Developer Operations

Security Considerations

Security in Cloud / DevOps

- Security often considered an **inhibitor** to cloud deployment
  - Isolation failure (*nosy neighbour* problem)
  - Credential leakage
  - Legal & regulatory issues
  - Loss of control
  - Data loss
  - Transition of legacy applications / models
  - Punctured perimeter (so network security devices like firewalls and intrusion detection lose effectiveness)

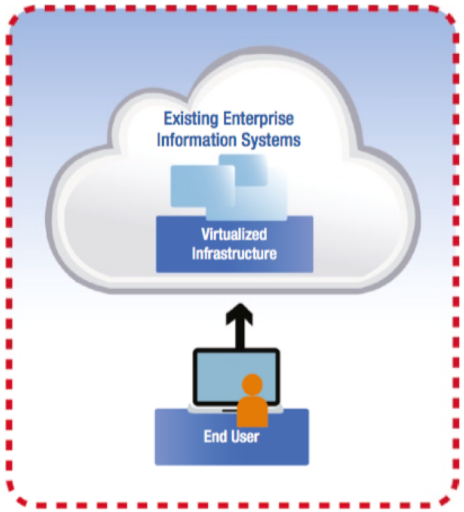
Security in Cloud / DevOps

- But security can also be an **enabler**
  - Security more easily outsourced to specialists
    - Especially relevant to PaaS and SaaS
  - New deployments allow security to be built in from the start
  - Specialist cloud security services (“security as a service”) can improve security – e.g.:
    - Encryption accelerators
    - Secure random number generators
    - Secure containers
    - Security monitoring
    - Online penetration testing

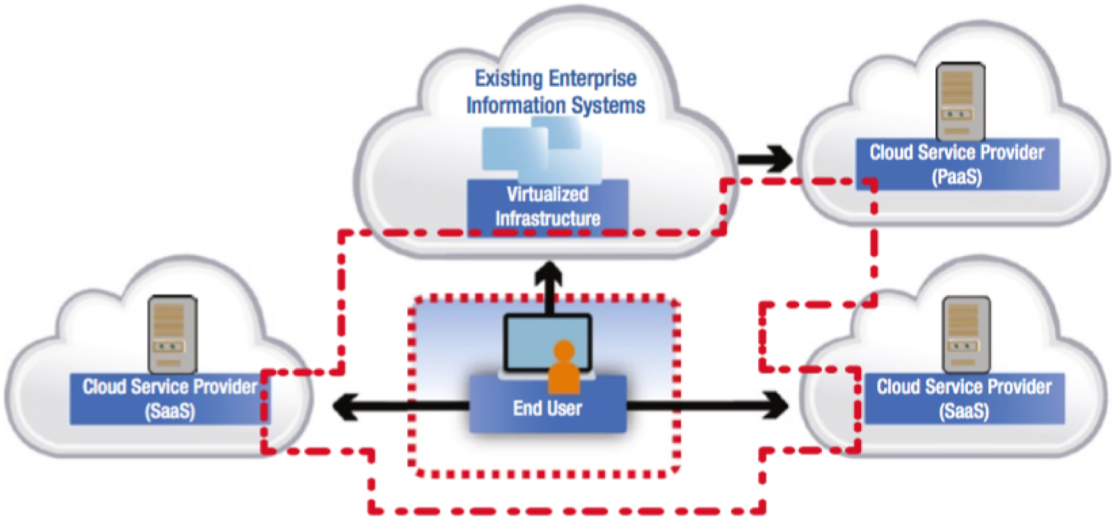
Trends impacting cloud security

- Virtualisation and cloud architectures
  - Multi-tenancy: hardware shared by different lines of business and even different businesses
- Increased attack sophistication
  - No longer just OS and system/application software
    - BIOS, firmware, hypervisor
  - Targeted attacks
  - More covert
- Legal and regulatory compliance
  - Increased regulation and audit of personally identifiable data, financial data, etc.

Perimeter evolution



Traditional perimeter



Cloud security perimeter

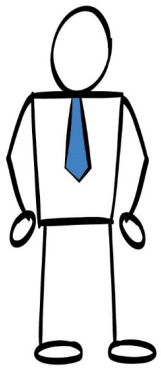
AWS Security

AWS Shared Responsibility Model

Responsible for security ***'in'*** the Cloud	AWS services ***you*** utilize to run your workloads (EC2 instances, S3 buckets, etc.)
Responsible for security ***'of'*** the Cloud	Policies and mechanisms ***AWS*** uses to protect the cloud itself

AWS Shared Responsibility Model

AWS Shared Responsibility Model



Customer

Responsible for security *'in'* the Cloud

AWS services *the customer* uses to run their workloads (EC2 instances, S3 buckets, etc.)

AWS

Responsible for security *'of'* the Cloud

Compute | Storage | Database | Networking

AWS Global Infrastructure

Regions

Availability Zones

Edge Locations

AWS Principal Services for Security

Areas	Key Services				
Data protection	 Elastic Load Balancing	 Amazon EBS	 Amazon S3	 Amazon RDS	 AWS Key Management Service (KMS)
Privilege management	 AWS IAM	 MFA token			
Infrastructure protection	 Amazon VPC				
Detective controls	 AWS CloudTrail	 AWS Config	 Amazon CloudWatch		

AWS Data Protection

- Many AWS services include encryption capabilities to protect data in transit and at rest, such as:
  - Elastic Load Balancing
  - Elastic Block Store (EBS),
  - Simple Storage Service (S3)
  - Relational Database Service (RDS).

- AWS Key Management Service (KMS)
  - Secure key storage, creation, rotation, usage

- Cloud HSM
  - Cloud-based hardware security module – managed by customer

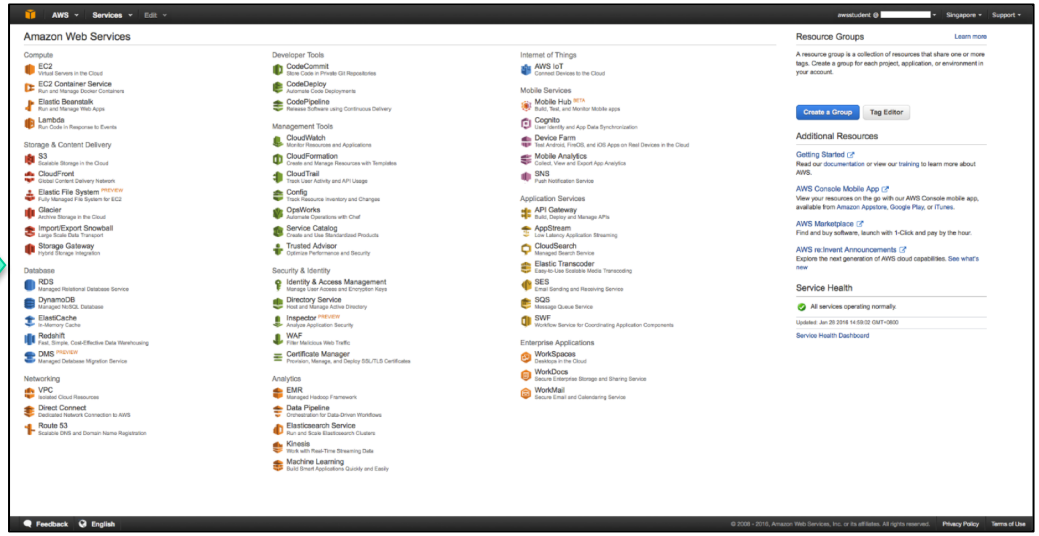
AWS Privilege Management

- Identity & Access Management (IAM)
  - Users & Groups
  - Roles
  - Permissions (policies)
  - Multi-factor authentication
  - API keys

AWS IAM

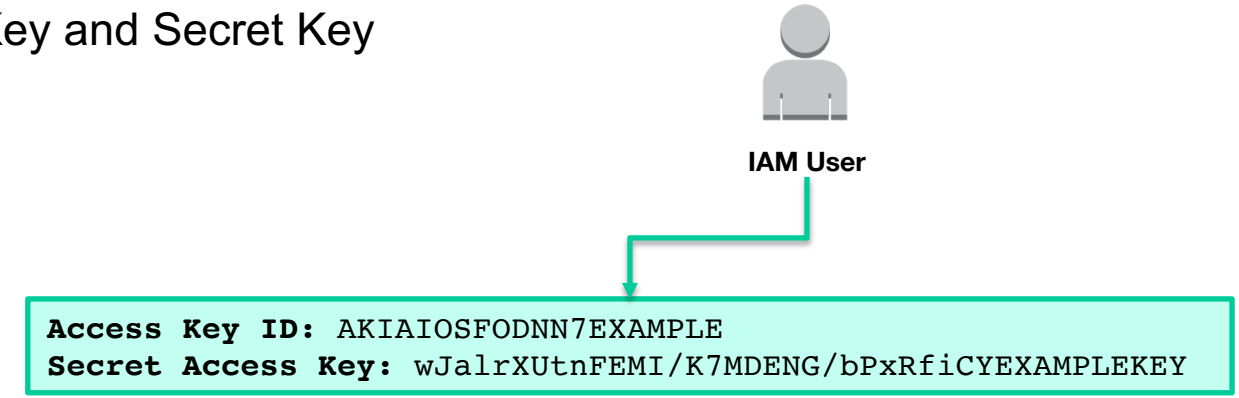
IAM Authentication: Management Console

- **AWS Management Console**
  - User Name and Password
  - MFA



IAM Authentication: CLI / API

- **AWS CLI or SDK API**
  - Access Key and Secret Key



AWS CLI

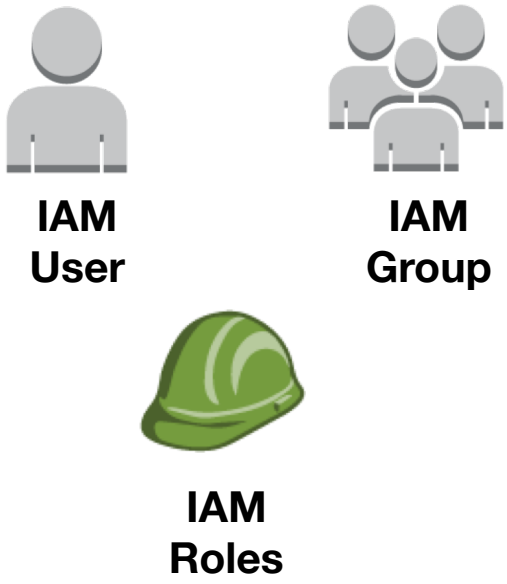
```
[redacted]:~ [redacted]$ aws configure
AWS Access Key ID [****************O22A]:
AWS Secret Access Key [****************4m8i]:
Default region name [ap-southeast-1]:
Default output format [json]:
```

AWS SDK & API

IAM Authorisation

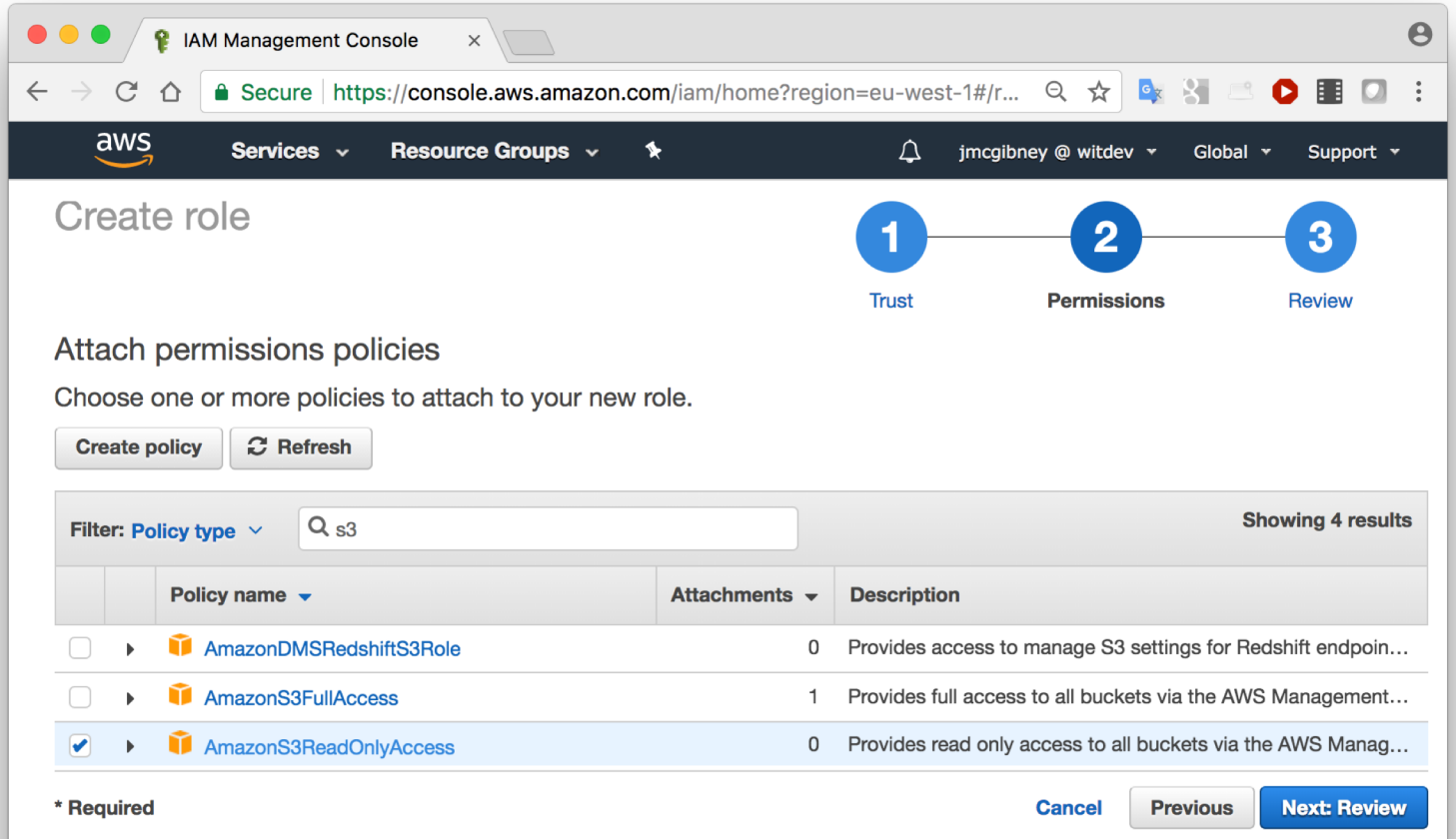
Policies:

- ✓ Are JSON documents to describe permissions.
- ✓ Are assigned to users, groups or roles.



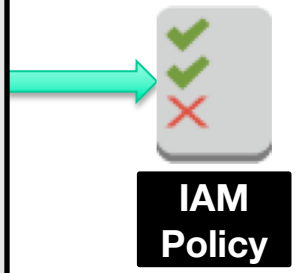
IAM Authorisation: Roles

- IAM roles are a secure way to grant permissions to specific entities
  - e.g. application code running on an EC2 instance that needs to perform some actions on AWS resources

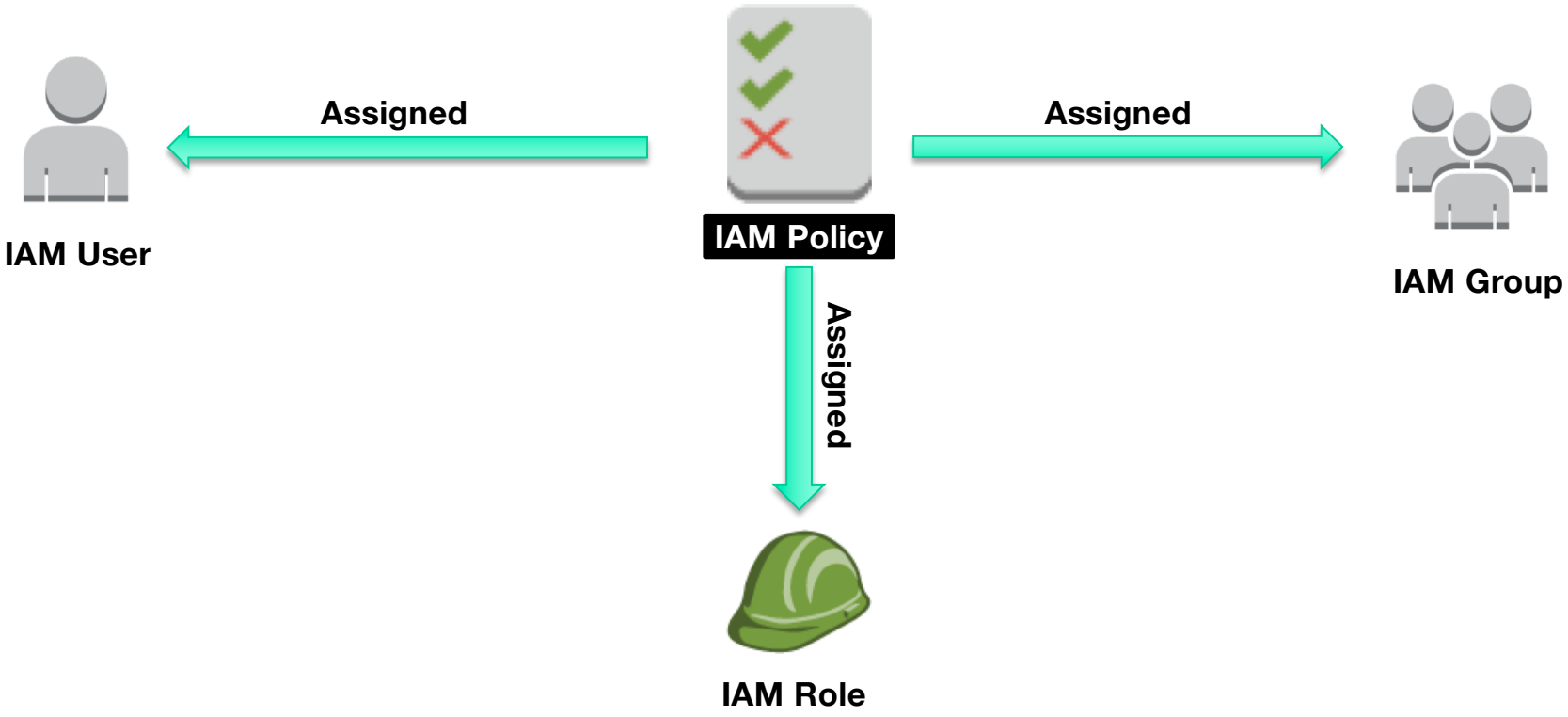


IAM Authorisation: Policy elements

```
{
  "Version": "2012-10-17",
  "Statement": [
   {
     "Sid": "Stmt1453690971587",
       "Action": [
       "ec2:Describe*",
       "ec2:StartInstances",
       "ec2:StopInstances”
       ],
       "Effect": "Allow",
       "Resource": "*",
       "Condition": {
         "IpAddress": {
            "aws:SourceIp": "54.64.34.65/32”
            }
       }
    },
    {
       "Sid": "Stmt1453690998327",
       "Action": [
         "s3:GetObject*”
         ],
       "Effect": "Allow",
       "Resource": "arn:aws:s3:::example_bucket/*”
       }
     ]
    }
```



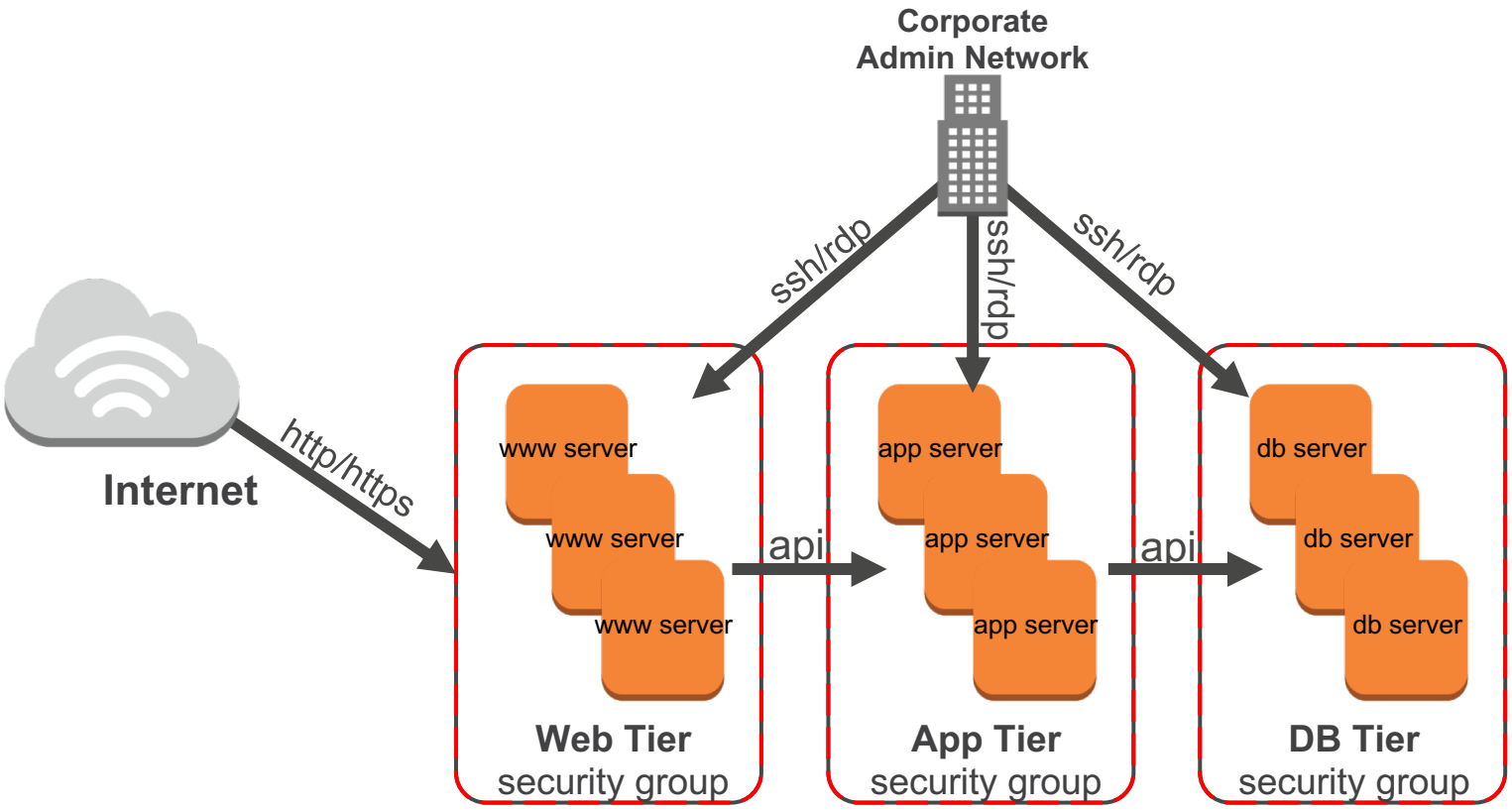
IAM Authorisation: Policy assignment



AWS Infrastructure protection

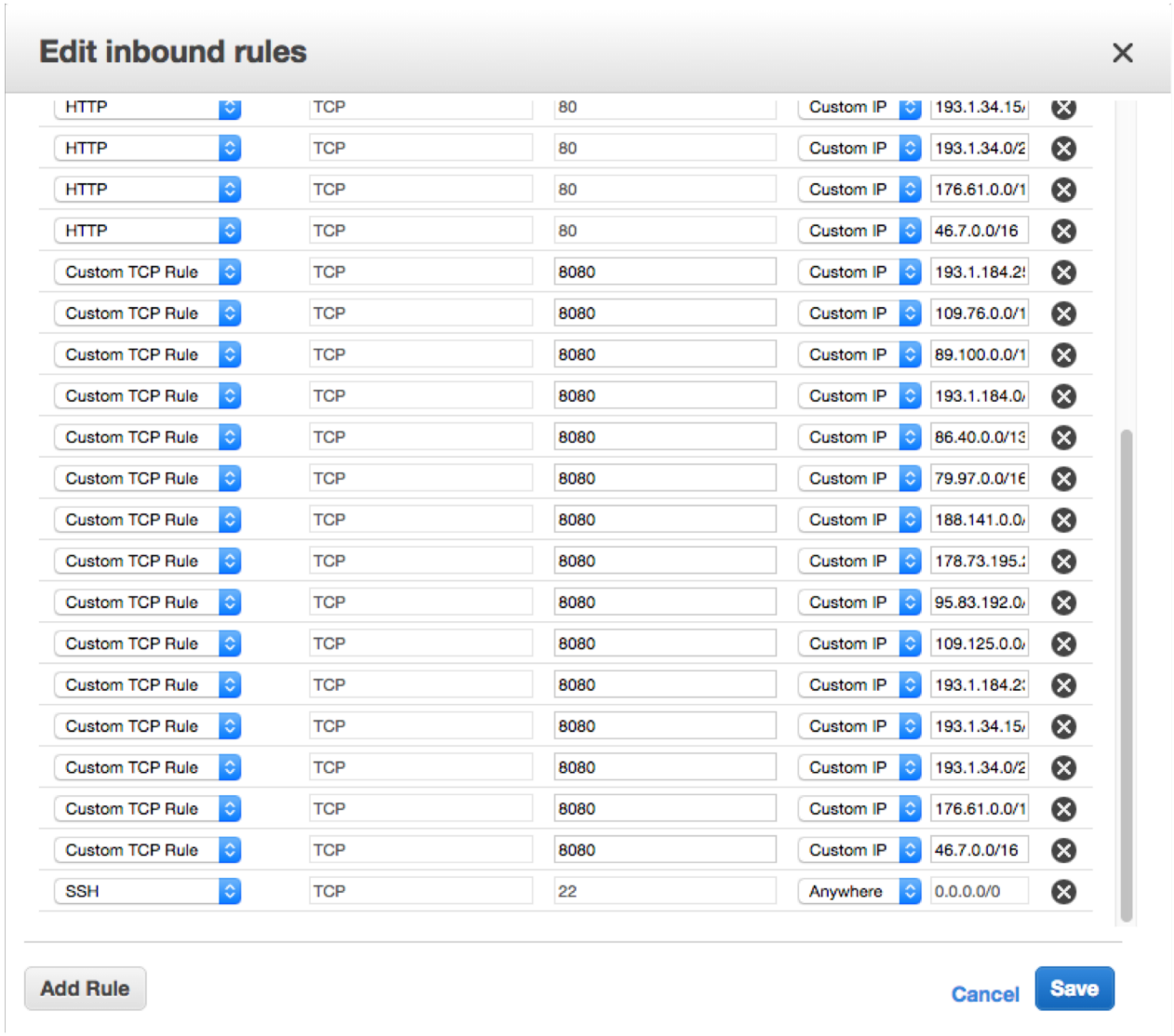
- Amazon Virtual Private Cloud (VPC) lets you provision a private, isolated section of the AWS cloud where you can launch AWS resources in a virtual network
- Public and private subnets
- NAT
- Security Groups
  - Control traffic to/from EC2 instances and RDS databases
- Network Access Control Lists (NACLs)
  - Control traffic to/from subnets
- VPN connections – for connecting to other networks, e.g. customer on-premises network

AWS Infrastructure protection



(all other ports are blocked)

Security Group configuration



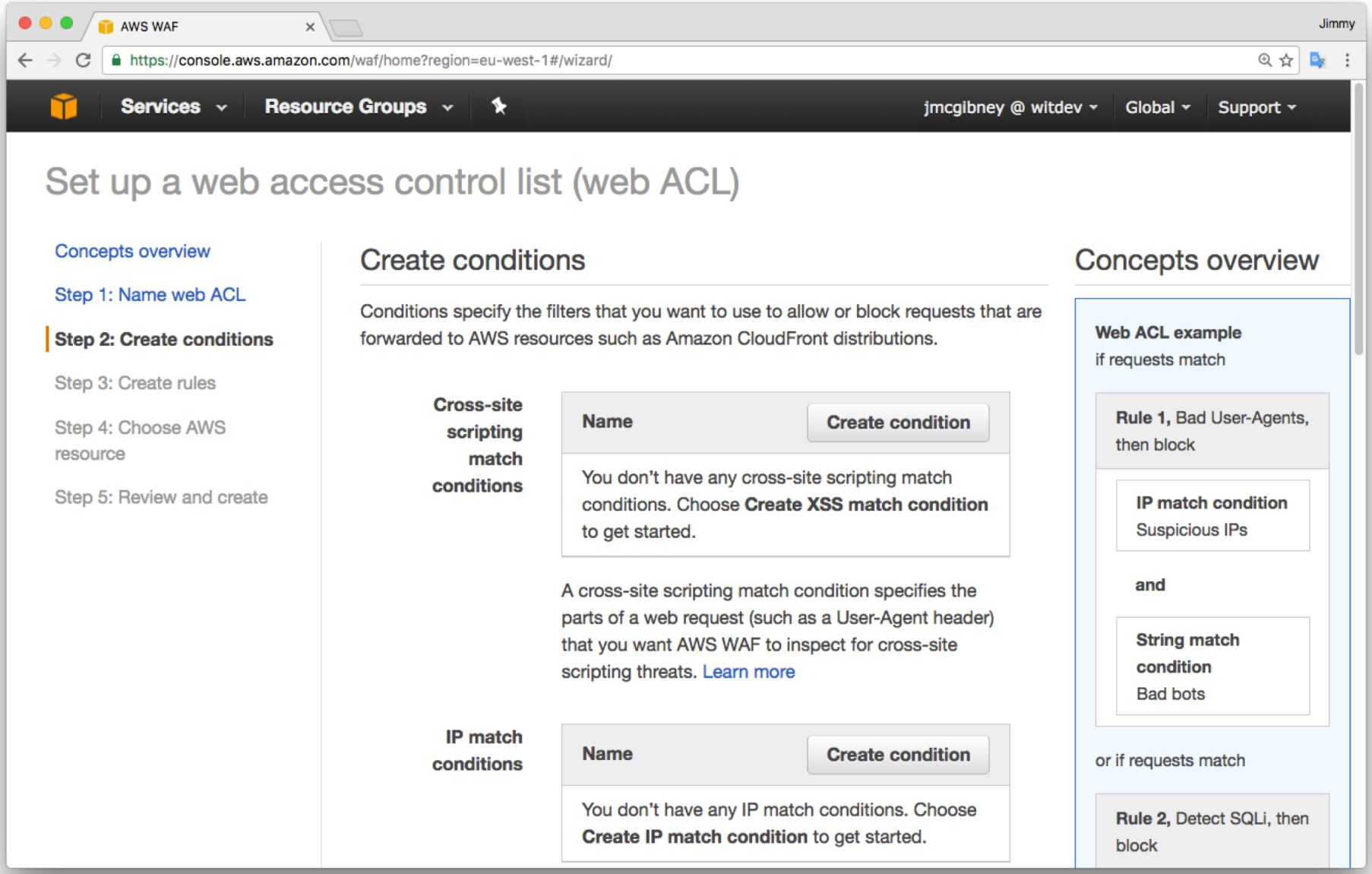
AWS Detective Controls

- AWS CloudTrail
  - records AWS API calls
- AWS Config
  - provides a detailed inventory of AWS resources and configuration
- Amazon CloudWatch
  - monitoring service for AWS resources

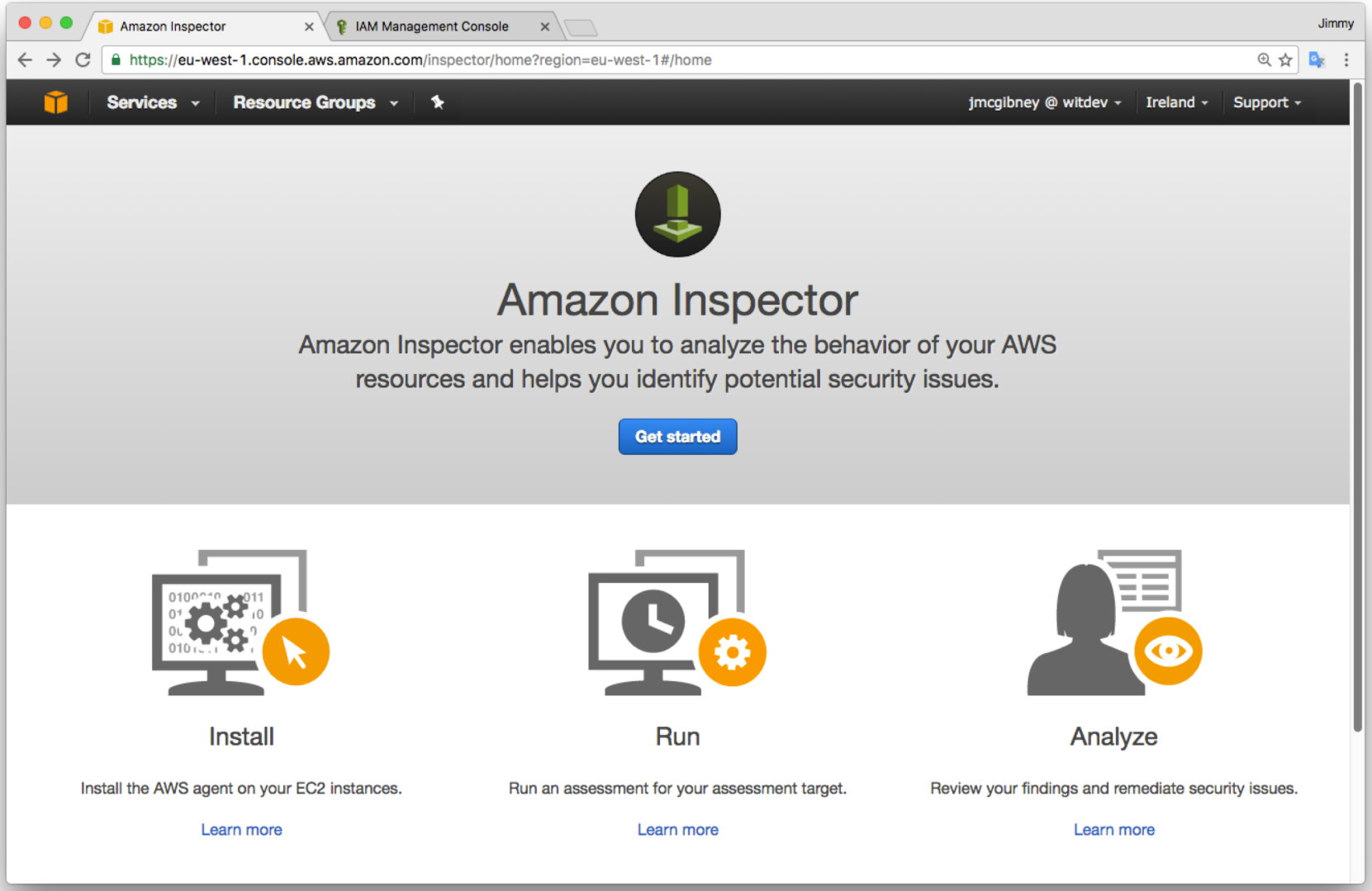
Some other AWS Security Features

- EC2 authentication
  - Key pair for Linux instances; username & password for Windows
- Web application firewall (WAF)
  - Monitors and filters HTTP/HTTPS requests to protect web apps
- Inspector
  - Application behaviour monitoring (installed on instances)
- Certificate Manager
  - TLS certificates deployment, management, renewal
- AWS Shield
  - Protection against DDoS (distributed denial of service)
- Trusted Advisor
  - Dashboard for monitoring AWS resources; includes security

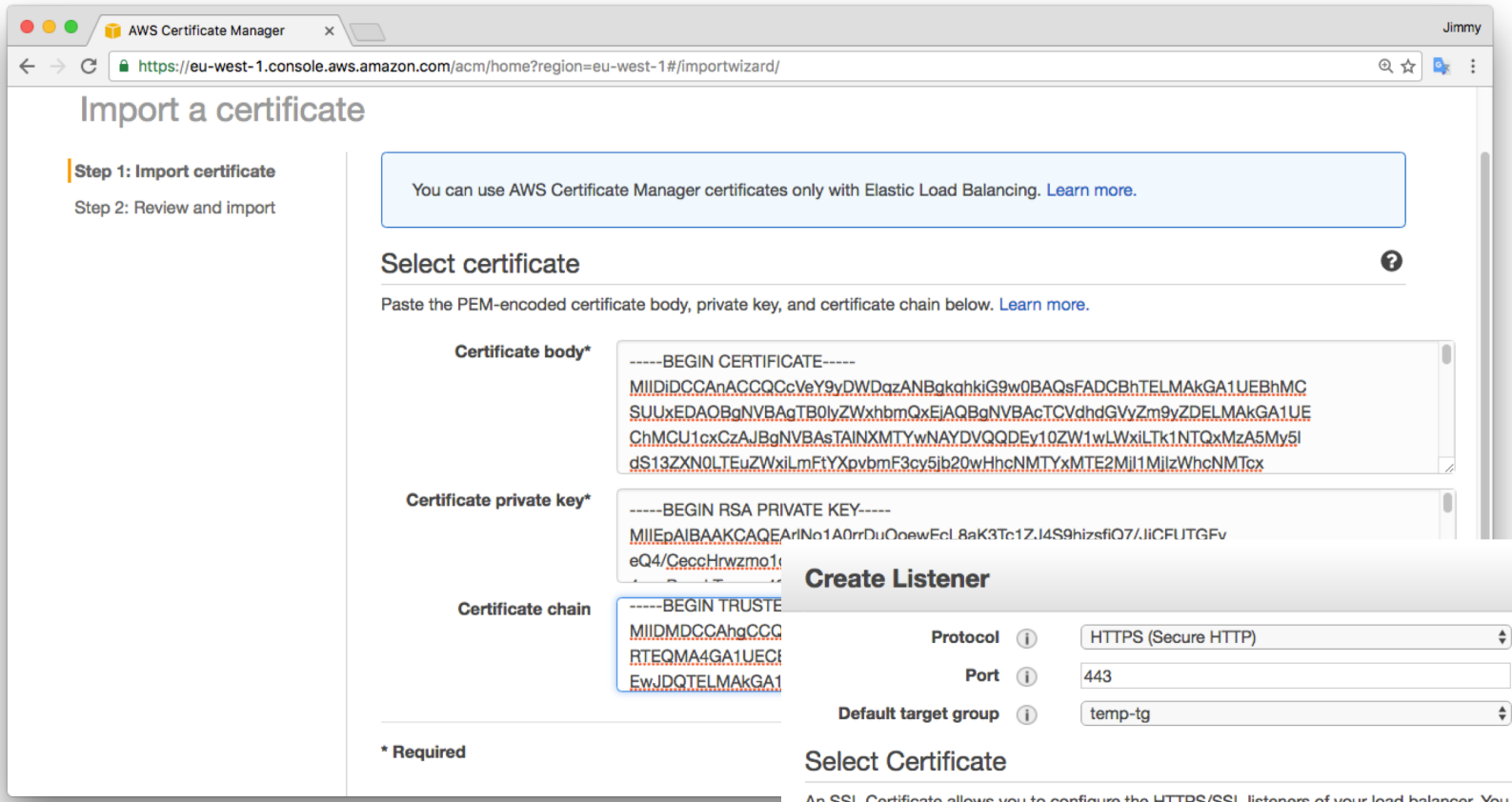
Web Application Firewall



Inspector


Amazon Inspector
IAM Management Console
Jimmy
https://eu-west-1.console.aws.amazon.com/inspector/home?region=eu-west-1#/home
Services
Resource Groups
jmcgibney @ witdev
Ireland
Support
Amazon Inspector
Amazon Inspector enables you to analyze the behavior of your AWS resources and helps you identify potential security issues.
Get started
Install
Install the AWS agent on your EC2 instances.
Learn more
Run
Run an assessment for your assessment target.
Learn more
Analyze
Review your findings and remediate security issues.
Learn more

Certificate Manager



EC2
(load balancer config)

Finally … protect credentials!

sign in | become a supporter | subscribe | search | find a job | dating | more | International edition

theguardian

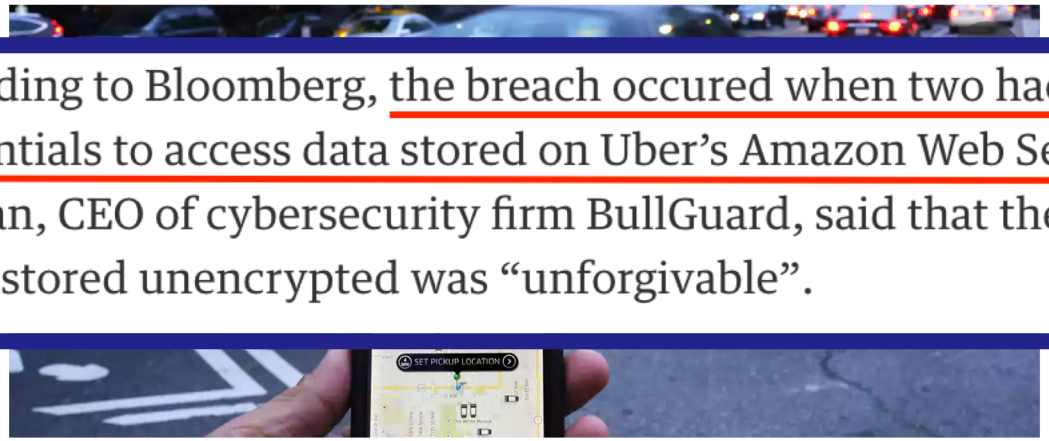
UK | world | sport | football | opinion | culture | business | lifestyle | fashion | environment | tech | travel | all sections

home › tech

Uber

Uber concealed massive hack that exposed data of 57m users and drivers

- Firm paid hackers $100,000 to delete data and keep breach quiet
- Chief security officer Joe Sullivan fired for concealing October 2016 breach



5357

Julia Ca
in San

@juli

email

Wednesday 22 November 2017 11.16 GMT

According to Bloomberg, the breach occured when two hackers obtained login credentials to access data stored on Uber's Amazon Web Services account. Paul Lipman, CEO of cybersecurity firm BullGuard, said that the fact that the data was being stored unencrypted was "unforgivable".