Comments are for use with amazon cloud specifically

Hold questions till the end

Security token service

describe the risk assessment

Add examples for everything

We went through the amazon compliance documents (talk about it) in security plans

example of a workload that might not be good for cloud that didn't work for us (generic)

picture for final slide, need to work on the "remember slide" tie it all together
Cloud Risks
   Perceived risks
   Risks to consider
Cloud Prep
   Engineer the cloud for long term success
Cloud Nirvana
   Advantages of the cloud over local infrastructure
• Perceived Risks
• Risks To Consider
Perceived Risks

- It's all out there on the internet
- Anyone can access my data
- The cloud crashes all the time
- The cloud is dangerous
Lack of Governance
- Compliance issues
- What data is going into the cloud
- Who is using the cloud

Cloud Creep
- Who can procure cloud
- Who can provision
- What can be provisioned

Lack of Training
- Do you know what you just did

Provider Risks
Are You Ready?

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

Trust
  …but verify
Security first
  Build in security upfront
Governance
  Establish policies and procedures
Training
Auditing
Trust… But Verify

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

Build a strong business relationship
  Understand the terms and conditions. Consider purchasing support
  (Developer, business, enterprise)
Have a valid risk assessment
  Implement mitigating controls
Lawyers, Auditors, and Project Managers
  Be transparent
  Educate and inform
  Get them on board
Build in security
  Automated asset configuration
  Automated compliance monitoring
Multi layered approach to security
  Account to App controls and protections
  Tight integration with existing systems
    Authentication & Authorization
    Encryption and key management (use amazons or your own)
  User your existing “Security stack”

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

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

Understand your users and use cases
Training
  • When to use the cloud
  • How to use the cloud
  • GUI vs API
  • Gotchas in the cloud
  • Roles and responsibility
Temper expectations
  • Cloud is not right for all workloads
Understand what you can and can’t collection
Network Visibility
Automate the collection using the AWS API
Trusted advisor
  Use it to see what is being over/under utilized and where security holes are.
As a solution provider you should understand the API
  Automate asset population to an existing asset database
  Ensure compliance with a CM tool
  Feed compliance data back to the SOC team for automatic notification
  and remediation
  Metrics and monitoring data all tie back into an existing OPS system.

Trusted advisor has its own API USE IT
Use case: Allow access to S3 buckets where the bucket name matches the IAM user’s name.

Implicit deny all access to S3
Explicit allow S3 functions
   ListAllMyBuckets
   All S3 actions on resource
      "arn:aws-us-gov:s3:::${aws:username}",
      "arn:aws-us-gov:s3:::${aws:username}/"

Explicit deny
   None needed

The right roles

Forensics roles
   Power user
Auditing, compliance, and asset tracking
   Read only
Developers
   No IAM
Sample policy

{
  "Statement": [{
    "Effect": "Deny",
    "Action": [
      "ec2:CreateVpc",
      "ec2:CreateVpnConnection",
      "ec2:CreateVpnGateway",
      "ec2:DeleteCustomerGateway",
      "ec2:DeleteDhcpOptions",
      "ec2:DeleteInternetGateway",
      "ec2:DeleteRoute",
      "ec2:DeleteRouteTable",
      "ec2:DeleteSubnet",
      "ec2:DeleteVpc",
      "ec2:DeleteRouteTable",
      "ec2:DeleteVpnConnection",
      "ec2:DeleteVpnGateway",
      "ec2:DeleteVpc",
      "ec2:DeleteInternetGateway",
      "ec2:DetachVpnGateway",
      "ec2:CreateCustomerGateway",
      "ec2:CreateDhcpOptions",
      "ec2:CreateRoute",
      "ec2:CreateRouteTable",
      "ec2:CreateSubnet"
    ],
    "Resource": "*" ]
  }
}
Advantages of the cloud over local infrastructure
  Incident response
  Visibility
  Data integrity and retention
  Compliance
  Access Control & Automation
AWS Security is more likely better than onsite security
Incident Response

- Quick Forensics
- Instant Segmentation
- Ubiquitous Access

Forensics
  - Image systems quick without service interruption
  - Talk about how we do it (memory dumps via support ticket)
Segmentation
  - Bad actors can be isolated on the fly
Ubiquitous access
  - Automated configuration builds in security access
Visibility

- On The Fly Metrics
- Tie Into Existing Systems

On my fly metrics
  - How many resources Internal/external
  - How many console users
  - Where are things running
  - Service performance metrics

Ties into asset tracking
  - Feed metrics into existing log and monitoring systems
  - What account
  - What instance type
  - What OS
  - Who owns it
  - What IP
Data Integrity

- Redundant Storage
- Automated Backups
- Geographic Diversity
- Access Control
Automate compliance
Deploy automated auditing & vulnerability mitigation
OIG/Auditors single view
Vendor Security

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