

# DataGuardian Pro

## GDPR Compliance Scan Report

Generated on: May 03, 2025 10:52

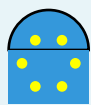
Scan ID: SOC-20250503-8fed57

### 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 10:52:42**. The scan identified a total of **161** compliance issues with **129** high-risk items. The overall compliance score is **99/100**. **Technologies Detected:** javascript, docker, pulumi, kubernetes, cloudformation, ansible, terraform 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	https://github.com/vishaal314/terrascan
Branch	master
Date & Time	2025-05-03 10:52:42
Technologies	javascript, docker, pulumi, kubernetes, cloudformation, ansible, terraform
Compliance Score	99/100
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

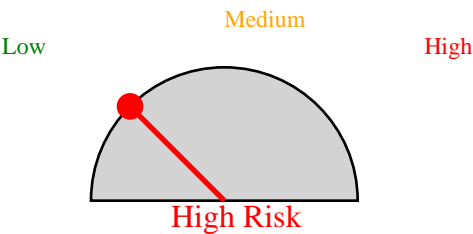
# Risk Assessment



## GDPR Compliance Protection

High risk of potential GDPR fines - immediate action required

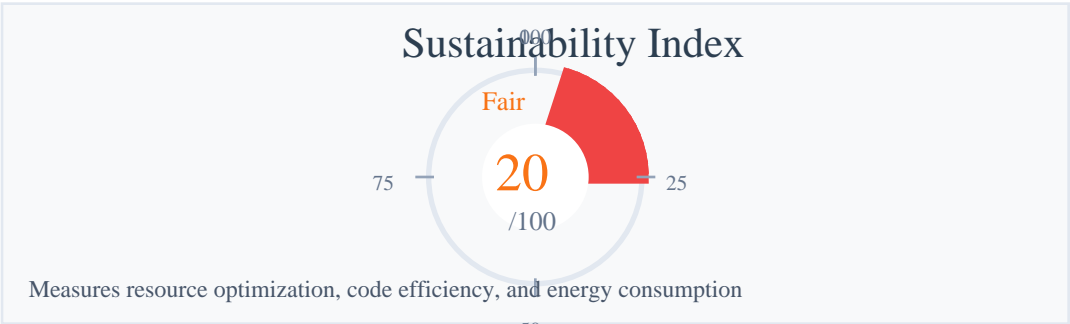
Potential fines up to €20 million or 4% of global revenue



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.



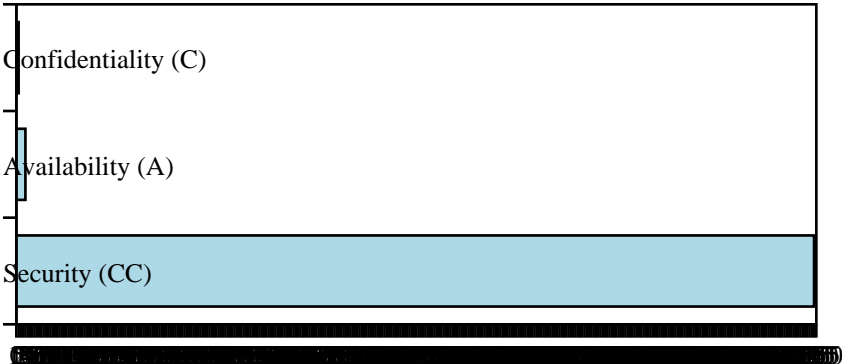
# Detailed Findings

## SOC2 Compliance Summary

This SOC2 compliance scan resulted in a score of 99/100, which is considered Good. The findings are categorized below based on Trust Services Criteria (TSC) categories to help with prioritization and remediation.

Repository	https://github.com/vishaal314/terrascan
Branch	master
Scan Date	2025-05-03 10:52:42
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/s3-deploy.yaml	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_test_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_test_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/23/web.tf	23	Security group with unrestricted ingress	HIGH	Security	CC6.6, CC6.7
pkg/downloader/module571/download_test.go	571	Hard-coded credentials or secrets	HIGH	Security	CC6.1, CC6.6, CC6.7
pkg/http-server/file-scan/1070	1070	Hard-coded credentials or secrets	HIGH	Security	CC6.1, CC6.6, CC6.7
pkg/http-server/file-scan/3955_test.go	3955	Hard-coded credentials or secrets	HIGH	Security	CC6.1, CC6.6, CC6.7
pkg/http-server/start.go	65	Hard-coded credentials or secrets	HIGH	Security	CC6.1, CC6.6, CC6.7
pkg/http-server/start.go	66	Hard-coded credentials or secrets	HIGH	Security	CC6.1, CC6.6, CC6.7
pkg/http-server/webhook/64-scan.go	64	Hard-coded credentials or secrets	HIGH	Security	CC6.1, CC6.6, CC6.7
pkg/http-server/webhook/68-scan.go	68	Hard-coded credentials or secrets	HIGH	Security	CC6.1, CC6.6, CC6.7
pkg/http-server/webhook/64-scan.go	64	Hard-coded credentials or secrets	HIGH	Security	CC6.1, CC6.6, CC6.7
pkg/http-server/webhook/24-scan.go	24	Hard-coded credentials or secrets	HIGH	Security	CC6.1, CC6.6, CC6.7
pkg/http-server/assets/6-bootstrap.html	6	Hard-coded credentials or secrets	HIGH	Security	CC6.1, CC6.6, CC6.7
pkg/http-server/testdata/testconf/14/s3	14	AWS provider without version constraint	MEDIUM	Security	CC1.1, CC1.2, CC1.3, CC1.4, CC2.1
pkg/http-server/testdata/testconf/50/s3	50	Security group with unrestricted ingress	HIGH	Security	CC6.6, CC6.7
pkg/http-server/testdata/testconf/56/s3	56	Security group with unrestricted ingress	HIGH	Security	CC6.6, CC6.7
.../v1/testdata/templates/s3-deploy.yaml	24	IAM policy with unrestricted access	HIGH	Security	CC6.1, CC6.3
.../v1/testdata/templates/s3-deploy.yaml	3	S3 bucket with public read access	HIGH	Confidentiality	C1.1
...testdata/templates/s3-deploy.yaml	24	IAM policy with unrestricted access	HIGH	Security	CC6.1, CC6.3
...testdata/templates/s3-deploy.yaml	3	S3 bucket with public read access	HIGH	Confidentiality	C1.1
...ac-providers/docker/40/parser.go	40	Hard-coded credentials or secrets	HIGH	Security	CC6.1, CC6.6, CC6.7
...bernetes/v1/testdata/164_template.yaml	164	Pod using hostPath volume	HIGH	Security	CC6.1, CC6.8
...bernetes/v1/testdata/165_template.yaml	165	Pod using hostPath volume	HIGH	Security	CC6.1, CC6.8
...data/file-test-data/test5bad_k8s.yaml	5	Container allowed to escalate privileges	HIGH	Security	CC1.1, CC1.2, CC1.3, CC1.4, CC2.1
...data/file-test-data/test3bad_k8s.yaml	3	Container allowed to escalate privileges	HIGH	Security	CC1.1, CC1.2, CC1.3, CC1.4, CC2.1
.../file-test-data/test_bad5meta.yaml	5	Container allowed to escalate privileges	HIGH	Security	CC1.1, CC1.2, CC1.3, CC1.4, CC2.1

.../file-test-data/test_badmeta	28	Container allowed to escalate privileges	HIGH	Security	CC1.1, CC1.2, CC1.3, CC1.4, CC2.1
...-test-data/test_badmeta	15	Container allowed to escalate privileges	HIGH	Security	CC1.1, CC1.2, CC1.3, CC1.4, CC2.1
...-test-data/test_badmeta	20	Container allowed to escalate privileges	HIGH	Security	CC1.1, CC1.2, CC1.3, CC1.4, CC2.1
...file-test-data/test_badnames	15	Container allowed to escalate privileges	HIGH	Security	CC1.1, CC1.2, CC1.3, CC1.4, CC2.1
...file-test-data/test_badnames	33	Container allowed to escalate privileges	HIGH	Security	CC1.1, CC1.2, CC1.3, CC1.4, CC2.1
...tdata/file-test-data/es4	14	Container allowed to escalate privileges	HIGH	Security	CC1.1, CC1.2, CC1.3, CC1.4, CC2.1
...tdata/file-test-data/es2	2	Container allowed to escalate privileges	HIGH	Security	CC1.1, CC1.2, CC1.3, CC1.4, CC2.1
...a/file-test-data/test_nt4	14	Container allowed to escalate privileges	HIGH	Security	CC1.1, CC1.2, CC1.3, CC1.4, CC2.1
...a/file-test-data/test_nt2	2	Container allowed to escalate privileges	HIGH	Security	CC1.1, CC1.2, CC1.3, CC1.4, CC2.1
...e-test-data/test_no14	14	Container allowed to escalate privileges	HIGH	Security	CC1.1, CC1.2, CC1.3, CC1.4, CC2.1
...e-test-data/test_no12	2	Container allowed to escalate privileges	HIGH	Security	CC1.1, CC1.2, CC1.3, CC1.4, CC2.1
...testdata/file-test-data/test	15	Container allowed to escalate privileges	HIGH	Security	CC1.1, CC1.2, CC1.3, CC1.4, CC2.1
...testdata/file-test-data/test	30	Container allowed to escalate privileges	HIGH	Security	CC1.1, CC1.2, CC1.3, CC1.4, CC2.1
...le-test-data/test_pod19	19	Container allowed to escalate privileges	HIGH	Security	CC1.1, CC1.2, CC1.3, CC1.4, CC2.1
...le-test-data/test_pod49	49	Container allowed to escalate privileges	HIGH	Security	CC1.1, CC1.2, CC1.3, CC1.4, CC2.1
...testdata/yaml-extends15	15	Container allowed to escalate privileges	HIGH	Security	CC1.1, CC1.2, CC1.3, CC1.4, CC2.1
...testdata/yaml-extends32	32	Container allowed to escalate privileges	HIGH	Security	CC1.1, CC1.2, CC1.3, CC1.4, CC2.1
...with-multiple-documents	11	Container allowed to escalate privileges	HIGH	Security	CC1.1, CC1.2, CC1.3, CC1.4, CC2.1
...with-multiple-documents	33	Container allowed to escalate privileges	HIGH	Security	CC1.1, CC1.2, CC1.3, CC1.4, CC2.1
.../erroneous-deployment	10	Container allowed to escalate privileges	HIGH	Security	CC1.1, CC1.2, CC1.3, CC1.4, CC2.1
...roviders/output/vulnerability	28	Hard-coded credentials or secrets	HIGH	Security	CC6.1, CC6.6, CC6.7
...roviders/output/vulnerability	30	Hard-coded credentials or secrets	HIGH	Security	CC6.1, CC6.6, CC6.7
...roviders/output/vulnerability	11	Hard-coded credentials or secrets	HIGH	Security	CC6.1, CC6.6, CC6.7
...raform/commons/cy28	28	Use of eval() function	HIGH	Security	CC5.1, CC6.8, CC7.2
...erraform/commons/lookup	15	Hard-coded credentials or secrets	HIGH	Security	CC6.1, CC6.6, CC6.7
...viders/terraform/commons	11	Hard-coded credentials or secrets	HIGH	Security	CC6.1, CC6.6, CC6.7
...v12/testdata/deep-modules	5	Unsafe provider without version constraint	MEDIUM	Security	CC1.1, CC1.2, CC1.3, CC1.4, CC2.1
...-module-source/invalid_source	5	Unsafe provider without version constraint	MEDIUM	Security	CC1.1, CC1.2, CC1.3, CC1.4, CC2.1
...estdata/invalid-moduleconfigs	1	Unsafe provider without version constraint	MEDIUM	Security	CC1.1, CC1.2, CC1.3, CC1.4, CC2.1
...rm/v12/testdata/moduleconfigs	1	Unsafe provider without version constraint	MEDIUM	Security	CC1.1, CC1.2, CC1.3, CC1.4, CC2.1
...v12/testdata/moduleconfigs	1	Security group with unrestricted ingress	HIGH	Security	CC6.6, CC6.7
...orm/v12/testdata/tfconfigs	1	Unsafe provider without version constraint	MEDIUM	Security	CC1.1, CC1.2, CC1.3, CC1.4, CC2.1

...orm/v12/testdata/tfconfigs/consul	49	Security group with unrestricted ingress	HIGH	Security	CC6.6, CC6.7
...orm/v12/testdata/tfconfigs/consul	50	Security group with unrestricted ingress	HIGH	Security	CC6.6, CC6.7
...12/testdata/tfjson/moduleconfigs/iam	501	IAM policy with unrestricted access	HIGH	Security	CC6.1, CC6.3
...v14/testdata/deep-modules/templates	502	AWSPolicy provider without version constraint	MEDIUM	Security	CC1.1, CC1.2, CC1.3, CC1.4, CC2.1
...-module-source/invalid_source	503	AWSPolicy provider without version constraint	MEDIUM	Security	CC1.1, CC1.2, CC1.3, CC1.4, CC2.1
...estdata/invalid-moduleconfigs/iam	504	AWSPolicy provider without version constraint	MEDIUM	Security	CC1.1, CC1.2, CC1.3, CC1.4, CC2.1
...rm/v14/testdata/moduleconfigs/iam	505	AWSPolicy provider without version constraint	MEDIUM	Security	CC1.1, CC1.2, CC1.3, CC1.4, CC2.1
...v14/testdata/moduleconfigs/consul	506	Security group with unrestricted ingress	HIGH	Security	CC6.6, CC6.7
...orm/v14/testdata/tfconfigs/consul	507	AWSPolicy provider without version constraint	MEDIUM	Security	CC1.1, CC1.2, CC1.3, CC1.4, CC2.1
...orm/v14/testdata/tfconfigs/consul	508	Security group with unrestricted ingress	HIGH	Security	CC6.6, CC6.7
...orm/v14/testdata/tfconfigs/consul	509	Security group with unrestricted ingress	HIGH	Security	CC6.6, CC6.7
...14/testdata/tfjson/moduleconfigs/iam	510	IAM policy with unrestricted access	HIGH	Security	CC6.1, CC6.3
...v15/testdata/deep-modules/templates	511	AWSPolicy provider without version constraint	MEDIUM	Security	CC1.1, CC1.2, CC1.3, CC1.4, CC2.1
...-module-source/invalid_source	512	AWSPolicy provider without version constraint	MEDIUM	Security	CC1.1, CC1.2, CC1.3, CC1.4, CC2.1
...estdata/invalid-moduleconfigs/iam	513	AWSPolicy provider without version constraint	MEDIUM	Security	CC1.1, CC1.2, CC1.3, CC1.4, CC2.1
...rm/v15/testdata/moduleconfigs/iam	514	AWSPolicy provider without version constraint	MEDIUM	Security	CC1.1, CC1.2, CC1.3, CC1.4, CC2.1
...v15/testdata/moduleconfigs/consul	515	Security group with unrestricted ingress	HIGH	Security	CC6.6, CC6.7
...orm/v15/testdata/tfconfigs/consul	516	AWSPolicy provider without version constraint	MEDIUM	Security	CC1.1, CC1.2, CC1.3, CC1.4, CC2.1
...orm/v15/testdata/tfconfigs/consul	517	Security group with unrestricted ingress	HIGH	Security	CC6.6, CC6.7
...orm/v15/testdata/tfconfigs/consul	518	Security group with unrestricted ingress	HIGH	Security	CC6.6, CC6.7
...15/testdata/tfjson/moduleconfigs/iam	519	IAM 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/validate-webhook	107	Hard-coded credentials or secrets	HIGH	Security	CC6.1, CC6.6, CC6.7
...mission-webhook/validate-webhook	108	Hard-coded credentials or secrets	HIGH	Security	CC6.1, CC6.6, CC6.7
...mission-webhook/validate-webhook	109	Hard-coded credentials or secrets	HIGH	Security	CC6.1, CC6.6, CC6.7
...on-webhook/validate-webhook	107	Hard-coded credentials or secrets	HIGH	Security	CC6.1, CC6.6, CC6.7
pkg/k8s/dblogs/webhook-log-sec	72	Log of exec function	HIGH	Security	CC6.1, CC6.8, CC7.2
pkg/k8s/dblogs/webhook-log-sec	206	Log of exec function	HIGH	Security	CC6.1, CC6.8, CC7.2
...viders/arm/config/audit-policy	205	Hard-coded credentials or secrets	HIGH	Security	CC6.1, CC6.6, CC6.7
...viders/arm/config/audit-policy	206	Hard-coded credentials or secrets	HIGH	Security	CC6.1, CC6.6, CC6.7
...ders/arm/config/kube-apiserver	206	Hard-coded credentials or secrets	HIGH	Security	CC6.1, CC6.6, CC6.7
...-providers/arm/config/audit-policy	207	Hard-coded credentials or secrets	HIGH	Security	CC6.1, CC6.6, CC6.7

...-providers/arm/config	36	ssq - Hard-coded credentials or secrets	HIGH	Security	CC6.1, CC6.6, CC6.7
...iac-providers/arm/functions	41	ions - Hard-coded credentials or secrets	HIGH	Security	CC6.1, CC6.6, CC6.7
...providers/arm/functions	66	parameters - Hard-coded credentials or secrets	HIGH	Security	CC6.1, CC6.6, CC6.7
...roviders/arm/functions	32	resources - Hard-coded credentials or secrets	HIGH	Security	CC6.1, CC6.6, CC6.7
...c-providers/arm/functions	66	ns/ct - Hard-coded credentials or secrets	HIGH	Security	CC6.1, CC6.6, CC6.7
...-providers/arm/functions	66	variables - Hard-coded credentials or secrets	HIGH	Security	CC6.1, CC6.6, CC6.7
...iac-providers/cft/functions	75	ns/s3 - Hard-coded credentials or secrets	HIGH	Security	CC6.1, CC6.6, CC6.7
...roviders/cft/functions	23	uri - Hard-coded credentials or secrets	HIGH	Security	CC6.1, CC6.6, CC6.7
...pper/iac-providers/cft/store	44	type - Hard-coded credentials or secrets	HIGH	Security	CC6.1, CC6.6, CC6.7
...pper/iac-providers/cft/store	64	type - Hard-coded credentials or secrets	HIGH	Security	CC6.1, CC6.6, CC6.7
...pper/iac-providers/cft/store	64	type - Hard-coded credentials or secrets	HIGH	Security	CC6.1, CC6.6, CC6.7
...pper/iac-providers/cft/store	64	type - Hard-coded credentials or secrets	HIGH	Security	CC6.1, CC6.6, CC6.7
...notifications/webhook	23	webhook - Hard-coded credentials or secrets	HIGH	Security	CC6.1, CC6.6, CC6.7
...nction/lambdaNotEnd	10	pted - Hard-coded credentials or secrets	HIGH	Security	CC6.1, CC6.6, CC6.7
...s/kubernetes_pod/app	10	more - Hard-coded credentials or secrets	HIGH	Security	CC6.1, CC6.6, CC6.7
pkg/utls/skip_rules_test	23	S3 bucket with public read access	HIGH	Confidentiality	C1.1
pkg/utls/http/request	40	Hard-coded credentials or secrets	HIGH	Security	CC6.1, CC6.6, CC6.7
pkg/vulnerability/acr	37	Possible hard-coded password	HIGH	Security	CC6.1, CC6.7
pkg/vulnerability/acr	208	Possible hard-coded password	HIGH	Security	CC6.1, CC6.7
pkg/vulnerability/gcr	251	Possible hard-coded password	HIGH	Security	CC6.1, CC6.7
pkg/vulnerability/harbo	85	Hard-coded credentials or secrets	HIGH	Security	CC6.1, CC6.6, CC6.7
pkg/vulnerability/harbo	74	Hard-coded credentials or secrets	HIGH	Security	CC6.1, CC6.6, CC6.7
pkg/vulnerability/harbo	83	Hard-coded credentials or secrets	HIGH	Security	CC6.1, CC6.6, CC6.7
test/e2e/scan/scan_test	117	Hard-coded credentials or secrets	HIGH	Security	CC6.1, CC6.6, CC6.7
...ata/iac/aws/aws_ami	1	violation - AWS provider without version constraint	MEDIUM	Security	CC1.1, CC1.2, CC1.3, CC1.4, CC2.1
...aws/aws_db_instance	1	violation - AWS provider without version constraint	MEDIUM	Security	CC1.1, CC1.2, CC1.3, CC1.4, CC2.1
...aws/aws_db_instance	21	violation - Possible hard-coded password	HIGH	Security	CC6.1, CC6.7
...aws/aws_db_instance	34	violation - Possible hard-coded password	HIGH	Security	CC6.1, CC6.7
...aws/aws_db_instance	51	violation - Possible hard-coded password	HIGH	Security	CC6.1, CC6.7
...aws/aws_db_instance	65	violation - Possible hard-coded password	HIGH	Security	CC6.1, CC6.7
...aws/aws_db_instance	78	violation - Possible hard-coded password	HIGH	Security	CC6.1, CC6.7
...aws/aws_db_instance	91	violation - Possible hard-coded password	HIGH	Security	CC6.1, CC6.7

...aws/aws_db_instance/11	Violation of possible	Resource with hard-coded password	HIGH	Security	CC6.1, CC6.7
...aws/aws_db_instance/130	Violation of possible	Resource with hard-coded password	HIGH	Security	CC6.1, CC6.7
...aws/aws_db_instance/149	Violation of possible	Resource with hard-coded password	HIGH	Security	CC6.1, CC6.7
...aws/aws_db_instance/189	Violation of possible	Resource with encryption disabled	HIGH	Confidentiality	C1.1
...aws/aws_db_instance/182	Violation of possible	Resource with backups disabled	MEDIUM	Availability	A1.2, A1.3
...aws/aws_db_instance/146	Violation of possible	Resource with backups disabled	MEDIUM	Availability	A1.2, A1.3
...aws/aws_db_instance/106	Violation of possible	Resource with backups disabled	MEDIUM	Availability	A1.2, A1.3
...aws/aws_db_instance/125	Violation of possible	Resource with backups disabled	MEDIUM	Availability	A1.2, A1.3
...aws/aws_db_instance/144	Violation of possible	Resource with backups disabled	MEDIUM	Availability	A1.2, A1.3
...ng/max_severity_set/12	Transformation of possible	Resource with hard-coded password	HIGH	Security	CC6.1, CC6.7
...x_severity_set_none/12	Transformation of possible	Resource with hard-coded password	HIGH	Security	CC6.1, CC6.7
...x_both_severity_set/13	Transformation of possible	Resource with hard-coded password	HIGH	Security	CC6.1, CC6.7
...ng/min_severity_set/12	Transformation of possible	Resource with hard-coded password	HIGH	Security	CC6.1, CC6.7
...rity_with_skip_rule/10	Transformation of possible	Resource with hard-coded password	HIGH	Security	CC6.1, CC6.7
...c/resource_skipping/1	Transformation of AWS provider without version constraint	Resource	MEDIUM	Security	CC1.1, CC1.2, CC1.3, CC1.4, CC2.1
...c/resource_skipping/2	Transformation of possible	Resource with hard-coded password	HIGH	Security	CC6.1, CC6.7
...c/resource_skipping/3	Transformation of possible	Resource with hard-coded password	HIGH	Security	CC6.1, CC6.7
...c/resource_skipping/5	Transformation of possible	Resource with hard-coded password	HIGH	Security	CC6.1, CC6.7
...c/resource_skipping/6	Transformation of possible	Resource with hard-coded password	HIGH	Security	CC6.1, CC6.7
...c/resource_skipping/8	Transformation of possible	Resource with hard-coded password	HIGH	Security	CC6.1, CC6.7
...c/resource_skipping/9	Transformation of possible	Resource with hard-coded password	HIGH	Security	CC6.1, CC6.7
...c/resource_skipping/10	Transformation of possible	Resource with hard-coded password	HIGH	Security	CC6.1, CC6.7
...c/resource_skipping/13	Transformation of possible	Resource with hard-coded password	HIGH	Security	CC6.1, CC6.7
...c/resource_skipping/15	Transformation of possible	Resource with hard-coded password	HIGH	Security	CC6.1, CC6.7
...c/resource_skipping/19	Transformation of possible	Resource with encryption disabled	HIGH	Confidentiality	C1.1
...c/resource_skipping/32	Transformation of possible	Resource with backups disabled	MEDIUM	Availability	A1.2, A1.3
...c/resource_skipping/46	Transformation of possible	Resource with backups disabled	MEDIUM	Availability	A1.2, A1.3
...c/resource_skipping/100	Transformation of possible	Resource with backups disabled	MEDIUM	Availability	A1.2, A1.3
...c/resource_skipping/126	Transformation of possible	Resource with backups disabled	MEDIUM	Availability	A1.2, A1.3
...c/resource_skipping/147	Transformation of possible	Resource with backups disabled	MEDIUM	Availability	A1.2, A1.3
...cursive/subFolder1/subFolder2	Transformation of AWS provider without version constraint	Resource	MEDIUM	Security	CC1.1, CC1.2, CC1.3, CC1.4, CC2.1
...ingwebhook/validating3	Webhook test id	Resource with credentials or secrets	HIGH	Security	CC6.1, CC6.6, CC6.7



...ingwebhook/validatingwebhook/ <del>test</del>	68	Hard-coded credentials or secrets	HIGH	Security	CC6.1, CC6.6, CC6.7
...ingwebhook/validatingwebhook/ <del>test</del>	70	Hard-coded credentials or secrets	HIGH	Security	CC6.1, CC6.6, CC6.7
...e/vulnerability/vulnerability_ <del>test</del>	72	Hard-coded credentials or secrets	HIGH	Security	CC6.1, CC6.6, CC6.7
...e/vulnerability/vulnerability_ <del>test</del>	74	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\_instance\_violation/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/deep-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\_instance\_violation/main.tf:32, test/e2e/test\_data/iac/aws/aws\_db\_instance\_violation/main.tf:46, test/e2e/test\_data/iac/aws/aws\_db\_instance\_violation/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	8fed57ff-ea58-4f44-bf8a-39e59106e1b5
Scan Type	soc2
Region	Global
Timestamp	2025-05-03 10:52:42
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.