

Generated on: May 03, 2025 12:40

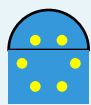
Scan ID: SOC-20250503-119a2a

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

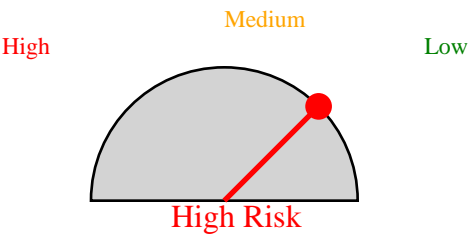
# Risk Assessment



## GDPR Compliance Protection

High risk of potential GDPR fines - immediate action required

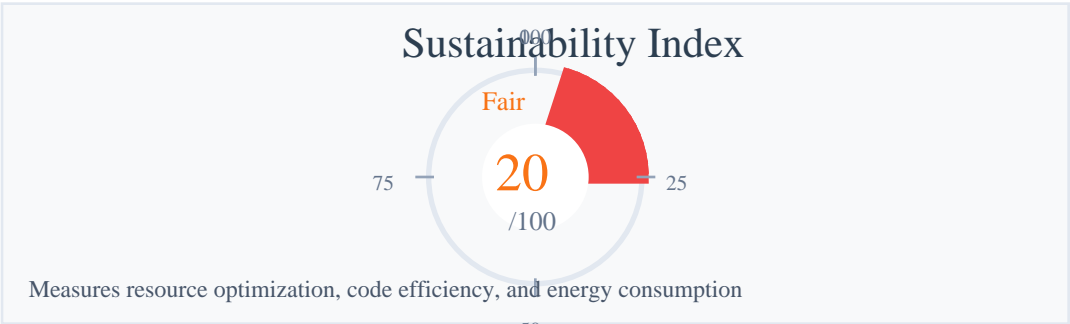
Potential fines up to €20 million or 4% of global revenue



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.



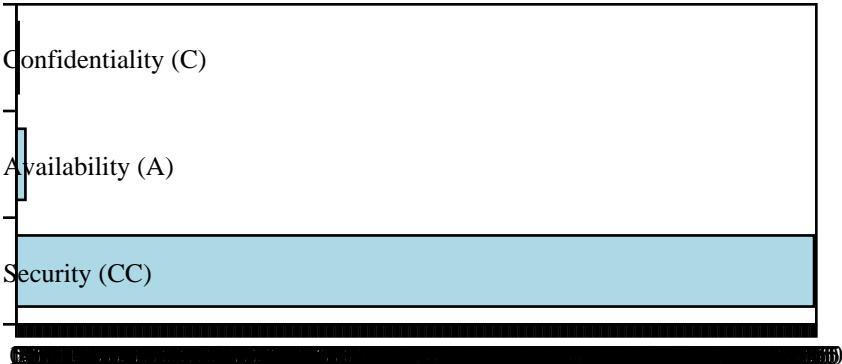
# Detailed Findings

## 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/deploy-container.yaml	32	Container running as non-root user	MEDIUM	Security	CC1.1, CC1.2, CC1.3, CC1.4, CC2.1
pkg/cli/testdata/run-test/23/main.tf	23	AWS provider without version constraint	MEDIUM	Security	CC1.1, CC1.2, CC1.3, CC1.4, CC2.1
pkg/cli/testdata/run-test/19/test_container.yaml	19	Container allowed to escalate privileges	HIGH	Security	CC1.1, CC1.2, CC1.3, CC1.4, CC2.1
pkg/cli/testdata/run-test/17/test_container.yaml	17	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/module/571/download.go	571	Hard-coded credentials or secrets	HIGH	Security	CC6.1, CC6.6, CC6.7
pkg/http-server/file-scan/107/go	107	Hard-coded credentials or secrets	HIGH	Security	CC6.1, CC6.6, CC6.7
pkg/http-server/file-scan/395/test.go	395	Hard-coded credentials or secrets	HIGH	Security	CC6.1, CC6.6, CC6.7
pkg/http-server/start.go	95	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/61/go	61	Hard-coded credentials or secrets	HIGH	Security	CC6.1, CC6.6, CC6.7
pkg/http-server/webhook-scan/68/go	68	Hard-coded credentials or secrets	HIGH	Security	CC6.1, CC6.6, CC6.7
pkg/http-server/webhook-scan/41/go	41	Hard-coded credentials or secrets	HIGH	Security	CC6.1, CC6.6, CC6.7
pkg/http-server/webhook-scan/24/go	24	Hard-coded credentials or secrets	HIGH	Security	CC6.1, CC6.6, CC6.7
pkg/http-server/assets/6/bootstrap.go	6	Hard-coded credentials or secrets	HIGH	Security	CC6.1, CC6.6, CC6.7
pkg/http-server/testdata/test/11/main.tf	11	AWS provider without version constraint	MEDIUM	Security	CC1.1, CC1.2, CC1.3, CC1.4, CC2.1
pkg/http-server/testdata/test/10/test.tf	10	Security group with unrestricted ingress	HIGH	Security	CC6.6, CC6.7
pkg/http-server/testdata/test/16/test.tf	16	Security group with unrestricted ingress	HIGH	Security	CC6.6, CC6.7
.../v1/testdata/templates/24/s3/deploy.yaml	24	AWSPolicy with unrestricted access	HIGH	Security	CC6.1, CC6.3
.../v1/testdata/templates/73/s3/deploy.yaml	73	AWSPolicy with public read access	HIGH	Confidentiality	C1.1
...testdata/templates/23/deploy.yaml	23	AWSPolicy with unrestricted access	HIGH	Security	CC6.1, CC6.3
...testdata/templates/73/deploy.yaml	73	AWSPolicy with public read access	HIGH	Confidentiality	C1.1

...ac-providers/docker/401/parsed	401	HostPath	Container allowed to escalate privileges	HIGH	Security	CC6.1, CC6.6, CC6.7
...bernetes/v1/testdata/44s_tenant	44s	HostPath	Container allowed to escalate privileges	HIGH	Security	CC6.1, CC6.8
...bernetes/v1/testdata/47s_tenant	47s	HostPath	Container allowed to escalate privileges	HIGH	Security	CC6.1, CC6.8
...data/file-test-data/test_55_bad	55	Container	Container allowed to escalate privileges	HIGH	Security	CC1.1, CC1.2, CC1.3, CC1.4, CC2
...data/file-test-data/test_53_bad	53	Container	Container allowed to escalate privileges	HIGH	Security	CC1.1, CC1.2, CC1.3, CC1.4, CC2
.../file-test-data/test_56_bad	56	Container	Container allowed to escalate privileges	HIGH	Security	CC1.1, CC1.2, CC1.3, CC1.4, CC2
.../file-test-data/test_58_bad	58	Container	Container allowed to escalate privileges	HIGH	Security	CC1.1, CC1.2, CC1.3, CC1.4, CC2
...-test-data/test_bad_15_metadata	15	Container	Container allowed to escalate privileges	HIGH	Security	CC1.1, CC1.2, CC1.3, CC1.4, CC2
...-test-data/test_bad_20_metadata	20	Container	Container allowed to escalate privileges	HIGH	Security	CC1.1, CC1.2, CC1.3, CC1.4, CC2
...file-test-data/test_bad_5_name	5	Container	Container allowed to escalate privileges	HIGH	Security	CC1.1, CC1.2, CC1.3, CC1.4, CC2
...file-test-data/test_bad_33_name	33	Container	Container allowed to escalate privileges	HIGH	Security	CC1.1, CC1.2, CC1.3, CC1.4, CC2
...tdata/file-test-data/test_44_no	44	Container	Container allowed to escalate privileges	HIGH	Security	CC1.1, CC1.2, CC1.3, CC1.4, CC2
...tdata/file-test-data/test_42_no	42	Container	Container allowed to escalate privileges	HIGH	Security	CC1.1, CC1.2, CC1.3, CC1.4, CC2
...a/file-test-data/test_16_metadata	16	Container	Container allowed to escalate privileges	HIGH	Security	CC1.1, CC1.2, CC1.3, CC1.4, CC2
...a/file-test-data/test_30_metadata	30	Container	Container allowed to escalate privileges	HIGH	Security	CC1.1, CC1.2, CC1.3, CC1.4, CC2
...e-test-data/test_no_14_metadata	14	Container	Container allowed to escalate privileges	HIGH	Security	CC1.1, CC1.2, CC1.3, CC1.4, CC2
...e-test-data/test_no_32_metadata	32	Container	Container allowed to escalate privileges	HIGH	Security	CC1.1, CC1.2, CC1.3, CC1.4, CC2
...testdata/file-test-data/test_57_pod	57	Container	Container allowed to escalate privileges	HIGH	Security	CC1.1, CC1.2, CC1.3, CC1.4, CC2
...testdata/file-test-data/test_50_pod	50	Container	Container allowed to escalate privileges	HIGH	Security	CC1.1, CC1.2, CC1.3, CC1.4, CC2
...le-test-data/test_pod_19_skip	19	Container	Container allowed to escalate privileges	HIGH	Security	CC1.1, CC1.2, CC1.3, CC1.4, CC2
...le-test-data/test_pod_43_skip	43	Container	Container allowed to escalate privileges	HIGH	Security	CC1.1, CC1.2, CC1.3, CC1.4, CC2
...testdata/yaml-extension2/55	55	Container	Container allowed to escalate privileges	HIGH	Security	CC1.1, CC1.2, CC1.3, CC1.4, CC2
...testdata/yaml-extension2/33	33	Container	Container allowed to escalate privileges	HIGH	Security	CC1.1, CC1.2, CC1.3, CC1.4, CC2
...with-multiple-documents/test_pod_15	15	Container	Container allowed to escalate privileges	HIGH	Security	CC1.1, CC1.2, CC1.3, CC1.4, CC2
...with-multiple-documents/test_pod_33	33	Container	Container allowed to escalate privileges	HIGH	Security	CC1.1, CC1.2, CC1.3, CC1.4, CC2



...v15/testdata/deep-modules/aws-provider	5	AWS provider without version constraint	MEDIUM	Security	CC1.1, CC1.2, CC1.3, CC1.4, CC2.1, CC2.2, CC2.3, CC2.4, CC2.5, CC2.6, CC2.7, CC2.8, CC2.9, CC2.10, CC2.11, CC2.12, CC2.13, CC2.14, CC2.15, CC2.16, CC2.17, CC2.18, CC2.19, CC2.20, CC2.21, CC2.22, CC2.23, CC2.24, CC2.25, CC2.26, CC2.27, CC2.28, CC2.29, CC2.30, CC2.31, CC2.32, CC2.33, CC2.34, CC2.35, CC2.36, CC2.37, CC2.38, CC2.39, CC2.40, CC2.41, CC2.42, CC2.43, CC2.44, CC2.45, CC2.46, CC2.47, CC2.48, CC2.49, CC2.50, CC2.51, CC2.52, CC2.53, CC2.54, CC2.55, CC2.56, CC2.57, CC2.58, CC2.59, CC2.60, CC2.61, CC2.62, CC2.63, CC2.64, CC2.65, CC2.66, CC2.67, CC2.68, CC2.69, CC2.70, CC2.71, CC2.72, CC2.73, CC2.74, CC2.75, CC2.76, CC2.77, CC2.78, CC2.79, CC2.80, CC2.81, CC2.82, CC2.83, CC2.84, CC2.85, CC2.86, CC2.87, CC2.88, CC2.89, CC2.90, CC2.91, CC2.92, CC2.93, CC2.94, CC2.95, CC2.96, CC2.97, CC2.98, CC2.99, CC2.100
...-module-source/invalid-source/aws-provider	5	AWS provider without version constraint	MEDIUM	Security	CC1.1, CC1.2, CC1.3, CC1.4, CC2.1, CC2.2, CC2.3, CC2.4, CC2.5, CC2.6, CC2.7, CC2.8, CC2.9, CC2.10, CC2.11, CC2.12, CC2.13, CC2.14, CC2.15, CC2.16, CC2.17, CC2.18, CC2.19, CC2.20, CC2.21, CC2.22, CC2.23, CC2.24, CC2.25, CC2.26, CC2.27, CC2.28, CC2.29, CC2.30, CC2.31, CC2.32, CC2.33, CC2.34, CC2.35, CC2.36, CC2.37, CC2.38, CC2.39, CC2.40, CC2.41, CC2.42, CC2.43, CC2.44, CC2.45, CC2.46, CC2.47, CC2.48, CC2.49, CC2.50, CC2.51, CC2.52, CC2.53, CC2.54, CC2.55, CC2.56, CC2.57, CC2.58, CC2.59, CC2.60, CC2.61, CC2.62, CC2.63, CC2.64, CC2.65, CC2.66, CC2.67, CC2.68, CC2.69, CC2.70, CC2.71, CC2.72, CC2.73, CC2.74, CC2.75, CC2.76, CC2.77, CC2.78, CC2.79, CC2.80, CC2.81, CC2.82, CC2.83, CC2.84, CC2.85, CC2.86, CC2.87, CC2.88, CC2.89, CC2.90, CC2.91, CC2.92, CC2.93, CC2.94, CC2.95, CC2.96, CC2.97, CC2.98, CC2.99, CC2.100
...estdata/invalid-moduleconfigs/aws-provider	1	AWS provider without version constraint	MEDIUM	Security	CC1.1, CC1.2, CC1.3, CC1.4, CC2.1, CC2.2, CC2.3, CC2.4, CC2.5, CC2.6, CC2.7, CC2.8, CC2.9, CC2.10, CC2.11, CC2.12, CC2.13, CC2.14, CC2.15, CC2.16, CC2.17, CC2.18, CC2.19, CC2.20, CC2.21, CC2.22, CC2.23, CC2.24, CC2.25, CC2.26, CC2.27, CC2.28, CC2.29, CC2.30, CC2.31, CC2.32, CC2.33, CC2.34, CC2.35, CC2.36, CC2.37, CC2.38, CC2.39, CC2.40, CC2.41, CC2.42, CC2.43, CC2.44, CC2.45, CC2.46, CC2.47, CC2.48, CC2.49, CC2.50, CC2.51, CC2.52, CC2.53, CC2.54, CC2.55, CC2.56, CC2.57, CC2.58, CC2.59, CC2.60, CC2.61, CC2.62, CC2.63, CC2.64, CC2.65, CC2.66, CC2.67, CC2.68, CC2.69, CC2.70, CC2.71, CC2.72, CC2.73, CC2.74, CC2.75, CC2.76, CC2.77, CC2.78, CC2.79, CC2.80, CC2.81, CC2.82, CC2.83, CC2.84, CC2.85, CC2.86, CC2.87, CC2.88, CC2.89, CC2.90, CC2.91, CC2.92, CC2.93, CC2.94, CC2.95, CC2.96, CC2.97, CC2.98, CC2.99, CC2.100
...rm/v15/testdata/moduleconfigs/aws-provider	1	AWS provider without version constraint	MEDIUM	Security	CC1.1, CC1.2, CC1.3, CC1.4, CC2.1, CC2.2, CC2.3, CC2.4, CC2.5, CC2.6, CC2.7, CC2.8, CC2.9, CC2.10, CC2.11, CC2.12, CC2.13, CC2.14, CC2.15, CC2.16, CC2.17, CC2.18, CC2.19, CC2.20, CC2.21, CC2.22, CC2.23, CC2.24, CC2.25, CC2.26, CC2.27, CC2.28, CC2.29, CC2.30, CC2.31, CC2.32, CC2.33, CC2.34, CC2.35, CC2.36, CC2.37, CC2.38, CC2.39, CC2.40, CC2.41, CC2.42, CC2.43, CC2.44, CC2.45, CC2.46, CC2.47, CC2.48, CC2.49, CC2.50, CC2.51, CC2.52, CC2.53, CC2.54, CC2.55, CC2.56, CC2.57, CC2.58, CC2.59, CC2.60, CC2.61, CC2.62, CC2.63, CC2.64, CC2.65, CC2.66, CC2.67, CC2.68, CC2.69, CC2.70, CC2.71, CC2.72, CC2.73, CC2.74, CC2.75, CC2.76, CC2.77, CC2.78, CC2.79, CC2.80, CC2.81, CC2.82, CC2.83, CC2.84, CC2.85, CC2.86, CC2.87, CC2.88, CC2.89, CC2.90, CC2.91, CC2.92, CC2.93, CC2.94, CC2.95, CC2.96, CC2.97, CC2.98, CC2.99, CC2.100
...v15/testdata/moduleconfigs/Security	1	Security group with unrestricted ingress	HIGH	Security	CC6.6, CC6.7
...orm/v15/testdata/tfconfigs/aws-provider	1	AWS provider without version constraint	MEDIUM	Security	CC1.1, CC1.2, CC1.3, CC1.4, CC2.1, CC2.2, CC2.3, CC2.4, CC2.5, CC2.6, CC2.7, CC2.8, CC2.9, CC2.10, CC2.11, CC2.12, CC2.13, CC2.14, CC2.15, CC2.16, CC2.17, CC2.18, CC2.19, CC2.20, CC2.21, CC2.22, CC2.23, CC2.24, CC2.25, CC2.26, CC2.27, CC2.28, CC2.29, CC2.30, CC2.31, CC2.32, CC2.33, CC2.34, CC2.35, CC2.36, CC2.37, CC2.38, CC2.39, CC2.40, CC2.41, CC2.42, CC2.43, CC2.44, CC2.45, CC2.46, CC2.47, CC2.48, CC2.49, CC2.50, CC2.51, CC2.52, CC2.53, CC2.54, CC2.55, CC2.56, CC2.57, CC2.58, CC2.59, CC2.60, CC2.61, CC2.62, CC2.63, CC2.64, CC2.65, CC2.66, CC2.67, CC2.68, CC2.69, CC2.70, CC2.71, CC2.72, CC2.73, CC2.74, CC2.75, CC2.76, CC2.77, CC2.78, CC2.79, CC2.80, CC2.81, CC2.82, CC2.83, CC2.84, CC2.85, CC2.86, CC2.87, CC2.88, CC2.89, CC2.90, CC2.91, CC2.92, CC2.93, CC2.94, CC2.95, CC2.96, CC2.97, CC2.98, CC2.99, CC2.100
...orm/v15/testdata/tfconfigs/Security	1	Security group with unrestricted ingress	HIGH	Security	CC6.6, CC6.7
...orm/v15/testdata/tfconfigs/Security	5	Security group with unrestricted ingress	HIGH	Security	CC6.6, CC6.7
...15/testdata/tfjson/moduleconfigs	1	Module config 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/v67dating	67	Hard-coded credentials or secrets	HIGH	Security	CC6.1, CC6.6, CC6.7
...mission-webhook/v67dating	70	Hard-coded credentials or secrets	HIGH	Security	CC6.1, CC6.6, CC6.7
...mission-webhook/v92dating	92	Hard-coded credentials or secrets	HIGH	Security	CC6.1, CC6.6, CC6.7
...on-webhook/validate67g-webhook-test.go	67	Hard-coded credentials or secrets	HIGH	Security	CC6.1, CC6.6, CC6.7
pkg/k8s/dblogs/webhook2k-scaler.go	72	Hard-coded credentials or secrets	HIGH	Security	CC6.1, CC6.8, CC7.2
pkg/k8s/dblogs/webhook206-scaler.go	206	Hard-coded credentials or secrets	HIGH	Security	CC6.1, CC6.8, CC7.2
...providers/arm/config/26editing	26	Hard-coded credentials or secrets	HIGH	Security	CC6.1, CC6.6, CC6.7
...providers/arm/config/30editing	30	Hard-coded credentials or secrets	HIGH	Security	CC6.1, CC6.6, CC6.7
...ders/arm/config/kubenetes	83	Hard-coded credentials or secrets	HIGH	Security	CC6.1, CC6.6, CC6.7
...-providers/arm/config/127mssql	127	Hard-coded credentials or secrets	HIGH	Security	CC6.1, CC6.6, CC6.7
...-providers/arm/config/13mssql	13	Hard-coded credentials or secrets	HIGH	Security	CC6.1, CC6.6, CC6.7
...iac-providers/arm/functions/44dandangle	44	Hard-coded credentials or secrets	HIGH	Security	CC6.1, CC6.6, CC6.7
...providers/arm/functions/138s/parallel	138	Hard-coded credentials or secrets	HIGH	Security	CC6.1, CC6.6, CC6.7
...roviders/arm/functions/138s/resource	138	Hard-coded credentials or secrets	HIGH	Security	CC6.1, CC6.6, CC6.7
...c-providers/arm/functions/138s/to	138	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.go	75	Hard-coded credentials or secrets	HIGH	Security	CC6.1, CC6.6, CC6.7
...roviders/cft/functions/s3-uri.go	27	Hard-coded credentials or secrets	HIGH	Security	CC6.1, CC6.6, CC6.7
...pper/iac-providers/cft/store/types.go	47	Hard-coded credentials or secrets	HIGH	Security	CC6.1, CC6.6, CC6.7
...pper/iac-providers/cft/store/types.go	67	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/webhooks/webhooks.go	23	Hard-coded credentials or secrets	HIGH	Security	CC6.1, CC6.6, CC6.7
...nction/lambdaNotEncryptedWithKms.go	10	Hard-coded credentials or secrets	HIGH	Security	CC6.1, CC6.6, CC6.7
...s/kubernetes_pod/api.go	100	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	97	Possible hard-coded password	HIGH	Security	CC6.1, CC6.7
pkg/vulnerability/acr.go	108	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	383	Hard-coded credentials or secrets	HIGH	Security	CC6.1, CC6.6, CC6.7
test/e2e/scan/scan_test.go	17	Hard-coded credentials or secrets	HIGH	Security	CC6.1, CC6.6, CC6.7
...ata/iac/aws/aws_ami_violations.go	1	AWS provider without version constraint	MEDIUM	Security	CC1.1, CC1.2, CC1.3, CC1.4, CC2
...aws/aws_db_instance_violations.go	1	AWS provider without version constraint	MEDIUM	Security	CC1.1, CC1.2, CC1.3, CC1.4, CC2
...aws/aws_db_instance_violations.go	21	Possible hard-coded password	HIGH	Security	CC6.1, CC6.7
...aws/aws_db_instance_violations.go	34	Possible hard-coded password	HIGH	Security	CC6.1, CC6.7
...aws/aws_db_instance_violations.go	51	Possible hard-coded password	HIGH	Security	CC6.1, CC6.7
...aws/aws_db_instance_violations.go	65	Possible hard-coded password	HIGH	Security	CC6.1, CC6.7

...aws/aws_db_instance/76	aws_db_instance.76	Possible if hard-coded password	HIGH	Security	CC6.1, CC6.7
...aws/aws_db_instance/81	aws_db_instance.81	Possible if hard-coded password	HIGH	Security	CC6.1, CC6.7
...aws/aws_db_instance/11	aws_db_instance.11	Possible if hard-coded password	HIGH	Security	CC6.1, CC6.7
...aws/aws_db_instance/130	aws_db_instance.130	Possible if hard-coded password	HIGH	Security	CC6.1, CC6.7
...aws/aws_db_instance/149	aws_db_instance.149	Possible if hard-coded password	HIGH	Security	CC6.1, CC6.7
...aws/aws_db_instance/69	aws_db_instance.69	Possible if encryption disabled	HIGH	Confidentiality	C1.1
...aws/aws_db_instance/32	aws_db_instance.32	Possible if backups disabled	MEDIUM	Availability	A1.2, A1.3
...aws/aws_db_instance/46	aws_db_instance.46	Possible if backups disabled	MEDIUM	Availability	A1.2, A1.3
...aws/aws_db_instance/106	aws_db_instance.106	Possible if backups disabled	MEDIUM	Availability	A1.2, A1.3
...aws/aws_db_instance/125	aws_db_instance.125	Possible if backups disabled	MEDIUM	Availability	A1.2, A1.3
...aws/aws_db_instance/144	aws_db_instance.144	Possible if backups disabled	MEDIUM	Availability	A1.2, A1.3
...ng/max_severity_set/12	terraform.12	Possible if hard-coded password	HIGH	Security	CC6.1, CC6.7
...x_severity_set_none/12	terraform.12	Possible if hard-coded password	HIGH	Security	CC6.1, CC6.7
...x_both_severity_set/13	terraform.13	Possible if hard-coded password	HIGH	Security	CC6.1, CC6.7
...ng/min_severity_set/12	terraform.12	Possible if hard-coded password	HIGH	Security	CC6.1, CC6.7
...rity_with_skip_rule/13	terraform.13	Possible if hard-coded password	HIGH	Security	CC6.1, CC6.7
...c/resource_skipping/16	terraform.AWS provider without version constraint	Possible if	MEDIUM	Security	CC1.1, CC1.2, CC1.3, CC1.4, CC2
...c/resource_skipping/21	terraform.21	Possible if hard-coded password	HIGH	Security	CC6.1, CC6.7
...c/resource_skipping/34	terraform.34	Possible if hard-coded password	HIGH	Security	CC6.1, CC6.7
...c/resource_skipping/51	terraform.51	Possible if hard-coded password	HIGH	Security	CC6.1, CC6.7
...c/resource_skipping/67	terraform.67	Possible if hard-coded password	HIGH	Security	CC6.1, CC6.7
...c/resource_skipping/81	terraform.81	Possible if hard-coded password	HIGH	Security	CC6.1, CC6.7
...c/resource_skipping/94	terraform.94	Possible if hard-coded password	HIGH	Security	CC6.1, CC6.7
...c/resource_skipping/104	terraform.104	Possible if hard-coded password	HIGH	Security	CC6.1, CC6.7
...c/resource_skipping/133	terraform.133	Possible if hard-coded password	HIGH	Security	CC6.1, CC6.7

...c/resource_skipping/52	9/52	Possible hard-coded password	HIGH	Security	CC6.1, CC6.7
...c/resource_skipping/92	9/92	Resource with encryption disabled	HIGH	Confidentiality	C1.1
...c/resource_skipping/92	9/92	Resource with backups disabled	MEDIUM	Availability	A1.2, A1.3
...c/resource_skipping/96	9/96	Resource with backups disabled	MEDIUM	Availability	A1.2, A1.3
...c/resource_skipping/99	9/99	Resource with backups disabled	MEDIUM	Availability	A1.2, A1.3
...c/resource_skipping/98	9/98	Resource with backups disabled	MEDIUM	Availability	A1.2, A1.3
...c/resource_skipping/47	9/47	Resource with backups disabled	MEDIUM	Availability	A1.2, A1.3
...cursive/subFolder1/subFolder2	1/28	provider without version constraint	MEDIUM	Security	CC1.1, CC1.2, CC1.3, CC1.4, CC2
...ingwebhook/validation	10	Hook does not check credentials or secrets	HIGH	Security	CC6.1, CC6.6, CC6.7
...ingwebhook/validation	10	Hook does not check credentials or secrets	HIGH	Security	CC6.1, CC6.6, CC6.7
...ingwebhook/validation	70	Hook does not check credentials or secrets	HIGH	Security	CC6.1, CC6.6, CC6.7
...e/vulnerability/vulnerability	42	Hard-coded credentials or secrets	HIGH	Security	CC6.1, CC6.6, CC6.7
...e/vulnerability/vulnerability	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.

## 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.