



**JPL**

CALIFORNIA INSTITUTE OF TECHNOLOGY

# Cloud Security

Matthew Derenski, Jet Propulsion Laboratory  
**Cyber Security Engineer**



# Agenda – Let's talk cloud



CALIFORNIA INSTITUTE OF TECHNOLOGY

- Cloud Risks
- Cloud Prep
- Cloud Nirvana



- Perceived Risks
- Risks To Consider



**JPL**

CALIFORNIA INSTITUTE OF TECHNOLOGY

# Perceived Risks



# Risks to Consider



CALIFORNIA INSTITUTE OF TECHNOLOGY

- Lack Of Governance
- Cloud Creep
- Lack Of Training
- Provider Risks



# Are You Ready?

**JPL**

CALIFORNIA INSTITUTE OF TECHNOLOGY

- Trust
- Security First
- Governance
- Training
- Auditing
- APIs
- Access Control



# Trust... But Verify



CALIFORNIA INSTITUTE OF TECHNOLOGY

- Build A Strong Relationship
- Have A Valid Risk Assessment
- Get Everyone Onboard



# Security First



CALIFORNIA INSTITUTE OF TECHNOLOGY

- Build In Security
- Use A Multilayer Approach (Account To App)





# Training



CALIFORNIA INSTITUTE OF TECHNOLOGY

- Understanding Users And Use Cases
- Ensure Training Is Thorough
- Temper Expectations



# Auditing



CALIFORNIA INSTITUTE OF TECHNOLOGY

- Understand What Can And Can't Be Done
- Automate Collection
- Leverage Provider Supplied Tools



# API



CALIFORNIA INSTITUTE OF TECHNOLOGY

- Understanding Of The Provider's API Is Critical



# Access Control



CALIFORNIA INSTITUTE OF TECHNOLOGY

- Order Of Operations
- Leverage Existing Roles
- Implement Least Privilege



# Sample policy



CALIFORNIA INSTITUTE OF TECHNOLOGY

```
{
  "Statement" : [ {
    "Effect" : "Deny",
    "Action": [
      "s3:PutBucketWebsite",
      "ec2:AllocateAddress",
      "ec2:AssociateAddress",
      "ec2:AttachInternetGateway",
      "ec2:CreateInternetGateway",
      "ec2:AssociateRouteTable",
      "ec2:AttachVpnGateway",
      "ec2:CreateCustomerGateway",
      "ec2:CreateDhcpOptions",
      "ec2:CreateRoute",
      "ec2:CreateRouteTable",
      "ec2:CreateSubnet",
      "ec2:CreateVpc",
      "ec2:CreateVpnConnection",
      "ec2:CreateVpnGateway",
      "ec2>DeleteCustomerGateway",
      "ec2>DeleteDhcpOptions",
      "ec2>DeleteInternetGateway",
      "ec2>DeleteRoute",
      "ec2>DeleteRouteTable",
      "ec2>DeleteSubnet",
      "ec2>DeleteVpc",
      "ec2>DeleteVpnConnection",
      "ec2>DeleteVpnGateway",
      "ec2:DetachInternetGateway",
      "ec2:DetachVpnGateway" ],
    "Resource": "*" } ]
}
```



# Cloud Nirvana



CALIFORNIA INSTITUTE OF TECHNOLOGY

- Incident Response
- Visibility
- Data Integrity
- Compliance
- Vendor Security



# Incident Response



CALIFORNIA INSTITUTE OF TECHNOLOGY

- Quick Forensics
- Instant Segmentation
- Ubiquitous Access



# Visibility



CALIFORNIA INSTITUTE OF TECHNOLOGY

- On The Fly Metrics
- Tie Into Existing Systems





# Data Integrity



CALIFORNIA INSTITUTE OF TECHNOLOGY

- Redundant Storage
- Automated Backups
- Geographic Diversity
- Access Control



# Compliance



CALIFORNIA INSTITUTE OF TECHNOLOGY

- Automated Compliance
- Single Pane Of Glass



# Vendor Security



CALIFORNIA INSTITUTE OF TECHNOLOGY

- See More Attacks
- More Diverse Install Base
- More Resources



**JPL**

CALIFORNIA INSTITUTE OF TECHNOLOGY

# Questions