DAREDE
à nuvem

Automação de resposta a incidentes na AWS

Sobre

Community:

AWS Community Hero

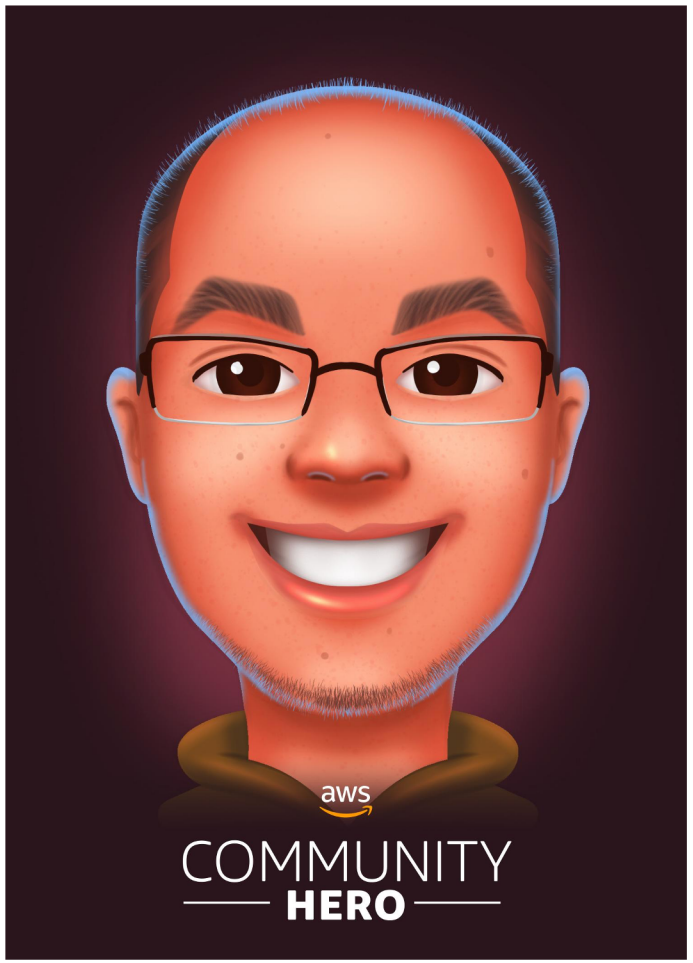
Founder:

AWS SP UG

Cloud Girls

Professional:

SRE @ Certain.com



DAREDE à nuvem

Agenda

Sobre automação
Lição de casa
Como a AWS pode nos ajudar
Anatomia de uma resposta
Resposta a incidente
Exemplo
Recursos
Referências

DAREDE à nuvem

Sobre automação

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

DAREDE à nuvem

Lição de casa

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

DAREDE à nuvem

Como a AWS pode nos ajudar

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

DAREDE à nuvem

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)

NOTA: Nenhum ser humano foi incomodado

DAREDE à nuvem

Resposta a incidente

- Cloudtrail
- Login incorreto
- Bucket público
- Site invadido

DAREDE à nuvem

DEMO

- Cloudtrail
- Login

Idéias

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

DAREDE à nuvem

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

DAREDE à nuvem

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=3phjk1CxhXM

DAREDE à nuvem

Dúvidas

DAREDE à nuvem

Contatos

https://medium.com/@franciscoed

https://github.com/franciscoed

https://twitter.com/franciscoed

OBRIGADO!