AWS re:Invent

NOV. 29 – DEC. 3, 2021 | LAS VEGAS, NV

SEC305-R2

Automate vulnerability management with Amazon Inspector

Rick Anthony
General Manager, Amazon Inspector
Amazon Web Services

Kashish Wadhwa
Product Manager, Amazon Inspector
Amazon Web Services

Ankit Kumar
Security Engineering
Uber

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Agenda

What security teams are saying about vulnerability management

Our approach to vulnerability management

How the new Amazon Inspector makes vulnerability management easier

Uber’s journey with Amazon Inspector

Demo

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

What security teams are saying about vulnerability management

1. Traditional vulnerability management solutions are not built for cloud; given the pace at which new resources are launched and terminated, we often miss scanning workloads for vulnerabilities, especially ephemeral resources

2. We spend a lot of time on deploying vulnerability management solutions, managing yet another security agent, and manually prioritizing the results

3. We want to scan 100% of our environment, but we spend a significant amount of time trying to discover our entire ecosystem and build custom dashboards to monitor the coverage

4. While we want to present the vulnerabilities to individual application development teams in the easiest way possible, we don't want to give them complete access to security tools and would rather push results to tools they use in their day-to-day lives; for example, Amazon Elastic Container Registry (Amazon ECR) to remediate the identified vulnerabilities

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

AWS approach to vulnerability management

We had **2 key philosophies** while designing the new Amazon Inspector service

1. Security teams should not be focused on upfront activities for vulnerability management activities such as deploying a solution, managing security tools, and even completing initial analysis and triage to prioritize what to remediate first; instead, security teams should focus on managing remediation of these findings
2. Security teams need not worry about what to scan, when to scan, or how often to scan – a solution should be intelligent enough to determine that while providing the best security value

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Amazon Inspector continual vulnerability management for scale

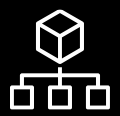
Now supports scanning of container images and Amazon EC2 instances

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

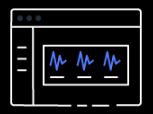
How the new Amazon Inspector makes vulnerability management easier

Philosophy #1

Security teams should not be focused on upfront activities for vulnerability management activities such as deploying a solution, managing security tools, and even completing initial analysis and triage to prioritize what to remediate first; instead, security teams should focus on managing remediation of these findings



Simplified one-click enablement and multi-account support with AWS Organizations



A single pane of glass for vulnerabilities across all resources, including EC2 instance and container images



Amazon Inspector

Highly contextualized Amazon Inspector score calculated for each finding for easy prioritization



Use widely adopted AWS Systems Manager (SSM) Agents for EC2 scans



aws

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

How the new Amazon Inspector makes vulnerability management easier

Philosophy #2

Security teams need not worry about what to scan, when to scan, or how often to scan – a solution should be intelligent enough to determine that while providing the best security value



© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Deep dive on key Amazon Inspector features

1. Frictionless one-click enablement and multi-account support with AWS Organizations

- ✓ 1-click enablement
- ✓ Integration with AWS Organizations
- ✓ Centralized view for the administrator account, while individual accounts can view their account-specific information
- ✓ Individual application teams can also view container-related findings in the Amazon ECR dashboard

2. Continual vulnerability and network reachability scanning

- ✓ Automated discovery of all resources
- ✓ Findings in real time through continual vulnerability and network reachability scanning
- ✓ Intelligent algorithm 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

3. Highly contextualized Amazon Inspector risk score

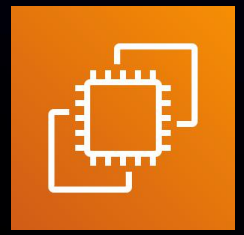
- ✓ Inspector risk score is calculated for each finding by correlating CVE metadata with the customer's environmental factors such as
  - ✓ Network exposure of an instance
  - ✓ Exploitability details
  - ✓ Potential security threats

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Uber’s journey with Amazon Inspector

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

A look at our compute environment



- Fleets of EC2 instances in use
- Long-lived as well as ephemeral instances spread across multiple
  - Regions
  - Accounts
  - Organizations



- Use-case specific images in use
- Heterogenous OS flavors

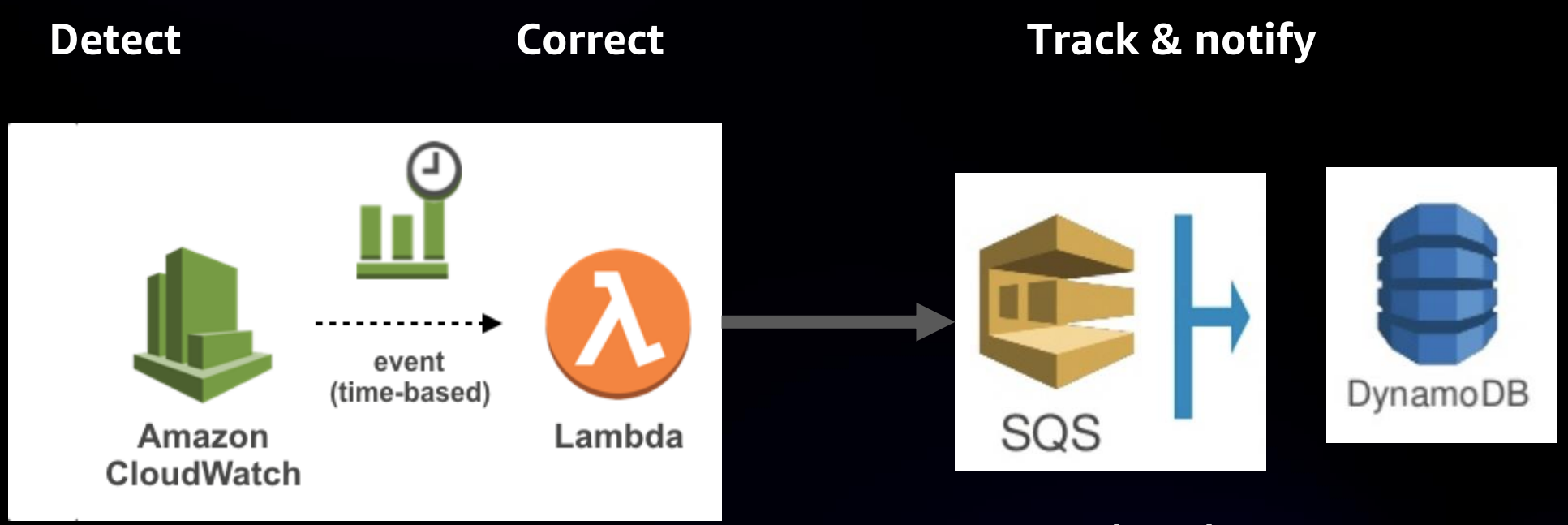
© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Challenges with vulnerability management

- Heterogenous instances across multitude of AWS accounts
- Agent management
- Image scanning
- Centralized real-time visibility
- Patch management

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

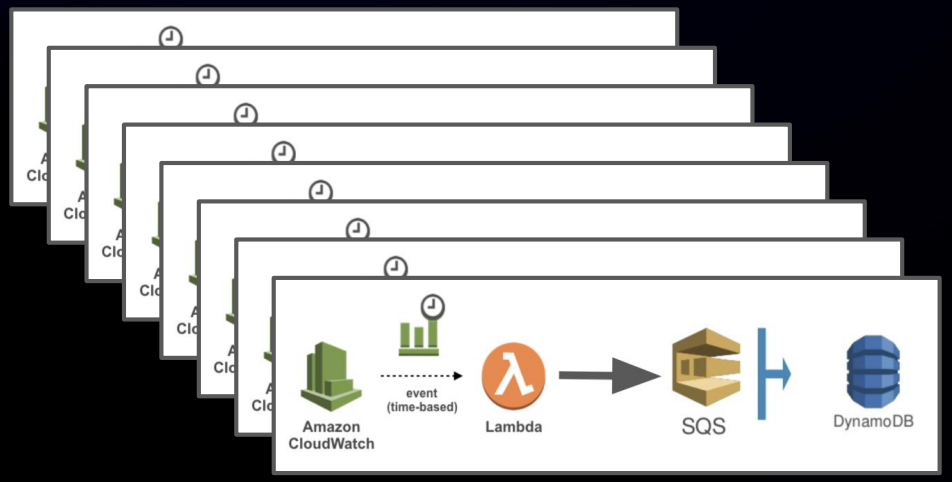
We use continuous, automated monitoring to detect changes to evolving usage patterns



Use cloud resources to secure cloud resources!

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Integration with Amazon Inspector Classic

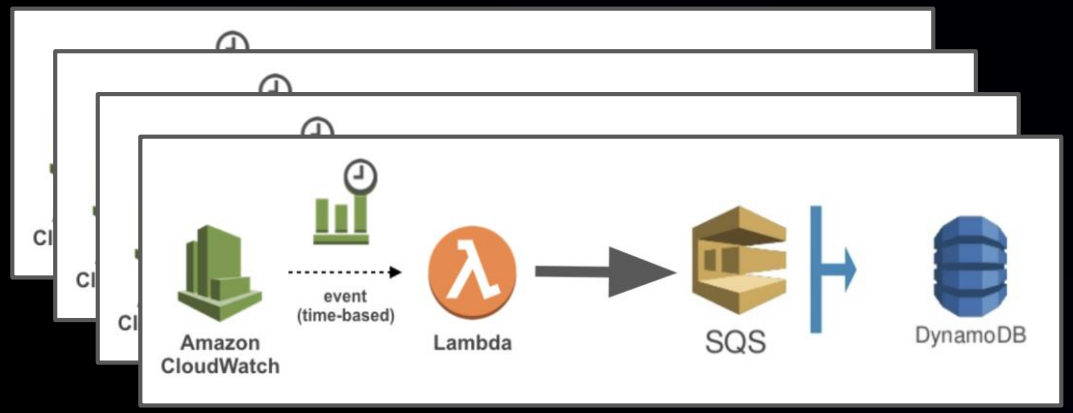


x All Regions x All accounts

- Create assessment target
- Create assessment template
- Create SNS topic and subscriptions for feedback
- Run assessment
- Get findings

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

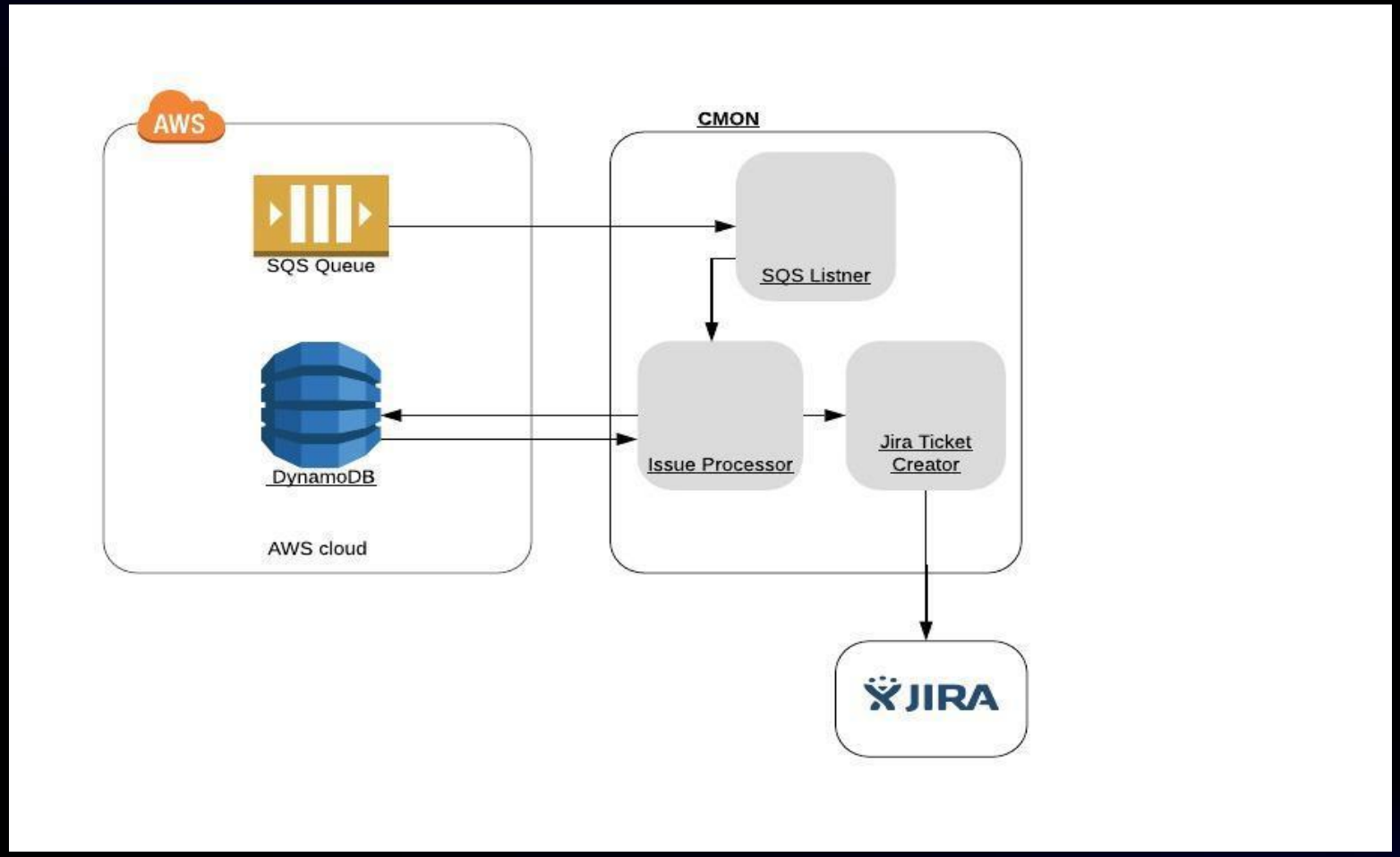
Integration with the new Amazon Inspector



Call GetFindings API

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Ticketify findings



© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Ticketify findings



Cloud Monitoring / CMON-44203

Authenticated Vulnerability Scan has detected "Critical" vulnerabilities in your AWS EC2 instance "i-0e823217fddcadad"

Edit | Comment | Assign | More | Reopen

Details

Type:	Bug	Status:	RESOLVED (View Workflow)
Priority:	Level 5	Resolution:	Done
Labels:	VULNS authenticatedscanfindings aws hammer inspector2_scanner unotify-monitor		
Data Source:	inspector2_scanner		
Incident Level:	Critical		
Account Number:	905547224245		
Resource Link:	https://us-east-1.console.aws.amazon.com/ec2/v2/home?region=us-east-1#Instances:search=i-0e823217fddcadad;sort=instanceId		
Tracking Number:	prod-hammer-inspector2-scan-findings:905547224245:i-0e823217fddcadad:critical		
Issue Category:	AWS Incident		
Value:	1,214		
Business Value:	0		

Click to edit

People

Assignee:	Ankit Kumar
Reporter:	svc-cloudmonitor
CC List:	Ankit Kumar
Votes:	0 Vote for this issue
Watchers:	0 Start watching this issue

Dates

Created:	17/Sep/21 9:14 AM
Updated:	30/Nov/21 2:48 PM
Resolved:	18/Sep/21 9:14 AM

Request Exception

Request Exception

Development

Create branch

Agile

View on Board

Slack

Elevator

There are no Elevator rosters available for this issue

Description

SLA

Risk Level	Fix Timeline	What to Do?
Critical	5 days	Fix issue as soon as possible - divert engineer effort if needed and loop in the Incident Response team to ensure no previous exploitation has occurred.

Vulnerability Details

Id	Severity	Recommendation
CVE-2021-13217 - linux-image-amd32	Critical	Update all packages in the vulnerable packages section to their latest versions.
CVE-2020-81371 - librtmp	Critical	Update all packages in the vulnerable packages section to their latest versions.
CVE-2019-202360 - python-urllib3	Critical	Update all packages in the vulnerable packages section to their latest versions.

Note: Multiple tickets representing varying levels of severity might have been opened for the same Instance. Resolving highest severity ticket first is highly suggested as it has cascading effect which may resolve lower severity vulnerabilities too.

Remediation Details

What is wrong and how to fix

This ticket is created because in our last authenticated vulnerability scan, we discovered that one of your cloud hosts has active vulnerabilities. As per our compliance requirements, all of our compute endpoints must not have any active vulnerabilities. Failure to comply with this requirement can put our compliance status at risk. For details on the vulnerability and how to fix, please refer to the Inspector Scan Findings TeamDot.

Instructions for handling this JIRA ticket

Assign a member of your team who can make this simple change. Or better yet, be a #securityhero and do it yourself! **Deploy the fix using the steps described above and change the ticket status to 'Fixed by Customer'. Please do not resolve the ticket once the fix has been deployed** as we want the monitoring solution to verify the fix and resolve the ticket automatically.

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Any prerequisites?

Yes, just one



Cloud Monitoring / CMON-44123

Your EC2 Instance i-0e823217fddcadad is Unmanaged

Edit | Comment | Assign | More | Reopen

Details

Type:	Bug	Status:	RESOLVED (View Workflow)
Priority:	Level 3	Resolution:	Done
Labels:	aws hammer ssh_ssm_analyzer unotify-monitor		
Data Source:	ssh_ssm_analyzer		
Incident Level:	Medium		
Account Number:	905547224245		
Resource Link:	https://us-west-2.console.aws.amazon.com/ec2/v2/home?region=us-west-2#Instances:search=i-0e823217fddcadad;sort=instanceId		
Tracking Number:	prod-hammer-unmanaged-ec2-instances-findings:905547224245:i-0e823217fddcadad		
Issue Category:	AWS Incident		
Value:	1,400		
Business Value:	0		

Description

Instance Details

Account ID	Instance ID	Public IP	SSH Key	Agent Status
905547224245	i-0e823217fddcadad	34.233.44.69	cloudsectest	notconnected

What does this mean? All active EC2 Instances are required to have a running SSM Agent. We could not initiate a connection with the agent in this Instance.

What do I need to do? We have setup the permissions for you. All you need to do is SSH into your instance, check the agent status and enable it if already installed following the guide here, or install the agent if not present following this guide.

How would this benefit me? No more SSH key management overhead. SSH into your instances directly using AWS console or via CLI using AWS Single Sign-On keys (**Note**: Make sure you are in us-west-2 region by running **export AWS_DEFAULT_REGION=us-west-2**).
Check out all the other features here.

If you need help from CloudSec, please reach out to the public cloud security Slack channel.

People

Assignee:	Ankit Kumar
Reporter:	svc-cloudmonitor
CC List:	Ankit Kumar
Votes:	0 Vote for this issue
Watchers:	1 Start watching this issue

Dates

Created:	14/Sep/21 9:12 AM
Updated:	30/Nov/21 2:37 PM
Resolved:	17/Sep/21 9:12 AM

Request Exception

Request Exception

Development

Create branch

Agile

View on Board

Slack

Elevator

There are no Elevator rosters available for this issue

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Metrics-driven evaluation



Amazon Inspector

- 90% reduction in time to deploy
- Manual overhead to manage the solution reduced by 40%
- Closed 87% of critical vulnerabilities within SLA
- Rescan result to end user reduced to under an hour

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Future work



Amazon Inspector

- Feed data to elastic search engine
- Auto remediate vulnerabilities on SLA breach
- Auto installation workflow for Systems Manager agents
- Migration to patched AMI
- Central integration for mergers & acquisitions

aws

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Resources

Uber’s continuous monitoring solution
https://medium.com/@ubersecurity/part-1-aws-continuous-monitoring-f39f81ea6801
https://medium.com/@ubersecurity/part-2-aws-monitoring-case-studies-9fbc613aff28

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Partners

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Partners

Vulnerability prioritization

rezilion VULCAN.

Vulnerability data provider

snyk

Cloud security management

paloalto NETWORKS WIZ

cavirin AN SRA COMPANY

Attack surface management

AXONIUS XM CYBER



Amazon Inspector

Detection and response

SentinelOne

FIREEYE SOPHOS Cybersecurity evolved.

Security event management

IBM Security sumo logic

Managed security services

Deloitte. CloudHesive

aws

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Thank you!

Kashish Wadhwa
LinkedIn: kashishwadhwa

Ankit Kumar
LinkedIn: ankit-cybersec

Rick Anthony
LinkedIn: rick-anthony

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.