AWS Cloud Inspector

Topics : AWS
Written on December 09, 2023

Amazon Inspector is an AWS service designed to help you discover security vulnerabilities and compliance issues in your applications and workloads. It automatically assesses applications for common vulnerabilities and provides a detailed report with prioritized findings. Amazon Inspector is particularly useful for improving the security posture of your Amazon Elastic Compute Cloud (EC2) instances and applications.

1. **Vulnerability Assessments:**
    - Amazon Inspector performs automated security assessments of your applications by analyzing the behavior, state, and configurations of your AWS resources. It checks for common vulnerabilities, security best practices, and deviations from secure configurations.
2. **Agent-Based Architecture:**
    - Amazon Inspector uses an agent-based architecture where an Inspector agent is installed on the target EC2 instances. The agent collects data about the instance and sends it securely to the Inspector service for analysis.
3. **Security Rules Packages:**
    - Amazon Inspector uses rules packages that contain security rules based on industry standards and best practices. These rules packages cover various areas, such as common vulnerabilities and exposures (CVEs), Center for Internet Security (CIS) benchmarks, and AWS security best practices.
4. **Assessment Templates:**
    - You define an assessment template in Amazon Inspector to specify the rules packages, duration, and other settings for a security assessment. Assessment templates allow you to customize the scope and depth of the assessment.
5. **Prioritized Findings:**
    - Amazon Inspector provides a detailed report of findings, including information about each vulnerability or security issue discovered during the assessment. Findings are prioritized based on severity, helping you focus on the most critical issues first.
6. **Integration with AWS Config:**

- Amazon Inspector integrates with AWS Config, allowing you to use Inspector findings as a compliance source in AWS Config rules. This integration helps you maintain continuous compliance with security best practices.

7. **Automated and On-Demand Assessments:**
   - You can schedule regular automated security assessments using Amazon Inspector. Additionally, you can perform on-demand assessments whenever needed to validate the security posture of your applications.

8. **Integration with AWS CloudFormation:**
   - Amazon Inspector is integrated with AWS CloudFormation, allowing you to automate the deployment and configuration of Inspector assessments as part of your infrastructure as code (IaC) practices.

9. **Integration with AWS Security Hub:**
   - Amazon Inspector findings can be sent to AWS Security Hub, which provides a comprehensive view of your security alerts and compliance status. This centralizes security information for easier analysis.

10. **API Access:**
    - Amazon Inspector provides an API that allows you to programmatically interact with the service. This is useful for integrating Inspector into your existing workflows and security processes.

11. **Scalability:**
    - Amazon Inspector is designed to scale with your infrastructure. You can assess a single EC2 instance or thousands of instances simultaneously, depending on your needs.