# DataGuardian Pro

## GDPR Compliance Scan Report

Generated on: May 01, 2025 21:59

Scan ID: SOC-20250501-03f7f4

## 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 21:59:36**. The scan identified a total of **161** compliance issues with **129** high-risk items. The overall compliance score is **99/100**. **Technologies Detected:** docker, pulumi, javascript, kubernetes, cloudformation, ansible, terraform Each finding in this report is mapped to specific SOC2 Trust Services Criteria (TSC) to help you understand how it impacts your compliance posture. The TSC categories include: • CC: Common Criteria (Security) • A: Availability • PI: Processing Integrity • C: Confidentiality • P: Privacy

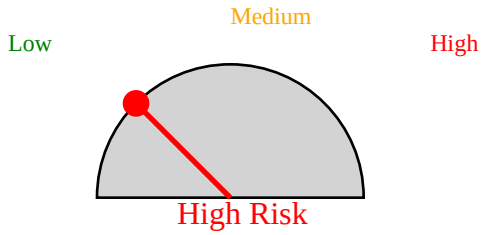
| | |
|---|---|
| Scan Type | soc2 |
| Repository URL | https://github.com/vishaal314/terrascan |
| Branch | master |
| Date & Time | 2025-05-01 21:59:36 |
| Technologies | docker, pulumi, javascript, kubernetes, cloudformation, ansible, terraform |
| Compliance Score | 99/100 |
| IaC Files Found | 1662 |
| Total Files Scanned | 2202 |
| High Risk Issues | 129 |
| Medium Risk Issues | 32 |
| Low Risk Issues | 0 |
| Security Issues | 146 |
| Availability Issues | 10 |
| Confidentiality Issues | 5 |

# Risk Assessment

## GDPR Compliance Protection

High risk of potential GDPR fines - immediate action required

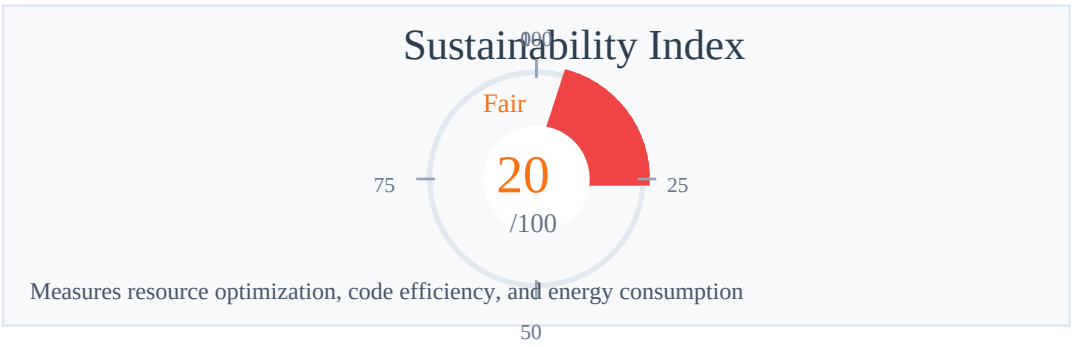
Potential fines up to €20 million or 4% of global revenue




This scan has identified a high number of high-risk PII items. Immediate action is recommended to ensure GDPR compliance and protect sensitive data.

## Data Sustainability Compliance

Data sustainability measures how efficiently your organization manages personal data in compliance with GDPR principles of data minimization, storage limitation, and purpose limitation. A higher score indicates better long-term data governance practices.



# Detailed Findings

| 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, CC1.4, CC2.1 |
| pkg/cli/testdata/run-test/main.tf | 2 | AWS provider without version constraint | MEDIUM | Security | CC1.1, CC1.2, CC1.3, CC1.4, CC2.1 |
| pkg/cli/testdata/run-test/test_pod.yaml | 19 | Container allowed to escalate privileges | HIGH | Security | CC1.1, CC1.2, CC1.3, CC1.4, CC2.1 |
| pkg/cli/testdata/run-test/test_pod.yaml | 48 | Container allowed to escalate privileges | HIGH | Security | CC1.1, CC1.2, CC1.3, CC1.4, CC2.1 |
| pkg/cli/testdata/run-test/web.tf | 14 | Security group with unrestricted ingress | HIGH | Security | CC6.6, CC6.7 |
| pkg/cli/testdata/run-test/web.tf | 29 | Security group with unrestricted ingress | HIGH | Security | CC6.6, CC6.7 |
| pkg/downloader/module_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 | 84 | 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 | 44 | 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/1/test.tf | 1 | AWS provider without version constraint | MEDIUM | Security | CC1.1, CC1.2, CC1.3, CC1.4, CC2.1 |
| pkg/http-server/testdata/testconfig/1/test.tf | 50 | Security group with unrestricted ingress | HIGH | Security | CC6.6, CC6.7 |
| pkg/http-server/testdata/testconfig/1/test.tf | 56 | Security group with unrestricted ingress | HIGH | Security | CC6.6, CC6.7 |
| pkg/iac-providers/cft/v1/testdata/AWS/policy/s3/deploy.json | 24 | AWS policy with wildcard access | HIGH | Security | CC6.1, CC6.3 |
| pkg/iac-providers/cft/v1/testdata/AWS/policy/s3/deploy.json | 7 | S3 bucket without public access block | HIGH | Confidentiality | C1.1 |
| pkg/iac-providers/cft/v1/testdata/AWS/policy/s3/deploy.template | 24 | AWS policy with wildcard access | HIGH | Security | CC6.1, CC6.3 |
| pkg/iac-providers/cft/v1/testdata/AWS/policy/s3/deploy.template | 7 | S3 bucket without public access block | HIGH | Confidentiality | C1.1 |
| pkg/iac-providers/docker/v1/parser_test.go | 40 | Hard-coded credentials or secrets | HIGH | Security | CC6.1, CC6.6, CC6.7 |
| pkg/iac-providers/kubernetes/v1/testdata/k8s_path/values.yaml | 164 | Privileged container | HIGH | Security | CC6.1, CC6.8 |
| pkg/iac-providers/kubernetes/v1/testdata/k8s_path/values.yaml | 167 | Privileged container | HIGH | Security | CC6.1, CC6.8 |
| pkg/iac-providers/kubernetes/v1/testdata/test-data/test_bad_kinds.yaml | 15 | Container allowed to escalate privileges | HIGH | Security | CC1.1, CC1.2, CC1.3, CC1.4, CC2.1 |
| pkg/iac-providers/kubernetes/v1/testdata/test-data/test_bad_kinds.yaml | 33 | Container allowed to escalate privileges | HIGH | Security | CC1.1, CC1.2, CC1.3, CC1.4, CC2.1 |
| pkg/iac-providers/kubernetes/v1/testdata/test-data/test_bad_kinds_data.yaml | 15 | Container allowed to escalate privileges | HIGH | Security | CC1.1, CC1.2, CC1.3, CC1.4, CC2.1 |

| | | | | | |
|---|---|---|---|---|---|
| pkg/iac-providers/kubernetes/v1/Container/allowed-data/test_privileged.yaml | 28 | Container/allowed-data/test_privileged | HIGH | Security | CC1.1, CC1.2, CC1.3, CC1.4, CC2.1 |
| pkg/iac-providers/kubernetes/v1/Container/allowed-data/test_privileged_name.yaml | 15 | Container/allowed-data/test_privileged | HIGH | Security | CC1.1, CC1.2, CC1.3, CC1.4, CC2.1 |
| pkg/iac-providers/kubernetes/v1/Container/allowed-data/test_privileged_name.yaml | 29 | Container/allowed-data/test_privileged | HIGH | Security | CC1.1, CC1.2, CC1.3, CC1.4, CC2.1 |
| pkg/iac-providers/kubernetes/v1/Container/allowed-data/test_privilegespace.yaml | 15 | Container/allowed-data/test_privilegespace | HIGH | Security | CC1.1, CC1.2, CC1.3, CC1.4, CC2.1 |
| pkg/iac-providers/kubernetes/v1/Container/allowed-data/test_privilegespace.yaml | 33 | Container/allowed-data/test_privilegespace | HIGH | Security | CC1.1, CC1.2, CC1.3, CC1.4, CC2.1 |
| pkg/iac-providers/kubernetes/v1/Container/allowed-data/test_req_privileged | 14 | Container/allowed-data/test_req_privileged | HIGH | Security | CC1.1, CC1.2, CC1.3, CC1.4, CC2.1 |
| pkg/iac-providers/kubernetes/v1/Container/allowed-data/test_req_privileged | 32 | Container/allowed-data/test_req_privileged | HIGH | Security | CC1.1, CC1.2, CC1.3, CC1.4, CC2.1 |
| pkg/iac-providers/kubernetes/v1/Container/allowed-data/test_req_privileges.yaml | 14 | Container/allowed-data/test_req_privileges | HIGH | Security | CC1.1, CC1.2, CC1.3, CC1.4, CC2.1 |
| pkg/iac-providers/kubernetes/v1/Container/allowed-data/test_req_privileges.yaml | 32 | Container/allowed-data/test_req_privileges | HIGH | Security | CC1.1, CC1.2, CC1.3, CC1.4, CC2.1 |
| pkg/iac-providers/kubernetes/v1/Container/allowed-data/test_req_privileges_name.yaml | 14 | Container/allowed-data/test_req_privileges | HIGH | Security | CC1.1, CC1.2, CC1.3, CC1.4, CC2.1 |
| pkg/iac-providers/kubernetes/v1/Container/allowed-data/test_req_privileges_name.yaml | 32 | Container/allowed-data/test_req_privileges | HIGH | Security | CC1.1, CC1.2, CC1.3, CC1.4, CC2.1 |
| pkg/iac-providers/kubernetes/v1/Container/allowed/test_privileged | 15 | Container/allowed/test_privileged | HIGH | Security | CC1.1, CC1.2, CC1.3, CC1.4, CC2.1 |
| pkg/iac-providers/kubernetes/v1/Container/allowed/test_privileged | 33 | Container/allowed/test_privileged | HIGH | Security | CC1.1, CC1.2, CC1.3, CC1.4, CC2.1 |
| pkg/iac-providers/kubernetes/v1/Container/allowed-rules/test_privileges.yaml | 19 | Container/allowed-rules/test_privileges | HIGH | Security | CC1.1, CC1.2, CC1.3, CC1.4, CC2.1 |
| pkg/iac-providers/kubernetes/v1/Container/allowed-rules/test_privileges.yaml | 43 | Container/allowed-rules/test_privileges | HIGH | Security | CC1.1, CC1.2, CC1.3, CC1.4, CC2.1 |
| pkg/iac-providers/kubernetes/v1/Container/allowed-test-issue2/test_privileged | 15 | Container/allowed-test-issue2/test_privileged | HIGH | Security | CC1.1, CC1.2, CC1.3, CC1.4, CC2.1 |
| pkg/iac-providers/kubernetes/v1/Container/allowed-test-issue2/test_privileged | 33 | Container/allowed-test-issue2/test_privileged | HIGH | Security | CC1.1, CC1.2, CC1.3, CC1.4, CC2.1 |
| pkg/iac-providers/kubernetes/v1/Container/allowed-with-multiple-containers/test_poc.yaml | 15 | Container/allowed-with-multiple-containers/test_poc | HIGH | Security | CC1.1, CC1.2, CC1.3, CC1.4, CC2.1 |
| pkg/iac-providers/kubernetes/v1/Container/allowed-with-multiple-containers/test_poc.yaml | 33 | Container/allowed-with-multiple-containers/test_poc | HIGH | Security | CC1.1, CC1.2, CC1.3, CC1.4, CC2.1 |
| pkg/iac-providers/kustomize/common/test/data/resource-deployment/deployment.yaml | 16 | Container/test/data/resource-deployment/deployment | HIGH | Security | CC1.1, CC1.2, CC1.3, CC1.4, CC2.1 |
| pkg/iac-providers/output/vulnerability_test.go | 28 | Hard-coded credentials or secrets | HIGH | Security | CC6.1, CC6.6, CC6.7 |
| pkg/iac-providers/output/vulnerability_test.go | 30 | Hard-coded credentials or secrets | HIGH | Security | CC6.1, CC6.6, CC6.7 |
| pkg/iac-providers/output/vulnerability_test.go | 113 | Hard-coded credentials or secrets | HIGH | Security | CC6.1, CC6.6, CC6.7 |
| pkg/iac-providers/terraform/common/eval_functions_test.go | 287 | Use of eval() function | HIGH | Security | CC5.1, CC6.8, CC7.2 |
| pkg/iac-providers/terraform/common/test/data/hard-coded-credentials.go | 52 | Hard-coded credentials or secrets | HIGH | Security | CC6.1, CC6.6, CC6.7 |
| pkg/iac-providers/terraform/common/test/data/hard-coded-credentials.go | 31 | Hard-coded credentials or secrets | HIGH | Security | CC6.1, CC6.6, CC6.7 |
| pkg/iac-providers/terraform/v12/AWS/data/deep-without-version-constraint | 5 | AWS data provider without version constraint | MEDIUM | Security | CC1.1, CC1.2, CC1.3, CC1.4, CC2.1 |
| pkg/iac-providers/terraform/v12/AWS/data/provider-without-source-constraint | 5 | AWS data provider without source constraint | MEDIUM | Security | CC1.1, CC1.2, CC1.3, CC1.4, CC2.1 |
| pkg/iac-providers/terraform/v12/AWS/data/provider-without-versions-constraint | 1 | AWS data provider without versions constraint | MEDIUM | Security | CC1.1, CC1.2, CC1.3, CC1.4, CC2.1 |
| pkg/iac-providers/terraform/v12/AWS/data/provider-without-version-constraint | 1 | AWS data provider without version constraint | MEDIUM | Security | CC1.1, CC1.2, CC1.3, CC1.4, CC2.1 |
| pkg/iac-providers/terraform/v12/Security/group/with-inline-ingress-rule | 11 | Security group with inline ingress rule | HIGH | Security | CC6.6, CC6.7 |
| pkg/iac-providers/terraform/v12/AWS/provider/config-without-version-constraint | 1 | AWS provider config without version constraint | MEDIUM | Security | CC1.1, CC1.2, CC1.3, CC1.4, CC2.1 |

| | | | | | |
|---|---|---|---|---|---|
| pkg/iac-providers/terraform/v12/testdata/fixtures/config1.tf | 49 | Security group with unrestricted ingress | HIGH | Security | CC6.6, CC6.7 |
| pkg/iac-providers/terraform/v12/testdata/fixtures/config1.tf | 55 | Security group with unrestricted ingress | HIGH | Security | CC6.6, CC6.7 |
| pkg/iac-providers/terraform/v12/testdata/fixtures/config1.tf | 591 | AWS policy with unrestricted access | HIGH | Security | CC6.1, CC6.3 |
| pkg/iac-providers/terraform/v14/testdata/deprecated.tf | 5 | AWS provider without version constraint | MEDIUM | Security | CC1.1, CC1.2, CC1.3, CC1.4, CC2.1 |
| pkg/iac-providers/terraform/v14/testdata/module_source_install_source/main.tf | 5 | AWS provider without version constraint | MEDIUM | Security | CC1.1, CC1.2, CC1.3, CC1.4, CC2.1 |
| pkg/iac-providers/terraform/v14/testdata/module_versions/main.tf | 1 | AWS provider without version constraint | MEDIUM | Security | CC1.1, CC1.2, CC1.3, CC1.4, CC2.1 |
| pkg/iac-providers/terraform/v14/testdata/unlocked/main.tf | 1 | AWS provider without version constraint | MEDIUM | Security | CC1.1, CC1.2, CC1.3, CC1.4, CC2.1 |
| pkg/iac-providers/terraform/v14/testdata/with_modules/config1.tf | 11 | Security group with unrestricted ingress | HIGH | Security | CC6.6, CC6.7 |
| pkg/iac-providers/terraform/v14/testdata/with_modules/config1.tf | 1 | AWS provider without version constraint | MEDIUM | Security | CC1.1, CC1.2, CC1.3, CC1.4, CC2.1 |
| pkg/iac-providers/terraform/v14/testdata/with_modules/config1.tf | 49 | Security group with unrestricted ingress | HIGH | Security | CC6.6, CC6.7 |
| pkg/iac-providers/terraform/v14/testdata/with_modules/config1.tf | 55 | Security group with unrestricted ingress | HIGH | Security | CC6.6, CC6.7 |
| pkg/iac-providers/terraform/v14/testdata/with_modules/config1.tf | 591 | AWS policy with unrestricted access | HIGH | Security | CC6.1, CC6.3 |
| pkg/iac-providers/terraform/v15/testdata/deprecated.tf | 5 | AWS provider without version constraint | MEDIUM | Security | CC1.1, CC1.2, CC1.3, CC1.4, CC2.1 |
| pkg/iac-providers/terraform/v15/testdata/module_source_install_source/main.tf | 5 | AWS provider without version constraint | MEDIUM | Security | CC1.1, CC1.2, CC1.3, CC1.4, CC2.1 |
| pkg/iac-providers/terraform/v15/testdata/module_versions/main.tf | 1 | AWS provider without version constraint | MEDIUM | Security | CC1.1, CC1.2, CC1.3, CC1.4, CC2.1 |
| pkg/iac-providers/terraform/v15/testdata/unlocked/main.tf | 1 | AWS provider without version constraint | MEDIUM | Security | CC1.1, CC1.2, CC1.3, CC1.4, CC2.1 |
| pkg/iac-providers/terraform/v15/testdata/with_modules/config1.tf | 11 | Security group with unrestricted ingress | HIGH | Security | CC6.6, CC6.7 |
| pkg/iac-providers/terraform/v15/testdata/with_modules/config1.tf | 1 | AWS provider without version constraint | MEDIUM | Security | CC1.1, CC1.2, CC1.3, CC1.4, CC2.1 |
| pkg/iac-providers/terraform/v15/testdata/with_modules/config1.tf | 49 | Security group with unrestricted ingress | HIGH | Security | CC6.6, CC6.7 |
| pkg/iac-providers/terraform/v15/testdata/with_modules/config1.tf | 55 | Security group with unrestricted ingress | HIGH | Security | CC6.6, CC6.7 |
| pkg/iac-providers/terraform/v15/testdata/with_modules/config1.tf | 591 | AWS 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 |
| pkg/k8s/admission-webhook/validate/pod/pod.go | 67 | Hard-coded credentials or secrets | HIGH | Security | CC6.1, CC6.6, CC6.7 |
| pkg/k8s/admission-webhook/validate/pod/pod.go | 73 | Hard-coded credentials or secrets | HIGH | Security | CC6.1, CC6.6, CC6.7 |
| pkg/k8s/admission-webhook/validate/pod/pod.go | 92 | Hard-coded credentials or secrets | HIGH | Security | CC6.1, CC6.6, CC6.7 |
| pkg/k8s/admission-webhook/validate/pod/pod_test.go | 67 | Hard-coded credentials or secrets | HIGH | Security | CC6.1, CC6.6, CC6.7 |
| pkg/k8s/dblogs/webhook-scan-logger.go | 72 | Logger.exec function | HIGH | Security | CC6.1, CC6.8, CC7.2 |
| pkg/k8s/dblogs/webhook-scan-logger.go | 206 | Logger.exec function | HIGH | Security | CC6.1, CC6.8, CC7.2 |
| pkg/mapper/iac-providers/arm/testdata/audit-credentials.go | 26 | Hard-coded credentials or secrets | HIGH | Security | CC6.1, CC6.6, CC6.7 |
| pkg/mapper/iac-providers/arm/testdata/audit-credentials.go | 33 | Hard-coded credentials or secrets | HIGH | Security | CC6.1, CC6.6, CC6.7 |
| pkg/mapper/iac-providers/arm/testdata/kubernetes-cluster.go | 83 | Hard-coded credentials or secrets | HIGH | Security | CC6.1, CC6.6, CC6.7 |
| pkg/mapper/iac-providers/arm/testdata/mssql-server.go | 27 | Hard-coded credentials or secrets | HIGH | Security | CC6.1, CC6.6, CC6.7 |

| | | | | | |
|---|---|---|---|---|---|
| pkg/mapper/iac-prov | 33 | Hard-coded credentials or secrets | HIGH | Security | CC6.1, CC6.6, CC6.7 |
| pkg/mapper/iac-prov | 34 | Hard-coded credentials or secrets | HIGH | Security | CC6.1, CC6.6, CC6.7 |
| pkg/mapper/iac-prov | 38 | Hard-coded credentials or secrets | HIGH | Security | CC6.1, CC6.6, CC6.7 |
| pkg/mapper/iac-prov | 38 | Hard-coded credentials or secrets | HIGH | Security | CC6.1, CC6.6, CC6.7 |
| pkg/mapper/iac-prov | 38 | Hard-coded credentials or secrets | HIGH | Security | CC6.1, CC6.6, CC6.7 |
| pkg/mapper/iac-prov | 38 | Hard-coded credentials or secrets | HIGH | Security | CC6.1, CC6.6, CC6.7 |
| pkg/mapper/iac-prov | 75 | Hard-coded credentials or secrets | HIGH | Security | CC6.1, CC6.6, CC6.7 |
| pkg/mapper/iac-prov | 27 | Hard-coded credentials or secrets | HIGH | Security | CC6.1, CC6.6, CC6.7 |
| pkg/mapper/iac-prov | 41 | Hard-coded credentials or secrets | HIGH | Security | CC6.1, CC6.6, CC6.7 |
| pkg/mapper/iac-prov | 61 | Hard-coded credentials or secrets | HIGH | Security | CC6.1, CC6.6, CC6.7 |
| pkg/mapper/iac-prov | 64 | Hard-coded credentials or secrets | HIGH | Security | CC6.1, CC6.6, CC6.7 |
| pkg/mapper/iac-prov | 80 | Hard-coded credentials or secrets | HIGH | Security | CC6.1, CC6.6, CC6.7 |
| pkg/notifications/webhook/webhook_test.go | 28 | Hard-coded credentials or secrets | HIGH | Security | CC6.1, CC6.6, CC6.7 |
| pkg/policies/opa/rego/aws/aws_lambda_function_variable_doesNotExistEncryptedWithKms.rego | 10 | Hard-coded credentials or secrets | HIGH | Security | CC6.1, CC6.6, CC6.7 |
| pkg/policies/opa/rego/k8s/k8s_hard_coded_apparmor_profile.rego | 33 | Hard-coded credentials or secrets | HIGH | Security | CC6.1, CC6.6, CC6.7 |
| pkg/utils/skip_rules_test.go | 128 | 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 | 87 | 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 | 85 | 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 |
| test/e2e/test_data/iac/a | 1 | AWS provider without version constraint | MEDIUM | Security | CC1.1, CC1.2, CC1.3, CC1.4, CC2.1 |
| test/e2e/test_data/iac/a | 1 | AWS provider without version constraint | MEDIUM | Security | CC1.1, CC1.2, CC1.3, CC1.4, CC2.1 |
| test/e2e/test_data/iac/a | 21 | Possible hard-coded password | HIGH | Security | CC6.1, CC6.7 |
| test/e2e/test_data/iac/a | 34 | Possible hard-coded password | HIGH | Security | CC6.1, CC6.7 |
| test/e2e/test_data/iac/a | 51 | Possible hard-coded password | HIGH | Security | CC6.1, CC6.7 |
| test/e2e/test_data/iac/a | 65 | Possible hard-coded password | HIGH | Security | CC6.1, CC6.7 |
| test/e2e/test_data/iac/a | 78 | Possible hard-coded password | HIGH | Security | CC6.1, CC6.7 |
| test/e2e/test_data/iac/a | 91 | Possible hard-coded password | HIGH | Security | CC6.1, CC6.7 |

| | | | | | |
|---|---|---|---|---|---|
| test/e2e/test_data/iac/main.tf | 111 | aws_db_instance - database password | HIGH | Security | CC6.1, CC6.7 |
| test/e2e/test_data/iac/main.tf | 139 | aws_db_instance - database password | HIGH | Security | CC6.1, CC6.7 |
| test/e2e/test_data/iac/main.tf | 149 | aws_db_instance - database password | HIGH | Security | CC6.1, CC6.7 |
| test/e2e/test_data/iac/main.tf | 89 | aws_db_instance - encryption disabled | HIGH | Confidentiality | C1.1 |
| test/e2e/test_data/iac/main.tf | 82 | aws_db_instance - backups disabled | MEDIUM | Availability | A1.2, A1.3 |
| test/e2e/test_data/iac/main.tf | 46 | aws_db_instance - backups disabled | MEDIUM | Availability | A1.2, A1.3 |
| test/e2e/test_data/iac/main.tf | 106 | aws_db_instance - backups disabled | MEDIUM | Availability | A1.2, A1.3 |
| test/e2e/test_data/iac/main.tf | 125 | aws_db_instance - backups disabled | MEDIUM | Availability | A1.2, A1.3 |
| test/e2e/test_data/iac/main.tf | 144 | aws_db_instance - backups disabled | MEDIUM | Availability | A1.2, A1.3 |
| test/e2e/test_data/iac/resource_provisioning/main.tf | 12 | Possible hard-coded password | HIGH | Security | CC6.1, CC6.7 |
| test/e2e/test_data/iac/resource_provisioning/main.tf | 12 | Possible hard-coded password | HIGH | Security | CC6.1, CC6.7 |
| test/e2e/test_data/iac/resource_provisioning/main.tf | 13 | Possible hard-coded password | HIGH | Security | CC6.1, CC6.7 |
| test/e2e/test_data/iac/resource_provisioning/main.tf | 12 | Possible hard-coded password | HIGH | Security | CC6.1, CC6.7 |
| test/e2e/test_data/iac/resource_provisioning/main.tf | 13 | Possible hard-coded password | HIGH | Security | CC6.1, CC6.7 |
| test/e2e/test_data/iac/resource_provisioning/main.tf | 1 | AWS provider without version constraint | MEDIUM | Security | CC1.1, CC1.2, CC1.3, CC1.4, CC2.1 |
| test/e2e/test_data/iac/resource_skipping/main.tf | 21 | Possible hard-coded password | HIGH | Security | CC6.1, CC6.7 |
| test/e2e/test_data/iac/resource_skipping/main.tf | 34 | Possible hard-coded password | HIGH | Security | CC6.1, CC6.7 |
| test/e2e/test_data/iac/resource_skipping/main.tf | 51 | Possible hard-coded password | HIGH | Security | CC6.1, CC6.7 |
| test/e2e/test_data/iac/resource_skipping/main.tf | 67 | Possible hard-coded password | HIGH | Security | CC6.1, CC6.7 |
| test/e2e/test_data/iac/resource_skipping/main.tf | 81 | Possible hard-coded password | HIGH | Security | CC6.1, CC6.7 |
| test/e2e/test_data/iac/resource_skipping/main.tf | 94 | Possible hard-coded password | HIGH | Security | CC6.1, CC6.7 |
| test/e2e/test_data/iac/resource_skipping/main.tf | 114 | Possible hard-coded password | HIGH | Security | CC6.1, CC6.7 |
| test/e2e/test_data/iac/resource_skipping/main.tf | 133 | Possible hard-coded password | HIGH | Security | CC6.1, CC6.7 |
| test/e2e/test_data/iac/resource_skipping/main.tf | 152 | Possible hard-coded password | HIGH | Security | CC6.1, CC6.7 |
| test/e2e/test_data/iac/resource_skipping/main.tf | 92 | aws_db_instance - encryption disabled | HIGH | Confidentiality | C1.1 |
| test/e2e/test_data/iac/resource_skipping/main.tf | 82 | aws_db_instance - backups disabled | MEDIUM | Availability | A1.2, A1.3 |
| test/e2e/test_data/iac/resource_skipping/main.tf | 46 | aws_db_instance - backups disabled | MEDIUM | Availability | A1.2, A1.3 |
| test/e2e/test_data/iac/resource_skipping/main.tf | 109 | aws_db_instance - backups disabled | MEDIUM | Availability | A1.2, A1.3 |
| test/e2e/test_data/iac/resource_skipping/main.tf | 128 | aws_db_instance - backups disabled | MEDIUM | Availability | A1.2, A1.3 |
| test/e2e/test_data/iac/resource_skipping/main.tf | 147 | aws_db_instance - backups disabled | MEDIUM | Availability | A1.2, A1.3 |
| test/e2e/test_data/iac/terraform_AWS_provider_folder1/subfolder2/main.tf | 1 | AWS provider without version constraint | MEDIUM | Security | CC1.1, CC1.2, CC1.3, CC1.4, CC2.1 |
| test/e2e/validatingwebhook/validating_checks.go | 43 | Hard-coded credentials or secrets | HIGH | Security | CC6.1, CC6.6, CC6.7 |

| | | | | | |
|---|---|---|---|---|---|
| test/e2e/validatingwebhook/validating_webhook_test.go | 88 | Hard-coded credentials or secrets | HIGH | Security | CC6.1, CC6.6, CC6.7 |
| test/e2e/validatingwebhook/validating_webhook_test.go | 76 | Hard-coded credentials or secrets | HIGH | Security | CC6.1, CC6.6, CC6.7 |
| test/e2e/vulnerability/vulnerability_test.go | 42 | Hard-coded credentials or secrets | HIGH | Security | CC6.1, CC6.6, CC6.7 |
| test/e2e/vulnerability/vulnerability_test.go | 44 | Hard-coded credentials or 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 | 03f7f46e-0946-4400-96f2-128540999389 |
| Scan Type | soc2 |
| Region | Global |
| Timestamp | 2025-05-01 21:59:36 |
| 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 |