Implementation of a SOC service in the Cloud for the Cloud

How to secure and manage the Spacefinder App

Aristide Bouix, IT Security Consultant

AWS Solutions Architect Associate Certified

September 14th, 2017

devoteam

Innovative technology consulting for business

Table of Contents


1
SpaceFinder
Presentation

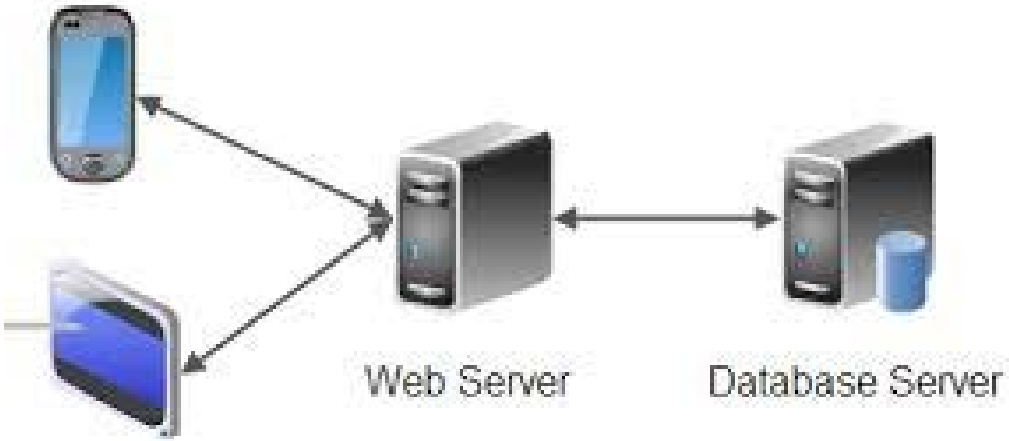
SpaceFinder

An application presented during the Re:Invent 2016 event

Github: /awslabs/aws-serverless-auth-reference-app

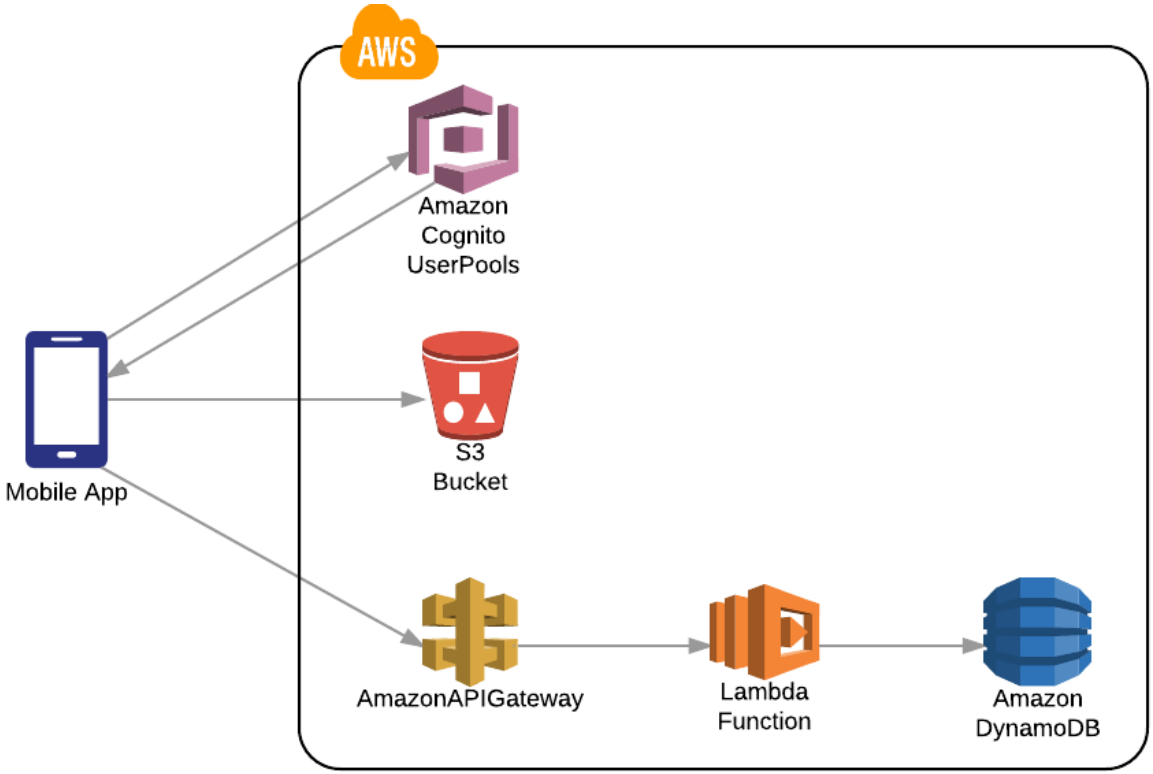
SpaceFinder

What it would look like on-premise



SpaceFinder

What it looks like in real

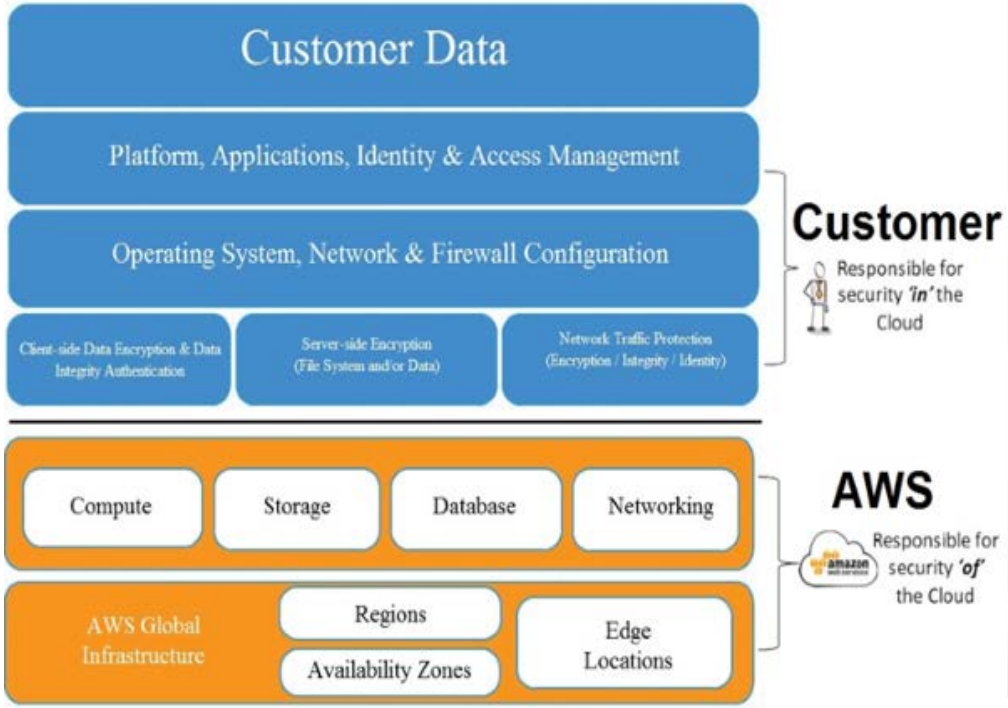


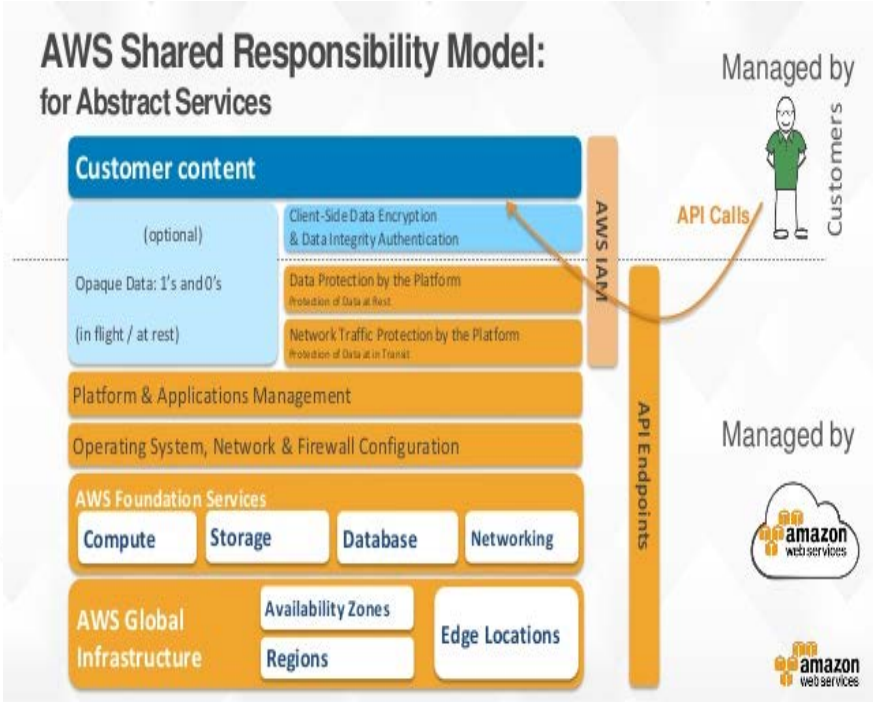
2

Serverless Specificities

Serverless

What does Serverless mean?





Why choosing a Serverless Application

- Low layers level protection already enforced by AWS
- Fewer types of attacks to look for
- Allow to focus only on your application functionalities
- Attractive prices
- Future is serverless! (aws.amazon.com/startups/)

What security is AWS already providing us?

AWS BlackWatch :anti-DDOS protection on every Datacenter and Edge Location

Native transport layers attack mitigation, such as:

- UDP Reflexion
- UDP Floods
- TCP SYN Floods

Used indicators (packets size, destination ports, source addresses, no ACK response …)

7th layers Endpoints protection mechanismes: request throttling with predefined limits (1000 rps for API Gateway), authorizations using Signature Version 4 (SHA-256 HMAC with a secret access key), endpoint are directly sized and monitored by AWS, connexion to the Internet is automatically done via TLS 1.2 and the s2n library...

What we still have to do?

Application level security:

- Secure services access through AWS IAM
- Secure AWS access keys for CLI API access
- Configuring roles (For instance to allow your Application to write in CloudWatch)
- Updating the “server” side code and enabling logging
- Throttling some API calls in API Gateway (methods without authentication)

3

Attack Approach

Attack

Model Weakness

Pricing:

- S3 is charged according to the number of accessing requests as wall as for the quantity of stored data
- Lambda is billed per invocation (execution duration + used memory)
- API Gateway is billed following the number of authenticated requests (GET ‘\login’) :
  - 1000 * 3600 * 24 * 31 * $3.50 / 1000000 ~ $9k per month

Limited protection at the applicative level, some attacks remain valid in Serverless :

- NoSQL injections at DynamoDB level
- Forged queries

A Successful Cloud Attack = Maximal Billing


4
Detection
Infrastructure

Detection

Some Best Practices

User ⇒ Human
Service ⇒ Role

Never give an API key to a service

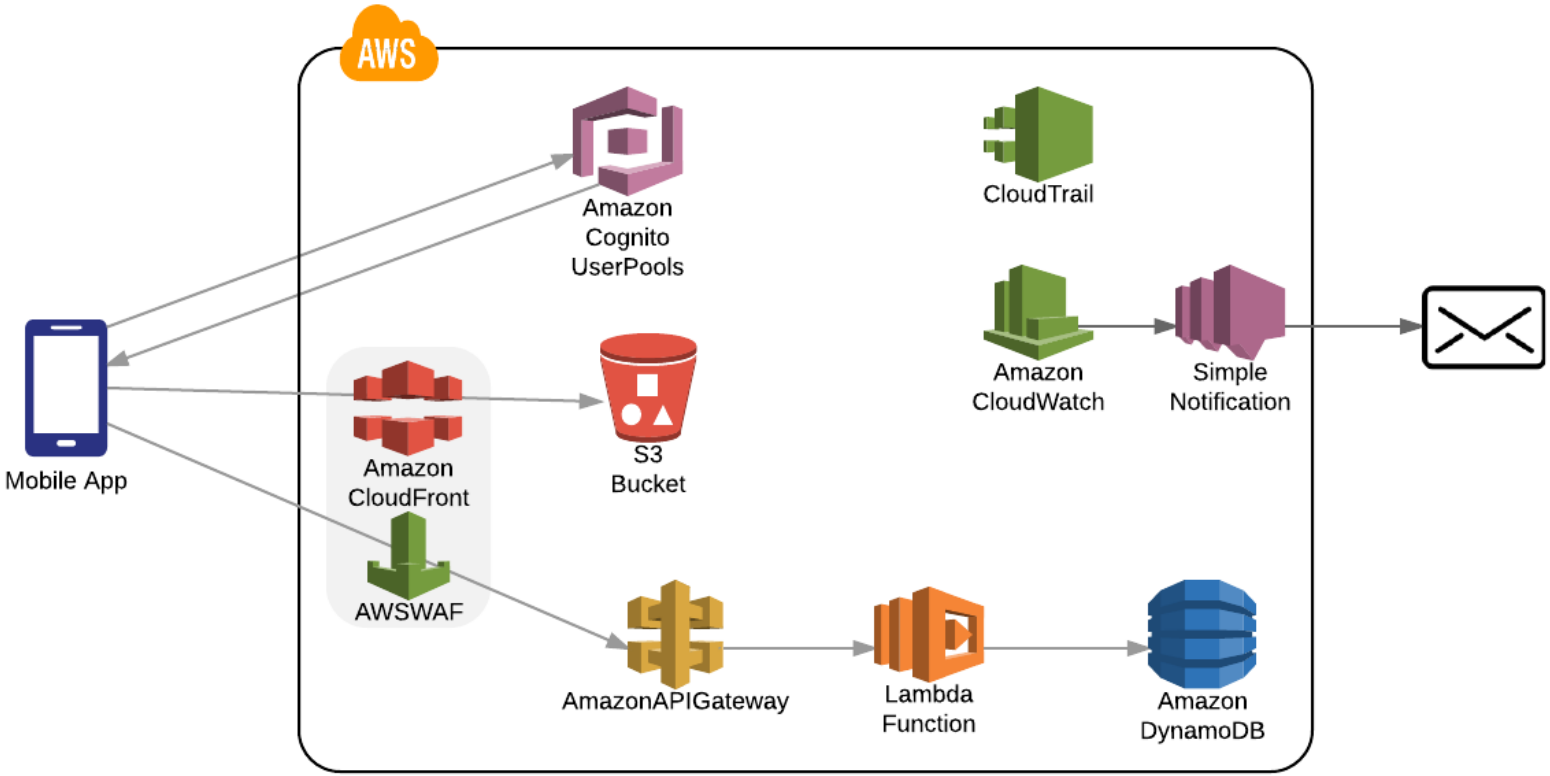
Always give minimal permissions, adding is easier than removing.

Proscribe the use of Root Account and FullAccess policy, segregate user permissions according to their function (Developer, SysOps, Compliance …)

Fundamental services to control: IAM and Cloudtrail

Detection

A Resilient Infrastructure



Detection

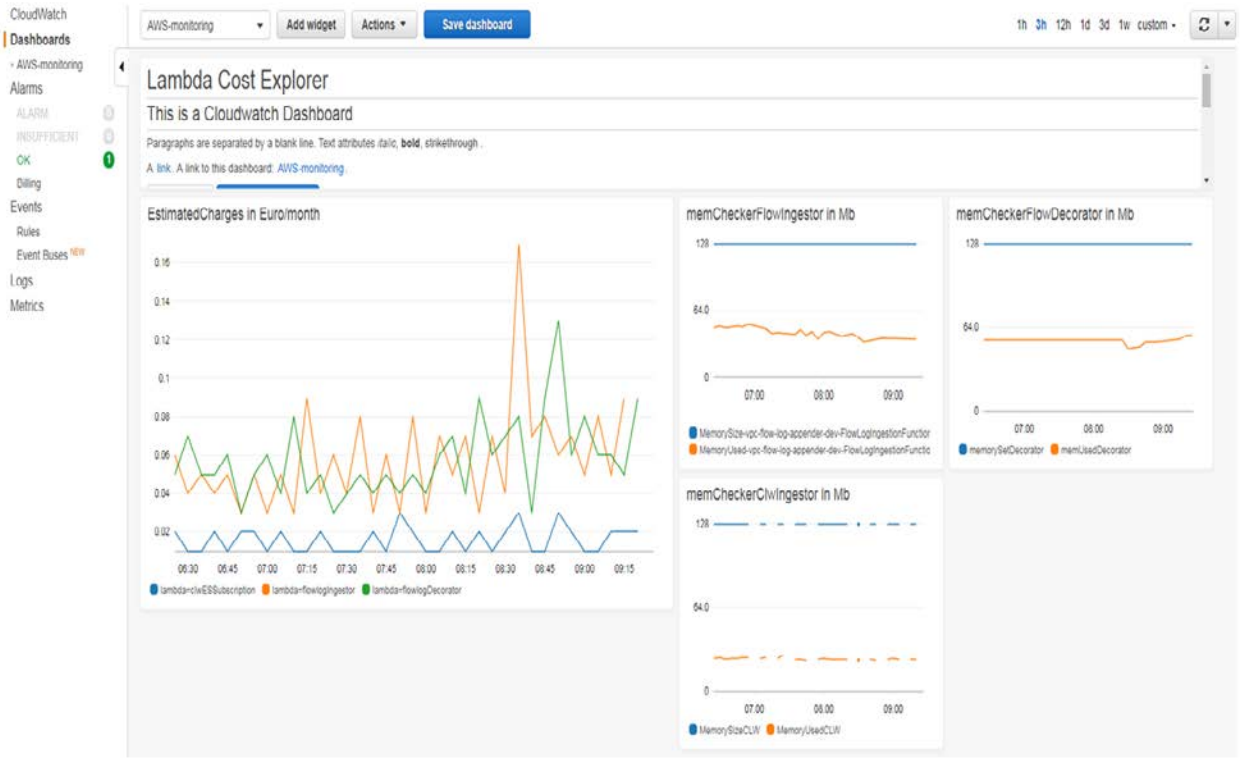
Monitoring with CloudWatch

- Log lambda entries
- Define Custom metrics
- Controlling database actions: CREATE, DELETE, WRITE
- Generate alarms and send them via email or sms with SNS

Fundamental Alert :
BILLING

Detection

CloudWatch limits



$3 per dashboard/month (10 dashboards: $30)

$0.30 per metric/month for the 10,000 first metrics ($3000)
$0.10 per month to 240,000 ($24,000)
$0.05 per month to 750,000 ($37,500)
$0.02 per month above 1,000,000 ($20,000)

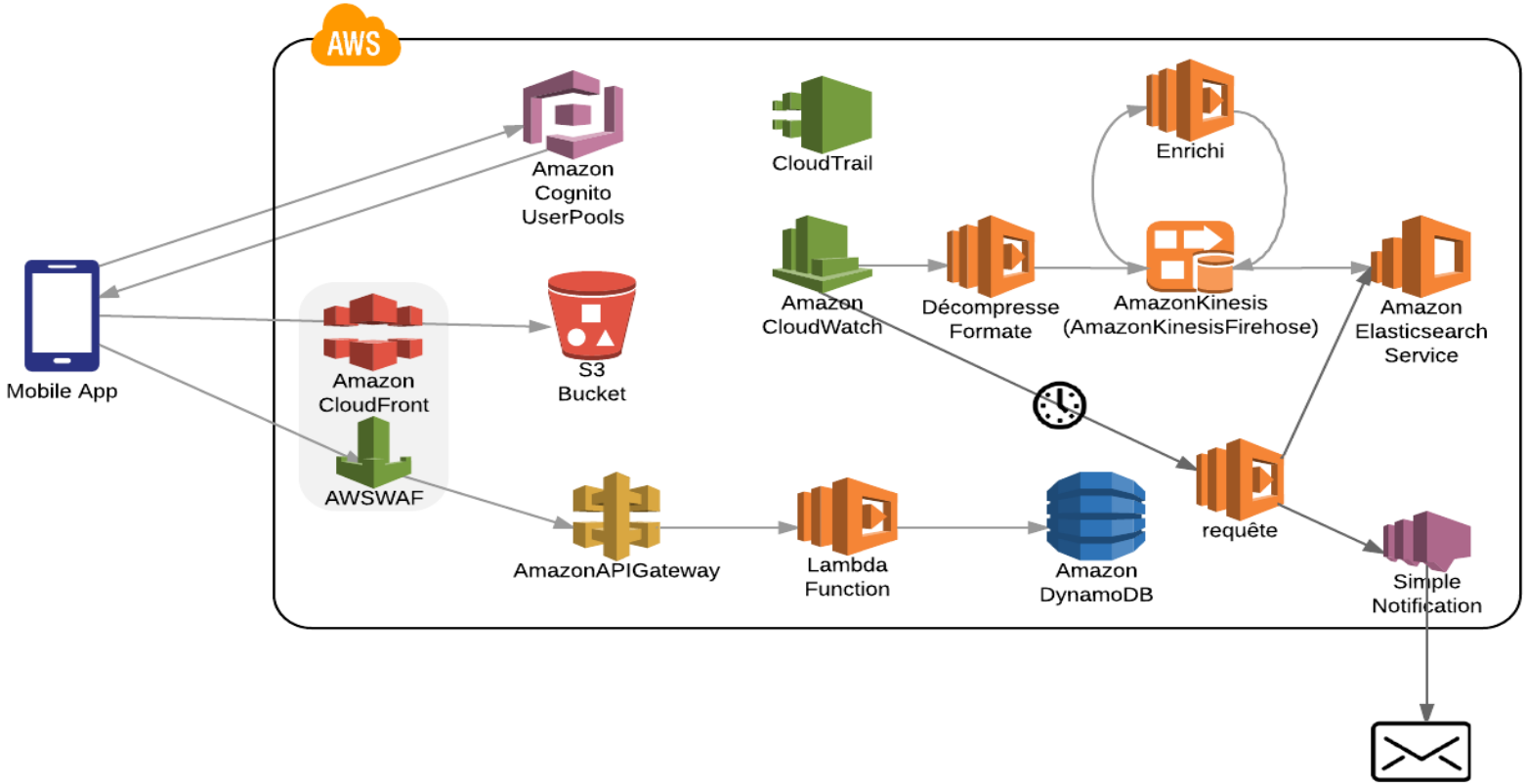
$0.10 per alarm/month (500 alarms: $50)

$0.57 per ingested Gb of data/month (500 Gb: $285)
$0.03 per Gb of archived data/month (3Tb for 6 months of retention : $90)

Total: $755

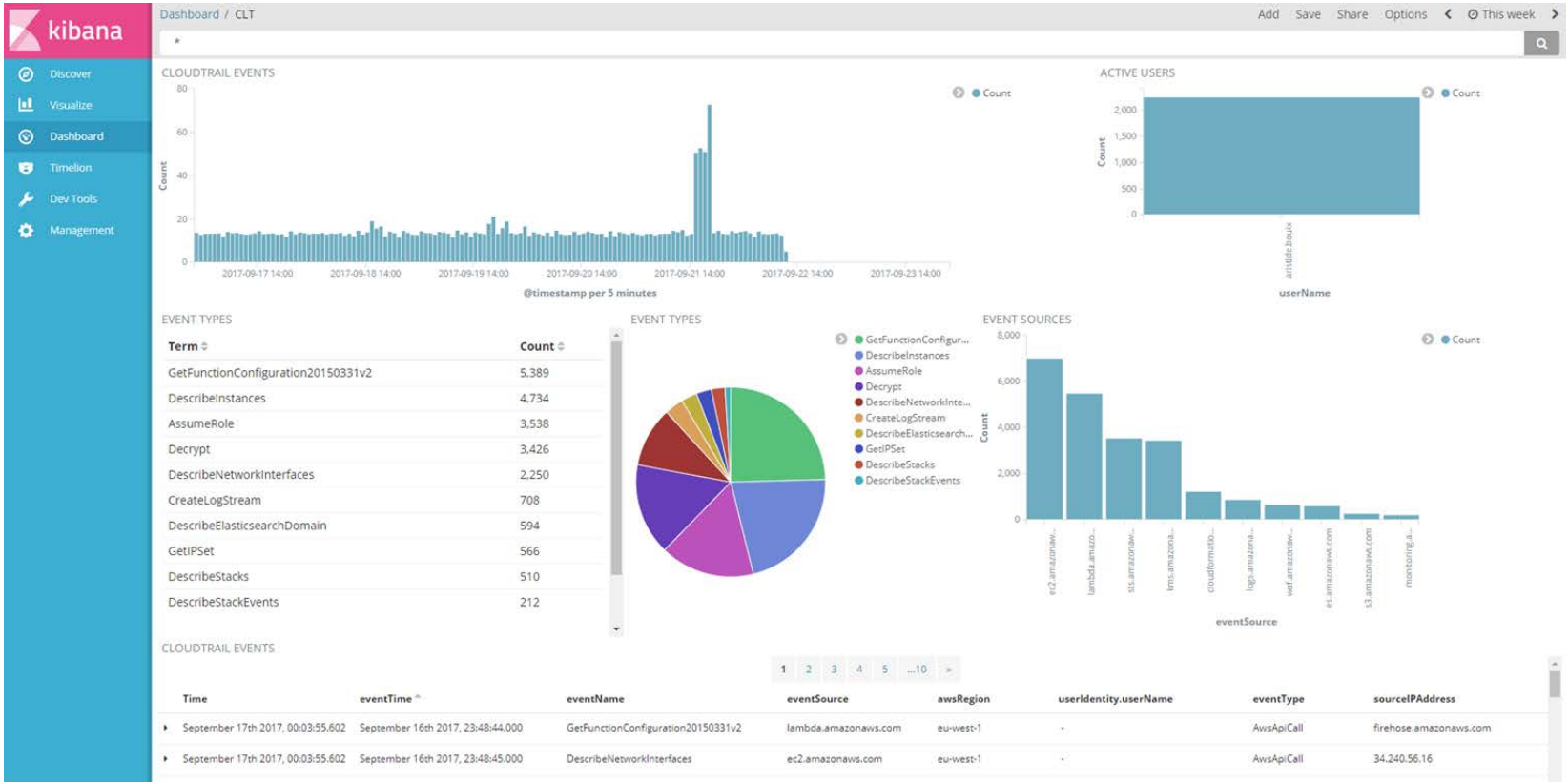
Detection

ELK as a service



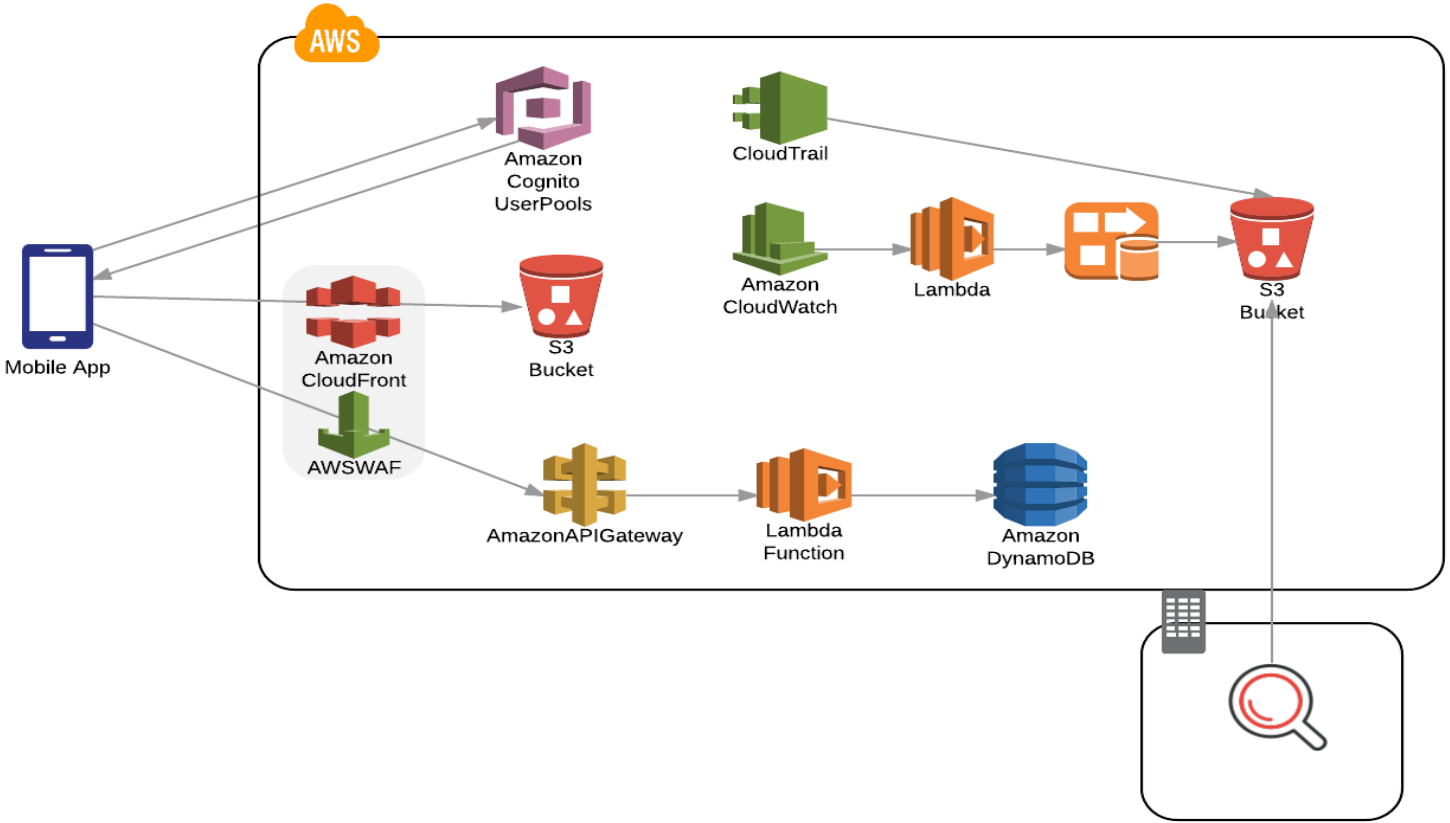
Detection

ELK as a service



Detection

Alternative: I bring my SIEM



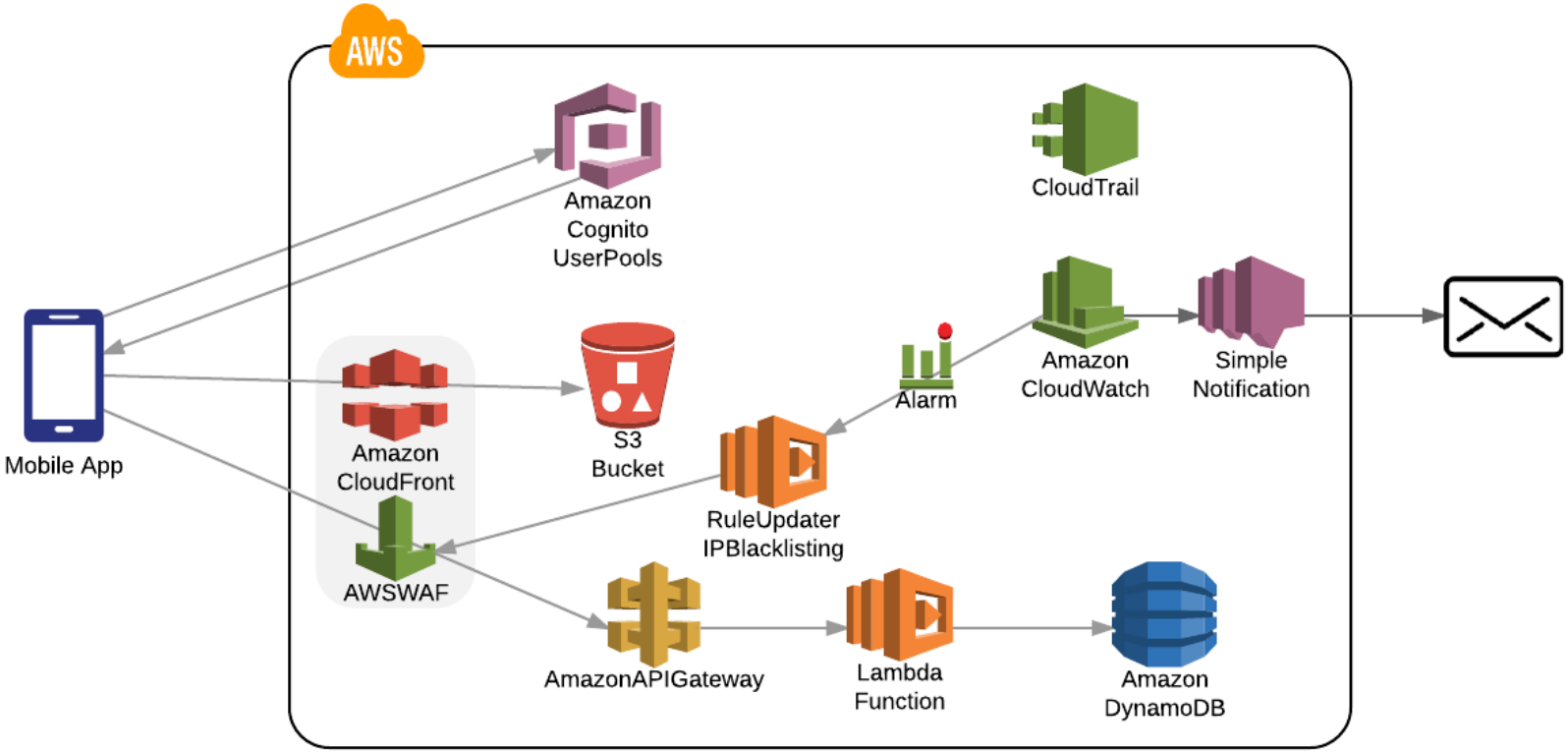
Detection

SaaS / MSSP


5
Response
Automation

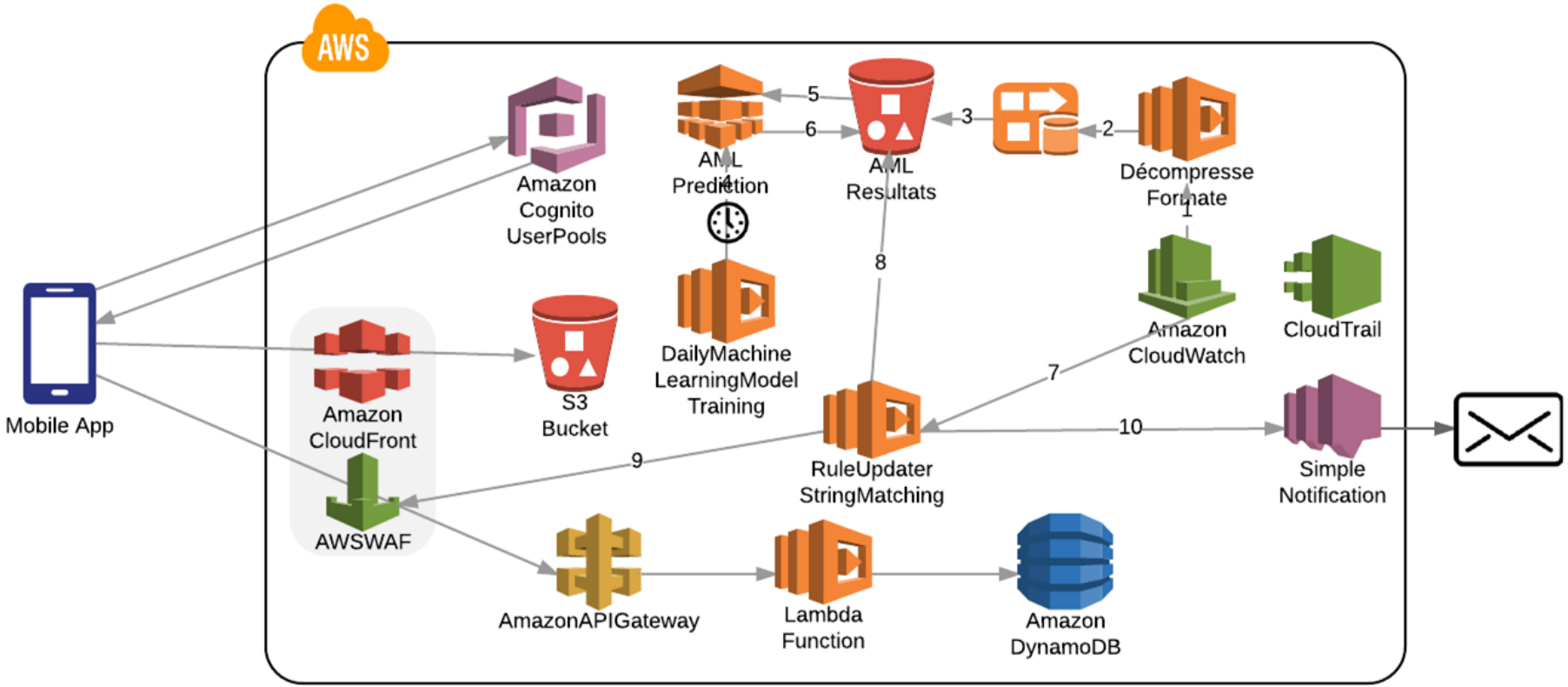
Automation

Recurrent Events



Automation

Singular Events



References:

Re:Invent 2016:

- Serverless Authentication and Authorization: Identity Management for Serverless Architectures (MBL306)
- Serverless Architectural Patterns and Best Practices (ARC402)
- Mitigating DDoS Attacks on AWS: Five Vectors and Four Use Cases (SEC310)
- Securing Serverless Architectures, and API Filtering at Layer 7 (SAC310)
- Security Automation: Spend Less Time Securing Your Applications (SAC316)
- Predictive Security: Using Big Data to Fortify Your Defenses (SAC304)

Blog AWS:

- Implementing Alerting on Amazon Elasticsearch Data (28 novembre 2016)

Aristide Bouix

Information Systems Security Consultant
Devoteam Risk & Security
+33 6 60 49 23 08

aristide.bouix@devoteam.com

devoteam

Questions?