Terraform static code analysis

Unique rules to find Bugs, Vulnerabilities, Security Hotspots, and Code Smells in your TERRAFORM code

1. Creating public APIs is security-sensitive
   Security Hotspot
2. Allowing public network access to cloud resources is security-sensitive
   Security Hotspot
3. Having AWS policies that grant access to all resources of an account is security-sensitive
   Security Hotspot
4. Having policies that grant all privileges is security-sensitive
   Security Hotspot
5. Policies authorizing public access to resources are security-sensitive
   Security Hotspot
6. Granting access to S3 buckets to all or authenticated users is security-sensitive
   Security Hotspot
7. AWS IAM policies should not allow privilege escalation
   Vulnerability
8. Weak SSL/TLS protocols should not be used
   Vulnerability
9. Allowing public ACLs or policies on a S3 bucket is security-sensitive
   Security Hotspot
10. Authorizing HTTP communications with S3 buckets is security-sensitive
    Security Hotspot
11. Using clear-text protocols is security-sensitive
    Security Hotspot
12. Google Cloud load balancers SSL policies should not offer weak cipher suites
    Vulnerability
13. Azure custom roles should not grant subscription Owner capabilities
    Vulnerability
14. Excluding users or groups activities from audit logs is security-sensitive
    Security Hotspot
15. Defining a short log retention duration is security-sensitive
    Security Hotspot
16.

	Enabling Attribute-Based Access Control for Kubernetes is security-sensitive Security Hotspot
17.	
	Creating custom roles allowing privilege escalation is security-sensitive Security Hotspot
18.	
	Creating App Engine handlers without requiring TLS is security-sensitive Security Hotspot
19.	
	Excessive granting of GCP IAM permissions is security-sensitive Security Hotspot
20.	
	Enabling project-wide SSH keys to access VM instances is security-sensitive Security Hotspot
21.	
	Granting public access to GCP resources is security-sensitive Security Hotspot
22.	
	Creating GCP SQL instances without requiring TLS is security-sensitive Security Hotspot
23.	
	Creating DNS zones without DNSSEC enabled is security-sensitive Security Hotspot
24.	
	Creating keys without a rotation period is security-sensitive Security Hotspot
25.	
	Granting highly privileged GCP resource rights is security-sensitive Security Hotspot
26.	
	Using unencrypted cloud storages is security-sensitive Security Hotspot
27.	
	Azure role assignments that grant access to all resources of a subscription are security-sensitive Security Hotspot
28.	
	Disabling Role-Based Access Control on Azure resources is security-sensitive Security Hotspot
29.	
	Disabling certificate-based authentication is security-sensitive Security Hotspot
30.	
	Assigning high privileges Azure Resource Manager built-in roles is security-sensitive Security Hotspot
31.	
	Authorizing anonymous access to Azure resources is security-sensitive Security Hotspot
32.	
	Enabling Azure resource-specific admin accounts is security-sensitive Security Hotspot

33. Disabling Managed Identities for Azure resources is security-sensitive
Security Hotspot

34. Assigning high privileges Azure Active Directory built-in roles is security-sensitive
Security Hotspot

35. Defining a short backup retention duration is security-sensitive
Security Hotspot

36. Using unencrypted EFS file systems is security-sensitive
Security Hotspot

37. Using unencrypted SQS queues is security-sensitive
Security Hotspot

38. Using unencrypted SNS topics is security-sensitive
Security Hotspot

39. Using unencrypted SageMaker notebook instances is security-sensitive
Security Hotspot

40. Using unencrypted Elasticsearch domains is security-sensitive
Security Hotspot

41. Using unencrypted RDS databases is security-sensitive
Security Hotspot

42. Using unencrypted EBS volumes is security-sensitive
Security Hotspot

43. Disabling logging is security-sensitive
Security Hotspot

44. Administration services access should be restricted to specific IP addresses
Vulnerability

45. Unversioned Google Cloud Storage buckets are security-sensitive
Security Hotspot

46. Disabling S3 bucket MFA delete is security-sensitive
Security Hotspot

47. Disabling versioning of S3 buckets is security-sensitive
Security Hotspot

48. Disabling server-side encryption of S3 buckets is security-sensitive
Security Hotspot

49. AWS tag keys should comply with a naming convention
Code Smell

50.
Terraform parsing failure Code Smell