RSAConference2022
San Francisco & Digital | June 6 – 9

TRANSFORM

SESSION ID: CSCS-W01

Shift-left! Scanning for Security Compliance from Day Zero

Joe McCrea
DevOps Engineer
SAP

Rohit Joshi
SecDevOps Engineer
SAP

Disclaimer

Presentations are intended for educational purposes only and do not replace independent professional judgment. Statements of fact and opinions expressed are those of the presenters individually and, unless expressly stated to the contrary, are not the opinion or position of RSA Conference LLC or any other co-sponsors. RSA Conference does not endorse or approve, and assumes no responsibility for, the content, accuracy or completeness of the information presented.

Attendees should note that sessions may be audio- or video-recorded and may be published in various media, including print, audio and video formats without further notice. The presentation template and any media capture are subject to copyright protection.

RSAConference2022

Introduction

Misconfigurations?

Errors in the configuration of resources hosted on the cloud, leaving it vulnerable.

For example:

- There is critical information stored in a storage bucket.
- When configuring the bucket, a mistake was made, making it public.
- This information is now available for anyone to access.

The Numbers

Survey from Vugue on incidents caused by cloud misconfiguration:

- **73%** of organisations citing more than **10 per day**.
- **36%** citing more than **100 per day**.
- **10%** citing more than **500 per day**.

https://www.fugue.co/press/releases/fugue-survey-finds-widespread-concern-over-cloud-security-risks-during-the-covid-19-crisis

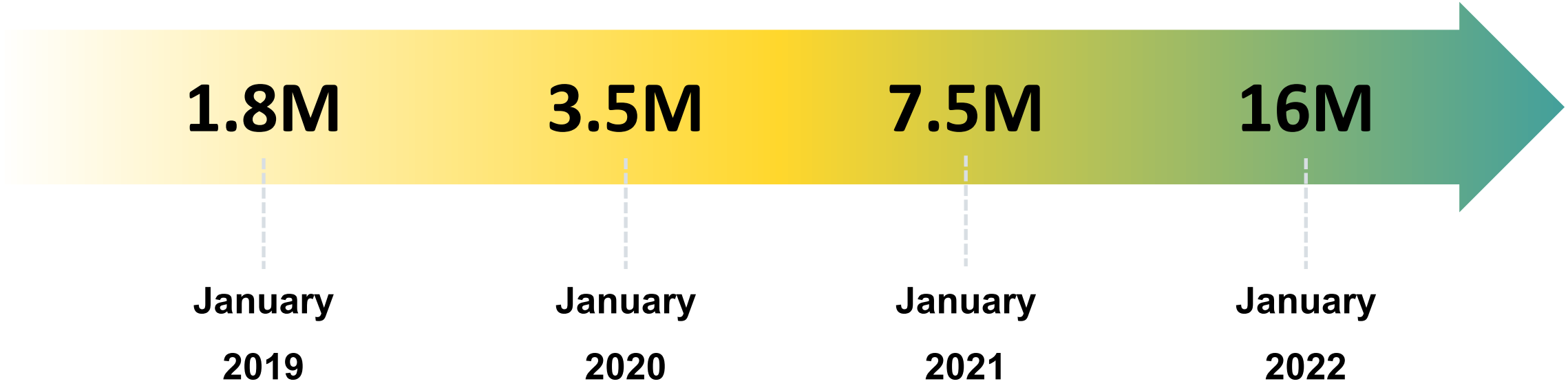
Policies to detect misconfigurations

- A policy is released, which shows how information should be securely stored within storage buckets.
- It shows how to encrypt the information stored, as well as how the access policy should be written in order to keep the information private.
- But how do we enforce this?

Manually enforced policies

- An option may be to access the cloud account and manually check that the policy is being followed.
- Open to human-error, as something may be missed.
- This would be fine in the situation where your organisation has a small number of accounts.

SAP's Public Cloud Growth



RSAConference2022

Policy Implementation at SAP scale

Dealing with Misconfigurations at Scale

- Take existing policies
- Convert to code
- Execute against account
- Scale it up
- Report findings to the appropriate people

Sample Policy

- All data in buckets should be encrypted
- All policies for bucket access should be private

Policy -> Code

```
describe bucket(bucket_id: id)
    it should not be public
    it should be encrypted
end
```

Technical Demo

Results

Good configuration

- Private and Encrypted buckets

```
✓ storage_buckets_private_and_encrypted: Storage buckets should not be public and default encryption must be enabled
  ✓ S3 Bucket inspec-tf-enc-test-983346b0 is expected not to be public
  ✓ S3 Bucket inspec-tf-enc-test-983346b0 is expected to have default encryption enabled
  ✓ S3 Bucket inspec-tf-priv-test-983346b0 is expected not to be public
  ✓ S3 Bucket inspec-tf-priv-test-983346b0 is expected to have default encryption enabled
```

Bad configuration

- Public and Un-encrypted buckets

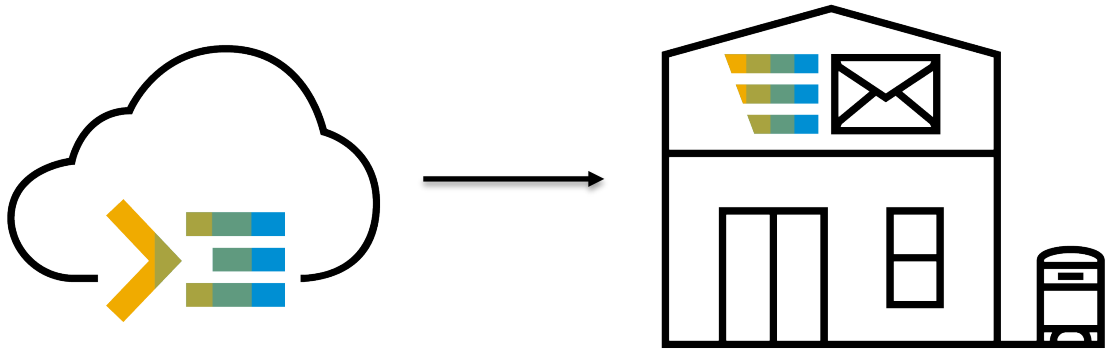
```
× storage_buckets_private_and_encrypted: Storage buckets should not be public and default encryption must be enabled (4 failed)
  × S3 Bucket inspec-tf-pub-test-176848d0 is expected not to be public
  expected `S3 Bucket inspec-tf-pub-test-176848d0.public?` to be falsey, got true
  × S3 Bucket inspec-tf-pub-test-176848d0 is expected to have default encryption enabled
  expected `S3 Bucket inspec-tf-pub-test-176848d0.has_default_encryption_enabled?` to be truthy, got false
  × S3 Bucket inspec-tf-unenc-test-176848d0 is expected not to be public
  expected `S3 Bucket inspec-tf-unenc-test-176848d0.public?` to be falsey, got true
  × S3 Bucket inspec-tf-unenc-test-176848d0 is expected to have default encryption enabled
  expected `S3 Bucket inspec-tf-unenc-test-176848d0.has_default_encryption_enabled?` to be truthy, got false
```

RSAConference2022

Scaling up!

Listing Accounts – 'Dispatcher'

- Reach out to API of Cloud Provider.
- Request all accounts that are under the SAP organization.
- Attach metadata to account IDs.
- Sends the list of accounts to a message queue to be scanned.



Scanning Accounts – 'Scanner'

- Wrap the scanning executable in a container
- Make the workload stateless

Inputs

Message created by dispatcher, retrieved from the message queue.

Secrets retrieved from Secret Manager.

Scanning workload

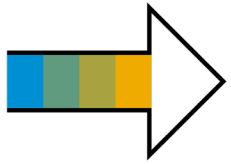
Executes previously demonstrated tests, gets compliance status of each resource, generates a report of the current compliance status of account.

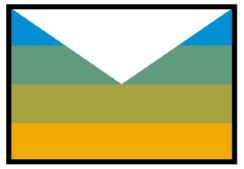
Outputs

Report on the configuration status of each resource in account, attached to the input message from queue.

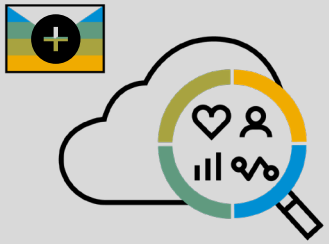
Put it in Kubernetes!

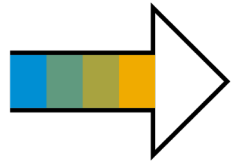
kubernetes

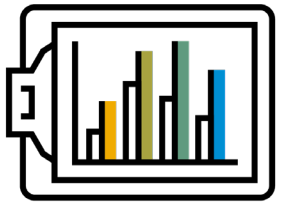


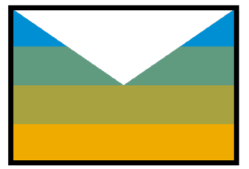


Cloud ID & Metadata



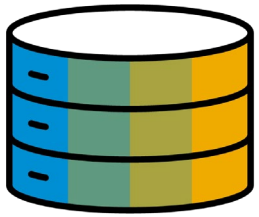




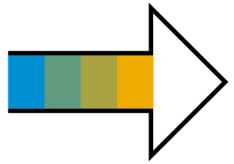


Cloud ID & Metadata
+ Compliance Report

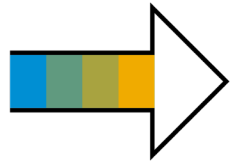
Reporting the Results Produced

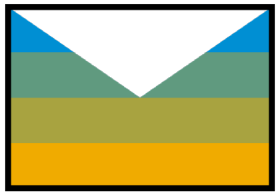


Reports produced with cloud compliance report and metadata



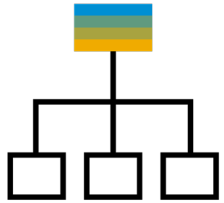
Based on metadata, we can determine account ownership





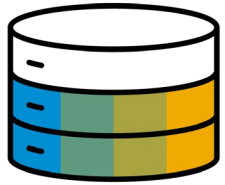
Inform relevant people for the account with their compliance report

Reporting to Engineering Teams



Executive Reporting

Data Exports



API Access

Dashboards

RSAConference2022

Putting the tools in the hands of developers

Shifting Security to the Left

- As the solution is in a container, with standard inputs and outputs, we are able to distribute this out to teams within SAP.
- Packaged along with the documentation, we can distribute this out for use in CICD pipelines across the company.
- This allows teams to shift security to the left, meaning they can detect these misconfigurations during the development phase.

Developer Workflow

- User makes changes to infrastructure as code
- Changes are run via CICD pipeline
- Verify changes using scanning image, revert if necessary

RSAConference2022

Next steps

Shifting left in six months

- Next week you should:
  - List the security policies your organisation needs to implement.
- In the first three months following this presentation you should:
  - Convert these to code and not just plain text, use a tool of choice. (Make these clear cut!)
- Within six months you should:
  - Figure out who needs this info and scale it up!

Disclaimer

Presentations are intended for educational purposes only and do not replace independent professional judgment. Statements of fact and opinions expressed are those of the presenters individually and, unless expressly stated to the contrary, are not the opinion or position of RSA Conference LLC or any other co-sponsors. RSA Conference does not endorse or approve, and assumes no responsibility for, the content, accuracy or completeness of the information presented.

Attendees should note that sessions may be audio- or video-recorded and may be published in various media, including print, audio and video formats without further notice. The presentation template and any media capture are subject to copyright protection.