CLOUD CUSTODIAN

AND

A CORPORATION'S JOURNEY TO THE CLOUD

Jamison Roberts – Lead DevOps Engineer
Cloud Custodian User & Fanatic since 2017

Contact me on in or at JamisonRoberts83@gmail.com

OUR JOURNEY TO THE CLOUD

Security & Compliance

Near real-time remediation or termination of resources created with bad configurations

- Unencrypted -> encrypted / terminate
- Ssl3 / tls1 / tls1.1 -> tls1.2
- Public -> internal / terminate
- logging off -> on
- S3 data exfiltration attempt -> locked s3 bucket
- public sg -> remove public rule
- Root / external IP login / access attempt -> notify security and admins

OUR JOURNEY TO THE CLOUD

Standardization across accounts

- IAM user password requirements
- CloudTrail and Flow Log configurations
- Standardized base policy set across all accounts
- Customer contributed policy sets
- Canary, Non-Prod, and Prod releases using c7n-org config yaml tags

OUR JOURNEY TO THE CLOUD

Cost Savings

- Off-Hours gives customers easy solution via tag to save tons of $ on dev EC2 servers and ASGs. Only running servers 8 hours per day Monday-Friday saves 75% on compute costs each week
- Identify, notify, mark unused resources, follow up with customers again and delete them if still unused

OUR JOURNEY TO THE CLOUD

Metrics For Dashboards

- Helped us visually discover anomalies
- Saved us $$$$ on error looping Lambdas
- Identifies winning / struggling customers
- Gives upper management a visual on how different business units are doing in the cloud

OUR JOURNEY TO THE CLOUD

Real world struggles implementing controls and standards

- With a large global customer base, keeping up with their needs and the pace they want to develop and innovate can be challenging
- Having a large cloud presence with hundreds of accounts and growing, numerous global business units, and lots of production resources made it nearly impossible for us to deploy new policies and keep up with new securing new accounts
- Even the slightest of change in the cloud environments or processes could be very disruptive to business and could cause headaches for everyone (customers often have to update thousands of CFTs when we introduce new requirements so that their resources are compliant with our policies)

OUR JOURNEY TO THE CLOUD

How we overcame these issues

- We got global backing from senior management, security teams, divisional security officers and anyone else that could back us.
- We created a monthly scheduled release plan
  - Documented which policies we will be deploying each month
  - Documented the dates each month for Canary, Non-Prod, and Prod releases, leaving a week between Non-Prod and Prod for customer feedback and to correct any issues
  - Documented release plans for over 1 year in advance for non-critical items.
  - Hosting bi-weekly conference calls where we go over the next release cycle and encourage ALL developer groups and relevant parties to join. Get customer feedback.

OUR JOURNEY TO THE CLOUD

How we overcame these issues

- Cloud Custodian allowed us to create our guardrails and remediation controls very quickly via YAML policies as they are often very easy to write
- With c7n-org we are able to implement and deploy our policies to all accounts (or a filtered subset) in a fraction of the time it would take to write and deploy a custom solution
- Daily deployments and real-time deployments to new accounts ensure consistent experience for customers and enforces our desired state

ANY QUESTIONS?

Jamison Roberts – Lead DevOps Engineer
Cloud Custodian User & Fanatic since 2017

Contact me on in or at JamisonRoberts83@gmail.com