

# Automação de resposta a incidentes na AWS

## DEV06

# About me

Community:

AWS Community Hero

Founder:

AWS SP UG

Cloud Girls

Professional:

SRE @ Certain.com



# Agenda

Sobre automação

Lição de casa

Como a AWS pode nos ajudar

Anatomia de uma resposta

Resposta a incidente

Exemplo

Recursos

Referências

# Sobre automação

- Não somente resposta a incidentes
- "Salvar" tempo
- Evitar burn-out
- Baby sitting
- Evitar ser acordado durante o on-call
- May break

# Lição de casa

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

# Como a AWS pode nos ajudar

- Lambda
- Step Functions
- SNS
- Guard Duty
- Macie
- Cloudwatch
- Flow logs
- Blogs e etc..

# Anatomia de uma resposta

- Incidente
- CONTER: Runbook
- Extrair dados importantes (logs, dados, etc)
- Mapear contatos
- Notificar o contato
- Oferecer suporte e mais informações
- Gerar relatório
- Forense (opcional)

Nenhum ser humano foi incomodado

# Resposta a incidente

- Cloudtrail
- Login incorreto
- Bucket público
- Site invadido



# Demo

- Cloudtrail
- Login

# Idéias

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

# Recursos

- <https://github.com/aws-labs/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/Netflix/security_monkey)
- <https://github.com/mozilla/mig>

# Referências

- 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=3phjk1CxbXM>

# Q&A

# Obrigado!!!

@franciscoed

<https://medium.com/@franciscoed>

<https://github.com/franciscoed>