DataGuardian Pro
Enterprise Privacy Compliance Platform

SOC2 Compliance Report

Generated on:	May 03, 2025 18:11	**Scan ID:**	SOC-20250503-7174fb

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 18:11:03**. The scan identified a total of **161** compliance issues with **129** high-risk items. The overall compliance score is **1/100**. **Technologies Detected:** terraform, kubernetes, javascript, ansible, docker, cloudformation, 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	https://github.com/vishaal314/terrascan
Branch	master
Date & Time	2025-05-03 18:11:03
Technologies	terraform, kubernetes, javascript, ansible, docker, cloudformation, 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

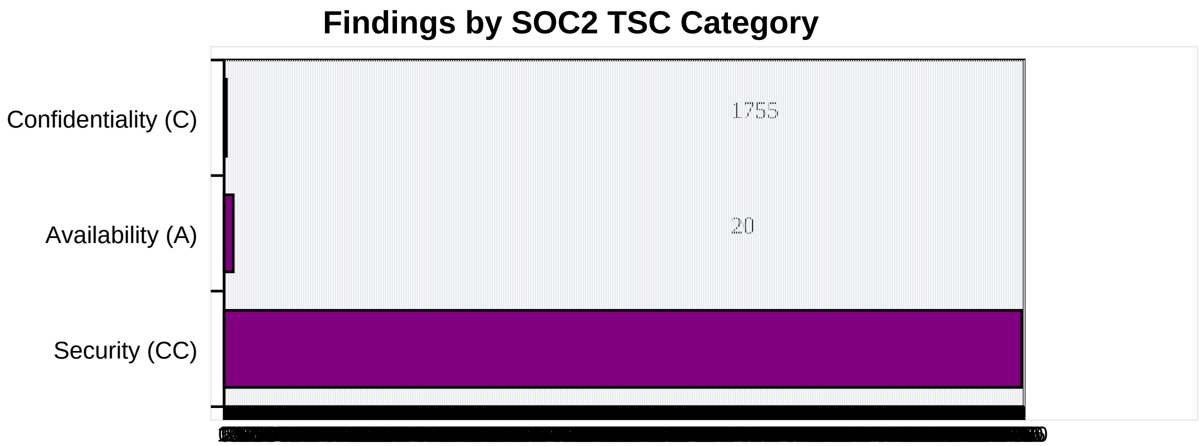
Detailed Findings

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 18:11:03
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/deployment.yaml	32	Container not running as non-root user	MEDIUM	Security	CC1.1, CC1.2, CC1.3, C
pkg/cli/testdata/run-test/main.tf	2	AWS provider without version constraint	MEDIUM	Security	CC1.1, CC1.2, CC1.3, C
pkg/cli/testdata/run-test/test_pod.yaml	10	Container allowed to escalate privileges	HIGH	Security	CC1.1, CC1.2, CC1.3, C
pkg/cli/testdata/run-test/test_pod.yaml	43	Container allowed to escalate privileges	HIGH	Security	CC1.1, CC1.2, CC1.3, C
pkg/cli/testdata/run-test/web.tf	14	Security group with unrestricted ingress	HIGH	Security	CC6.6, CC6.7
pkg/cli/testdata/run-test/web.tf	23	Security group with unrestricted ingress	HIGH	Security	CC6.6, CC6.7
pkg/downloader/module-download_test.go	571	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_test.go	395	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	96	Hard-coded credentials or secrets	HIGH	Security	CC6.1, CC6.6, CC6.7
pkg/http-server/webhook-scan-logs.go	81	Hard-coded credentials or secrets	HIGH	Security	CC6.1, CC6.6, CC6.7
pkg/http-server/webhook-scan.go	38	Hard-coded credentials or secrets	HIGH	Security	CC6.1, CC6.6, CC6.7
pkg/http-server/webhook-scan.go	41	Hard-coded credentials or secrets	HIGH	Security	CC6.1, CC6.6, CC6.7
pkg/http-server/webhook-scan_test.go	24	Hard-coded credentials or secrets	HIGH	Security	CC6.1, CC6.6, CC6.7
pkg/http-server/assets/bootstrap.min.css	6	Hard-coded credentials or secrets	HIGH	Security	CC6.1, CC6.6, CC6.7
pkg/http-server/testdata/testconfig.tf	1	AWS provider without version constraint	MEDIUM	Security	CC1.1, CC1.2, CC1.3, C
pkg/http-server/testdata/testconfig.tf	50	Security group with unrestricted ingress	HIGH	Security	CC6.6, CC6.7
pkg/http-server/testdata/testconfig.tf	56	Security group with unrestricted ingress	HIGH	Security	CC6.6, CC6.7
.../v1/testdata/templates/s3/deploy.json	243	IAM policy with unrestricted access	HIGH	Security	CC6.1, CC6.3
.../v1/testdata/templates/s3/deploy.json	7	S3 bucket with public read access	HIGH	Confidentiality	C1.1

...testdata/templates/s3/deploy.template	24	IAM policy with unrestricted access	HIGH	Security	CC6.1, CC6.3
...testdata/templates/s3/deploy.template	7	S3 bucket with public read access	HIGH	Confidentiality	C1.1
...ac-providers/docker/v1/parser_test.go	40	Hard-coded credentials or secrets	HIGH	Security	CC6.1, CC6.6, CC6.7
...bernetes/v1/testdata/k8s_templates.go	164	Pod using hostPath volume	HIGH	Security	CC6.1, CC6.8
...bernetes/v1/testdata/k8s_templates.go	187	Pod using hostPath volume	HIGH	Security	CC6.1, CC6.8
...data/file-test-data/test_bad_kind.yml	15	Container allowed to escalate privileges	HIGH	Security	CC1.1, CC1.2, CC1.3, C
...data/file-test-data/test_bad_kind.yml	33	Container allowed to escalate privileges	HIGH	Security	CC1.1, CC1.2, CC1.3, C
.../file-test-data/test_bad_metadata.yml	15	Container allowed to escalate privileges	HIGH	Security	CC1.1, CC1.2, CC1.3, C
.../file-test-data/test_bad_metadata.yml	28	Container allowed to escalate privileges	HIGH	Security	CC1.1, CC1.2, CC1.3, C
...-test-data/test_bad_metadata_name.yml	15	Container allowed to escalate privileges	HIGH	Security	CC1.1, CC1.2, CC1.3, C
...-test-data/test_bad_metadata_name.yml	29	Container allowed to escalate privileges	HIGH	Security	CC1.1, CC1.2, CC1.3, C
...file-test-data/test_bad_namespace.yml	15	Container allowed to escalate privileges	HIGH	Security	CC1.1, CC1.2, CC1.3, C
...file-test-data/test_bad_namespace.yml	33	Container allowed to escalate privileges	HIGH	Security	CC1.1, CC1.2, CC1.3, C
...tdata/file-test-data/test_no_kind.yml	14	Container allowed to escalate privileges	HIGH	Security	CC1.1, CC1.2, CC1.3, C
...tdata/file-test-data/test_no_kind.yml	32	Container allowed to escalate privileges	HIGH	Security	CC1.1, CC1.2, CC1.3, C
...a/file-test-data/test_no_metadata.yml	14	Container allowed to escalate privileges	HIGH	Security	CC1.1, CC1.2, CC1.3, C
...a/file-test-data/test_no_metadata.yml	32	Container allowed to escalate privileges	HIGH	Security	CC1.1, CC1.2, CC1.3, C
...e-test-data/test_no_metadata_name.yml	14	Container allowed to escalate privileges	HIGH	Security	CC1.1, CC1.2, CC1.3, C
...e-test-data/test_no_metadata_name.yml	32	Container allowed to escalate privileges	HIGH	Security	CC1.1, CC1.2, CC1.3, C
...testdata/file-test-data/test_pod.yml	15	Container allowed to escalate privileges	HIGH	Security	CC1.1, CC1.2, CC1.3, C
...testdata/file-test-data/test_pod.yml	33	Container allowed to escalate privileges	HIGH	Security	CC1.1, CC1.2, CC1.3, C
...le-test-data/test_pod_skip_rules.yaml	19	Container allowed to escalate privileges	HIGH	Security	CC1.1, CC1.2, CC1.3, C
...le-test-data/test_pod_skip_rules.yaml	43	Container allowed to escalate privileges	HIGH	Security	CC1.1, CC1.2, CC1.3, C
...testdata/yaml-extension/test_pod.yml	152	Container allowed to escalate privileges	HIGH	Security	CC1.1, CC1.2, CC1.3, C

...testdata/yaml-extension/test_pod.yaml	332	Container allowed to escalate privileges	HIGH	Security	CC1.1, CC1.2, CC1.3, C
...with-multiple-documents/test_pod.yaml	15	Container allowed to escalate privileges	HIGH	Security	CC1.1, CC1.2, CC1.3, C
...with-multiple-documents/test_pod.yaml	33	Container allowed to escalate privileges	HIGH	Security	CC1.1, CC1.2, CC1.3, C
.../erroneous-deployment/deployment.yaml	16	Container allowed to escalate privileges	HIGH	Security	CC1.1, CC1.2, CC1.3, C
...roviders/output/vulnerability_test.go	28	Hard-coded credentials or secrets	HIGH	Security	CC6.1, CC6.6, CC6.7
...roviders/output/vulnerability_test.go	30	Hard-coded credentials or secrets	HIGH	Security	CC6.1, CC6.6, CC6.7
...roviders/output/vulnerability_test.go	113	Hard-coded credentials or secrets	HIGH	Security	CC6.1, CC6.6, CC6.7
...raform/commons/cty-converters_test.go	287	Use of eval() function	HIGH	Security	CC5.1, CC6.8, CC7.2
...erraform/commons/lookup-references.go	52	Hard-coded credentials or secrets	HIGH	Security	CC6.1, CC6.6, CC6.7
...viders/terraform/commons/test/util.go	31	Hard-coded credentials or secrets	HIGH	Security	CC6.1, CC6.6, CC6.7
...v12/testdata/deep-modules/template.tf	5	AWS provider without version constraint	MEDIUM	Security	CC1.1, CC1.2, CC1.3, C
...-module-source/invalid_source/main.tf	5	AWS provider without version constraint	MEDIUM	Security	CC1.1, CC1.2, CC1.3, C
...estdata/invalid-module-configs/main.tf	1	AWS provider without version constraint	MEDIUM	Security	CC1.1, CC1.2, CC1.3, C
...rm/v12/testdata/module-configs/main.tf	1	AWS provider without version constraint	MEDIUM	Security	CC1.1, CC1.2, CC1.3, C
...v12/testdata/module-configs/security.tf	11	Security group with unrestricted ingress	HIGH	Security	CC6.6, CC6.7
...orm/v12/testdata/tfconfigs/config1.tf	1	AWS provider without version constraint	MEDIUM	Security	CC1.1, CC1.2, CC1.3, C
...orm/v12/testdata/tfconfigs/config1.tf	49	Security group with unrestricted ingress	HIGH	Security	CC6.6, CC6.7
...orm/v12/testdata/tfconfigs/config1.tf	55	Security group with unrestricted ingress	HIGH	Security	CC6.6, CC6.7
...12/testdata/tfjson/module-config.json	591	IAM policy with unrestricted access	HIGH	Security	CC6.1, CC6.3
...v14/testdata/deep-modules/template.tf	5	AWS provider without version constraint	MEDIUM	Security	CC1.1, CC1.2, CC1.3, C
...-module-source/invalid_source/main.tf	5	AWS provider without version constraint	MEDIUM	Security	CC1.1, CC1.2, CC1.3, C
...estdata/invalid-module-configs/main.tf	1	AWS provider without version constraint	MEDIUM	Security	CC1.1, CC1.2, CC1.3, C
...rm/v14/testdata/module-configs/main.tf	1	AWS provider without version constraint	MEDIUM	Security	CC1.1, CC1.2, CC1.3, C
...v14/testdata/module-configs/security.tf	11	Security group with unrestricted ingress	HIGH	Security	CC6.6, CC6.7

...orm/v14/testdata/tfconfigs/config1.tf	1	AWS provider without version constraint	MEDIUM	Security	CC1.1, CC1.2, CC1.3, C
...orm/v14/testdata/tfconfigs/config1.tf	49	Security group with unrestricted ingress	HIGH	Security	CC6.6, CC6.7
...orm/v14/testdata/tfconfigs/config1.tf	55	Security group with unrestricted ingress	HIGH	Security	CC6.6, CC6.7
...14/testdata/tfjson/moduleconfigs.json	591	IAM policy with unrestricted access	HIGH	Security	CC6.1, CC6.3
...v15/testdata/deep-modules/template.tf	5	AWS provider without version constraint	MEDIUM	Security	CC1.1, CC1.2, CC1.3, C
...-module-source/invalid_source/main.tf	5	AWS provider without version constraint	MEDIUM	Security	CC1.1, CC1.2, CC1.3, C
...estdata/invalid-moduleconfigs/main.tf	1	AWS provider without version constraint	MEDIUM	Security	CC1.1, CC1.2, CC1.3, C
...rm/v15/testdata/moduleconfigs/main.tf	1	AWS provider without version constraint	MEDIUM	Security	CC1.1, CC1.2, CC1.3, C
...v15/testdata/moduleconfigs/security.tf	11	Security group with unrestricted ingress	HIGH	Security	CC6.6, CC6.7
...orm/v15/testdata/tfconfigs/config1.tf	1	AWS provider without version constraint	MEDIUM	Security	CC1.1, CC1.2, CC1.3, C
...orm/v15/testdata/tfconfigs/config1.tf	49	Security group with unrestricted ingress	HIGH	Security	CC6.6, CC6.7
...orm/v15/testdata/tfconfigs/config1.tf	55	Security group with unrestricted ingress	HIGH	Security	CC6.6, CC6.7
...15/testdata/tfjson/moduleconfigs.json	591	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/validating-webhook.go	67	Hard-coded credentials or secrets	HIGH	Security	CC6.1, CC6.6, CC6.7
...mission-webhook/validating-webhook.go	73	Hard-coded credentials or secrets	HIGH	Security	CC6.1, CC6.6, CC6.7
...mission-webhook/validating-webhook.go	92	Hard-coded credentials or secrets	HIGH	Security	CC6.1, CC6.6, CC6.7
...on-webhook/validating-webhook_test.go	67	Hard-coded credentials or secrets	HIGH	Security	CC6.1, CC6.6, CC6.7
pkg/k8s/dblogs/webhook-scan-logger.go	72	Use of exec function	HIGH	Security	CC6.1, CC6.8, CC7.2
pkg/k8s/dblogs/webhook-scan-logger.go	206	Use of exec function	HIGH	Security	CC6.1, CC6.8, CC7.2
...oviders/arm/config/auditing-policy.go	26	Hard-coded credentials or secrets	HIGH	Security	CC6.1, CC6.6, CC6.7
...oviders/arm/config/auditing-policy.go	33	Hard-coded credentials or secrets	HIGH	Security	CC6.1, CC6.6, CC6.7
...ders/arm/config/kubernetes-cluster.go	83	Hard-coded credentials or secrets	HIGH	Security	CC6.1, CC6.6, CC6.7
...-providers/arm/config/mssql-server.go	27	Hard-coded credentials or secrets	HIGH	Security	CC6.1, CC6.6, CC6.7

...-providers/arm/config/mssql-server.go	33	Hard-coded credentials or secrets	HIGH	Security	CC6.1, CC6.6, CC6.7
...iac-providers/arm/functions/concat.go	34	Hard-coded credentials or secrets	HIGH	Security	CC6.1, CC6.6, CC6.7
...providers/arm/functions/parameters.go	38	Hard-coded credentials or secrets	HIGH	Security	CC6.1, CC6.6, CC6.7
...roviders/arm/functions/resource-id.go	38	Hard-coded credentials or secrets	HIGH	Security	CC6.1, CC6.6, CC6.7
...c-providers/arm/functions/to-lower.go	38	Hard-coded credentials or secrets	HIGH	Security	CC6.1, CC6.6, CC6.7
...-providers/arm/functions/variables.go	38	Hard-coded credentials or secrets	HIGH	Security	CC6.1, CC6.6, CC6.7
...iac-providers/cft/functions/s3-uri.go	75	Hard-coded credentials or secrets	HIGH	Security	CC6.1, CC6.6, CC6.7
...roviders/cft/functions/s3-uri_test.go	23	Hard-coded credentials or secrets	HIGH	Security	CC6.1, CC6.6, CC6.7
...pper/iac-providers/cft/store/types.go	41	Hard-coded credentials or secrets	HIGH	Security	CC6.1, CC6.6, CC6.7
...pper/iac-providers/cft/store/types.go	61	Hard-coded credentials or secrets	HIGH	Security	CC6.1, CC6.6, CC6.7
...pper/iac-providers/cft/store/types.go	64	Hard-coded credentials or secrets	HIGH	Security	CC6.1, CC6.6, CC6.7
...pper/iac-providers/cft/store/types.go	80	Hard-coded credentials or secrets	HIGH	Security	CC6.1, CC6.6, CC6.7
...notifications/webhook/webhook_test.go	23	Hard-coded credentials or secrets	HIGH	Security	CC6.1, CC6.6, CC6.7
...nction/lambdaNotEncryptedWithKms.rego	10	Hard-coded credentials or secrets	HIGH	Security	CC6.1, CC6.6, CC6.7
...s/kubernetes_pod/appArmorProfile.rego	106	Hard-coded credentials or secrets	HIGH	Security	CC6.1, CC6.6, CC6.7
pkg/utils/skip_rules_test.go	123	S3 bucket with public read access	HIGH	Confidentiality	C1.1
pkg/utils/http/request.go	40	Hard-coded credentials or secrets	HIGH	Security	CC6.1, CC6.6, CC6.7
pkg/vulnerability/acr.go	37	Possible hard-coded password	HIGH	Security	CC6.1, CC6.7
pkg/vulnerability/acr.go	208	Possible hard-coded password	HIGH	Security	CC6.1, CC6.7
pkg/vulnerability/gcr.go	251	Possible hard-coded password	HIGH	Security	CC6.1, CC6.7
pkg/vulnerability/harbor.go	35	Hard-coded credentials or secrets	HIGH	Security	CC6.1, CC6.6, CC6.7
pkg/vulnerability/harbor.go	74	Hard-coded credentials or secrets	HIGH	Security	CC6.1, CC6.6, CC6.7
pkg/vulnerability/harbor_test.go	338	Hard-coded credentials or secrets	HIGH	Security	CC6.1, CC6.6, CC6.7
test/e2e/scan/scan_test.go	317	Hard-coded credentials or secrets	HIGH	Security	CC6.1, CC6.6, CC6.7

...ata/iac/aws/aws_ami_violation/main.tf	1	AWS provider without version constraint	MEDIUM	Security	CC1.1, CC1.2, CC1.3, C
...aws/aws_db_instance_violation/main.tf	1	AWS provider without version constraint	MEDIUM	Security	CC1.1, CC1.2, CC1.3, C
...aws/aws_db_instance_violation/main.tf	21	Possible hard-coded password	HIGH	Security	CC6.1, CC6.7
...aws/aws_db_instance_violation/main.tf	34	Possible hard-coded password	HIGH	Security	CC6.1, CC6.7
...aws/aws_db_instance_violation/main.tf	51	Possible hard-coded password	HIGH	Security	CC6.1, CC6.7
...aws/aws_db_instance_violation/main.tf	65	Possible hard-coded password	HIGH	Security	CC6.1, CC6.7
...aws/aws_db_instance_violation/main.tf	78	Possible hard-coded password	HIGH	Security	CC6.1, CC6.7
...aws/aws_db_instance_violation/main.tf	91	Possible hard-coded password	HIGH	Security	CC6.1, CC6.7
...aws/aws_db_instance_violation/main.tf	111	Possible hard-coded password	HIGH	Security	CC6.1, CC6.7
...aws/aws_db_instance_violation/main.tf	130	Possible hard-coded password	HIGH	Security	CC6.1, CC6.7
...aws/aws_db_instance_violation/main.tf	149	Possible hard-coded password	HIGH	Security	CC6.1, CC6.7
...aws/aws_db_instance_violation/main.tf	89	Resource with encryption disabled	HIGH	Confidentiality	C1.1
...aws/aws_db_instance_violation/main.tf	32	Resource with backups disabled	MEDIUM	Availability	A1.2, A1.3
...aws/aws_db_instance_violation/main.tf	46	Resource with backups disabled	MEDIUM	Availability	A1.2, A1.3
...aws/aws_db_instance_violation/main.tf	106	Resource with backups disabled	MEDIUM	Availability	A1.2, A1.3
...aws/aws_db_instance_violation/main.tf	125	Resource with backups disabled	MEDIUM	Availability	A1.2, A1.3
...aws/aws_db_instance_violation/main.tf	144	Resource with backups disabled	MEDIUM	Availability	A1.2, A1.3
...ng/max_severity_set/terraform/main.tf	12	Possible hard-coded password	HIGH	Security	CC6.1, CC6.7
...x_severity_set_none/terraform/main.tf	12	Possible hard-coded password	HIGH	Security	CC6.1, CC6.7
...x_both_severity_set/terraform/main.tf	13	Possible hard-coded password	HIGH	Security	CC6.1, CC6.7
...ng/min_severity_set/terraform/main.tf	12	Possible hard-coded password	HIGH	Security	CC6.1, CC6.7
...rity_with_skip_rule/terraform/main.tf	13	Possible hard-coded password	HIGH	Security	CC6.1, CC6.7
...c/resource_skipping/terraform/main.tf	1	AWS provider without version constraint	MEDIUM	Security	CC1.1, CC1.2, CC1.3, C
...c/resource_skipping/terraform/main.tf	21	Possible hard-coded password	HIGH	Security	CC6.1, CC6.7

...c/resource_skipping/terraform/main.tf	34	Possible hard-coded password	HIGH	Security	CC6.1, CC6.7
...c/resource_skipping/terraform/main.tf	51	Possible hard-coded password	HIGH	Security	CC6.1, CC6.7
...c/resource_skipping/terraform/main.tf	67	Possible hard-coded password	HIGH	Security	CC6.1, CC6.7
...c/resource_skipping/terraform/main.tf	81	Possible hard-coded password	HIGH	Security	CC6.1, CC6.7
...c/resource_skipping/terraform/main.tf	94	Possible hard-coded password	HIGH	Security	CC6.1, CC6.7
...c/resource_skipping/terraform/main.tf	114	Possible hard-coded password	HIGH	Security	CC6.1, CC6.7
...c/resource_skipping/terraform/main.tf	133	Possible hard-coded password	HIGH	Security	CC6.1, CC6.7
...c/resource_skipping/terraform/main.tf	152	Possible hard-coded password	HIGH	Security	CC6.1, CC6.7
...c/resource_skipping/terraform/main.tf	92	Resource with encryption disabled	HIGH	Confidentiality	C1.1
...c/resource_skipping/terraform/main.tf	32	Resource with backups disabled	MEDIUM	Availability	A1.2, A1.3
...c/resource_skipping/terraform/main.tf	46	Resource with backups disabled	MEDIUM	Availability	A1.2, A1.3
...c/resource_skipping/terraform/main.tf	109	Resource with backups disabled	MEDIUM	Availability	A1.2, A1.3
...c/resource_skipping/terraform/main.tf	128	Resource with backups disabled	MEDIUM	Availability	A1.2, A1.3
...c/resource_skipping/terraform/main.tf	147	Resource with backups disabled	MEDIUM	Availability	A1.2, A1.3
...cursive/subFolder1/subFolder2/main.tf	1	AWS provider without version constraint	MEDIUM	Security	CC1.1, CC1.2, CC1.3, C
...ingwebhook/validating_webhook_test.go	43	Hard-coded credentials or secrets	HIGH	Security	CC6.1, CC6.6, CC6.7
...ingwebhook/validating_webhook_test.go	88	Hard-coded credentials or secrets	HIGH	Security	CC6.1, CC6.6, CC6.7
...ingwebhook/validatingwebhook_utils.go	76	Hard-coded credentials or secrets	HIGH	Security	CC6.1, CC6.6, CC6.7
...e/vulnerability/vulnerability_test.go	42	Hard-coded credentials or secrets	HIGH	Security	CC6.1, CC6.6, CC6.7
...e/vulnerability/vulnerability_test.go	44	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.

Scan Metadata

Scan ID	7174fb53-4c2d-4187-96a3-de40a1c33086
Scan Type	soc2
Region	Global
Timestamp	2025-05-03 18:11:03
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.