CloudFormation static code analysis

Unique rules to find Bugs, Vulnerabilities, Security Hotspots, and Code Smells in your CLOUDFORMATION 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. "Log Groups" should be configured with a retention policy
    Code Smell
13. Defining a short backup retention duration is security-sensitive
    Security Hotspot
14. Using unencrypted EFS file systems is security-sensitive
    Security Hotspot
15. Using unencrypted SQS queues is security-sensitive
    Security Hotspot
16.

	Using unencrypted SNS topics is security-sensitive Security Hotspot
17.	
	Using unencrypted SageMaker notebook instances is security-sensitive Security Hotspot
18.	
	Using unencrypted Elasticsearch domains is security-sensitive Security Hotspot
19.	
	Using unencrypted RDS databases is security-sensitive Security Hotspot
20.	
	Using unencrypted EBS volumes is security-sensitive Security Hotspot
21.	
	Disabling logging is security-sensitive Security Hotspot
22.	
	"Log Groups" should be declared explicitly Code Smell
23.	
	Administration services access should be restricted to specific IP addresses Vulnerability
24.	
	Disabling versioning of S3 buckets is security-sensitive Security Hotspot
25.	
	Disabling server-side encryption of S3 buckets is security-sensitive Security Hotspot
26.	
	AWS tag keys should comply with a naming convention Code Smell
27.	
	CloudFormation parsing failure Code Smell