**Amazon Inspector**

Amazon Inspector is a security assessment service that helps improve the security and compliance of applications deployed on AWS. It assesses the security and compliance of EC2 instances and applications running on those instances. Amazon Inspector helps identify potential security vulnerabilities in the application environment by performing automated security assessments.

**What is Amazon Inspector Used For:**

1. **Security Assessment:** Amazon Inspector helps identify security vulnerabilities and deviations from best practices in EC2 instances and applications.
2. **Compliance Auditing:** It assists in evaluating the security posture of your applications against compliance standards such as CIS Benchmarks and PCI DSS.
3. **Continuous Monitoring:** Amazon Inspector provides ongoing assessment and monitoring of your EC2 instances and applications to detect security threats and vulnerabilities.
4. **Integration with DevOps Pipeline:** It integrates seamlessly with CI/CD pipelines to automate security assessments as part of the deployment process.

**Information Provided by Amazon Inspector:**

1. **Security Findings:** Amazon Inspector generates findings that highlight security vulnerabilities, potential security misconfigurations, and deviations from best practices.
2. **Detailed Reports:** It provides detailed reports with actionable recommendations to remediate security findings and improve the overall security posture.
3. **Severity Levels:** Findings are categorized into severity levels (e.g., High, Medium, Low) based on the potential impact on security.
4. **CVEs and Common Weakness Enumeration (CWE):** Amazon Inspector identifies Common Vulnerabilities and Exposures (CVEs) and Common Weakness Enumeration (CWE) identifiers associated with security findings.

**Services Monitored by Amazon Inspector:**

Amazon Inspector primarily monitors EC2 instances and applications running on those instances. It analyzes the operating system, installed software packages, network configuration, and application dependencies to identify security vulnerabilities and compliance violations.

**How to Enable Amazon Inspector:**

1. Log in to the AWS Management Console using your AWS account credentials.
2. Open the Amazon Inspector service from the list of available AWS services.
3. Click on “Get Started”.

**How to Use Amazon Inspector:**

1. **Create Assessment Targets:**

* Define assessment targets by selecting the EC2 instances or applications you want to assess.

1. **Configure Assessment Templates:**

* Create assessment templates specifying the rules packages and duration for the assessment.

1. **Start Assessment Runs:**

* Initiate assessment runs based on the configured templates to evaluate the security and compliance of the selected targets.

1. **Review Findings:**

* Review the findings generated by Amazon Inspector, including security vulnerabilities, compliance violations, and actionable recommendations.

1. **Remediate Security Findings:**

* Address security findings by following the recommended remediation steps provided in the Amazon Inspector reports.

1. **Monitor Ongoing Assessments:**

* Monitor ongoing assessment runs and review new findings as they are generated to ensure continuous security and compliance.

**Cost of Amazon Inspector:**

Amazon Inspector pricing is based on a pay-as-you-go model, where you are charged for the number of assessment runs and the duration of each run. Pricing varies by region and depends on factors such as the number of instances assessed and the assessment templates used.

Docs: [Amazon Inspector pricing](https://aws.amazon.com/inspector/pricing/)

Amazon Inspector is a valuable tool for assessing the security and compliance of applications deployed on AWS. By performing automated security assessments, Amazon Inspector helps identify and remediate security vulnerabilities and compliance violations, thereby improving the overall security posture of your environment. With its seamless integration with AWS services and CI/CD pipelines, Amazon Inspector enables organizations to adopt a proactive approach to security and compliance.