC1.2, CC1.3, CC1.4, CC2.1
...with-multiple-documents33/testContainer allowed to escalate privileges	HIGH	Security	CC1.1, CC1.2, CC1.3, CC1.4, CC2.1
.../erroneous-deployment18/deployContainer allowed to escalate privileges	HIGH	Security	CC1.1, CC1.2, CC1.3, CC1.4, CC2.1
...roviders/output/vulnerability22/testHardcoded credentials or secrets	HIGH	Security	CC6.1, CC6.6, CC6.7
...roviders/output/vulnerability36/testHardcoded credentials or secrets	HIGH	Security	CC6.1, CC6.6, CC6.7
...roviders/output/vulnerability113/testHardcoded credentials or secrets	HIGH	Security	CC6.1, CC6.6, CC6.7
...raform/commons/crypto27/testSetSecret() function	HIGH	Security	CC5.1, CC6.8, CC7.2
...erraform/commons/lookup52/testHardcoded credentials or secrets	HIGH	Security	CC6.1, CC6.6, CC6.7
...viders/terraform/common81/testHardcoded credentials or secrets	HIGH	Security	CC6.1, CC6.6, CC6.7
...v12/testdata/deep-modules/testAWSprovider without version constraint	MEDIUM	Security	CC1.1, CC1.2, CC1.3, CC1.4, CC2.1
...-module-source/invalid_source55/testAWSprovider without version constraint	MEDIUM	Security	CC1.1, CC1.2, CC1.3, CC1.4, CC2.1
...testdata/invalid-module-configs58/testAWSprovider without version constraint	MEDIUM	Security	CC1.1, CC1.2, CC1.3, CC1.4, CC2.1
...rm/v12/testdata/module-configuration58/testAWSprovider without version constraint	MEDIUM	Security	CC1.1, CC1.2, CC1.3, CC1.4, CC2.1
...v12/testdata/module-configs83/testSecuritygroup with unrestricted ingress	HIGH	Security	CC6.6, CC6.7
...orm/v12/testdata/tfcollections/configAWSprovider without version constraint	MEDIUM	Security	CC1.1, CC1.2, CC1.3, CC1.4, CC2.1

...orm/v12/testdata/tfconfig	45	Security group with unrestricted ingress	HIGH	Security	CC6.6, CC6.7
...orm/v12/testdata/tfconfig	55	Security group with unrestricted ingress	HIGH	Security	CC6.6, CC6.7
...12/testdata/tfjson/moduleconfigs	591	AMSI policy with unrestricted access	HIGH	Security	CC6.1, CC6.3
...v14/testdata/deep-m5modules/testdata	141	AMSI provider without version constraint	MEDIUM	Security	CC1.1, CC1.2, CC1.3, CC1.4, CC2.1
...-module-source/invalid_source	151	AMSI provider without version constraint	MEDIUM	Security	CC1.1, CC1.2, CC1.3, CC1.4, CC2.1
...estdata/invalid-moduleconfigs	155	AMSI provider without version constraint	MEDIUM	Security	CC1.1, CC1.2, CC1.3, CC1.4, CC2.1
...rm/v14/testdata/moduleconfigs	159	AMSI provider without version constraint	MEDIUM	Security	CC1.1, CC1.2, CC1.3, CC1.4, CC2.1
...v14/testdata/moduleconfigs/securitygroup	163	Security group with unrestricted ingress	HIGH	Security	CC6.6, CC6.7
...orm/v14/testdata/tfconfig	171	AMSI provider without version constraint	MEDIUM	Security	CC1.1, CC1.2, CC1.3, CC1.4, CC2.1
...orm/v14/testdata/tfconfig	181	Security group with unrestricted ingress	HIGH	Security	CC6.6, CC6.7
...orm/v14/testdata/tfconfig	191	Security group with unrestricted ingress	HIGH	Security	CC6.6, CC6.7
...14/testdata/tfjson/moduleconfigs	195	AMSI policy with unrestricted access	HIGH	Security	CC6.1, CC6.3
...v15/testdata/deep-m5modules/testdata	199	AMSI provider without version constraint	MEDIUM	Security	CC1.1, CC1.2, CC1.3, CC1.4, CC2.1
...-module-source/invalid_source	211	AMSI provider without version constraint	MEDIUM	Security	CC1.1, CC1.2, CC1.3, CC1.4, CC2.1
...estdata/invalid-moduleconfigs	215	AMSI provider without version constraint	MEDIUM	Security	CC1.1, CC1.2, CC1.3, CC1.4, CC2.1
...rm/v15/testdata/moduleconfigs	219	AMSI provider without version constraint	MEDIUM	Security	CC1.1, CC1.2, CC1.3, CC1.4, CC2.1
...v15/testdata/moduleconfigs/securitygroup	223	Security group with unrestricted ingress	HIGH	Security	CC6.6, CC6.7
...orm/v15/testdata/tfconfig	231	AMSI provider without version constraint	MEDIUM	Security	CC1.1, CC1.2, CC1.3, CC1.4, CC2.1
...orm/v15/testdata/tfconfig	241	Security group with unrestricted ingress	HIGH	Security	CC6.6, CC6.7
...orm/v15/testdata/tfconfig	251	Security group with unrestricted ingress	HIGH	Security	CC6.6, CC6.7
...15/testdata/tfjson/moduleconfigs	255	AMSI policy with unrestricted access	HIGH	Security	CC6.1, CC6.3
pkg/initialize/run.go	76	Hard-coded credentials or secrets	HIGH	Security	CC6.1, CC6.6, CC6.7
...mission-webhook/validation	167	Hard-coded credentials or secrets	HIGH	Security	CC6.1, CC6.6, CC6.7
...mission-webhook/validation	173	Hard-coded credentials or secrets	HIGH	Security	CC6.1, CC6.6, CC6.7
...mission-webhook/validation	182	Hard-coded credentials or secrets	HIGH	Security	CC6.1, CC6.6, CC6.7
...on-webhook/validation	187	Hard-coded credentials or secrets	HIGH	Security	CC6.1, CC6.6, CC6.7
pkg/k8s/dblogs/webhook	192	scan-logger exec function	HIGH	Security	CC6.1, CC6.8, CC7.2
pkg/k8s/dblogs/webhook	206	scan-logger exec function	HIGH	Security	CC6.1, CC6.8, CC7.2
...oviders/arm/config/authn	211	playgrounded credentials or secrets	HIGH	Security	CC6.1, CC6.6, CC6.7
...oviders/arm/config/authn	231	playgrounded credentials or secrets	HIGH	Security	CC6.1, CC6.6, CC6.7
...ders/arm/config/kube	236	beta-credentials	HIGH	Security	CC6.1, CC6.6, CC6.7
...-providers/arm/config	237	inssq-credentials	HIGH	Security	CC6.1, CC6.6, CC6.7

...providers/arm/config@0sq	108	Hard-coded credentials or secrets	HIGH	Security	CC6.1, CC6.6, CC6.7
...iac-providers/arm/functions@04	109	Hard-coded credentials or secrets	HIGH	Security	CC6.1, CC6.6, CC6.7
...providers/arm/functions@08/parameters@05	110	Hard-coded credentials or secrets	HIGH	Security	CC6.1, CC6.6, CC6.7
...roviders/arm/functions@02/resource@04	111	Hard-coded credentials or secrets	HIGH	Security	CC6.1, CC6.6, CC6.7
...c-providers/arm/functions@08/to@01	112	Hard-coded credentials or secrets	HIGH	Security	CC6.1, CC6.6, CC6.7
...-providers/arm/functions@08/variables@05	113	Hard-coded credentials or secrets	HIGH	Security	CC6.1, CC6.6, CC6.7
...iac-providers/cft/functions@s3@05	114	Hard-coded credentials or secrets	HIGH	Security	CC6.1, CC6.6, CC6.7
...roviders/cft/functions@23/uri@01	115	Hard-coded credentials or secrets	HIGH	Security	CC6.1, CC6.6, CC6.7
...pper/iac-providers/cft@04/store@01/type@01	116	Hard-coded credentials or secrets	HIGH	Security	CC6.1, CC6.6, CC6.7
...pper/iac-providers/cft@04/store@01/type@02	117	Hard-coded credentials or secrets	HIGH	Security	CC6.1, CC6.6, CC6.7
...pper/iac-providers/cft@04/store@01/type@03	118	Hard-coded credentials or secrets	HIGH	Security	CC6.1, CC6.6, CC6.7
...pper/iac-providers/cft@04/store@01/type@04	119	Hard-coded credentials or secrets	HIGH	Security	CC6.1, CC6.6, CC6.7
...notifications/webhook@02/webhook@01	120	Hard-coded credentials or secrets	HIGH	Security	CC6.1, CC6.6, CC6.7
...nction/lambdaNotEnd@01/option@01	121	Hard-coded credentials or secrets	HIGH	Security	CC6.1, CC6.6, CC6.7
...s/kubernetes_pod/app@01/mcr@01	122	Hard-coded credentials or secrets	HIGH	Security	CC6.1, CC6.6, CC6.7
pkg/utils/skip_rules_test@01	123	S3 bucket with public read access	HIGH	Confidentiality	C1.1
pkg/utils/http/request.go@01	124	Hard-coded credentials or secrets	HIGH	Security	CC6.1, CC6.6, CC6.7
pkg/vulnerability/acr.go@07	125	Possible hard-coded password	HIGH	Security	CC6.1, CC6.7
pkg/vulnerability/acr.go@208	126	Possible hard-coded password	HIGH	Security	CC6.1, CC6.7
pkg/vulnerability/gcr.go@251	127	Possible hard-coded password	HIGH	Security	CC6.1, CC6.7
pkg/vulnerability/harbo@050	128	Hard-coded credentials or secrets	HIGH	Security	CC6.1, CC6.6, CC6.7
pkg/vulnerability/harbo@740	129	Hard-coded credentials or secrets	HIGH	Security	CC6.1, CC6.6, CC6.7
pkg/vulnerability/harbo@830/st.go@01	130	Hard-coded credentials or secrets	HIGH	Security	CC6.1, CC6.6, CC6.7
test/e2e/scan/scan_test@01	131	Hard-coded credentials or secrets	HIGH	Security	CC6.1, CC6.6, CC6.7
...ata/iac/aws/aws_ami@1/violation@01	132	Amazon S3 provider without version constraint	MEDIUM	Security	CC1.1, CC1.2, CC1.3, CC1.4, CC2.1
...aws/aws_db_instance@01/violation@01	133	Amazon S3 provider without version constraint	MEDIUM	Security	CC1.1, CC1.2, CC1.3, CC1.4, CC2.1
...aws/aws_db_instance@21/violation@01	134	Possible hard-coded password	HIGH	Security	CC6.1, CC6.7
...aws/aws_db_instance@34/violation@01	135	Possible hard-coded password	HIGH	Security	CC6.1, CC6.7
...aws/aws_db_instance@51/violation@01	136	Possible hard-coded password	HIGH	Security	CC6.1, CC6.7
...aws/aws_db_instance@65/violation@01	137	Possible hard-coded password	HIGH	Security	CC6.1, CC6.7
...aws/aws_db_instance@78/violation@01	138	Possible hard-coded password	HIGH	Security	CC6.1, CC6.7
...aws/aws_db_instance@91/violation@01	139	Possible hard-coded password	HIGH	Security	CC6.1, CC6.7

...aws/aws_db_instance	11	Violation	Possible	hard-coded password	HIGH	Security	CC6.1, CC6.7
...aws/aws_db_instance	130	Violation	Possible	hard-coded password	HIGH	Security	CC6.1, CC6.7
...aws/aws_db_instance	149	Violation	Possible	hard-coded password	HIGH	Security	CC6.1, CC6.7
...aws/aws_db_instance	89	Violation	Possible	Resource with encryption disabled	HIGH	Confidentiality	C1.1
...aws/aws_db_instance	82	Violation	Possible	Resource with backups disabled	MEDIUM	Availability	A1.2, A1.3
...aws/aws_db_instance	46	Violation	Possible	Resource with backups disabled	MEDIUM	Availability	A1.2, A1.3
...aws/aws_db_instance	100	Violation	Possible	Resource with backups disabled	MEDIUM	Availability	A1.2, A1.3
...aws/aws_db_instance	25	Violation	Possible	Resource with backups disabled	MEDIUM	Availability	A1.2, A1.3
...aws/aws_db_instance	44	Violation	Possible	Resource with backups disabled	MEDIUM	Availability	A1.2, A1.3
...ng/max_severity_set	12	Terraform	Possible	hard-coded password	HIGH	Security	CC6.1, CC6.7
...x_severity_set_none	12	Terraform	Possible	hard-coded password	HIGH	Security	CC6.1, CC6.7
...x_both_severity_set	13	Terraform	Possible	hard-coded password	HIGH	Security	CC6.1, CC6.7
...ng/min_severity_set	12	Terraform	Possible	hard-coded password	HIGH	Security	CC6.1, CC6.7
...rity_with_skip_rule	18	Terraform	Possible	hard-coded password	HIGH	Security	CC6.1, CC6.7
...c/resource_skipping	10	Terraform	AVG	Script provider without version constraint	MEDIUM	Security	CC1.1, CC1.2, CC1.3, CC1.4, CC2.1
...c/resource_skipping	21	Terraform	Possible	hard-coded password	HIGH	Security	CC6.1, CC6.7
...c/resource_skipping	84	Terraform	Possible	hard-coded password	HIGH	Security	CC6.1, CC6.7
...c/resource_skipping	51	Terraform	Possible	hard-coded password	HIGH	Security	CC6.1, CC6.7
...c/resource_skipping	67	Terraform	Possible	hard-coded password	HIGH	Security	CC6.1, CC6.7
...c/resource_skipping	81	Terraform	Possible	hard-coded password	HIGH	Security	CC6.1, CC6.7
...c/resource_skipping	81	Terraform	Possible	hard-coded password	HIGH	Security	CC6.1, CC6.7
...c/resource_skipping	88	Terraform	Possible	hard-coded password	HIGH	Security	CC6.1, CC6.7
...c/resource_skipping	104	Terraform	Possible	hard-coded password	HIGH	Security	CC6.1, CC6.7
...c/resource_skipping	138	Terraform	Possible	hard-coded password	HIGH	Security	CC6.1, CC6.7
...c/resource_skipping	152	Terraform	Possible	hard-coded password	HIGH	Security	CC6.1, CC6.7
...c/resource_skipping	82	Terraform	Result	Resource with encryption disabled	HIGH	Confidentiality	C1.1
...c/resource_skipping	82	Terraform	Result	Resource with backups disabled	MEDIUM	Availability	A1.2, A1.3
...c/resource_skipping	48	Terraform	Result	Resource with backups disabled	MEDIUM	Availability	A1.2, A1.3
...c/resource_skipping	108	Terraform	Result	Resource with backups disabled	MEDIUM	Availability	A1.2, A1.3
...c/resource_skipping	128	Terraform	Result	Resource with backups disabled	MEDIUM	Availability	A1.2, A1.3
...c/resource_skipping	147	Terraform	Result	Resource with backups disabled	MEDIUM	Availability	A1.2, A1.3
...cursive/subFolder1/subFolder2	AVG	Script provider	without version constraint		MEDIUM	Security	CC1.1, CC1.2, CC1.3, CC1.4, CC2.1
...ingwebhook/validating	43	webhook	check	credentials or secrets	HIGH	Security	CC6.1, CC6.6, CC6.7

...ingwebhook/validating <del>83</del> webhook <del>hard-coded</del> credentials or secrets	HIGH	Security	CC6.1, CC6.6, CC6.7
...ingwebhook/validating <del>79</del> webhook <del>hard-coded</del> credentials or secrets	HIGH	Security	CC6.1, CC6.6, CC6.7
...e/vulnerability/vulnerability <del>12</del> <del>test</del> hard-coded credentials or secrets	HIGH	Security	CC6.1, CC6.6, CC6.7
...e/vulnerability/vulnerability <del>15</del> <del>test</del> hard-coded credentials or secrets	HIGH	Security	CC6.1, CC6.6, CC6.7

# SOC2 Recommendations

The following recommendations are based on the scan findings. Implementing these recommendations will help improve your SOC2 compliance posture and reduce risks.

## 1. Recommendation 1 (Priority: Medium)

SOC2 Security - Disable privilege escalation for containers

Implementation Steps:

- Review and remove hard-coded credentials and secrets
- Implement proper secret management
- Update security configurations to follow least privilege principle
- Focus on files: pkg/cli/testdata/run-test/test\_pod.yaml:19, pkg/cli/testdata/run-test/test\_pod.yaml:43, pkg/iac-providers/kubernetes/v1/testdata/file-test-data/test\_bad\_kind.yml:15...
- SOC2 TSC Criteria: CC1.1, CC1.2, CC1.3, CC1.4, CC2.1, CC2.2, CC2.3, CC3.1, CC3.2, CC3.3, CC3.4, CC4.1, CC4.2, CC5.1, CC5.2, CC5.3, CC6.1, CC6.2, CC6.3, CC6.4, CC6.5, CC6.6, CC6.7, CC6.8, CC7.1, CC7.2, CC7.3, CC7.4, CC7.5, CC8.1, CC9.1, CC9.2

## 2. Recommendation 2 (Priority: Medium)

SOC2 Security - Restrict ingress traffic to known IP ranges or specific sources

Implementation Steps:

- Review and remove hard-coded credentials and secrets
- Implement proper secret management
- Update security configurations to follow least privilege principle
- Focus on files: pkg/cli/testdata/run-test/web.tf:14, pkg/cli/testdata/run-test/web.tf:23, pkg/http-server/testdata/testconfig.tf:50...
- SOC2 TSC Criteria: CC6.6, CC6.7

## 3. Recommendation 3 (Priority: Medium)

SOC2 Security - Store sensitive information in environment variables or a secure vault

Implementation Steps:

- Review and remove hard-coded credentials and secrets
- Implement proper secret management
- Update security configurations to follow least privilege principle
- Focus on files: pkg/downloader/module-download\_test.go:571, pkg/http-server/file-scan.go:107, pkg/http-server/file-scan\_test.go:395...

- SOC2 TSC Criteria: CC6.1, CC6.6, CC6.7

## 4. Recommendation 4 (Priority: Medium)

SOC2 Security - Follow the principle of least privilege by limiting permissions

Implementation Steps:

- Review and remove hard-coded credentials and secrets
- Implement proper secret management
- Update security configurations to follow least privilege principle
- Focus on files: pkg/iac-providers/cft/v1/testdata/templates/s3/deploy.json:24, pkg/iac-providers/cft/v1/testdata/templates/s3/deploy.template:24, pkg/iac-providers/terraform/v12/testdata/tfjson/moduleconfigs.json:591...
- SOC2 TSC Criteria: CC6.1, CC6.3

## 5. Recommendation 5 (Priority: Medium)

SOC2 Confidentiality - Restrict S3 bucket access to only required principals

Implementation Steps:

- Enable encryption for data at rest and in transit
- Review and update access controls
- Focus on files: pkg/iac-providers/cft/v1/testdata/templates/s3/deploy.json:7, pkg/iac-providers/cft/v1/testdata/templates/s3/deploy.template:7, pkg/utils/skip\_rules\_test.go:123
- SOC2 TSC Criteria: C1.1

## 6. Recommendation 6 (Priority: Medium)

SOC2 Security - Avoid using hostPath as it allows access to host filesystem

Implementation Steps:

- Review and remove hard-coded credentials and secrets
- Implement proper secret management
- Update security configurations to follow least privilege principle
- Focus on files: pkg/iac-providers/kubernetes/v1/testdata/k8s\_templates.go:164, pkg/iac-providers/kubernetes/v1/testdata/k8s\_templates.go:167
- SOC2 TSC Criteria: CC6.1, CC6.8

## 7. Recommendation 7 (Priority: Medium)

SOC2 Security - Avoid using eval() as it can lead to code injection vulnerabilities

Implementation Steps:

- Review and remove hard-coded credentials and secrets
- Implement proper secret management
- Update security configurations to follow least privilege principle
- Focus on files: pkg/iac-providers/terraform/commons/cty-converters\_test.go:287
- SOC2 TSC Criteria: CC5.1, CC6.8, CC7.2

## 8. Recommendation 8 (Priority: Medium)

SOC2 Security - Avoid using exec() as it can lead to command injection vulnerabilities

Implementation Steps:

- Review and remove hard-coded credentials and secrets
- Implement proper secret management
- Update security configurations to follow least privilege principle
- Focus on files: pkg/k8s/dblogs/webhook-scan-logger.go:72, pkg/k8s/dblogs/webhook-scan-logger.go:206
- SOC2 TSC Criteria: CC6.1, CC6.8, CC7.2

## 9. Recommendation 9 (Priority: Medium)

SOC2 Security - Use secrets manager instead of hard-coded passwords

Implementation Steps:

- Review and remove hard-coded credentials and secrets
- Implement proper secret management
- Update security configurations to follow least privilege principle
- Focus on files: pkg/vulnerability/acr.go:37, pkg/vulnerability/acr.go:208, pkg/vulnerability/gcr.go:251...
- SOC2 TSC Criteria: CC6.1, CC6.7

## 10. Recommendation 10 (Priority: Medium)

SOC2 Confidentiality - Enable encryption for data protection

Implementation Steps:

- Enable encryption for data at rest and in transit
- Review and update access controls
- Focus on files: test/e2e/test\_data/iac/aws/aws\_db\_instanceViolation/main.tf:89, test/e2e/test\_data/iac/resource\_skipping/terraform/main.tf:92
- SOC2 TSC Criteria: C1.1

## 11. Recommendation 11 (Priority: Medium)

SOC2 Security - Run containers as non-root users

Implementation Steps:

- Update security configurations to follow best practices
- Implement proper access controls
- Focus on files: deploy/helm/templates/deployments.yaml:32
- SOC2 TSC Criteria: CC1.1, CC1.2, CC1.3, CC1.4, CC2.1, CC2.2, CC2.3, CC3.1, CC3.2, CC3.3, CC3.4, CC4.1, CC4.2, CC5.1, CC5.2, CC5.3, CC6.1, CC6.2, CC6.3, CC6.4, CC6.5, CC6.6, CC6.7, CC6.8, CC7.1, CC7.2, CC7.3, CC7.4, CC7.5, CC8.1, CC9.1, CC9.2

## 12. Recommendation 12 (Priority: Medium)

SOC2 Security - Specify provider version constraints for better stability and security

Implementation Steps:

- Update security configurations to follow best practices
- Implement proper access controls
- Focus on files: pkg/cli/testdata/run-test/main.tf:2, pkg/http-server/testdata/testconfig.tf:1, pkg/iac-providers/terraform/v12/testdata深深-modules/template.tf:5...
- SOC2 TSC Criteria: CC1.1, CC1.2, CC1.3, CC1.4, CC2.1, CC2.2, CC2.3, CC3.1, CC3.2, CC3.3, CC3.4, CC4.1, CC4.2, CC5.1, CC5.2, CC5.3, CC6.1, CC6.2, CC6.3, CC6.4, CC6.5, CC6.6, CC6.7, CC6.8, CC7.1, CC7.2, CC7.3, CC7.4, CC7.5, CC8.1, CC9.1, CC9.2

## 13. Recommendation 13 (Priority: Medium)

SOC2 Availability - Enable backup for data protection and availability

Implementation Steps:

- Enable backup and disaster recovery features
- Implement proper redundancy and failover mechanisms
- Focus on files: test/e2e/test\_data/iac/aws/aws\_db\_instanceViolation/main.tf:32, test/e2e/test\_data/iac/aws/aws\_db\_instanceViolation/main.tf:46, test/e2e/test\_data/iac/aws/aws\_db\_instanceViolation/main.tf:106...
- SOC2 TSC Criteria: A1.2, A1.3

## SOC2 Trust Services Criteria (TSC) Explanation

SOC2 Trust Services Criteria refer to the specific control points used to assess compliance:  
• CC: Common Criteria (security)  
• A: Availability  
• PI: Processing Integrity  
• C: Confidentiality  
• P: Privacy  
Each finding in this report references specific TSC criteria to help understand how it impacts compliance posture.

## Recommendations & Next Steps

- Implement a formal process for assigning and managing access rights in accordance with the principle of least privilege.
- Develop a comprehensive risk management process that includes automated scanning strategies for Infrastructure-as-Code.
- Conduct periodic reviews of security configurations and apply best practices across all SOC2 Trust Services Criteria.
- Document and verify all control measures relevant to the TSC criteria noted in the findings.
- Implement automated compliance checks in CI/CD pipelines to detect deviations early in the development cycle.

## High-Risk Item Recommendations

- Prioritize immediate remediation of high-risk findings related to CC security-critical components.
- Implement strict access controls for sensitive infrastructure components applying the principle of least privilege.
- Conduct detailed risk assessment for all Common Criteria-related findings.
- Document and test incident response processes for all high-risk vulnerabilities.
- Install an automated validation process that checks IaC changes before they are applied to production environments.

## Data Sustainability Recommendations

- Implement data minimization practices to collect only necessary personal data.
- Establish clear data retention periods and automated deletion processes.
- Regularly audit and clean databases to remove redundant or obsolete data.
- Design systems with privacy by design principles to improve sustainability.
- Consider data storage optimization to reduce environmental impact of data centers.

## Scan Metadata

Scan ID	0805a181-1d22-422c-9997-9da9da4637c7
Scan Type	soc2
Region	Global
Timestamp	2025-05-03 11:15:17
Repository Provider	GitHub
Repository URL	Not available
Repository Path	Not available
Branch	master
Username	vishaal
Files Scanned	2202
CC Findings	0
A Findings	0
PI Findings	0
C Findings	0
P Findings	0

Disclaimer: This report is provided for informational purposes only and should not be considered legal or compliance advice. The findings in this report are based on automated scanning and may not identify all SOC2-relevant security issues. The Trust Services Criteria (TSC) mapping is intended as guidance. We recommend consulting with a qualified SOC2 auditor or compliance specialist for specific SOC2 compliance guidance.