

Generated on: May 03, 2025 12:40

Scan ID:

SOC-20250503-119a2a

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 12:40:01**. The scan identified a total of **161** compliance issues with **129** high-risk items. The overall compliance score is **1/100**. **Technologies Detected:** pulumi, kubernetes, docker, terraform, javascript, ansible, cloudformation 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 12:40:01
Technologies	pulumi, kubernetes, docker, terraform, javascript, ansible, cloudformation
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

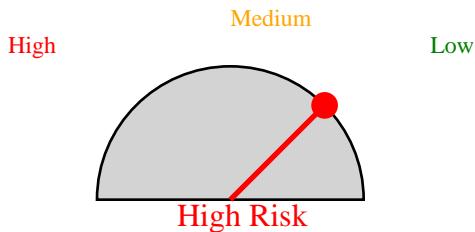
Risk Assessment



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	https://github.com/vishaal314/terrascan
Branch	master
Scan Date	2025-05-03 12:40:01
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/32/deployContainer.go	32	Container running as non-root user	MEDIUM	Security	CC1.1, CC1.2, CC1.3, CC1.4, CC2.1
pkg/cli/testdata/run-test/main.go	33	AWS provider without version constraint	MEDIUM	Security	CC1.1, CC1.2, CC1.3, CC1.4, CC2.1
pkg/cli/testdata/run-test/main.go	39	Container allowed to escalate privileges	HIGH	Security	CC1.1, CC1.2, CC1.3, CC1.4, CC2.1
pkg/cli/testdata/run-test/main.go	43	Container allowed to escalate privileges	HIGH	Security	CC1.1, CC1.2, CC1.3, CC1.4, CC2.1
pkg/cli/testdata/run-test/web.go	51	Security group with unrestricted ingress	HIGH	Security	CC6.6, CC6.7
pkg/cli/testdata/run-test/web.go	53	Security group with unrestricted ingress	HIGH	Security	CC6.6, CC6.7
pkg/downloader/module.go	57	Hard-coded credentials or secrets	HIGH	Security	CC6.1, CC6.6, CC6.7
pkg/http-server/file-scan.go	107	Hard-coded credentials or secrets	HIGH	Security	CC6.1, CC6.6, CC6.7
pkg/http-server/file-scan.go	205	Hard-coded credentials or secrets	HIGH	Security	CC6.1, CC6.6, CC6.7
pkg/http-server/start.go	15	Hard-coded credentials or secrets	HIGH	Security	CC6.1, CC6.6, CC6.7
pkg/http-server/start.go	36	Hard-coded credentials or secrets	HIGH	Security	CC6.1, CC6.6, CC6.7
pkg/http-server/webhook-scan.go	80	Hard-coded credentials or secrets	HIGH	Security	CC6.1, CC6.6, CC6.7
pkg/http-server/webhook-scan.go	88	Hard-coded credentials or secrets	HIGH	Security	CC6.1, CC6.6, CC6.7
pkg/http-server/webhook-scan.go	140	Hard-coded credentials or secrets	HIGH	Security	CC6.1, CC6.6, CC6.7
pkg/http-server/webhook-scan.go	201	Hard-coded credentials or secrets	HIGH	Security	CC6.1, CC6.6, CC6.7
pkg/http-server/assets/bootstrapper.go	6	Hard-coded credentials or secrets	HIGH	Security	CC6.1, CC6.6, CC6.7
pkg/http-server/testdata/testContainer.go	14	AWS provider without version constraint	MEDIUM	Security	CC1.1, CC1.2, CC1.3, CC1.4, CC2.1
pkg/http-server/testdata/testContainer.go	18	Security group with unrestricted ingress	HIGH	Security	CC6.6, CC6.7
pkg/http-server/testdata/testContainer.go	26	Security group with unrestricted ingress	HIGH	Security	CC6.6, CC6.7
.../v1/testdata/templates/24/s3/dump.go	14	Bucket with unrestricted access	HIGH	Security	CC6.1, CC6.3
.../v1/testdata/templates/s3/dump.go	23	Bucket with public read access	HIGH	Confidentiality	C1.1
...testdata/templates/24/deployApp.go	14	Bucket with unrestricted access	HIGH	Security	CC6.1, CC6.3
...testdata/templates/23/deployTemplate.go	23	Bucket with public read access	HIGH	Confidentiality	C1.1

...ac-providers/docker_101/parse_secrets	Tested credentials or secrets	HIGH	Security	CC6.1, CC6.6, CC6.7
...bernetes/v1/testdata_188s_te_PopulatingHostPath volume	Populating hostPath volume	HIGH	Security	CC6.1, CC6.8
...bernetes/v1/testdata_188s_te_PopulatingHostPath volume	Populating hostPath volume	HIGH	Security	CC6.1, CC6.8
...data/file-test-data/test_155_bad_Condainer	Container allowed to escalate privileges	HIGH	Security	CC1.1, CC1.2, CC1.3, CC1.4, CC2
...data/file-test-data/test_155_bad_Condainer	Container allowed to escalate privileges	HIGH	Security	CC1.1, CC1.2, CC1.3, CC1.4, CC2
.../file-test-data/test_b15_metalContainer	Container allowed to escalate privileges	HIGH	Security	CC1.1, CC1.2, CC1.3, CC1.4, CC2
.../file-test-data/test_b26_metalContainer	Container allowed to escalate privileges	HIGH	Security	CC1.1, CC1.2, CC1.3, CC1.4, CC2
...-test-data/test_bad_15etadaContainer	Container allowed to escalate privileges	HIGH	Security	CC1.1, CC1.2, CC1.3, CC1.4, CC2
...-test-data/test_bad_20etadaContainer	Container allowed to escalate privileges	HIGH	Security	CC1.1, CC1.2, CC1.3, CC1.4, CC2
...file-test-data/test_b46_nameContainer	Container allowed to escalate privileges	HIGH	Security	CC1.1, CC1.2, CC1.3, CC1.4, CC2
...file-test-data/test_b48_nameContainer	Container allowed to escalate privileges	HIGH	Security	CC1.1, CC1.2, CC1.3, CC1.4, CC2
...tdata/file-test-data/t44t_no_Condainer	Container allowed to escalate privileges	HIGH	Security	CC1.1, CC1.2, CC1.3, CC1.4, CC2
...tdata/file-test-data/t82t_no_Condainer	Container allowed to escalate privileges	HIGH	Security	CC1.1, CC1.2, CC1.3, CC1.4, CC2
...a/file-test-data/test_116_metalContainer	Container allowed to escalate privileges	HIGH	Security	CC1.1, CC1.2, CC1.3, CC1.4, CC2
...a/file-test-data/test_320_metalContainer	Container allowed to escalate privileges	HIGH	Security	CC1.1, CC1.2, CC1.3, CC1.4, CC2
...e-test-data/test_no_14etadaContainer	Container allowed to escalate privileges	HIGH	Security	CC1.1, CC1.2, CC1.3, CC1.4, CC2
...e-test-data/test_no_32etadaContainer	Container allowed to escalate privileges	HIGH	Security	CC1.1, CC1.2, CC1.3, CC1.4, CC2
...testdata/file-test-data_157_test_podContainer	Container allowed to escalate privileges	HIGH	Security	CC1.1, CC1.2, CC1.3, CC1.4, CC2
...testdata/file-test-data_237_test_podContainer	Container allowed to escalate privileges	HIGH	Security	CC1.1, CC1.2, CC1.3, CC1.4, CC2
...le-test-data/test_pod19skip_OContainer	Container allowed to escalate privileges	HIGH	Security	CC1.1, CC1.2, CC1.3, CC1.4, CC2
...le-test-data/test_pod43skip_OContainer	Container allowed to escalate privileges	HIGH	Security	CC1.1, CC1.2, CC1.3, CC1.4, CC2
...testdata/yaml-exten55on2/testContainer	Container allowed to escalate privileges	HIGH	Security	CC1.1, CC1.2, CC1.3, CC1.4, CC2
...testdata/yaml-exten33on2/testContainer	Container allowed to escalate privileges	HIGH	Security	CC1.1, CC1.2, CC1.3, CC1.4, CC2
...with-multiple-documents/testContainer	Container allowed to escalate privileges	HIGH	Security	CC1.1, CC1.2, CC1.3, CC1.4, CC2
...with-multiple-documents/testContainer	Container allowed to escalate privileges	HIGH	Security	CC1.1, CC1.2, CC1.3, CC1.4, CC2

.../erroneous-deployment/18	Container may be allowed to escalate privileges	HIGH	Security	CC1.1, CC1.2, CC1.3, CC1.4, CC2
.../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/31	Hard-coded credentials or secrets	HIGH	Security	CC6.1, CC6.6, CC6.7
.../raform/commons/ct287	Use of eval()	HIGH	Security	CC5.1, CC6.8, CC7.2
.../erraform/commons/52	Hard-coded credentials or secrets	HIGH	Security	CC6.1, CC6.6, CC6.7
.../viders/terraform/conditions/test/31	Hard-coded credentials or secrets	HIGH	Security	CC6.1, CC6.6, CC6.7
...v12/testdata/deep-r5modules/53	AWS provider without version constraint	MEDIUM	Security	CC1.1, CC1.2, CC1.3, CC1.4, CC2
...-module-source/invalid_source/54	AWS provider without version constraint	MEDIUM	Security	CC1.1, CC1.2, CC1.3, CC1.4, CC2
...estdata/invalid-moduleconfig/54	AWS provider without version constraint	MEDIUM	Security	CC1.1, CC1.2, CC1.3, CC1.4, CC2
...rm/v12/testdata/moduleconfig/54	AWS provider without version constraint	MEDIUM	Security	CC1.1, CC1.2, CC1.3, CC1.4, CC2
...v12/testdata/moduledonfigs/55	Security group with unrestricted ingress	HIGH	Security	CC6.6, CC6.7
...orm/v12/testdata/tfcbnfigs/c49	AWS provider without version constraint	MEDIUM	Security	CC1.1, CC1.2, CC1.3, CC1.4, CC2
...orm/v12/testdata/tfcnfigs/c49	Security group with unrestricted ingress	HIGH	Security	CC6.6, CC6.7
...orm/v12/testdata/tfcnfigs/c55	Security group with unrestricted ingress	HIGH	Security	CC6.6, CC6.7
...12/testdata/tfjson/moduleconfig/56	AWS provider with unrestricted access	HIGH	Security	CC6.1, CC6.3
...v14/testdata/deep-r5modules/57	AWS provider without version constraint	MEDIUM	Security	CC1.1, CC1.2, CC1.3, CC1.4, CC2
...-module-source/invalid_source/58	AWS provider without version constraint	MEDIUM	Security	CC1.1, CC1.2, CC1.3, CC1.4, CC2
...estdata/invalid-moduleconfig/58	AWS provider without version constraint	MEDIUM	Security	CC1.1, CC1.2, CC1.3, CC1.4, CC2
...rm/v14/testdata/moduleconfig/58	AWS provider without version constraint	MEDIUM	Security	CC1.1, CC1.2, CC1.3, CC1.4, CC2
...v14/testdata/moduledonfigs/59	Security group with unrestricted ingress	HIGH	Security	CC6.6, CC6.7
...orm/v14/testdata/tfcbnfigs/c49	AWS provider without version constraint	MEDIUM	Security	CC1.1, CC1.2, CC1.3, CC1.4, CC2
...orm/v14/testdata/tfcnfigs/c49	Security group with unrestricted ingress	HIGH	Security	CC6.6, CC6.7
...orm/v14/testdata/tfcnfigs/c55	Security group with unrestricted ingress	HIGH	Security	CC6.6, CC6.7
...14/testdata/tfjson/moduleconfig/59	AWS provider with unrestricted access	HIGH	Security	CC6.1, CC6.3

...v15/testdata/deep-r6odules	AMSpaintder without version constraint	MEDIUM	Security	CC1.1, CC1.2, CC1.3, CC1.4, CC2
...-module-source/invalid_sou	AMSpaintder without version constraint	MEDIUM	Security	CC1.1, CC1.2, CC1.3, CC1.4, CC2
...estdata/invalid-moduleconfig	AMSpaintder without version constraint	MEDIUM	Security	CC1.1, CC1.2, CC1.3, CC1.4, CC2
...rm/v15/testdata/modulecon	AMSpaintder without version constraint	MEDIUM	Security	CC1.1, CC1.2, CC1.3, CC1.4, CC2
...v15/testdata/modulenfigs	Security group with unrestricted ingress	HIGH	Security	CC6.6, CC6.7
...orm/v15/testdata/tfcbnfigs	AMSpaintder without version constraint	MEDIUM	Security	CC1.1, CC1.2, CC1.3, CC1.4, CC2
...orm/v15/testdata/tfcnfigs/c	Security group with unrestricted ingress	HIGH	Security	CC6.6, CC6.7
...orm/v15/testdata/tfcnfigs/c	Security group with unrestricted ingress	HIGH	Security	CC6.6, CC6.7
...15/testdata/tfjson/m	AMSpaintder 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/v	Hard-coded credentials or secrets	HIGH	Security	CC6.1, CC6.6, CC6.7
...mission-webhook/v	Hard-coded credentials or secrets	HIGH	Security	CC6.1, CC6.6, CC6.7
...mission-webhook/v	Hard-coded credentials or secrets	HIGH	Security	CC6.1, CC6.6, CC6.7
...on-webhook/validate	Hard-coded credentials or secrets	HIGH	Security	CC6.1, CC6.6, CC6.7
pkg/k8s/dblogs/webh	7ak-scan trigger exec function	HIGH	Security	CC6.1, CC6.8, CC7.2
pkg/k8s/dblogs/webh	20k-scan trigger exec function	HIGH	Security	CC6.1, CC6.8, CC7.2
...oviders/arm/config/2	Hard-coded credentials or secrets	HIGH	Security	CC6.1, CC6.6, CC6.7
...oviders/arm/config/3	Hard-coded credentials or secrets	HIGH	Security	CC6.1, CC6.6, CC6.7
...ders/arm/config/kub	83netes Hard-coded credentials or secrets	HIGH	Security	CC6.1, CC6.6, CC6.7
...-providers/arm/config/	77mssql Hard-coded credentials or secrets	HIGH	Security	CC6.1, CC6.6, CC6.7
...-providers/arm/config/	83mssql Hard-coded credentials or secrets	HIGH	Security	CC6.1, CC6.6, CC6.7
...iac-providers/arm/f	83actions Hard-coded credentials or secrets	HIGH	Security	CC6.1, CC6.6, CC6.7
...providers/arm/fun	83s/pars Hard-coded credentials or secrets	HIGH	Security	CC6.1, CC6.6, CC6.7
...roviders/arm/fun	83s/resolutio Hard-coded credentials or secrets	HIGH	Security	CC6.1, CC6.6, CC6.7
...c-providers/arm/fun	88ons/t Hard-coded credentials or secrets	HIGH	Security	CC6.1, CC6.6, CC6.7

...-providers/arm/functions/validate	Hard-coded credentials or secrets	HIGH	Security	CC6.1, CC6.6, CC6.7
...iac-providers/cft/functions/store	Blind-coded credentials or secrets	HIGH	Security	CC6.1, CC6.6, CC6.7
...roviders/cft/function/uri	Hard-coded credentials or secrets	HIGH	Security	CC6.1, CC6.6, CC6.7
...pper/iac-providers/attr/store/type	Hard-coded credentials or secrets	HIGH	Security	CC6.1, CC6.6, CC6.7
...pper/iac-providers/attr/store/type	Hard-coded credentials or secrets	HIGH	Security	CC6.1, CC6.6, CC6.7
...pper/iac-providers/attr/store/type	Hard-coded credentials or secrets	HIGH	Security	CC6.1, CC6.6, CC6.7
...pper/iac-providers/attr/store/type	Hard-coded credentials or secrets	HIGH	Security	CC6.1, CC6.6, CC6.7
...pper/iac-providers/attr/store/type	Hard-coded credentials or secrets	HIGH	Security	CC6.1, CC6.6, CC6.7
...notifications/webhook	Hard-coded credentials or secrets	HIGH	Security	CC6.1, CC6.6, CC6.7
...nection/lambdaNotEncrypted	Hard-coded credentials or secrets	HIGH	Security	CC6.1, CC6.6, CC6.7
...s/kubernetes_pod/app/armd	Hard-coded credentials or secrets	HIGH	Security	CC6.1, CC6.6, CC6.7
pkg/utils/skip_rules_t	S3 bucket with public read access	HIGH	Confidentiality	C1.1
pkg/utils/http/request	Hard-coded credentials or secrets	HIGH	Security	CC6.1, CC6.6, CC6.7
pkg/vulnerability/acr	Possible hard-coded password	HIGH	Security	CC6.1, CC6.7
pkg/vulnerability/acr	Possible hard-coded password	HIGH	Security	CC6.1, CC6.7
pkg/vulnerability/gcr	Possible hard-coded password	HIGH	Security	CC6.1, CC6.7
pkg/vulnerability/harb	Hard-coded credentials or secrets	HIGH	Security	CC6.1, CC6.6, CC6.7
pkg/vulnerability/harb	Hard-coded credentials or secrets	HIGH	Security	CC6.1, CC6.6, CC6.7
pkg/vulnerability/harb	Hard-coded credentials or secrets	HIGH	Security	CC6.1, CC6.6, CC6.7
test/e2e/scan/scan_t	Hard-coded credentials or secrets	HIGH	Security	CC6.1, CC6.6, CC6.7
...ata/iac/aws/aws_amplify_provider	AWS provider without version constraint	MEDIUM	Security	CC1.1, CC1.2, CC1.3, CC1.4, CC2
...aws/aws_db_instance_provider	AWS provider without version constraint	MEDIUM	Security	CC1.1, CC1.2, CC1.3, CC1.4, CC2
...aws/aws_db_instance_provider	Possible hard-coded password	HIGH	Security	CC6.1, CC6.7
...aws/aws_db_instance_provider	Possible hard-coded password	HIGH	Security	CC6.1, CC6.7
...aws/aws_db_instance_provider	Possible hard-coded password	HIGH	Security	CC6.1, CC6.7
...aws/aws_db_instance_provider	Possible hard-coded password	HIGH	Security	CC6.1, CC6.7

...aws/aws_db_instance	78	Possible hard-coded password	HIGH	Security	CC6.1, CC6.7
...aws/aws_db_instance	86	Possible hard-coded password	HIGH	Security	CC6.1, CC6.7
...aws/aws_db_instance	101	Possible hard-coded password	HIGH	Security	CC6.1, CC6.7
...aws/aws_db_instance	120	Possible hard-coded password	HIGH	Security	CC6.1, CC6.7
...aws/aws_db_instance	149	Possible hard-coded password	HIGH	Security	CC6.1, CC6.7
...aws/aws_db_instance	189	Possible with encryption disabled	HIGH	Confidentiality	C1.1
...aws/aws_db_instance	192	Possible with backups disabled	MEDIUM	Availability	A1.2, A1.3
...aws/aws_db_instance	196	Possible with backups disabled	MEDIUM	Availability	A1.2, A1.3
...aws/aws_db_instance	199	Possible with backups disabled	MEDIUM	Availability	A1.2, A1.3
...aws/aws_db_instance	225	Possible with backups disabled	MEDIUM	Availability	A1.2, A1.3
...aws/aws_db_instance	244	Possible with backups disabled	MEDIUM	Availability	A1.2, A1.3
...ng/max_severity_set	12	Possible hard-coded password	HIGH	Security	CC6.1, CC6.7
...x_severity_set_none	12	Possible hard-coded password	HIGH	Security	CC6.1, CC6.7
...x_both_severity_set	18	Possible hard-coded password	HIGH	Security	CC6.1, CC6.7
...ng/min_severity_set	12	Possible hard-coded password	HIGH	Security	CC6.1, CC6.7
...rity_with_skip_rule/terraform	13	Possible hard-coded password	HIGH	Security	CC6.1, CC6.7
...c/resource_skipping/terraform	14	Provider without version constraint	MEDIUM	Security	CC1.1, CC1.2, CC1.3, CC1.4, CC2.1
...c/resource_skipping	21	Possible hard-coded password	HIGH	Security	CC6.1, CC6.7
...c/resource_skipping	34	Possible hard-coded password	HIGH	Security	CC6.1, CC6.7
...c/resource_skipping	51	Possible hard-coded password	HIGH	Security	CC6.1, CC6.7
...c/resource_skipping	67	Possible hard-coded password	HIGH	Security	CC6.1, CC6.7
...c/resource_skipping	83	Possible hard-coded password	HIGH	Security	CC6.1, CC6.7
...c/resource_skipping	94	Possible hard-coded password	HIGH	Security	CC6.1, CC6.7
...c/resource_skipping	104	Possible hard-coded password	HIGH	Security	CC6.1, CC6.7
...c/resource_skipping	123	Possible hard-coded password	HIGH	Security	CC6.1, CC6.7

...c/resource_skipping/151	Possible hard-coded password	HIGH	Security	CC6.1, CC6.7
...c/resource_skipping/92	Terraform Resource with encryption disabled	HIGH	Confidentiality	C1.1
...c/resource_skipping/32	Terraform Resource with backups disabled	MEDIUM	Availability	A1.2, A1.3
...c/resource_skipping/16	Terraform Resource with backups disabled	MEDIUM	Availability	A1.2, A1.3
...c/resource_skipping/109	Terraform Resource with backups disabled	MEDIUM	Availability	A1.2, A1.3
...c/resource_skipping/128	Terraform Resource with backups disabled	MEDIUM	Availability	A1.2, A1.3
...c/resource_skipping/167	Terraform Resource with backups disabled	MEDIUM	Availability	A1.2, A1.3
...cursive/subFolder1/subFolder2	AVS provider without version constraint	MEDIUM	Security	CC1.1, CC1.2, CC1.3, CC1.4, CC2
...ingwebhook/validating/149_web	Hard-coded credentials or secrets	HIGH	Security	CC6.1, CC6.6, CC6.7
...ingwebhook/validating/168_web	Hard-coded credentials or secrets	HIGH	Security	CC6.1, CC6.6, CC6.7
...ingwebhook/validating/76_web	Hard-coded credentials or secrets	HIGH	Security	CC6.1, CC6.6, CC6.7
...e/vulnerability/vuln42	Hard-coded credentials or secrets	HIGH	Security	CC6.1, CC6.6, CC6.7
...e/vulnerability/vuln44	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	119a2aaa-1870-4a0d-8136-04ea21194ca4
Scan Type	soc2
Region	Global
Timestamp	2025-05-03 12:40:01
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.