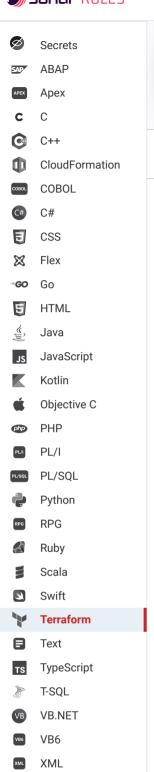
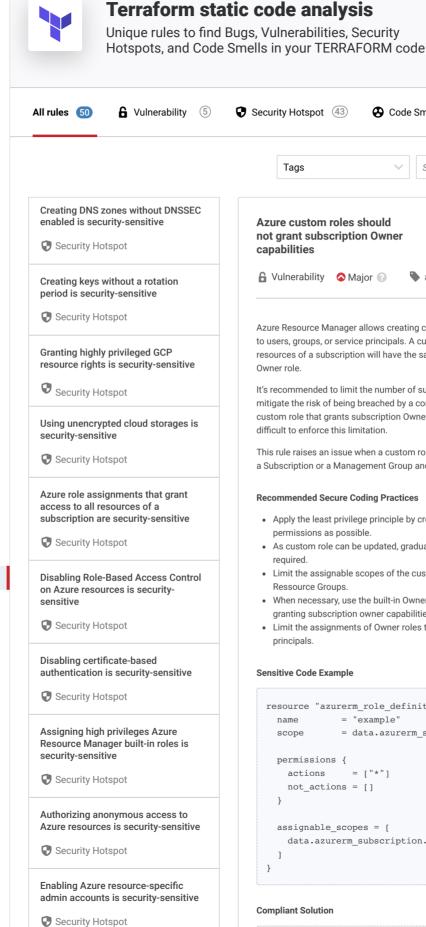


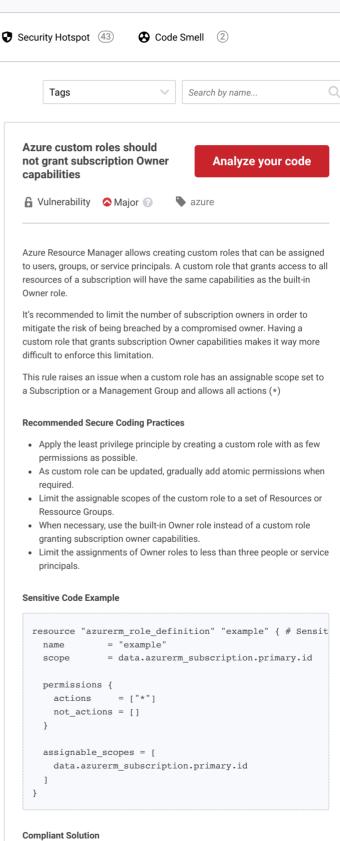
Products ∨





Disabling Managed Identities for

Azure resources is security-sensitive



resource "azurerm role definition" "example" {

= data.azurerm subscription.primary.id

= "example

name

scope

Security Hotspot Assigning high privileges Azure Active Directory built-in roles is securitysensitive Security Hotspot Defining a short backup retention duration is security-sensitive Security Hotspot Using unencrypted EFS file systems is security-sensitive Security Hotspot Using unencrypted SQS queues is security-sensitive Security Hotspot

```
permissions {
 actions
             = ["Microsoft.Compute/*"]
 not_actions = []
assignable_scopes = [
 data.azurerm subscription.primary.id
```

- OWASP Top 10 2021 Category A1 Broken Access Control
- OWASP Top 10 2021 Category A4 Insecure Design
- OWASP Top 10 2017 Category A5 Broken Access Control
- MITRE, CWE-266 Incorrect Privilege Assignment
- Azure Documentation Azure custom roles
- Azure Documentation Best practices for Azure RBAC

Available In:

sonarcloud 🐼 | sonarqube

© 2008-2022 SonarSource S.A., Switzerland. All content is copyright protected. SONAR, SONARSOURCE, SONARLINT, SONARQUBE and SONARCLOUD are trademarks of SonarSource S.A. All other trademarks and copyrights are the property of their respective owners. All rights are expressly reserved. Privacy Policy