Misconfigurations Report

Scan Date/Time: Saturday, April 05, 2025 20:03:01

Scan Duration: 12.84 seconds

Scanned GCP Project name: *capstone-test-project-450805*

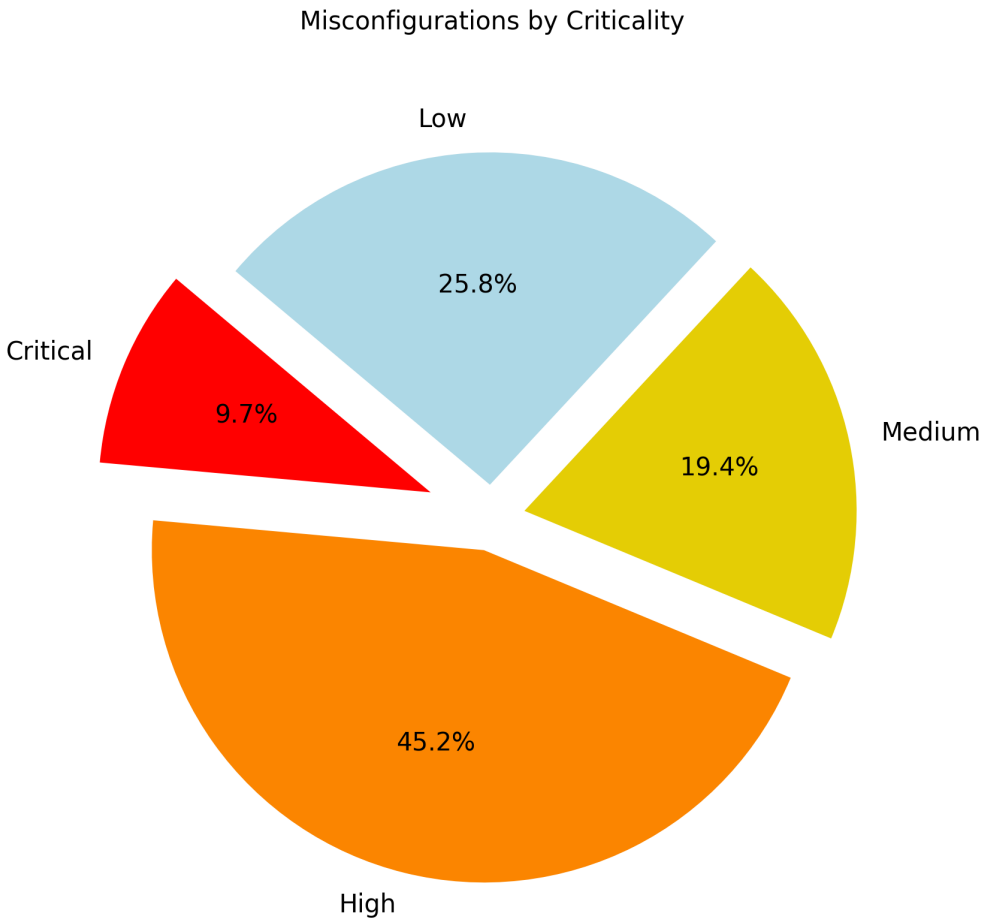
The purpose of this scan is to generate a report of all potential misconfigurations identified across the cloud components in the selected GCP project. This section provides a comprehensive list of all misconfigurations identified during the scan, their criticality and actionable measures needed to remediate them.

Severity	Misconfiguration	Recommendation
Critical	- Public bucket access for the bucket {insecure-folder}	Remove Public access(allUsers/allAuthenticatedUsers) to the bucket
Critical	- CIS violation allowing all traffic in f/w rule 'default-allow-icmp'	Amend the firewall rule to not allow all traffic (0.0.0.0/0)
Critical	- CIS violation allowing all traffic in f/w rule 'default-allow-rdp'	Amend the firewall rule to not allow all traffic (0.0.0.0/0)
High	- PII/PHI/PCI violation in 'customer_ph_nbr' in table customer.customer_info	Protect/Restrict sensitive data by applying Data masking or column-level security
High	- PII/PHI/PCI violation in 'role' in table employee.employee	Protect/Restrict sensitive data by applying Data masking or column-level security
High	- PII/PHI/PCI violation in 'emp_email_id' in table employee.employee_personal_info	Protect/Restrict sensitive data by applying Data masking or column-level security
High	- PII/PHI/PCI violation in 'emp_phone_number' in table employee.employee_personal_info	Protect/Restrict sensitive data by applying Data masking or column-level security
High	- PII/PHI/PCI violation in 'emp_credit_card_number' in table employee.employee_personal_info	Protect/Restrict sensitive data by applying Data masking or column-level security
High	- PII/PHI/PCI violation in 'emp_ssn' in table employee.employee_personal_info	Protect/Restrict sensitive data by applying Data masking or column-level security
High	- CIS violation - misconfiguration not logging traffic in 'default-allow-icmp'	Update the network rule to enable logging
High	- CIS violation - misconfiguration not logging traffic in 'default-allow-internal'	Update the network rule to enable logging
High	- CIS violation - misconfiguration not logging traffic in 'default-allow-rdp'	Update the network rule to enable logging
High	- CIS violation - misconfiguration not logging traffic in 'default-allow-ssh'	Update the network rule to enable logging
High	- CIS violation - misconfiguration not logging traffic in 'gke-test-cluster-1-ddcfccb2-all'	Update the network rule to enable logging
High	- CIS violation - misconfiguration not logging traffic in 'gke-test-cluster-1-ddcfccb2-exkubelet'	Update the network rule to enable logging
High	- CIS violation - misconfiguration not logging traffic in 'gke-test-cluster-1-ddcfccb2-inkubelet'	Update the network rule to enable logging
High	- CIS violation - misconfiguration not logging traffic in 'gke-test-cluster-1-ddcfccb2-vms'	Update the network rule to enable logging
Medium	- Overly permissive roles found in bucket IAM policy	Apply 'Principle of Least Privilege'/remove broad permissions
Medium	- Overly permissive 'cluster-admin' role granted for : cluster-admin	Apply restrictive role bindings and remove broad grants/permissions
Medium	- The 'system:masters' group has cluster-wide administrative access	Remove broad grants/permissions from the group

Medium	- No control entries found for table customer_info	IAM roles or ACLs need to be defined for the table
Medium	- No control entries found for table employee	IAM roles or ACLs need to be defined for the table
Medium	- No control entries found for table employee_personal_info	IAM roles or ACLs need to be defined for the table
Low	- No subjects found for this ClusterRoleBinding: kubelet-cluster-admin	Either add subjects to the role binding or remove the binding(if not needed)
Low	- No subjects found for this ClusterRoleBinding: system:node	Either add subjects to the role binding or remove the binding(if not needed)
Low	- Pod test-pod-1 in namespace default has no resource limits set	Memory and CPU settings needed for pod; use kubectl to configure.
Low	- Pod test-pod-2 in namespace default has no resource limits set	Memory and CPU settings needed for pod; use kubectl to configure.
Low	- Pod test-pod-3 in namespace default has no resource limits set	Memory and CPU settings needed for pod; use kubectl to configure.
Low	- Table customer_info does not use CMEK	Enable CMEK on tables to better control encryption
Low	- Table employee does not use CMEK	Enable CMEK on tables to better control encryption
Low	- Table employee_personal_info does not use CMEK	Enable CMEK on tables to better control encryption

Misconfiguration Summary

The chart here summarizes the count of identified potential vulnerabilities categorized based on their severity or the impact they could have on the security of the environment if they are not remediated. The criticality of the misconfiguration is also determined by the negative impact the misconfiguration would potentially create on the environment if any malicious hacker exploits the vulnerability exposed by the misconfiguration. This pie chart here represents the percentage distribution of misconfigurations according to their criticality.



Cloud Scan Trend

This trend graph here shows the progress of the security posture of the scanned GCP project over a period of time. The x-axis shows the dates when the scans were executed whereas the y-axis shows the count of misconfigurations identified after every scan. Each colored line represents a criticality level.