

DataGuardian Pro

GDPR Compliance Scan Report

Generated on: May 01, 2025 22:26

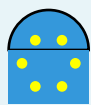
Scan ID: SOC-20250501-e2f377

Executive Summary

This report presents the findings of a SOC2 compliance analysis conducted on <https://github.com/vishaal314/terrascan> (branch: **master**) on **2025-05-01 22:26:29**. 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, kubernetes, pulumi, 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	2025-05-01 22:26:29
Technologies	javascript, docker, kubernetes, pulumi, 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

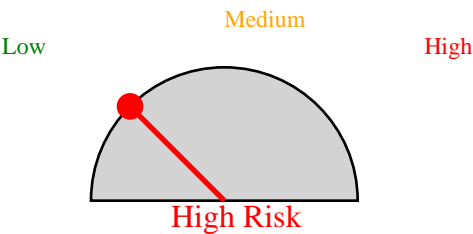
Risk Assessment



GDPR Compliance Protection

High risk of potential GDPR fines - immediate action required

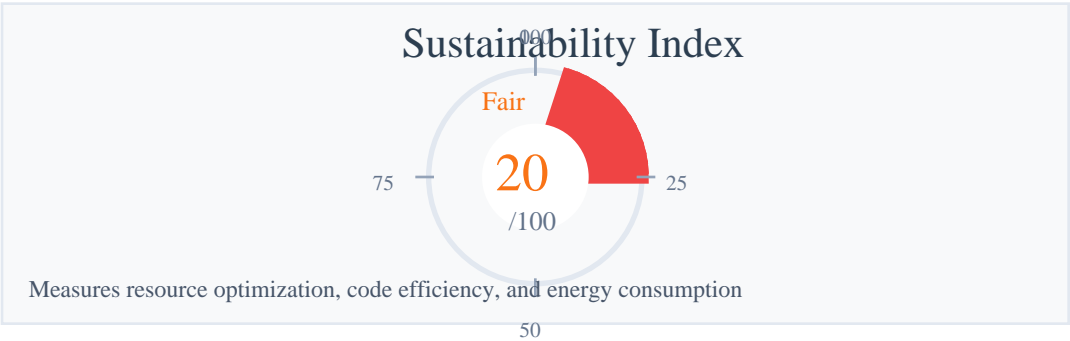
Potential fines up to €20 million or 4% of global revenue



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

File	Line	Description	Risk	Category	SOC2 TSC
deploy/helm/templates/32_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-test2/main.tf	2	AWS provider without version constraint	MEDIUM	Security	CC1.1, CC1.2, CC1.3, CC1.4, CC2.1
pkg/cli/testdata/run-test19/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-test48/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-test14/web.tf	14	Security group with unrestricted ingress	HIGH	Security	CC6.6, CC6.7
pkg/cli/testdata/run-test29/web.tf	29	Security group with unrestricted ingress	HIGH	Security	CC6.6, CC6.7
pkg/downloader/module57/download_test.go	57	Hard-coded credentials or secrets	HIGH	Security	CC6.1, CC6.6, CC6.7
pkg/http-server/file-scan107.go	107	Hard-coded credentials or secrets	HIGH	Security	CC6.1, CC6.6, CC6.7
pkg/http-server/file-scan395/test.go	395	Hard-coded credentials or secrets	HIGH	Security	CC6.1, CC6.6, CC6.7
pkg/http-server/start.go65	65	Hard-coded credentials or secrets	HIGH	Security	CC6.1, CC6.6, CC6.7
pkg/http-server/start.go96	96	Hard-coded credentials or secrets	HIGH	Security	CC6.1, CC6.6, CC6.7
pkg/http-server/webhook64-scan.go	64	Hard-coded credentials or secrets	HIGH	Security	CC6.1, CC6.6, CC6.7
pkg/http-server/webhook38-scan.go	38	Hard-coded credentials or secrets	HIGH	Security	CC6.1, CC6.6, CC6.7
pkg/http-server/webhook44-scan.go	44	Hard-coded credentials or secrets	HIGH	Security	CC6.1, CC6.6, CC6.7
pkg/http-server/webhook24-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/testconf106/main.tf	106	AWS provider without version constraint	MEDIUM	Security	CC1.1, CC1.2, CC1.3, CC1.4, CC2.1
pkg/http-server/testdata/testconf50/web.tf	50	Security group with unrestricted ingress	HIGH	Security	CC6.6, CC6.7
pkg/http-server/testdata/testconf50/web.tf	50	Security group with unrestricted ingress	HIGH	Security	CC6.6, CC6.7
pkg/iac-providers/cft/v2/testdata/14/updates/v8/deploy.yaml	14	Template with unrestricted access	HIGH	Security	CC6.1, CC6.3
pkg/iac-providers/cft/v17/testdata/36/updates/v30/deploy.yaml	36	Template with unrestricted access	HIGH	Confidentiality	C1.1
pkg/iac-providers/cft/v24/testdata/44/updates/v8/deploy.yaml	44	Template with unrestricted access	HIGH	Security	CC6.1, CC6.3
pkg/iac-providers/cft/v17/testdata/36/updates/v30/deploy.yaml	36	Template with unrestricted access	HIGH	Confidentiality	C1.1
pkg/iac-providers/docker/v1/pa10/test.go	10	Hard-coded credentials or secrets	HIGH	Security	CC6.1, CC6.6, CC6.7
pkg/iac-providers/kubernetes/v166/testdata/166/testdata/k8s/Template.yaml	166	Template with unrestricted access	HIGH	Security	CC6.1, CC6.8
pkg/iac-providers/kubernetes/v167/testdata/167/testdata/k8s/Template.yaml	167	Template with unrestricted access	HIGH	Security	CC6.1, CC6.8
pkg/iac-providers/kubernetes/v156/testdata/156/testdata/k8s/Template.yaml	156	Container allowed to escalate privileges	HIGH	Security	CC1.1, CC1.2, CC1.3, CC1.4, CC2.1
pkg/iac-providers/kubernetes/v153/testdata/153/testdata/k8s/Template.yaml	153	Container allowed to escalate privileges	HIGH	Security	CC1.1, CC1.2, CC1.3, CC1.4, CC2.1
pkg/iac-providers/kubernetes/v156/testdata/156/testdata/k8s/Template.yaml	156	Container allowed to escalate privileges	HIGH	Security	CC1.1, CC1.2, CC1.3, CC1.4, CC2.1

test/e2e/test_data/iac/141	aws/possible-execute-passwor	Possible-execute-passwor	HIGH	Security	CC6.1, CC6.7
test/e2e/test_data/iac/146	aws/possible-execute-passwor	Possible-execute-passwor	HIGH	Security	CC6.1, CC6.7
test/e2e/test_data/iac/149	aws/possible-execute-passwor	Possible-execute-passwor	HIGH	Security	CC6.1, CC6.7
test/e2e/test_data/iac/329	aws/Resistance-with-optional-main	Resistance-with-optional-main	HIGH	Confidentiality	C1.1
test/e2e/test_data/iac/325	aws/Resistance-with-backups-dis	Resistance-with-backups-dis	MEDIUM	Availability	A1.2, A1.3
test/e2e/test_data/iac/416	aws/Resistance-with-backups-dis	Resistance-with-backups-dis	MEDIUM	Availability	A1.2, A1.3
test/e2e/test_data/iac/406	aws/Resistance-with-backups-dis	Resistance-with-backups-dis	MEDIUM	Availability	A1.2, A1.3
test/e2e/test_data/iac/425	aws/Resistance-with-backups-dis	Resistance-with-backups-dis	MEDIUM	Availability	A1.2, A1.3
test/e2e/test_data/iac/444	aws/Resistance-with-backups-dis	Resistance-with-backups-dis	MEDIUM	Availability	A1.2, A1.3
test/e2e/test_data/iac/r12	source/Possible-incorrect-path-set	Possible-incorrect-path-set/terraform/main.tf	HIGH	Security	CC6.1, CC6.7
test/e2e/test_data/iac/r12	source/Possible-incorrect-path-set	Possible-incorrect-path-set/none/terraform/main.tf	HIGH	Security	CC6.1, CC6.7
test/e2e/test_data/iac/r13	source/Possible-incorrect-path-set	Possible-incorrect-path-set/severity_set/terraform/main.tf	HIGH	Security	CC6.1, CC6.7
test/e2e/test_data/iac/r12	source/Possible-incorrect-path-set	Possible-incorrect-path-set/terraform/main.tf	HIGH	Security	CC6.1, CC6.7
test/e2e/test_data/iac/r13	source/Possible-incorrect-path-set	Possible-incorrect-path-set/skip_rule/terraform/main.tf	HIGH	Security	CC6.1, CC6.7
test/e2e/test_data/iac/r1	AWSPolicyIdentifierConstraint	AWSPolicyIdentifierConstraint	MEDIUM	Security	CC1.1, CC1.2, CC1.3, CC1.4, CC2.1
test/e2e/test_data/iac/r21	Resisting/hardcode/pass	Resisting/hardcode/pass	HIGH	Security	CC6.1, CC6.7
test/e2e/test_data/iac/r34	Resisting/hardcode/pass	Resisting/hardcode/pass	HIGH	Security	CC6.1, CC6.7
test/e2e/test_data/iac/r51	Resisting/hardcode/pass	Resisting/hardcode/pass	HIGH	Security	CC6.1, CC6.7
test/e2e/test_data/iac/r63	Resisting/hardcode/pass	Resisting/hardcode/pass	HIGH	Security	CC6.1, CC6.7
test/e2e/test_data/iac/r81	Resisting/hardcode/pass	Resisting/hardcode/pass	HIGH	Security	CC6.1, CC6.7
test/e2e/test_data/iac/r94	Resisting/hardcode/pass	Resisting/hardcode/pass	HIGH	Security	CC6.1, CC6.7
test/e2e/test_data/iac/r154	Resisting/hardcode/pass	Resisting/hardcode/pass	HIGH	Security	CC6.1, CC6.7
test/e2e/test_data/iac/r133	Resisting/hardcode/pass	Resisting/hardcode/pass	HIGH	Security	CC6.1, CC6.7
test/e2e/test_data/iac/r152	Resisting/hardcode/pass	Resisting/hardcode/pass	HIGH	Security	CC6.1, CC6.7
test/e2e/test_data/iac/r92	Resisting/with-environment	Resisting/with-environment	HIGH	Confidentiality	C1.1
test/e2e/test_data/iac/r32	Resisting/with-backups-dis	Resisting/with-backups-dis	MEDIUM	Availability	A1.2, A1.3
test/e2e/test_data/iac/r46	Resisting/with-backups-dis	Resisting/with-backups-dis	MEDIUM	Availability	A1.2, A1.3
test/e2e/test_data/iac/r69	Resisting/with-backups-dis	Resisting/with-backups-dis	MEDIUM	Availability	A1.2, A1.3
test/e2e/test_data/iac/r28	Resisting/with-backups-dis	Resisting/with-backups-dis	MEDIUM	Availability	A1.2, A1.3
test/e2e/test_data/iac/r47	Resisting/with-backups-dis	Resisting/with-backups-dis	MEDIUM	Availability	A1.2, A1.3
test/e2e/test_data/iac/terraform	AWSPolicyIdentifierConstraint	AWSPolicyIdentifierConstraint	MEDIUM	Security	CC1.1, CC1.2, CC1.3, CC1.4, CC2.1
test/e2e/validatingwebhook	Hard-coded-credentials	Hard-coded-credentials	HIGH	Security	CC6.1, CC6.6, CC6.7

test/e2e/validatingwebhook/validatingwebhookcontrollersecrets	66	Hand-coded secrets	HIGH	Security	CC6.1, CC6.6, CC6.7
test/e2e/validatingwebhook/validatingwebhookcontrollersecrets	76	Hand-coded secrets	HIGH	Security	CC6.1, CC6.6, CC6.7
test/e2e/vulnerability/vulnerabilitytestsecrets	42	Hand-coded secrets	HIGH	Security	CC6.1, CC6.6, CC6.7
test/e2e/vulnerability/vulnerabilitytestsecrets	44	Hand-coded secrets	HIGH	Security	CC6.1, CC6.6, CC6.7

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	e2f377a8-7df4-47b3-88b8-4bbbd7810df6
Scan Type	soc2
Region	Global
Timestamp	2025-05-01 22:26:29
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.