

---

# DEV/SECOPS BOOTCAMP

BUILDING RUGGED SOFTWARE

YEAR ONE / WEEK SIX / LESSON THREE

---

# Agenda

- AWS IAM



# Quick IAM Overview

- Users
- Groups
- Roles
- Policies
  - Effect
  - Actions
  - Resources
  - Condition
- Allows for very granular control over access to specific parts of the AWS API (if you RTFM)
- Lots of JSON



# The Good

- Policy is specifically created for the application
- Least privilege
- Made to be as granular as possible

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "ec2:DescribeInstances",
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "ec2:StopInstances",
        "ec2:StartInstances"
      ],
      "Resource": [
        "arn:aws:ec2:us-west-2:987654321098:instance/i-98765432",
        "arn:aws:ec2:us-west-2:987654321098:instance/i-98765433"
      ]
    },
    {
      "Effect": "Allow",
      "Action": "ec2:TerminateInstances",
      "Resource": "arn:aws:ec2:us-west-2:987654321098:instance/i-98765432",
      "Condition": {
        "StringEquals": {
          "ec2:ResourceTag/purpose": "foobar"
        }
      }
    }
  ]
}
```

---

## The Bad

- ec2:\*
- iam:\*
- anything:\*

```
{  
  "Version": "2012-10-17",  
  "Statement": {  
    "Effect": "Allow",  
    "Action": "iam:*",  
    "Resource": "*"    
  }  
}
```

---

## The Ugly

- All access
- Great for dev
- Bad for security

```
{  
  "Version": "2012-10-17",  
  "Statement": {  
    "Effect": "Allow",  
    "Action": "/*:*",  
    "Resource": "*"  
  }  
}
```

---

# Instance Roles

- Storing access keys on your instance is a bad idea
- Keeps keys off your instance
- Allow very granular access to the AWS API from an instance
- One of the best “security features” AWS has implemented

---

# AWS Account Takeover

- Overly permissive instance role  
+ the right API calls = ATO
- ATO is a full account  
compromise
- Only way to be 100% sure is to  
scrap the account and start  
over



---

# Questions?

---

## Lab 3 – AWS Account Takeover