

















Discover Security Vulnerabilities in Terraform Configurations Using TFSec

OpsMx Delivery Shield includes Infrastructure as Code (IAC) Security as part of its comprehensive application security solution. OpsMx's IAC Security is built on TFSec, a robust, open-source security scanner that identifies potential security vulnerabilities in Terraform configurations before deployment. By integrating TFSec into your development pipeline, users ensure that the infrastructure on which they are deploying applications adheres to security best practices, reducing risks and bolstering compliance.

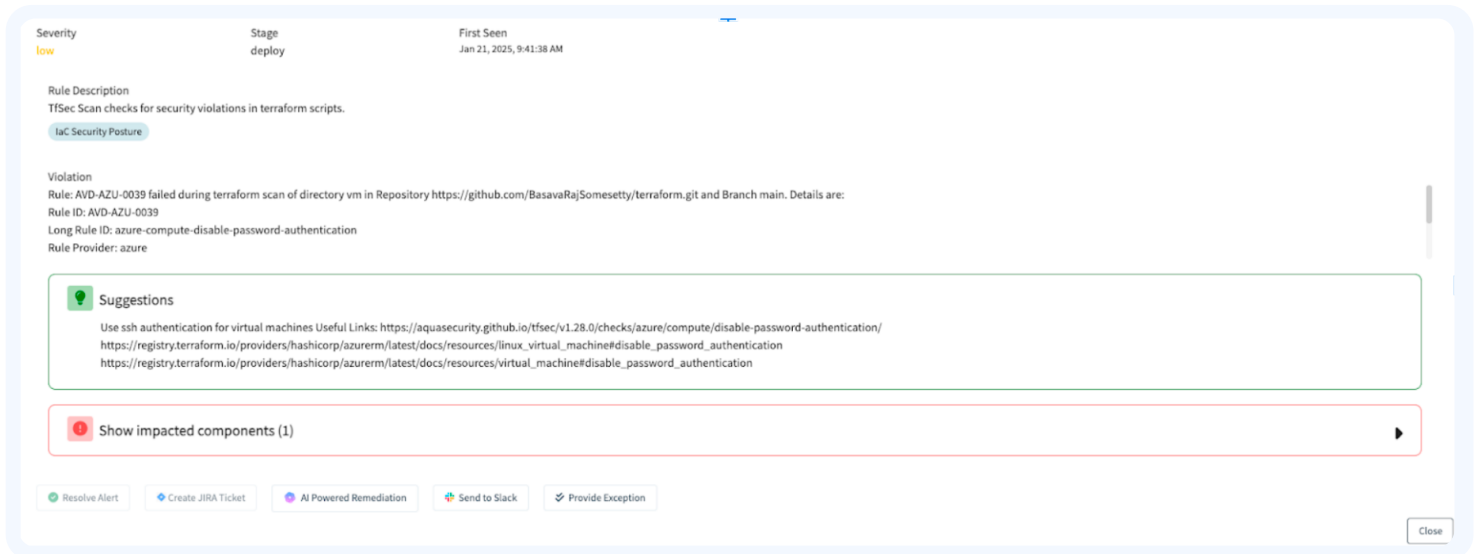
IAC Security Key Features

-  **Comprehensive Security Scanning**
 - Performs a deep analysis of Terraform configurations, identifying common vulnerabilities, misconfigurations, and deviations from security standards.
 - Supports both HCL (HashiCorp Configuration Language) and JSON-based Terraform files.
-  **Context-Aware Analysis**
 - Goes beyond static scanning by analyzing interdependencies between resources, ensuring accurate detection of vulnerabilities in complex configurations.
-  **Wide Rule Set**
 - Includes a vast library of built-in checks aligned with industry standards like CIS Benchmarks, AWS Well-Architected Framework, and NIST guidelines.
 - Rules are frequently updated to address new and emerging threats.
-  **Custom Rule Creation**
 - Enables users to define custom rules tailored to their organizational security policies.
 - Facilitates adaptability to unique use cases and environments.
-  **Multi-Cloud Support**
 - Compatible with major cloud providers such as AWS, Azure, and Google Cloud Platform, making it a versatile choice for diverse infrastructure setups.
-  **Shift-Left Security**
 - Designed to integrate seamlessly into CI/CD pipelines, empowering developers to identify and address security issues early in the development lifecycle.
-  **Clear and Actionable Reporting**
 - Provides detailed reports highlighting vulnerabilities, their potential impact, and remediation steps.
 - Supports output formats such as JSON and SARIF for integration with other tools.
-  **Extensibility and Integration**
 - Works with popular CI/CD platforms like GitHub Actions, GitLab CI, Jenkins, and CircleCI.
 - Integrates with tools like Docker and Visual Studio Code for enhanced usability.
-  **Fast and Lightweight**
 - Runs efficiently without compromising performance, making it suitable for frequent scans during development.

Core Capabilities

- 
Pre-Deployment Security Checks
 - Identifies and mitigates risks in Terraform configurations before deployment, preventing insecure infrastructure provisioning.
- 
Automated Policy Enforcement
 - Ensures adherence to organizational policies and compliance standards automatically, reducing manual oversight.
- 
Risk Prioritization
 - Assesses vulnerabilities based on their severity and impact, enabling teams to focus on high-priority issues.
- 
Audit and Compliance
 - Generates compliance-ready reports for audits, supporting governance and regulatory requirements.
- 
Developer Enablement
 - Offers insights and educational feedback for developers, promoting security awareness and best practices.

OpsMx Delivery Shield IaC Security simplifies infrastructure security by offering a proactive approach to risk management. Its user-friendly interface, powerful integrations, and extensive rule set make it a preferred tool for organizations aiming to efficiently and effectively secure their Terraform deployments as part of the application deployment process.



The screenshot shows a security alert interface with the following details:

- Severity:** low
- Stage:** deploy
- First Seen:** Jan 21, 2025, 9:41:38 AM
- Rule Description:** TFSec Scan checks for security violations in terraform scripts.
- Category:** IaC Security Posture
- Violation:** Rule: AVD-AZU-0039 failed during terraform scan of directory vm in Repository <https://github.com/BasavaRajSomesetty/terraform.git> and Branch main. Details are:
 - Rule ID: AVD-AZU-0039
 - Long Rule ID: azure-compute-disable-password-authentication
 - Rule Provider: azure
- Suggestions:**
 - Use ssh authentication for virtual machines Useful Links: <https://aquasecurity.github.io/tfsec/v1.28.0/checks/azure/compute/disable-password-authentication/>
 - https://registry.terraform.io/providers/hashicorp/azurerm/latest/docs/resources/linux_virtual_machine#disable_password_authentication
 - https://registry.terraform.io/providers/hashicorp/azurerm/latest/docs/resources/virtual_machine#disable_password_authentication
- Action:** Show impacted components (1)
- Actions:** Resolve Alert, Create JIRA Ticket, AI Powered Remediation, Send to Slack, Provide Exception

ABOUT US

OpsMx secures and intelligently automates software delivery from developer to deployment, building on an Open Software Delivery architecture and AI/ML-powered DevSecOps. OpsMx products and services enable hundreds of thousands of developers at Google, Cisco, Western Union, and other leading global enterprises to ship better software faster.

FOR MORE INFORMATION, CONTACT US:

OPSMX, INC | 350 OAKMEAD PKWY, SUNNYVALE, CA 94085 | INFO@OPSMX.COM
[WWW.OPSMX.COM/SECURE SOFTWARE DELIVERY](http://WWW.OPSMX.COM/SECURE_SOFTWARE_DELIVERY)