Terrascan - Infrastructure as Code (IaC) Security Scanner

# What is Terrascan?

Terrascan is an open-source static code analyzer developed by Tenable. It scans Infrastructure as Code (IaC) like Terraform, Kubernetes, and Helm charts to detect security risks, policy violations, and misconfigurations before deploying infrastructure.

# 🔒 Why Use Terrascan?

• Security Scanning – Detects misconfigured resources (e.g., public S3 buckets, open ports)

• Compliance Enforcement – Validates against CIS, NIST, PCI-DSS, and other frameworks

• Early Feedback – Prevents risky deployments before terraform apply

• Automation – Works well with CI/CD pipelines and Git workflows

# 🛠️ Installation (Windows)

Option 1: Using Chocolatey

choco install terrascan

Option 2: Manual

1. Download from https://github.com/tenable/terrascan/releases

2. Extract and add the executable to your system PATH

3. Run terrascan version to verify installation

# 📂 How to Scan Terraform Code

Navigate to your Terraform code directory and run:

terrascan scan -t terraform -d .

Scan a Terraform Plan File:

terraform plan -out=tfplan.binary

terraform show -json tfplan.binary > tfplan.json

terrascan scan -i terraform-plan -f tfplan.json

Scan a Specific Directory:

terrascan scan -t terraform -d ./modules/vpc

Scan with Specific Cloud Provider (e.g., AWS, GCP):

terrascan scan -t terraform -p gcp -d .

# 📊 Example Output

Violation detected:  
  
 File: main.tf  
 Resource: aws\_s3\_bucket.my\_bucket  
 Rule Name: aws\_s3\_bucket\_public\_read  
 Description: S3 bucket should not allow public READ access  
 Severity: HIGH

# 🔗 Terrascan Integration Options

• Local CLI – run terrascan in your development environment

• CI/CD – integrate in pipelines (GitHub Actions, GitLab, Jenkins)

• Git Hooks – enforce policies before code is committed

• IDE – use with VSCode or JetBrains plugins

# ✅ Summary

Terrascan helps secure your infrastructure by analyzing Terraform code before it's applied. It ensures security best practices, compliance requirements, and consistent IaC policy enforcement across your environments.