AWS - Inspector

Amazon Inspector (for EC2 and for contents of EC2)

- Amazon Inspector is an automated security assessment service that helps you
  - test the network accessibility of your Amazon EC2 instances and
  - the security state of your applications running on the instances.
- It does not provide a custom metric to track the memory and disk utilization of each and every EC2 instance in your VPC.

- Amazon Inspector is an automated security assessment service that helps improve the security and compliance of applications deployed on AWS.
- Amazon Inspector automatically assesses applications for exposure,
  - vulnerabilities, and
  - deviations from best practices.
- After performing an assessment, Amazon Inspector produces a detailed list of security findings prioritized by level of severity. These findings can be reviewed directly or as part of detailed assessment reports which are available via the Amazon Inspector console or API.
- Amazon Inspector security assessments help you
  - check for unintended network accessibility of your Amazon EC2 instances and
  - for vulnerabilities on those EC2 instances.
- Amazon Inspector assessments are offered to you as pre-defined rules packages mapped to common security best practices and vulnerability definitions.
- Examples of built-in rules include
  - checking for access to your EC2 instances from the internet,
  - remote root login being enabled, or vulnerable software versions installed.
- These rules are regularly updated by AWS security researchers.

https://aws.amazon.com/inspector/

Benefits

IDENTIFY APPLICATION SECURITY ISSUES

Amazon Inspector helps you to identify security vulnerabilities as well as deviations from security best practices in applications, both before they are deployed, and while they are running in a production environment. This helps improve the overall security posture of your applications deployed on AWS.

INTEGRATE SECURITY INTO DEVOPS

Amazon Inspector is an API-driven service that analyzes network configurations in your AWS account and uses an optional agent for visibility into your Amazon EC2 instances. This makes it easy for you to build Inspector assessments right into your existing DevOps process, decentralizing and automating vulnerability assessments, and empowering your development and operations teams to make security assessments an integral part of the deployment process.

INCREASE DEVELOPMENT AGILITY

Amazon Inspector helps you reduce the risk of introducing security issues during development and deployment by automating the security assessment of your applications and proactively identifying vulnerabilities. This allows you to develop and iterate on new applications quickly and assess compliance with best practices and policies.

LEVERAGE AWS SECURITY EXPERTISE

The AWS security organization is continuously assessing the AWS environment and updating a knowledge base of security best practices and rules. Amazon Inspector makes this expertise available to you in the form of a service that simplifies the process of establishing and enforcing best practices within your AWS environment.

STREAMLINE SECURITY COMPLIANCE

Amazon Inspector gives security teams and auditors visibility into the security testing that is being performed during development of applications on AWS. This streamlines the process of validating and demonstrating that security and compliance standards and best practices are being followed throughout the development process.

ENFORCE SECURITY STANDARDS

Amazon Inspector allows you to define standards and best practices for your applications and validate adherence to these standards. This simplifies enforcement of your organization’s security standards and best practices, and helps to proactively manage security issues before they impact your production application.