Event Driven Security in AWS with Lambda

WIFI: Holiday_Inn_Conf / Serverless

A CLOUD GURU

trek10

A CLOUD GURU

Jared **Short**

Aaron **Caito**

Agenda

A CLOUD GURU

9:00	Introduction & Agenda
9:30	**Lesson 1**
10:30	10 min break
10:40	**Lesson 2**
11:40	10 min break
11:50	**Lesson 3**
12:30	Lunch
1:30	Lesson 3 (cont)
2:00	10 min break
2:10	**Lesson 4**
3:10	10 min break
3:20	**Recap and discussion**
4:45	Goodbye!

Outcomes

A CLOUD GURU

- Security with Serverless
- Understanding Event Driven Security
- Methods of Event Driven Security
- Security of Serverless

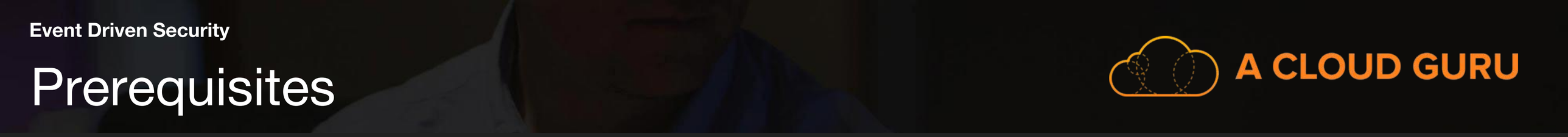
Lesson Structure

A CLOUD GURU

Lesson 1	Restricted Access
Lesson 2	Bad IPs
Lesson 3	Compromised Servers
Lesson 4	Bad Config

10 minute introduction
40 minute practical work
10 minute debrief

Prerequisites



A CLOUD GURU

- An **AWS** Account w/ Admin
  (some small charges may be incurred as a result of this workshop)
- AWS **CLI** set up (& term)
- **Can Do** attitude

First step… download

A CLOUD GURU

https://github.com/trek10inc/event-driven-security

or if you are lazy like me

bit.ly/e-d-s

bit.ly/install-aws-cli

What is Event Driven Security?

What is Event Driven Security?

A CLOUD GURU

- Security events and response
- Security automation
- Blocking the known (when we know it)

Why Event Driven Security?

A CLOUD GURU

- Traditional perimeter defence is not enough

Why Event Driven Security?

A CLOUD GURU

- Prevention is best, but fast response is just as important
- Access to live, automatable, reliable data...

Key AWS Services

CloudWatch, Logs, Events

CloudTrail

WAF

VPC **Flowlogs**

AWS **Config**, Rules

Lambda, lambda, lambda!