Amazon Inspector

Presented by Meghana Tammina

We have to two types of versions

~ Amazon Inspector Classic(Old version - 2016)

~ Amazon Inspector (New Version -2021)

Amazon Inspector Classic (Old Version-2016)

Amazon Inspector Classic tests the network accessibility of your Amazon EC2 instances and the security state of your applications that run on those instances. Amazon Inspector Classic assesses applications for exposure, vulnerabilities, and deviations from best practices. After performing an assessment, Amazon Inspector Classic produces a detailed list of security findings that is organized by level of severity.

With Amazon Inspector Classic, you can automate security vulnerability assessments throughout your development and deployment pipelines or for static production systems. This allows you to make security testing a regular part of development and IT operations.

Amazon Inspector Classic also offers predefined software called an agent that you can optionally install in the operating system of the EC2 instances that you want to assess. The agent monitors the behavior of the EC2 instances, including network, file system, and process activity. It also collects a wide set of behavior and configuration data (telemetry).

Why we get new version ?

What customers problems does amazon inspector solve ?

1. Built for Cloud

2. Manage vulnerabilities in near real time

3. Consolidate solution for all compute types

4. Automated patching and ticketing

~Amazon Inspector (New Version-2021)

New version of amazon inspector was introduced by

Rick Anthony- General Manager for inspector

Kashish Wadhwa- Project Manager for inspector

Automated and continual vulnerability management at scale

Immediately discover and scan AWS workloads for software vulnerabilities and unintended network exposure with a single click.

Consolidate your vulnerability management solutions for Amazon EC2, AWS Lambda functions, and container images in Amazon ECR into one fully managed service.

Use the highly accurate Inspector risk score to efficiently prioritize your remediation

.

Reduce mean time to remediate (MTTR) vulnerabilities and streamline workflow with Amazon EventBridge and AWS Security Hub integrations.

How Amazon Inspector works

Frictionless activation and management

Continual Vulnerability monitoring

Prioritized and Contextualized results

> *One-click activation*

> *Integration with AWS organizations*

> *Auto activation of new accounts*

> *Security by default with simple organization level configuration*

> *Centralized view for the administrator account,while individual accounts can view their account-specific information*
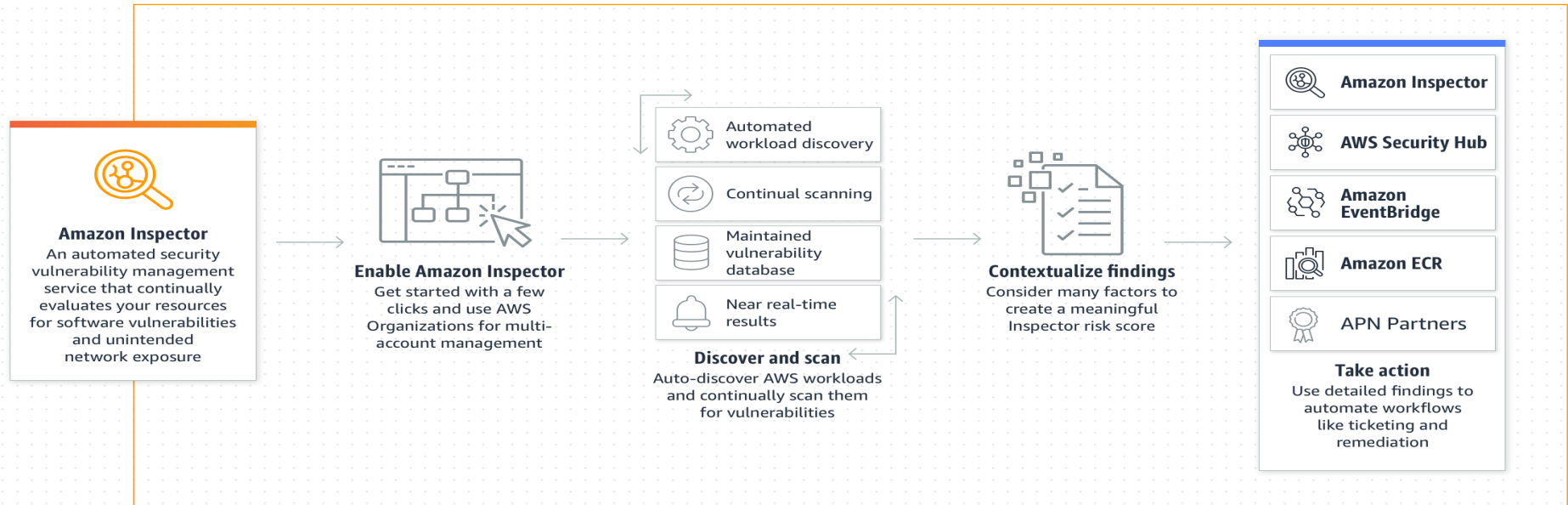
> *Automated discovery of all resources*

> *Findings in real time through continual vulnerability and network reachability Scanning*

> *Intelligent ainlgorithm determines what to scan,when to scan, or how often to scan based on event triggers:*

    ~ A new software package is installed
    ~ An instance is patched
    ~ A new CVE is published that impacts resources

> *Amazon inspector risk score is calculated for each finding correlating CVE metadata with the customer's environmental factors such as :*
    ~ Network exposure of an instance
    ~ Exploitability details
    ~ Potential security threats

> *Remediation details with ffixed-in package details*

> *Exploitability information with last known exploitation date*

Amazon Inspector is an automated vulnerability management service that continually scans AWS workloads for software vulnerabilities and unintended network exposure.

Amazon Inspector
An automated security vulnerability management service that continually evaluates your resources for software vulnerabilities and unintended network exposure

Enable Amazon Inspector
Get started with a few clicks and use AWS Organizations for multi-account management

Automated workload discovery

Continual scanning

Maintained vulnerability database

Near real-time results

Discover and scan
Auto-discover AWS workloads and continually scan them for vulnerabilities

Contextualize findings
Consider many factors to create a meaningful Inspector risk score

Amazon Inspector

AWS Security Hub

Amazon EventBridge

Amazon ECR

APN Partners

Take action
Use detailed findings to automate workflows like ticketing and remediation

Amazon Inspector pricing

Average number of Amazon EC2 instances scanned per month*

$1.2528 per instance

Number of container images scanned initially on-push to Amazon ECR per month

$0.09 per image

Number of automated rescans for container images in Amazon ECR configured for continuous scanning per month

$0.01 per rescan

Average number of AWS Lambda functions scanned per month**

$0.30 per Lambda functions

With Amazon Inspector, you pay only for what you use, with no minimum fees and no upfront commitments.

Equivalent resource of amazon inspector in GCP –

Google cloud security command center(cloud SCC)

Equivalent resource of amazon inspector in Azure -

Azure security center

Thank You !