Cloud Security Compliance Report

Scan ID:	scan_20251229_230910
Provider:	AWS
Timestamp:	2025-12-29T23:09:10.438279
CIS Compliance Score:	90.0%
Total Findings:	2
Critical:	1
High:	1
Medium:	0

Security Findings

Finding #1	
Rule ID:	CIS-AWS-1.2
Rule Name:	S3 Bucket Public Access
Severity:	CRITICAL
Resource Type:	S3 Bucket
Resource ID:	production-data-bucket
Description:	S3 bucket allows public read access
Remediation:	Apply bucket policy to restrict public access

Finding #2	

Rule ID:	CIS-AWS-4.1
Rule Name:	Overly Permissive Security Group
Severity:	HIGH
Resource Type:	Security Group
Resource ID:	sg-12345678
Description:	Security group allows SSH from 0.0.0.0/0
Remediation:	Restrict SSH access to specific IP ranges

Recommendations

1. Enable S3 bucket versioning
2. Restrict security group ingress rules
3. Enable CloudTrail logging
4. Use IAM roles instead of access keys

Generated on 2025-12-29 23:09:14 | Cloud Security Scanner v1.0