aws SUMMIT

Automation for IR Workflows

DEV06

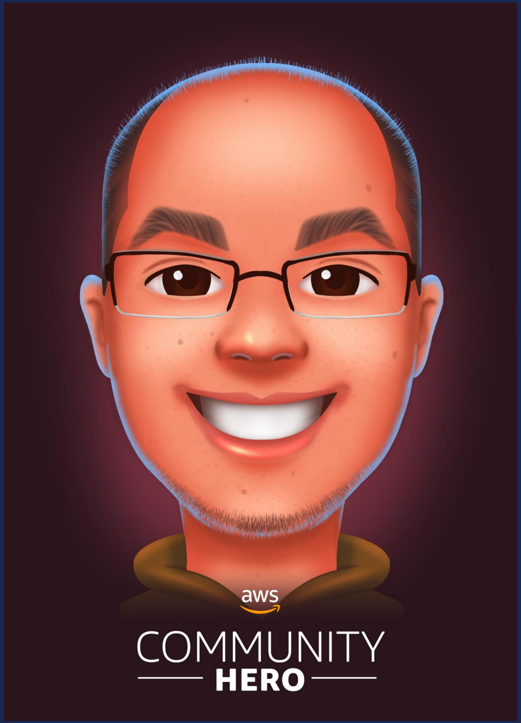
About me

Community:

- AWS Community Hero
- Founder:
  - AWS SP UG
  - Cloud Girls

Professional:

- SRE @ Certain.com



Agenda

A bit about automation
Before start (homework)
How AWS can help us
Anatomy of a response
Responding to an incident
Examples
Resources
References

A bit about automation

- It's not all about security
- Time "saving"
- Avoid burn-out
- Baby sitting
- Avoid sleep hours calls (on-call)
- Might break

Before start (homework)

- AWS Systems Manager
- Cloudtrail
- Guard Duty
- Config
- Logs
- Integrations

How AWS can help us

- Lambda
- Step Functions
- SNS
- Guard Duty
- Macie
- Cloudwatch
- Flow logs
- Blogs and more..

Anatomy of a response

- Incident
- Containment: Runbook
- Extract import data (logs, data, etc)
- Lookup contact info
- Notify contact
- Offer support and more info
- Report generation
- Forensic analysis (optional)

No human has been bothered!

Responding to an incident

- Cloudtrail
- Invalid Login
- Public S3 Bucket
- Website defacement

Demo

- Cloudtrail
- Login

Ideas/Examples

- Alexa
- IoT Button
- Slack
- Zapier
- Sage Maker

Recursos

- https://github.com/awslabs/aws-security-automation
- https://thehive-project.org/
- https://www.cyphon.io/
- https://wazuh.com/
- https://threatresponse.cloud/
- https://github.com/Netflix/security_monkey
- https://github.com/mozilla/mig

References

- SEC403 - https://www.youtube.com/watch?v=M5yQpegaYF8
- SID302 - https://www.youtube.com/watch?v=e6sokCFRlns
- SEC313 - https://www.youtube.com/watch?v=x4GkAGe65vE
- SEC327 - https://www.youtube.com/watch?v=vtMCjyE5nms
- https://aws.amazon.com/pt/blogs/publicsector/building-a-cloud-specific-incident-response-plan/
- https://www.youtube.com/watch?v=3phjk1CxhXM

Q&A

Thanks!!!

@franciscoed

https://medium.com/@franciscoed

https://github.com/franciscoed