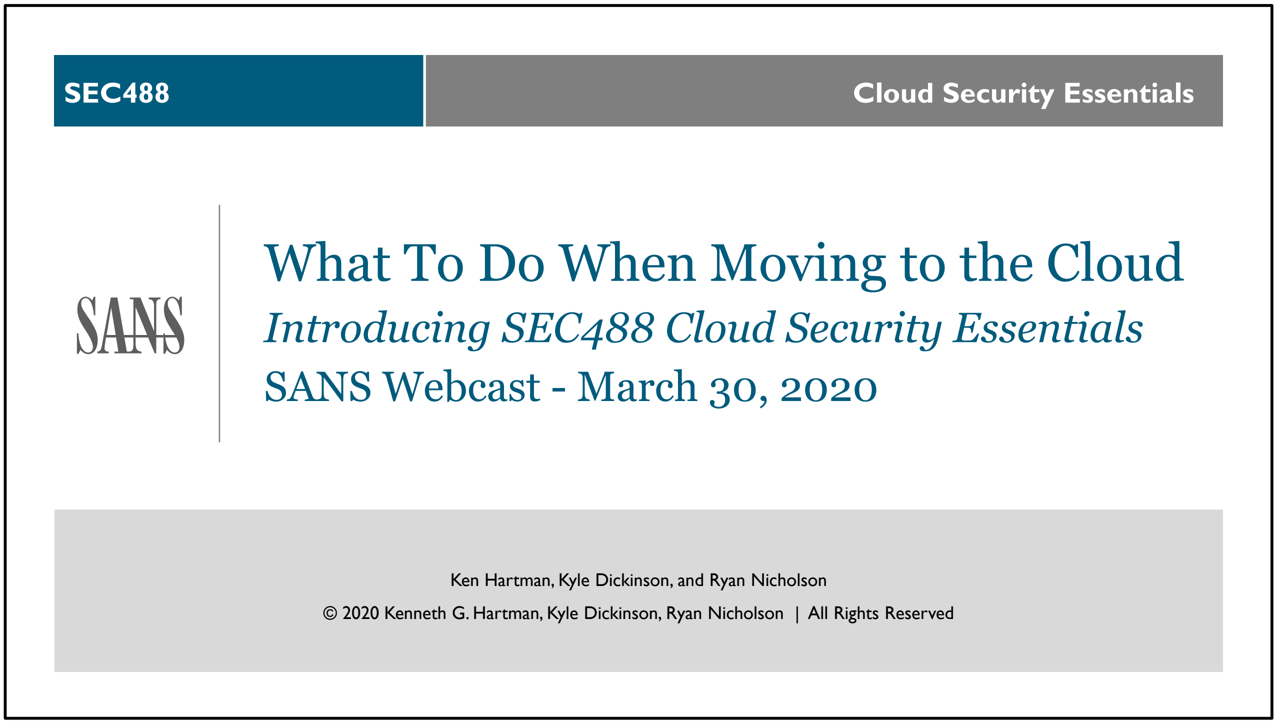


SEC488 Cloud Security Essentials

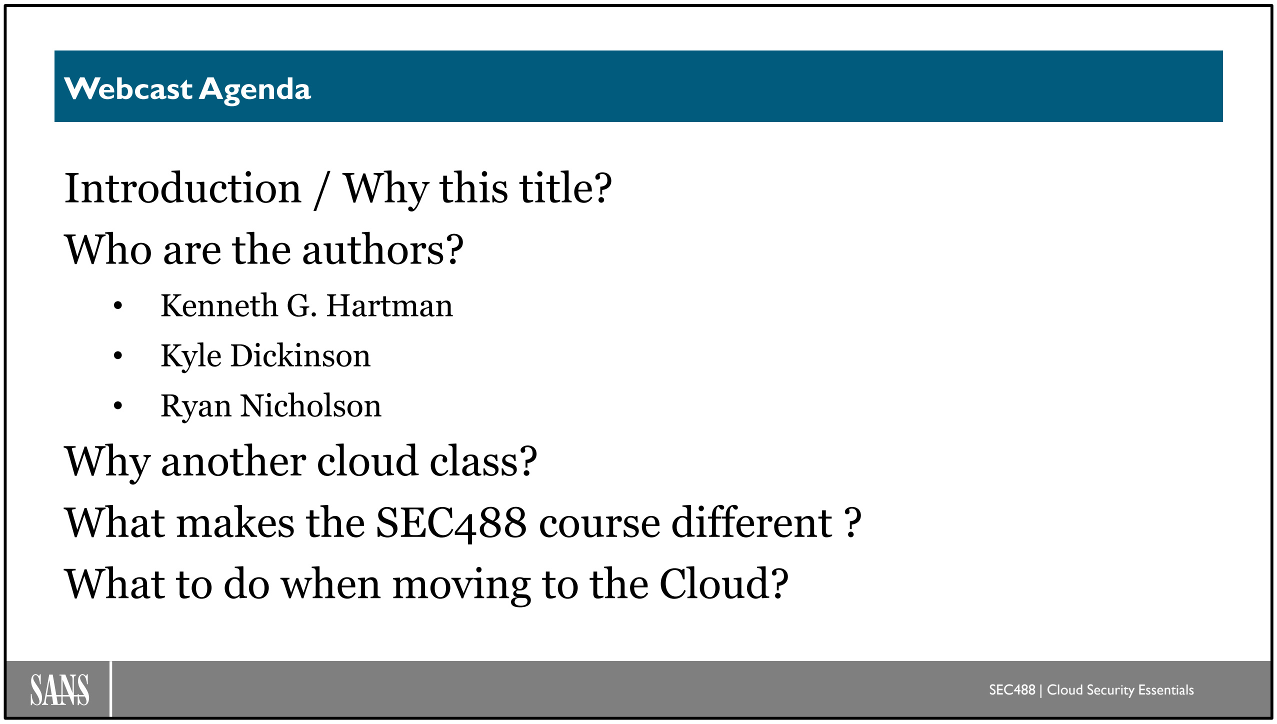
What To Do When Moving to the Cloud

Introducing SEC488 Cloud Security Essentials

SANS Webcast - March 30, 2020

Ken Hartman, Kyle Dickinson, and Ryan Nicholson

The Notes are Intentionally Blank



Webcast Agenda

Introduction / Why this title?

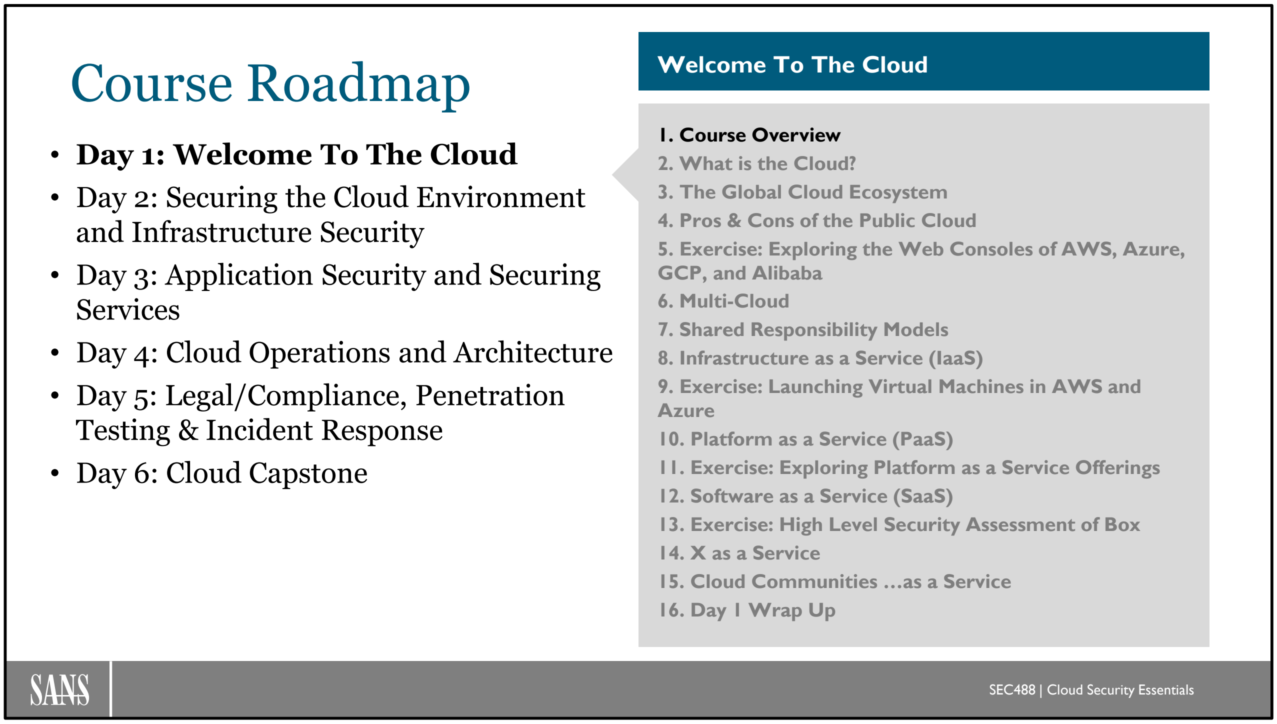
Who are the authors?

- Kenneth G. Hartman
- Kyle Dickinson
- Ryan Nicholson

Why another cloud class?

What makes the SEC488 course different ?

What to do when moving to the Cloud?



Course Roadmap

- **Day 1: Welcome To The Cloud**
- Day 2: Securing the Cloud Environment and Infrastructure Security
- Day 3: Application Security and Securing Services
- Day 4: Cloud Operations and Architecture
- Day 5: Legal/Compliance, Penetration Testing & Incident Response
- Day 6: Cloud Capstone

Welcome To The Cloud

1. Course Overview
2. What is the Cloud?
3. The Global Cloud Ecosystem
4. Pros & Cons of the Public Cloud
5. Exercise: Exploring the Web Consoles of AWS, Azure, GCP, and Alibaba
6. Multi-Cloud
7. Shared Responsibility Models
8. Infrastructure as a Service (IaaS)
9. Exercise: Launching Virtual Machines in AWS and Azure
10. Platform as a Service (PaaS)
11. Exercise: Exploring Platform as a Service Offerings
12. Software as a Service (SaaS)
13. Exercise: High Level Security Assessment of Box
14. X as a Service
15. Cloud Communities …as a Service
16. Day 1 Wrap Up

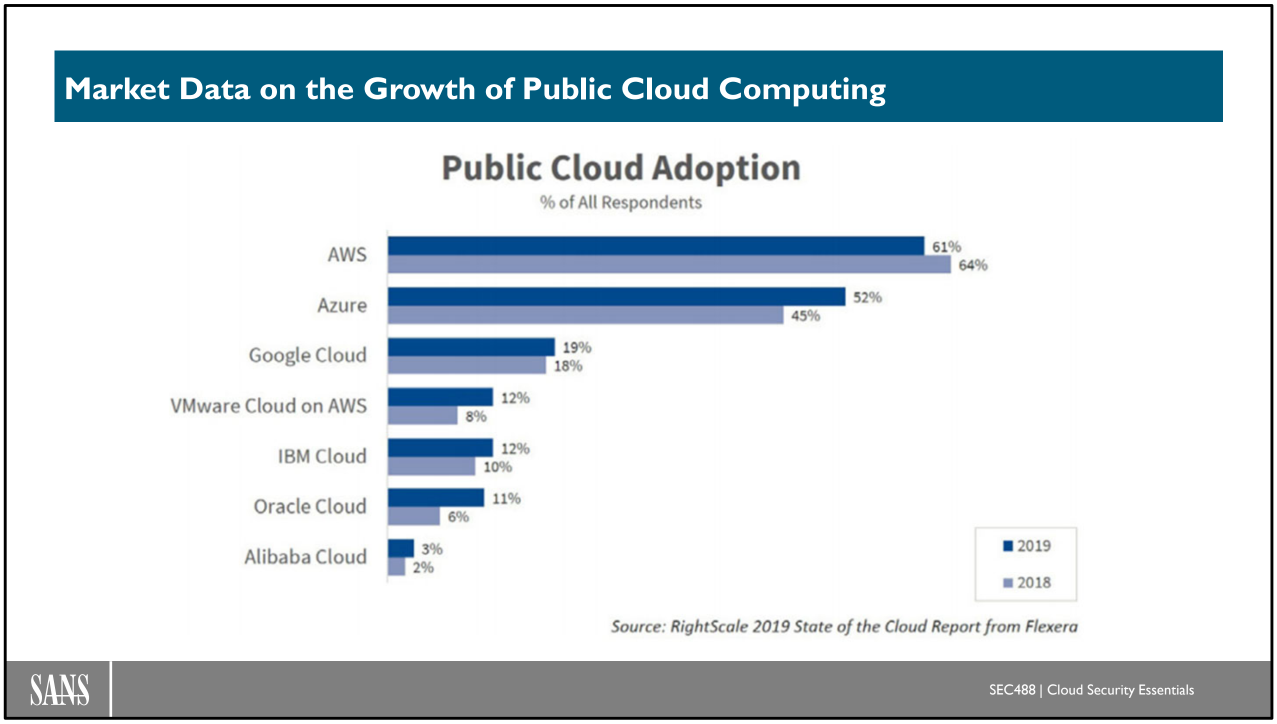
SANS

SEC488 | Cloud Security Essentials

Course Roadmap

Each section of this course presents a Course Roadmap slide to help you follow where we are in the course material. These “you are here” slides will also help you easily locate information for after-class review.

Before jumping into the “What is the Cloud” module, let’s cover an overview of the 488 course.



Market Data on the Growth of Public Cloud Computing

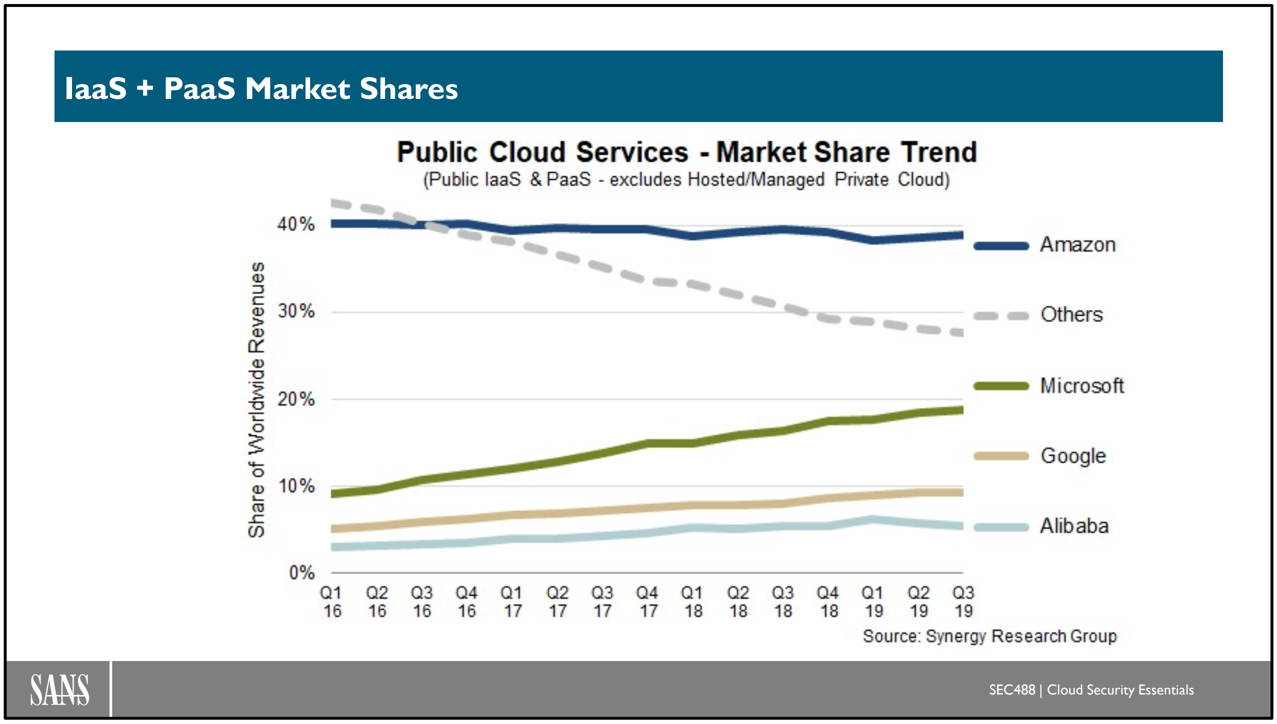
Source: RightScale 2019 State of the Cloud Report from Flexera

This slide shows data from the RightScale 2019 State of the Cloud Report.

Interestingly, in 2017 AWS Had 57% market share, Azure had 34%, and GCP had 15%

This slide shows *which* cloud service providers are being used, while the slide on the next page shows *how much* each provider is being used.

[1] https://www.rightscale.com/lp/state-of-the-cloud



IaaS + PaaS Market Shares

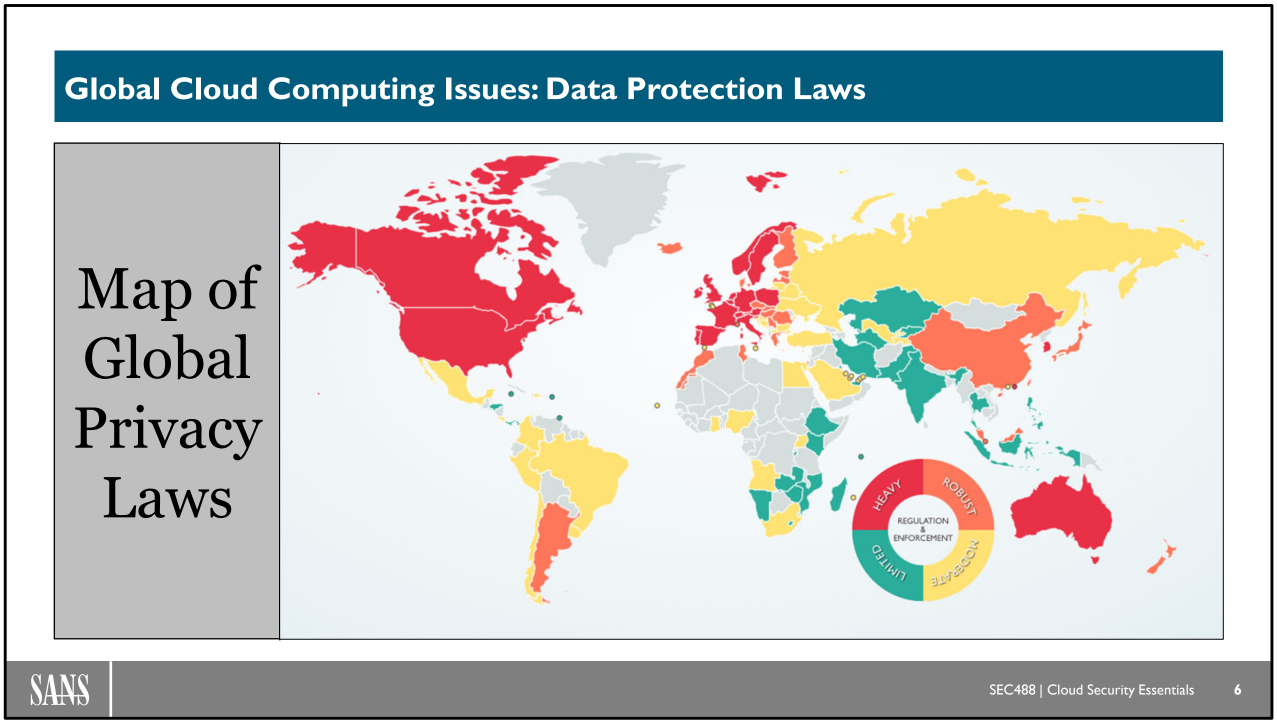
Source: Synergy Research Group

SANS

SEC488 | Cloud Security Essentials

According to the Synergy Research Group, Amazon is still the market leader by a significant margin. Microsoft is aggressively ramping up its cloud campaign in terms of maturing its cloud offerings as well as its and marketing efforts. Google is definitely a player with solid cloud products and loyal customers. It will be interesting to see what IBM does with their acquisition of RedHat, based on press releases talking about going after the hybrid cloud market. Alibaba will be certainly important to track as well, particularly as they expand their footprint outside of China.

[1] https://www.cnbc.com/2018/04/27/microsoft-gains-cloud-market-share-in-q1-but-aws-still-dominates.html



Global Cloud Computing Issues: Data Protection Laws

Map of Global Privacy Laws

Each sovereign country has the right to adopt data protection laws, and many countries have. The map on the slide above provides a visual indication of the extent of regulation and enforcement on a country by country basis. One of the most significant laws is GDPR, also known as The General Data Protection Regulation (Regulation (EU) 2016/679) which took effect on May 25, 2018 and applies to European Union member states.

Complying with the data protection laws everywhere that a company may operate adds a significant compliance burden and it is highly recommended that cloud security professionals work closely with the legal counsel that supports their organization to ensure awareness of and compliance to all applicable data protection laws. Operating in the public cloud adds additional layers of complexity to this challenge. Complicating factors include:

- The geographic location where the data is stored in the public cloud,
- Where the data is accessed from, and
- Where the data is transferred to.

Awareness of data protection laws is important for the cloud security professional so that they are aware of when to engage with the company's privacy attorneys. A good high-level analysis on a country by country basis is available at https://www.dlapiperdataprotection.com/.

Map from: https://www.dlapiperdataprotection.com/index.html?t=world-map

SEC488 - Day 1 Labs

Lab 1.1 - Exploring the Web Consoles of AWS, Azure, GCP, and Alibaba

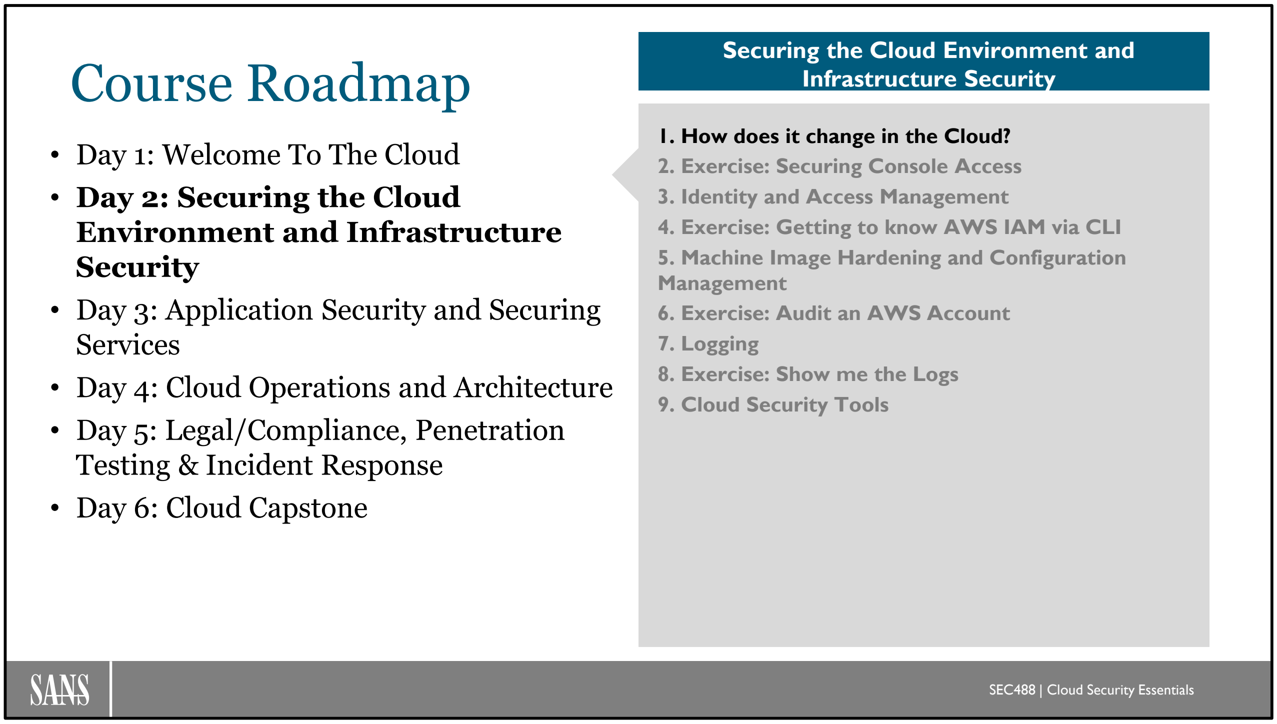
Lab 1.2 - Launching Virtual Machines in AWS and Azure¶

Lab 1.3 - Exploring Platform as a Service Offerings

Lab 1.4 - High Level Security Assessment of Box

SEC488 – Day 2

Kyle Dickinson



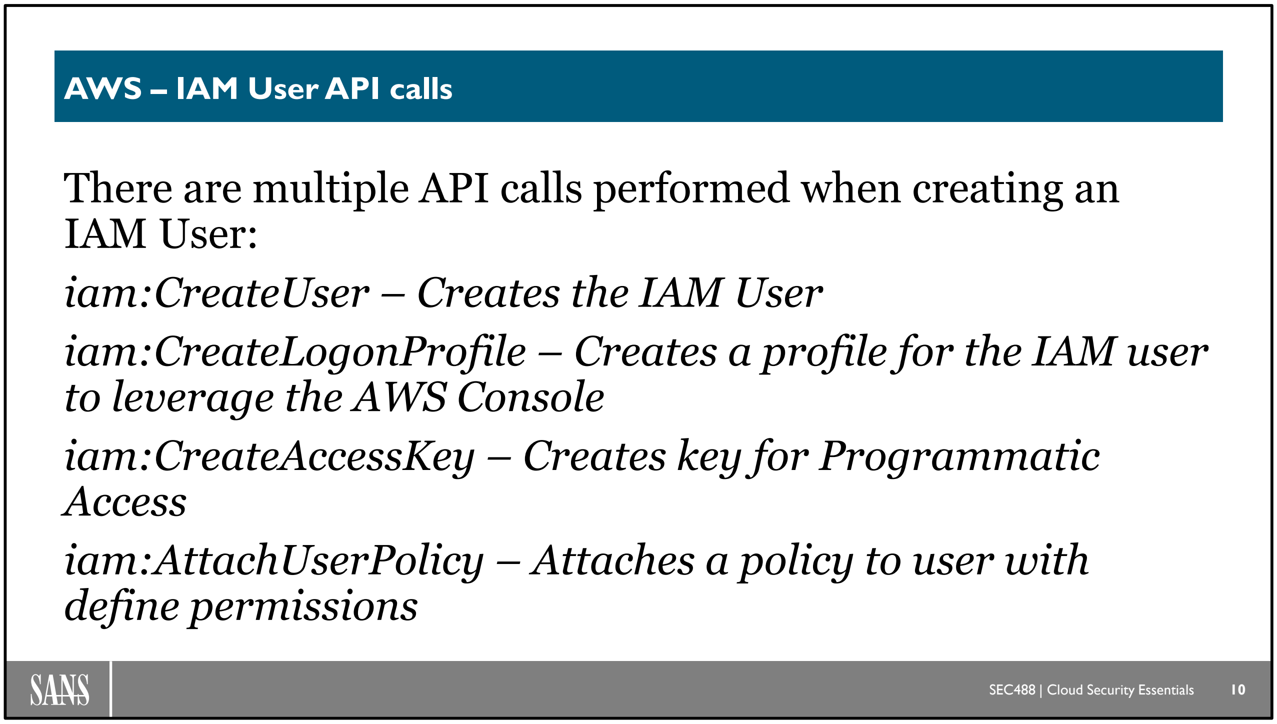
Course Roadmap

- Day 1: Welcome To The Cloud
- **Day 2: Securing the Cloud Environment and Infrastructure Security**
- Day 3: Application Security and Securing Services
- Day 4: Cloud Operations and Architecture
- Day 5: Legal/Compliance, Penetration Testing & Incident Response
- Day 6: Cloud Capstone

Securing the Cloud Environment and Infrastructure Security

1. **How does it change in the Cloud?**
2. Exercise: Securing Console Access
3. Identity and Access Management
4. Exercise: Getting to know AWS IAM via CLI
5. Machine Image Hardening and Configuration Management
6. Exercise: Audit an AWS Account
7. Logging
8. Exercise: Show me the Logs
9. Cloud Security Tools

Left blank intentionally



AWS – IAM User API calls

There are multiple API calls performed when creating an IAM User:

iam:CreateUser – Creates the IAM User

iam:CreateLogonProfile – Creates a profile for the IAM user to leverage the AWS Console

iam:CreateAccessKey – Creates key for Programmatic Access

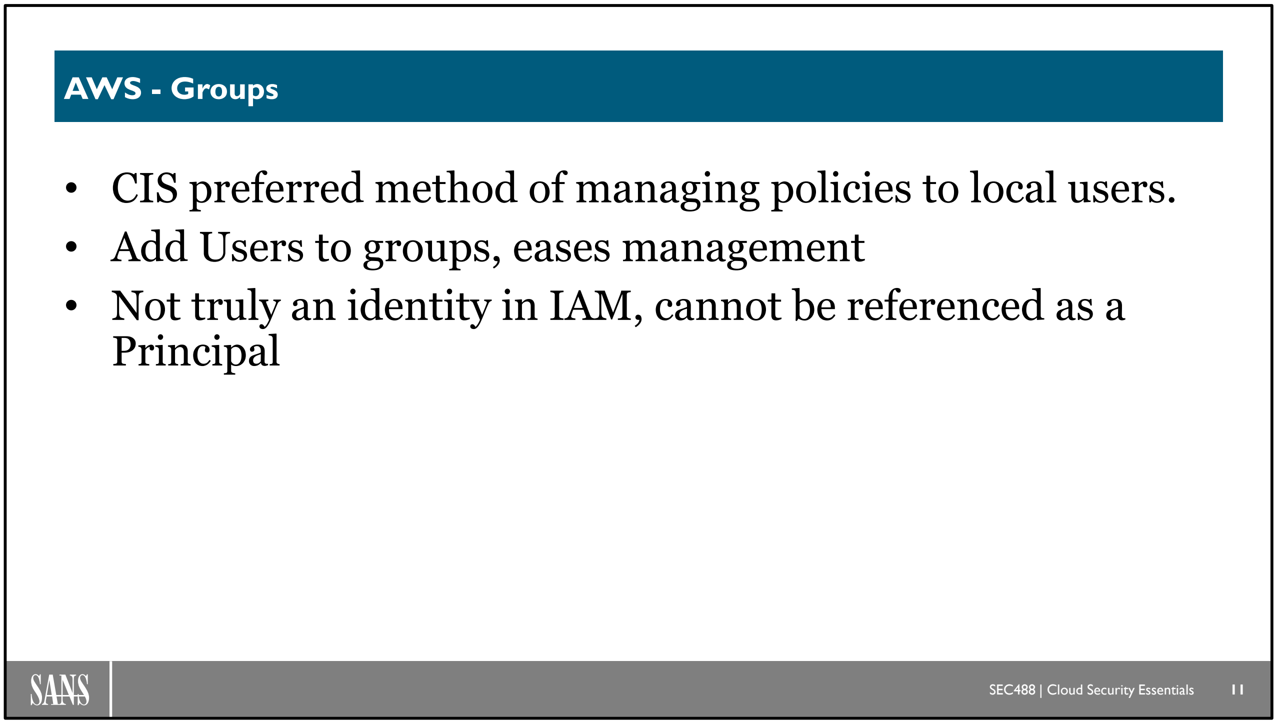
iam:AttachUserPolicy – Attaches a policy to user with define permissions

When creating IAM Users – it's good to know the assortment of API calls that are performed to create a user. This gives us granular control over the IAM User object – as well as the ability to alert on specific actions performed against IAM Users

Common Use Cases:

- Development team(s) can create Local IAM User with Access Key, however they do not have permission to assign a console password.

- Only the Security Team can create IAM Users; however the Development Team can create/rotate the access key for that user

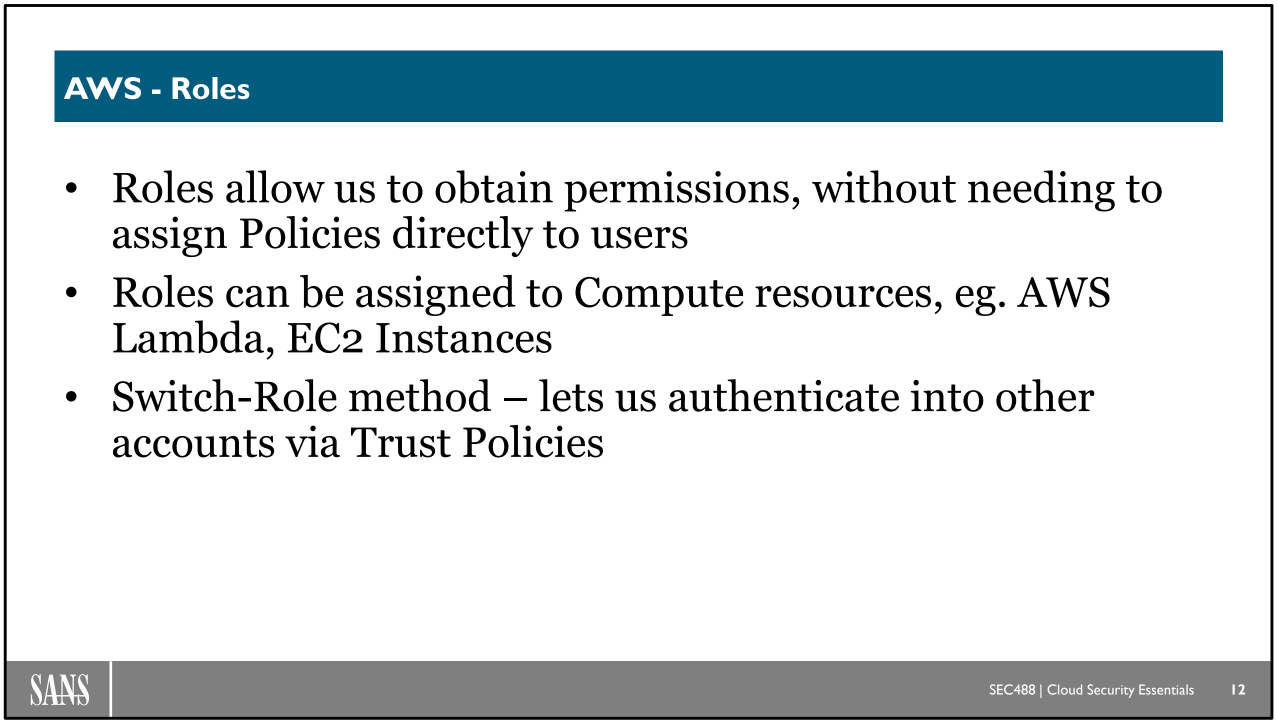


AWS - Groups

- CIS preferred method of managing policies to local users.
- Add Users to groups, eases management
- Not truly an identity in IAM, cannot be referenced as a Principal

AWS Groups can be compared to Active Directory Global Groups. It allows us to take multiple IAM Users, and group them with permissions. IAM Group cannot be nested.

Using groups aids in auditing what Users have access to – instead of having Policies attached directly to the user and follows the CIS Benchmarks for AWS recommendation.



AWS - Roles

- Roles allow us to obtain permissions, without needing to assign Policies directly to users
- Roles can be assigned to Compute resources, eg. AWS Lambda, EC2 Instances
- Switch-Role method – lets us authenticate into other accounts via Trust Policies

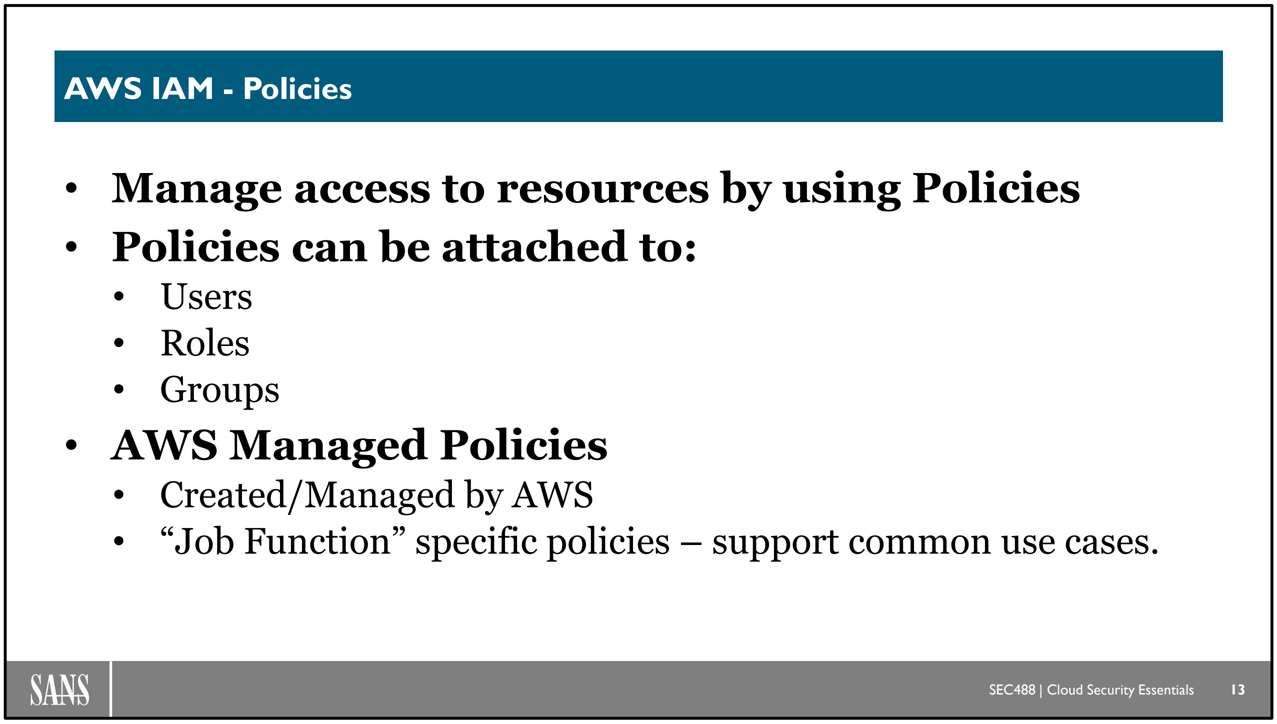
IAM Roles are similar to IAM Users in that we can assign policies to Roles and determines what can and cannot be done within our AWS Account(s). However IAM Roles are meant to be assumed by either a Federated User (using Single Sign-On), or Resource (EC2, Lambda, etc.).

Unlike IAM Users leveraging long-term Access Keys and Secrets. The benefits of using IAM Roles are the temporary, short-lived tokens that are generated to provide the authorized resource or user access to perform functions within AWS.

Roles consist of:

- Attached Policies for Permissions
- Trust relationship – Who is trusted to assume this role. This can be a federated identity, an AWS resource, or another AWS Account.
- Tags
- Access Advisor

Access Advisor allows us to audit what Services a role has permissions to, and when the last time the role accessed that service. This can help scope down permissions to roles.



AWS IAM - Policies

- **Manage access to resources by using Policies**
- **Policies can be attached to:**
  - Users
  - Roles
  - Groups
- **AWS Managed Policies**
  - Created/Managed by AWS
  - “Job Function” specific policies – support common use cases.

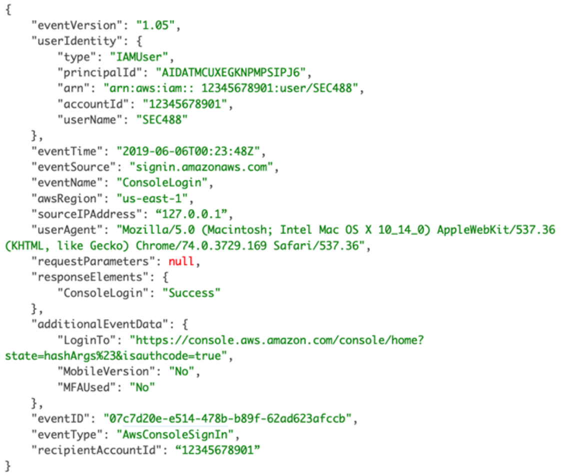
AWS IAM Policies are what provide the authorization to access different resources within our AWS environment. Policies, like most things within “the Cloud” are structured in JSON.

AWS Managed Policies are a great starting point, and AWS has the ability to update these ‘Managed’ policies as they come out with new services, and add more functionality to existing services.

With that said – your organization should look to evaluate the risk of if you want policies within your environment to be updated, without some approval pipeline.

CloudTrail Example

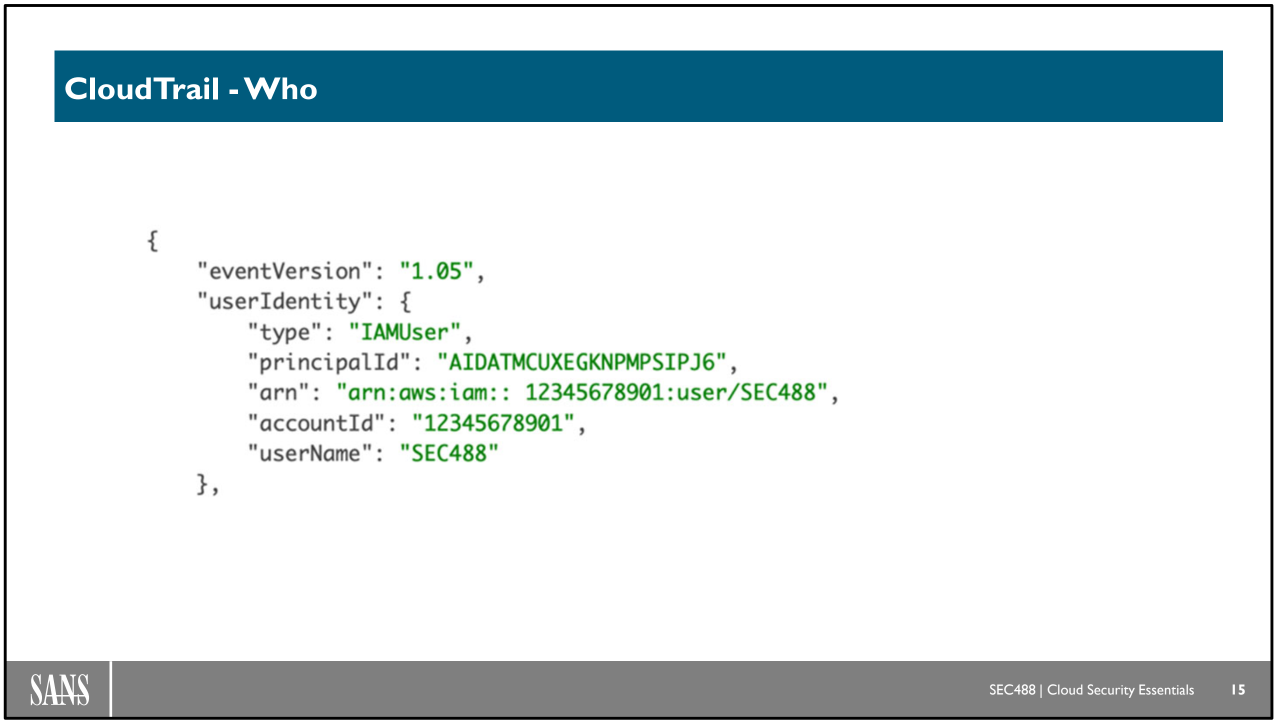
- CloudTrail events are in JSON format
- Details the:
  - Who/What/Where/When/How



```
{
    "eventVersion": "1.05",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "AIDATMCUXEGKNPMPSIPJ6",
        "arn": "arn:aws:iam:: 12345678901:user/SEC488",
        "accountId": "12345678901",
        "userName": "SEC488"
    },
    "eventTime": "2019-06-06T00:23:48Z",
    "eventSource": "signin.amazonaws.com",
    "eventName": "ConsoleLogin",
    "awsRegion": "us-east-1",
    "sourceIPAddress": “127.0.0.1”,
    "userAgent": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_0) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/74.0.3729.169 Safari/537.36",
    "requestParameters": null,
    "responseElements": {
        "ConsoleLogin": "Success"
    },
    "additionalEventData": {
        "LoginTo": "https://console.aws.amazon.com/console/home?
state=hashArgs%23&isauthcode=true",
        "MobileVersion": "No",
        "MFAUsed": "No"
    },
    "eventID": "07c7d20e-e514-478b-b89f-62ad623afccb",
    "eventType": "AwsConsoleSignIn",
    "recipientAccountId": “12345678901”
}
```

Here is an example of a CloudTrail log. Fortunately CloudTrail is in a structured format, JSON (JavaScript Object Notation) so that we’re able to iterate through it with automation, or 3rd party logging tools.

We’re going to break down the a CloudTrail entry in its entirety in the next couple of slides.



CloudTrail - Who

```
{
    "eventVersion": "1.05",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "AIDATMCUXEGKNPMPSIPJ6",
        "arn": "arn:aws:iam:: 12345678901:user/SEC488",
        "accountId": "12345678901",
        "userName": "SEC488"
    },
```

The first section of the CloudTrail Logs will tell us who is making the API call within the “**userIdentity**” stanza along with additional user details.

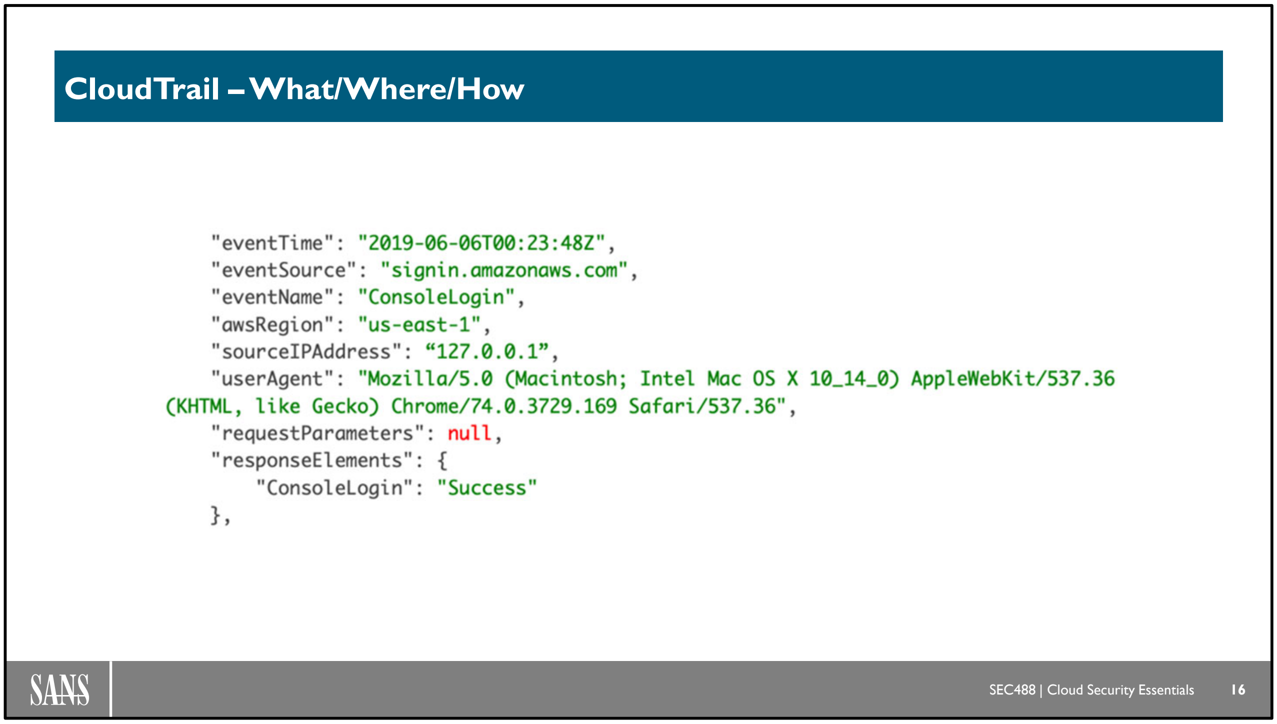
Under **userIdentity**:
type – This can be an IAM User, or Role

principalId – This is a unique identifier (similar to a SID) that AWS shows programmatically – you won’t find this in the AWS Console itself

Arn – This tells us the ARN of the User or Role that was used to Authenticate

accountId: Shows the Account ID that was authenticated into

userName: For local IAM Users, it will show the IAM User Name. For federated identities such as Active Directory – it will show the user’s Network ID, example: SMITHJ2



CloudTrail – What/Where/How

```
    "eventTime": "2019-06-06T00:23:48Z",
    "eventSource": "signin.amazonaws.com",
    "eventName": "ConsoleLogin",
    "awsRegion": "us-east-1",
    "sourceIPAddress": “127.0.0.1”,
    "userAgent": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_0) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/74.0.3729.169 Safari/537.36",
    "requestParameters": null,
    "responseElements": {
        "ConsoleLogin": "Success"
    },
```

In this section of the CloudTrail log:

eventTime - Time that the action was performed. This is logged in Zulu/epoch time

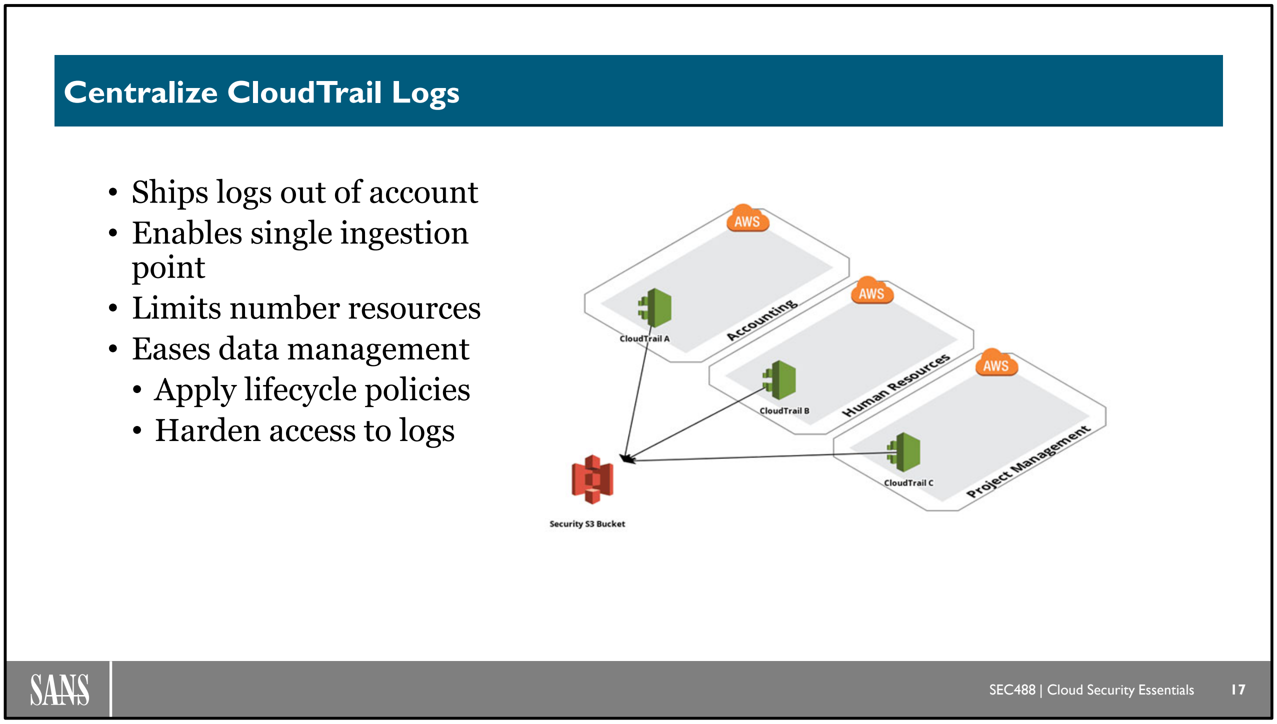
eventSource - Origin of the API call. There’s multiple eventSources, such as iam.amazonaws.com, ec2.amazonaws.com, etc…

eventName - The action that was performed, example: RunInstance, CreateUser, StopInstance

userAgent - This can be a browser version, CLI version, or SDK version

requestParameters: Information sent with the request, such as: Instance Type, AMI ID, Security Group ID

responseElements: If the action was successful, or if there was missing parameters

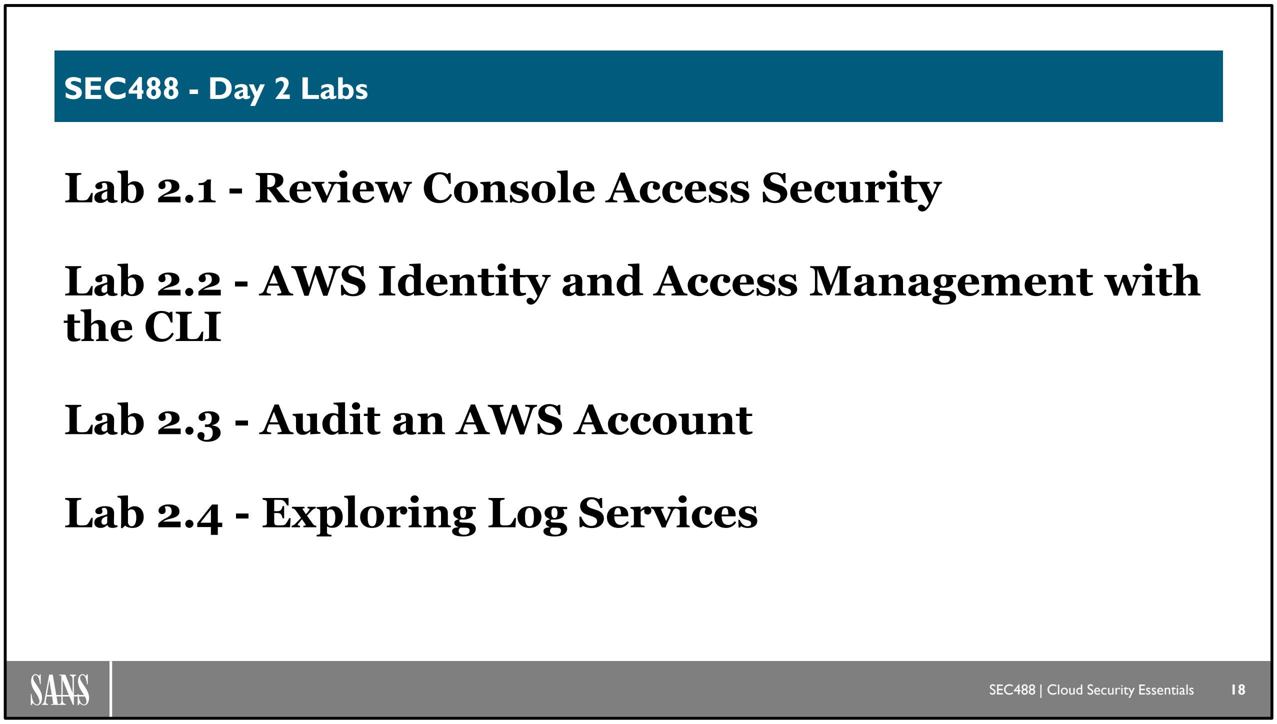


Centralize CloudTrail Logs

- Ships logs out of account
- Enables single ingestion point
- Limits number resources
- Eases data management
  - Apply lifecycle policies
  - Harden access to logs

Centralizing our CloudTrail logs allow us to reduce the technical debt and management overhead of having multiple points of ingestion throughout our environment. As you recall, we want to scale our security controls to an environment that can continuously grow.

https://docs.aws.amazon.com/awscloudtrail/latest/userguide/cloudtrail-receive-logs-from-multiple-accounts.html will outline the steps necessary to take for you to implement this into your environment



SEC488 - Day 2 Labs

Lab 2.1 - Review Console Access Security

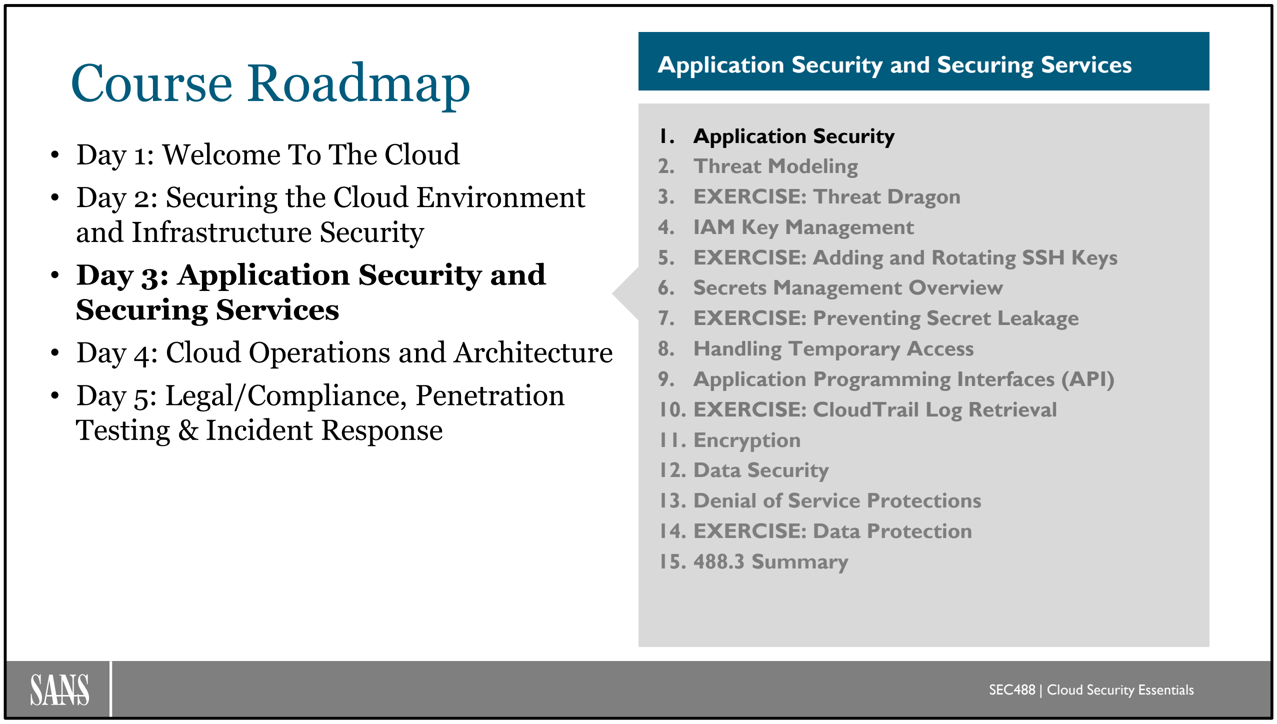
Lab 2.2 - AWS Identity and Access Management with the CLI

Lab 2.3 - Audit an AWS Account

Lab 2.4 - Exploring Log Services

SEC488 – Day 3

Ryan Nicholson



Course Roadmap

- Day 1: Welcome To The Cloud
- Day 2: Securing the Cloud Environment and Infrastructure Security
- **Day 3: Application Security and Securing Services**
- Day 4: Cloud Operations and Architecture
- Day 5: Legal/Compliance, Penetration Testing & Incident Response

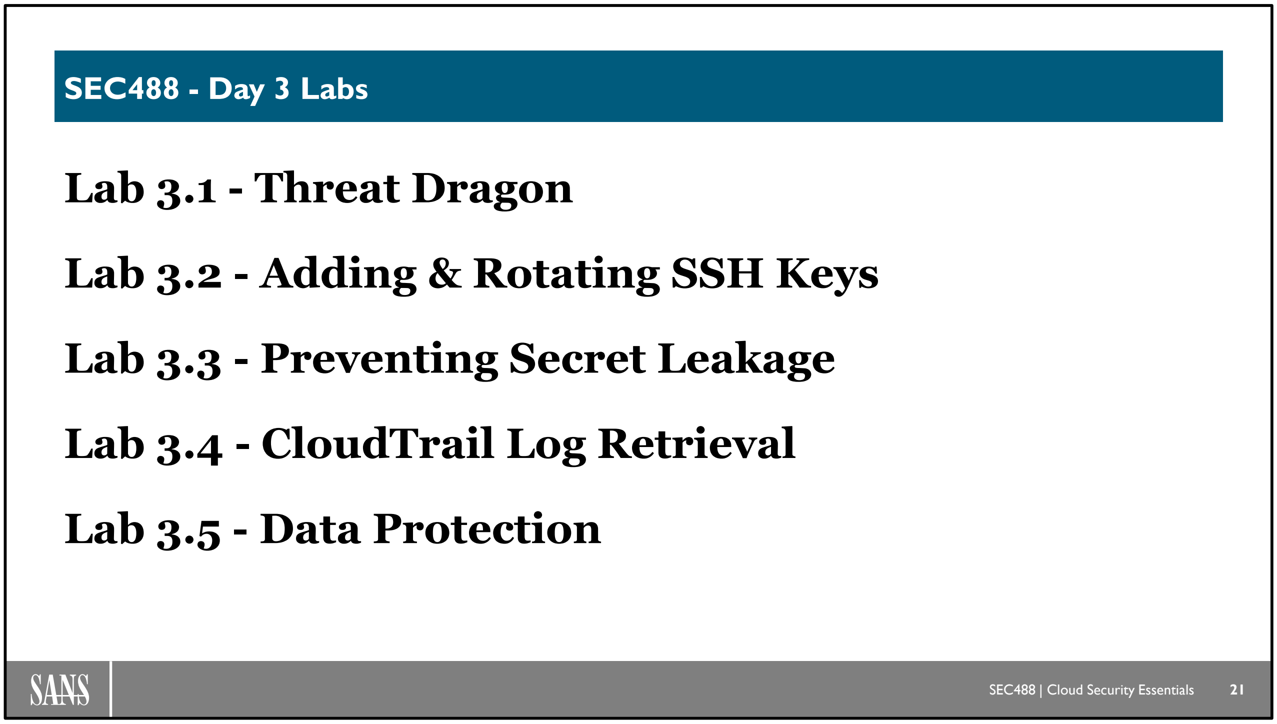
Application Security and Securing Services

1. **Application Security**
2. Threat Modeling
3. EXERCISE: Threat Dragon
4. IAM Key Management
5. EXERCISE: Adding and Rotating SSH Keys
6. Secrets Management Overview
7. EXERCISE: Preventing Secret Leakage
8. Handling Temporary Access
9. Application Programming Interfaces (API)
10. EXERCISE: CloudTrail Log Retrieval
11. Encryption
12. Data Security
13. Denial of Service Protections
14. EXERCISE: Data Protection
15. 488.3 Summary

SEC488 | Cloud Security Essentials

Course Roadmap

Welcome to book three of SEC488. We will begin discussion on application security fundamentals. The purpose of this section is to introduce the complexities of a secure application development lifecycle. This will support awareness of what challenges exist when migrating applications to the cloud and how the cloud could even aid in supporting a secure development life cycle.



SEC488 - Day 3 Labs

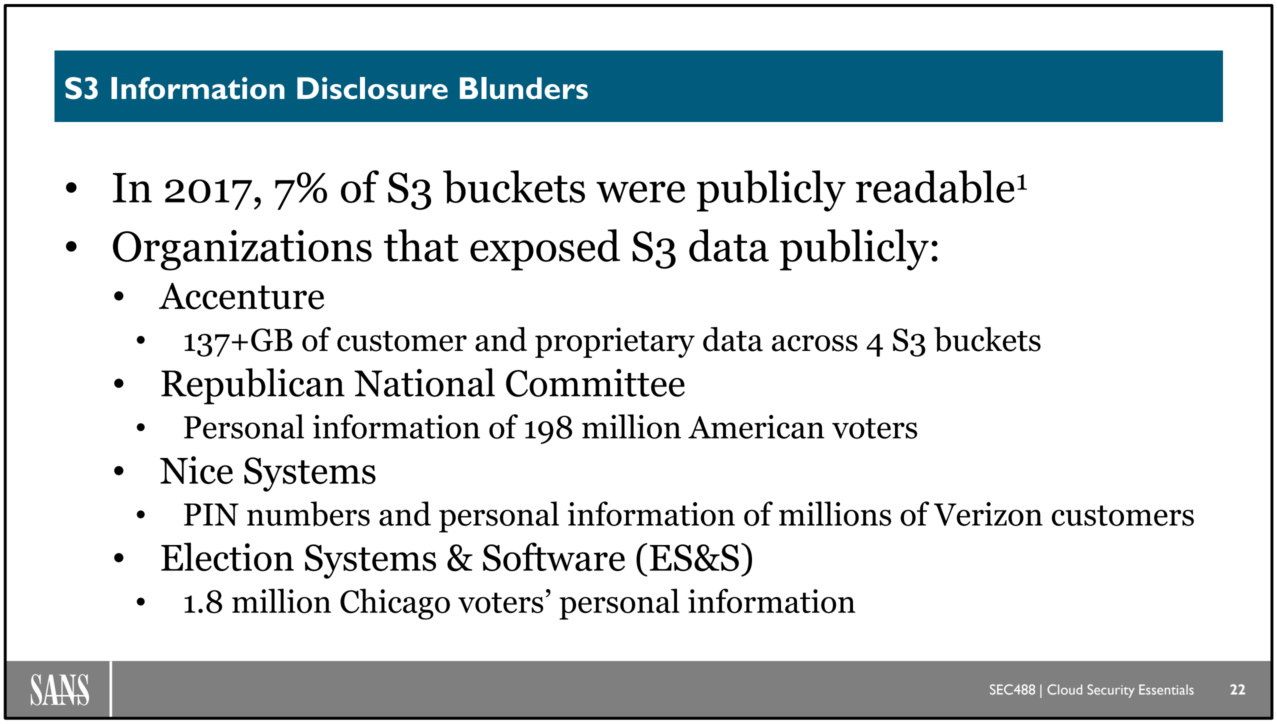
Lab 3.1 - Threat Dragon

Lab 3.2 - Adding & Rotating SSH Keys

Lab 3.3 - Preventing Secret Leakage

Lab 3.4 - CloudTrail Log Retrieval

Lab 3.5 - Data Protection



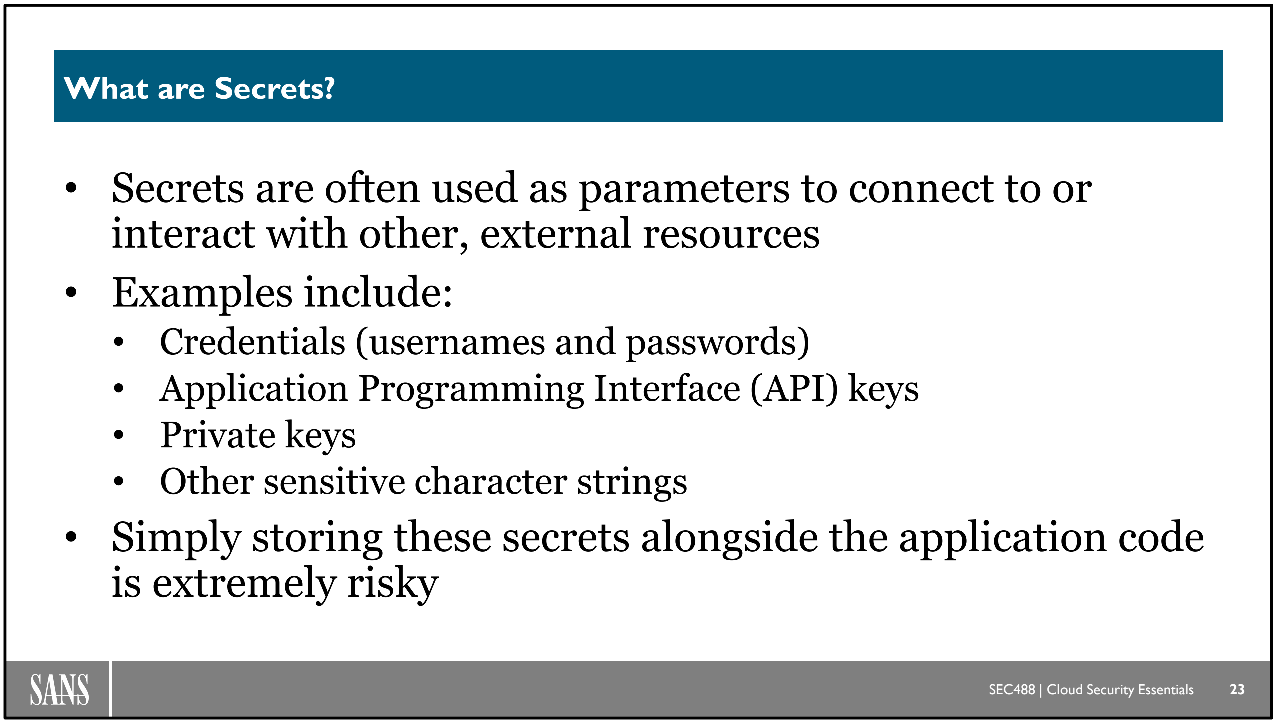
S3 Information Disclosure Blunders

- In 2017, 7% of S3 buckets were publicly readable[1]
- Organizations that exposed S3 data publicly:
  - Accenture
    - 137+GB of customer and proprietary data across 4 S3 buckets
  - Republican National Committee
    - Personal information of 198 million American voters
  - Nice Systems
    - PIN numbers and personal information of millions of Verizon customers
  - Election Systems & Software (ES&S)
    - 1.8 million Chicago voters' personal information

S3 Information Disclosure Blunders

Plenty of examples exist showcasing organizations' improper protection of data in cloud environments which lead to information disclosure. Above are just four high profile breaches from 2017 and what was lost as a result.

[1] https://www.skyhighnetworks.com/cloud-security-blog/reduce-aws-s3-bucket-data-exposures-with-the-right-protection/
[2] https://www.cybersecurity-insiders.com/top-5-cloud-security-related-data-breaches/



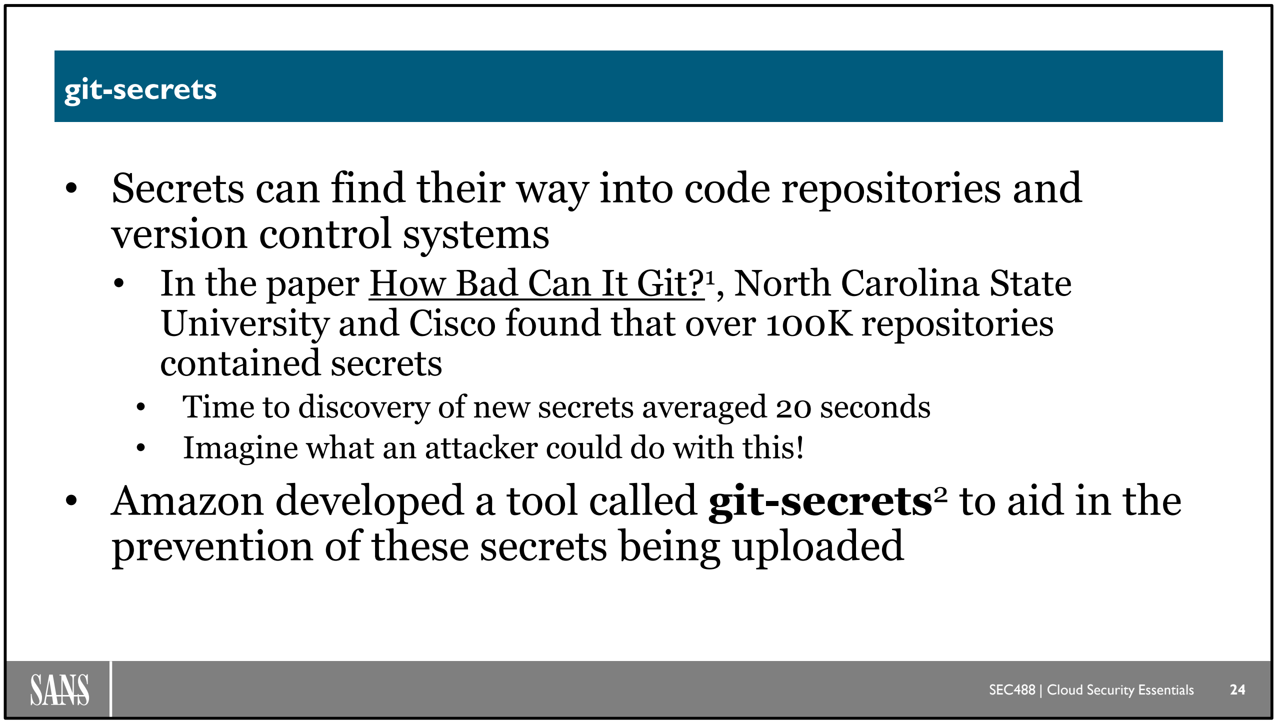
What are Secrets?

- Secrets are often used as parameters to connect to or interact with other, external resources
- Examples include:
  - Credentials (usernames and passwords)
  - Application Programming Interface (API) keys
  - Private keys
  - Other sensitive character strings
- Simply storing these secrets alongside the application code is extremely risky

What are Secrets?

Secrets are sensitive information that often provide a means to connect or interact with other resources. These range from application and database credentials, Application Programming Interface (API) keys, private keys, and anything else an organization may deem sensitive. A frequently occurring issue is that these secrets are stored in plaintext on a system (or even worse, upload to GitHub).

As an example of plaintext secrets storage, many web applications require access to a database to store and retrieve pertinent information. The secrets in this case would be the database username, database password, and the database name which is used by the application to connect to the database server and read/write the data held within. These secrets are often stored in configuration files used by the web application.



git-secrets

- Secrets can find their way into code repositories and version control systems
  - In the paper How Bad Can It Git?[1], North Carolina State University and Cisco found that over 100K repositories contained secrets
    - Time to discovery of new secrets averaged 20 seconds
    - Imagine what an attacker could do with this!
- Amazon developed a tool called **git-secrets**[2] to aid in the prevention of these secrets being uploaded

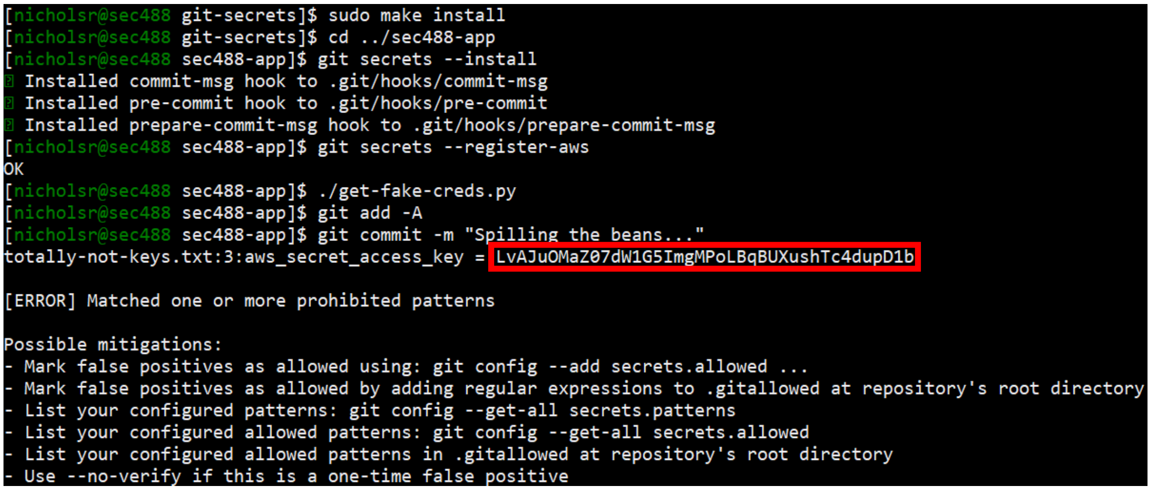
git-secrets

All too often secrets find their way into code repositories and version control systems like GitHub, GitLab, and Bitbucket. In the research paper How Bad Can It Git?[1], North Carolina State University and Cisco conducted a study on secrets stored in GitHub from October 2017 through April 2018. They found that over 100K repositories contained secrets. Not only that, but roughly 1000 code commits per day contained secrets. Their mean time to discover new secrets was only 20 seconds! Just imagine what an attacker could do with this.

To combat this, Amazon developed a tool called **git-secrets**[1] to aid in the prevention of these secrets being uploaded. This package is very easy to install and provides great assurance that most patterns that appear to be a potential secret will be detected. It gets better. You can configure git-secrets to run every time a code commit is issued in case a secret tries to sneak through when you forgot to run git-secrets manually. You can also add patterns of you choice to the .git/config file as well.

[1] https://www.ndss-symposium.org/wp-content/uploads/2019/02/ndss2019_04B-3_Meli_paper.pdf
[2] https://github.com/awslabs/git-secrets

git-secrets Cont.



```
[nicholsr@sec488 git-secrets]$ sudo make install
[nicholsr@sec488 git-secrets]$ cd ../sec488-app
[nicholsr@sec488 sec488-app]$ git secrets --install
⍰ Installed commit-msg hook to .git/hooks/commit-msg
⍰ Installed pre-commit hook to .git/hooks/pre-commit
⍰ Installed prepare-commit-msg hook to .git/hooks/prepare-commit-msg
[nicholsr@sec488 sec488-app]$ git secrets --register-aws
OK
[nicholsr@sec488 sec488-app]$ ./get-fake-creds.py
[nicholsr@sec488 sec488-app]$ git add -A
[nicholsr@sec488 sec488-app]$ git commit -m "Spilling the beans..."
totally-not-keys.txt:3:aws_secret_access_key = LvAJuOMaZ07dW1G5ImgMPoLBqBUXushTc4dupD1b

[ERROR] Matched one or more prohibited patterns

Possible mitigations:
- Mark false positives as allowed using: git config --add secrets.allowed ...
- Mark false positives as allowed by adding regular expressions to .gitallowed at repository's root directory
- List your configured patterns: git config --get-all secrets.patterns
- List your configured allowed patterns: git config --get-all secrets.allowed
- List your configured allowed patterns in .gitallowed at repository's root directory
- Use --no-verify if this is a one-time false positive
```

git-secrets Cont.

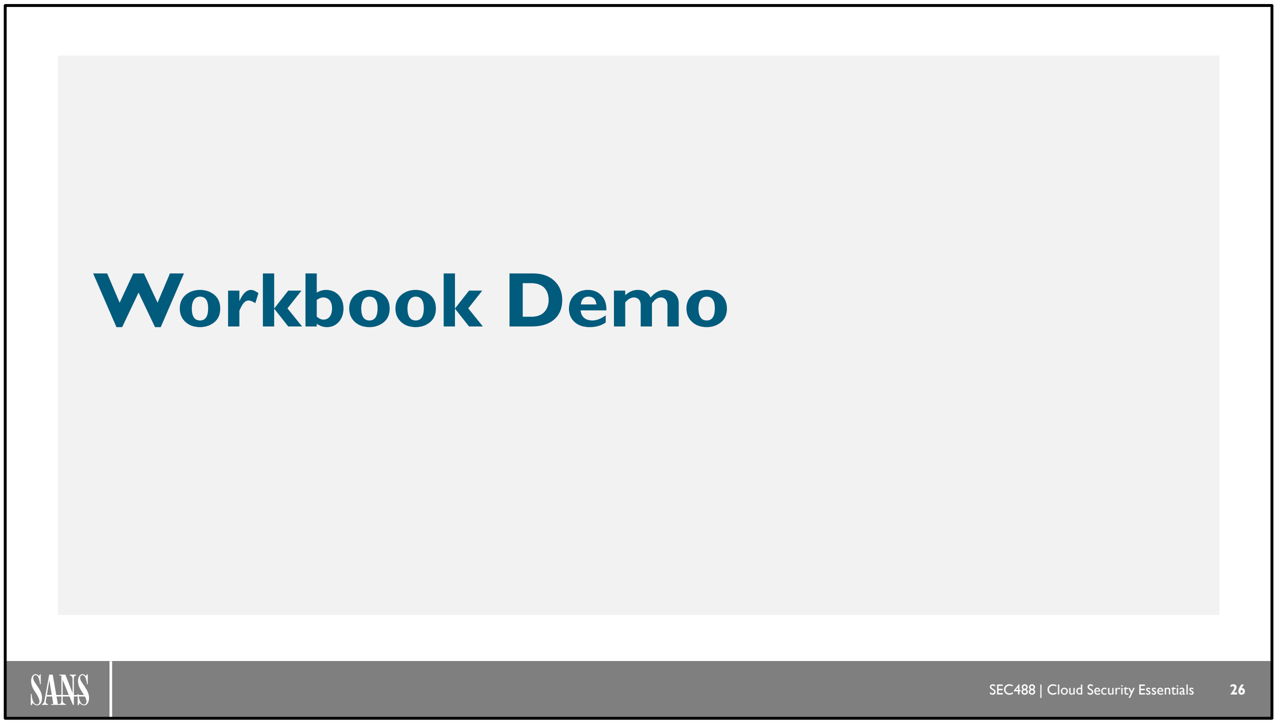
On this workstation, git-secrets was installed by simply pulling the code down and installing with a single command as follows:

```
git clone https://github.com/awslabs/git-secrets.git
make install
```

To ensure that all repositories will run git-secrets during an attempted commit, a few commands will need to be run inside the root of each repository directory:

```
git secrets --install
git secrets --register-aws
git secrets --add <pattern to match>
```

More information on how to configure git-secrets can be found at https://github.com/awslabs/git-secrets/blob/master/README.rst#advanced-configuration



Workbook Demo

Since I have the mic now, I'll discuss something I am very passionate about, not only because it's part of my day job, but because I love the fact that we can keep our material as fresh as possible. Most SANS classes have been moving to an electronic workbook that is contained inside your VM but, because we're a cloud course, there is no VM. Our electronic workbook is hosted in AWS. As one of the folks who own the rights to this material, I sure hope we're practicing what we're preaching...

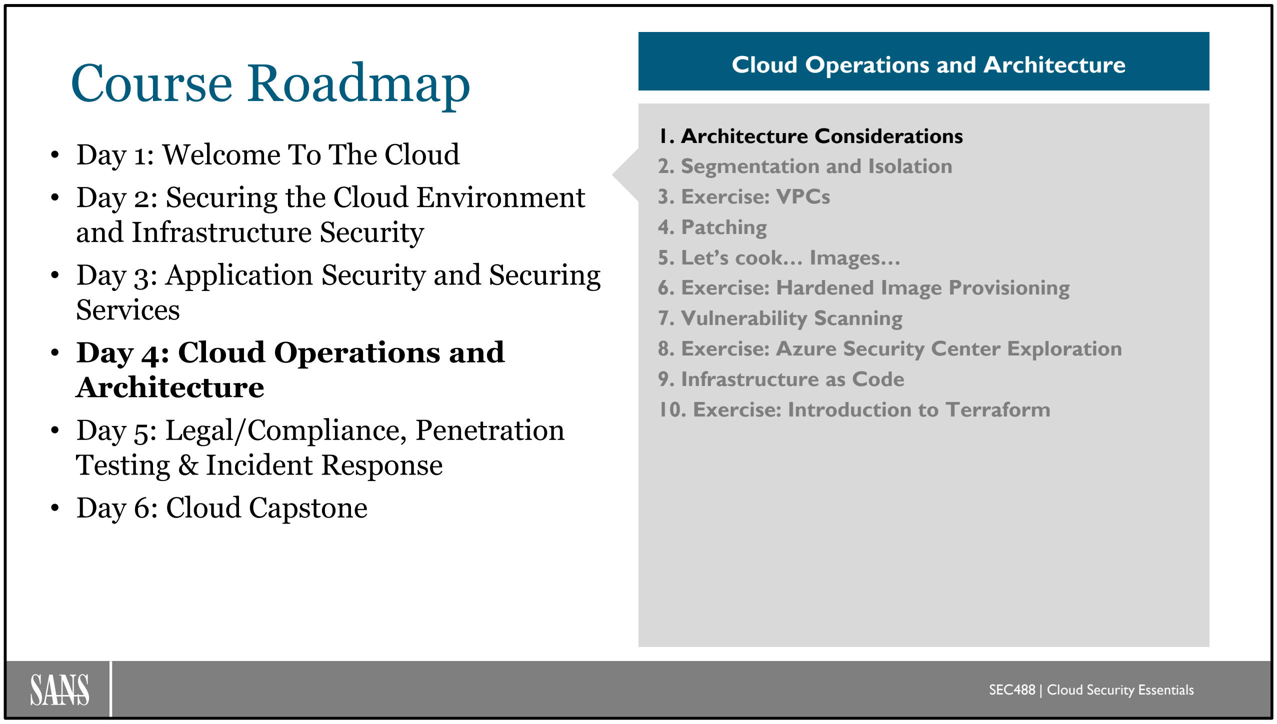
Anyway, I have this password protected so you shouldn't be able to access it (unless you are a student and we gave the credentials to you), but here is what you will see as a student when you go to https://workbook.sec488.com. The homepage could use some work as you can see, but will likely have the final course description, where to go when you have questions, etc, but that's not why I'm showing you this. I'm showing you this because of the labs. For example, the last lab I was discussing – lab 3.3 - is right here.

You will likely get a physical workbook with this course that has all of this in it, but there are many advantages to using the electronic workbook like... copy and paste. Many labs fail due to typos and, this isn't a typing class, so let's focus on what we're trying to achieve by helping the student avoid these mistakes. Not only that, but the authors can make any updates on the fly – something we cannot do with the physical workbook. These updates could range from grammar mistakes, student feedback saying that there is a better or more efficient way to do something, cloud vendors update things (they never do that right?), or even bonus labs that we feel you will benefit from – even after taking the class.

With that, I'll send you back to Kyle.

SEC488 – Day 4

Kyle Dickinson



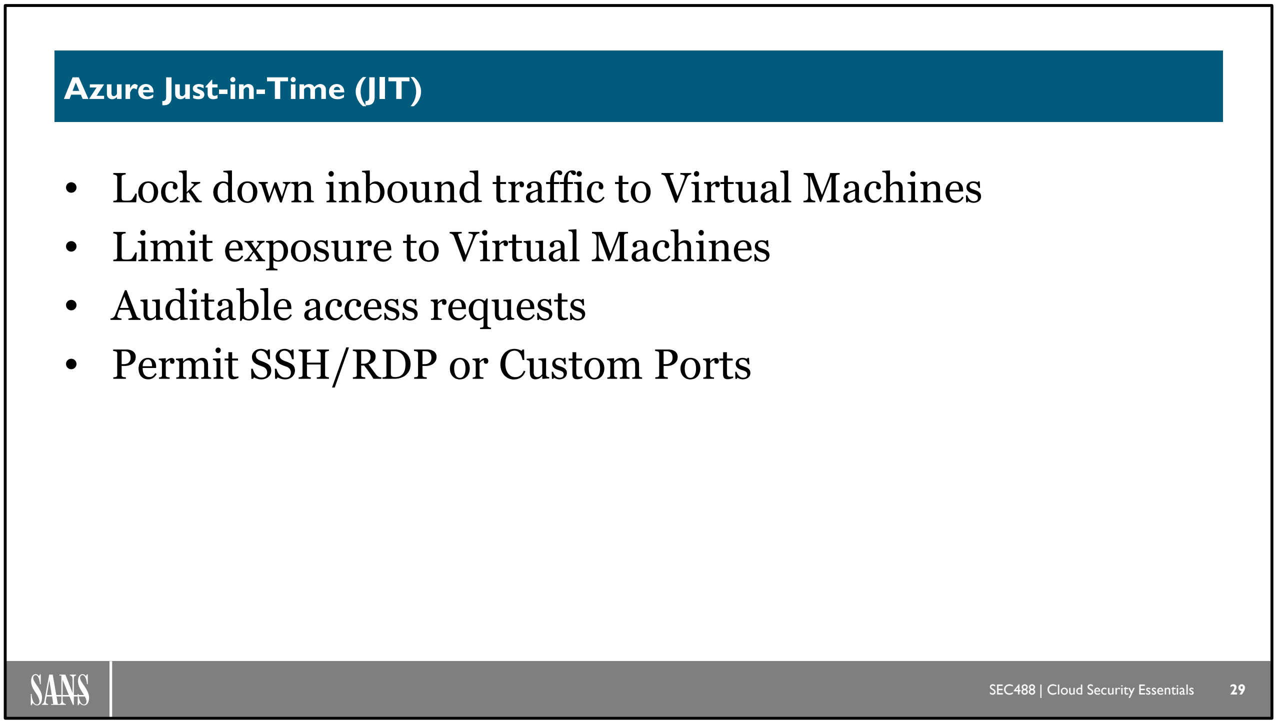
Course Roadmap

- Day 1: Welcome To The Cloud
- Day 2: Securing the Cloud Environment and Infrastructure Security
- Day 3: Application Security and Securing Services
- **Day 4: Cloud Operations and Architecture**
- Day 5: Legal/Compliance, Penetration Testing & Incident Response
- Day 6: Cloud Capstone

Cloud Operations and Architecture

1. **Architecture Considerations**
2. Segmentation and Isolation
3. Exercise: VPCs
4. Patching
5. Let’s cook… Images…
6. Exercise: Hardened Image Provisioning
7. Vulnerability Scanning
8. Exercise: Azure Security Center Exploration
9. Infrastructure as Code
10. Exercise: Introduction to Terraform

Left blank intentionally



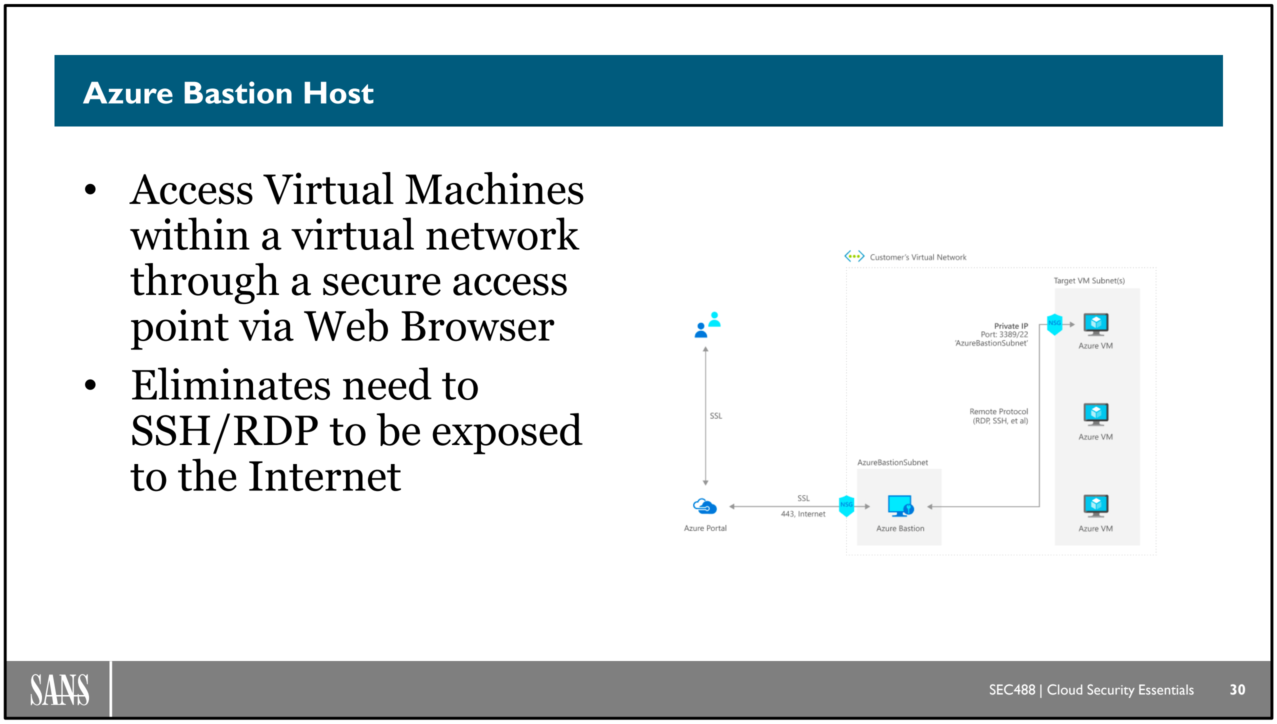
Azure Just-in-Time (JIT)

- Lock down inbound traffic to Virtual Machines
- Limit exposure to Virtual Machines
- Auditable access requests
- Permit SSH/RDP or Custom Ports

Placing Virtual Machines on the internet can be risky business – and part of this risk can originate from permitting SSH or Remote Desktop access to a Virtual Machine. There are use-cases where developers and support teams will need to have a sort of firefighter like access to a Virtual Machine. Just-in-Time access allows this type of access for a certain amount of time; this mitigate the "temporary access rule" that tends to last more than a temporary time.

Just-in-Time access will automatically close access to the permitted request, after the duration ends, and as an access request is performed on a Virtual Machine behind Azure Firewall. Security Center auto-configures the Network Security Group (NSG) and Firewall Policy rules for the duration of the request.

https://docs.microsoft.com/en-us/azure/security-center/security-center-just-in-time



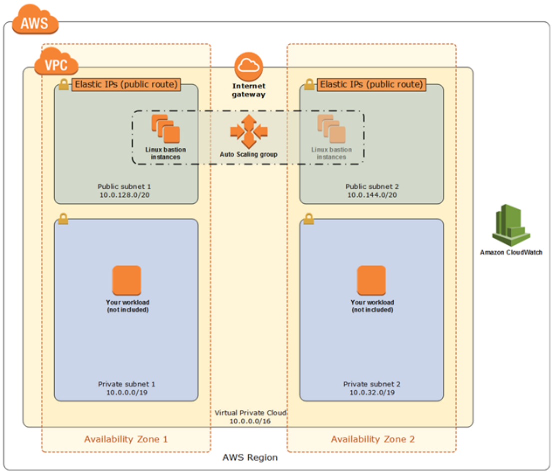
Azure Bastion Host

- Access Virtual Machines within a virtual network through a secure access point via Web Browser
- Eliminates need to SSH/RDP to be exposed to the Internet

Utilizing Bastion Hosts has been a common practice to access Virtual Machines – with Azure Bastion Host service, Azure deploys a fully managed Platform as a Service within your Virtual Network that provides connectivity to your Virtual Machines.

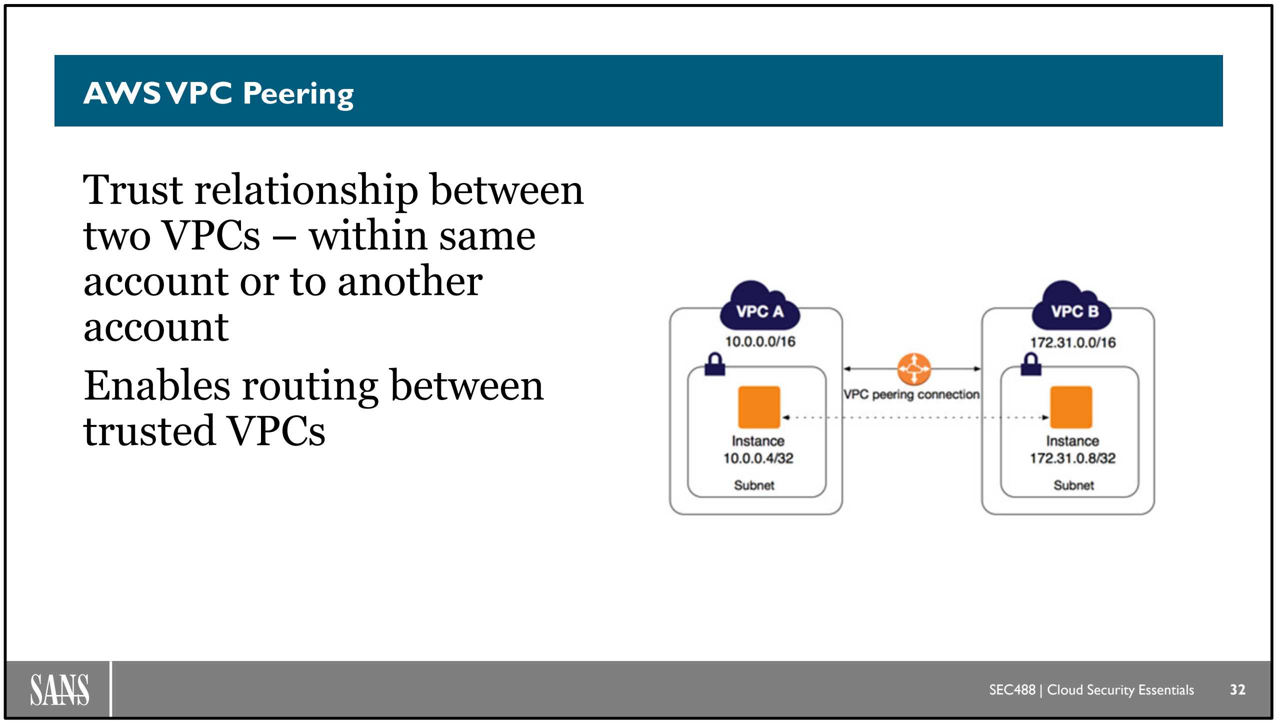
AWS Bastion Quickstart

- AWS offers a CloudFormation template to deploy a bastion host either to a new VPC, or existing VPC


AWS
VPC
Elastic IPs (public route)
Internet gateway
Elastic IPs (public route)
Linux bastion instances
Auto Scaling group
Linux bastion instances
Public subnet 1 10.0.128.0/20
Public subnet 2 10.0.144.0/20
Amazon CloudWatch
Your workload (not included)
Your workload (not included)
Private subnet 1 10.0.0.0/19
Private subnet 2 10.0.32.0/19
Virtual Private Cloud 10.0.0.0/16
Availability Zone 1
Availability Zone 2
AWS Region

AWS provides a CloudFormation Quickstart (Template) that can be deployed to an existing VPC or a new VPC. This CloudFormation template creates a redundant Bastion Host service, by deploying an EC2 within an autoscaling group. If you recall, autoscaling groups will replace EC2 instances if the EC2 instance is unhealthy.

In addition to the EC2 Instance, the CloudFormation also creates a CloudWatch Log Group, specific for the Bastion Host – along with host logging, so that commands that are executed within the Bastion Host are logged.



AWS VPC Peering

Trust relationship between two VPCs – within same account or to another account

Enables routing between trusted VPCs

VPC peering allows organizations to create connectivity between VPCs. This can allow for private routing throughout an environment. **VPCs may also be in different regions.**

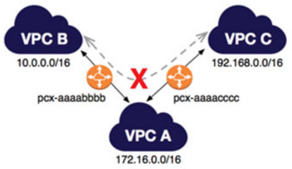
Common use-cases for VPC Peering could include:

- Centralizing Network Security appliances for all egress traffic (also known as a Transit Hub). The architecture could look like a Hub-and-Spoke with this deployment.
- EC2 Instances that do not have internet connectivity transferring data to other EC2 Instances without having to route over the Internet

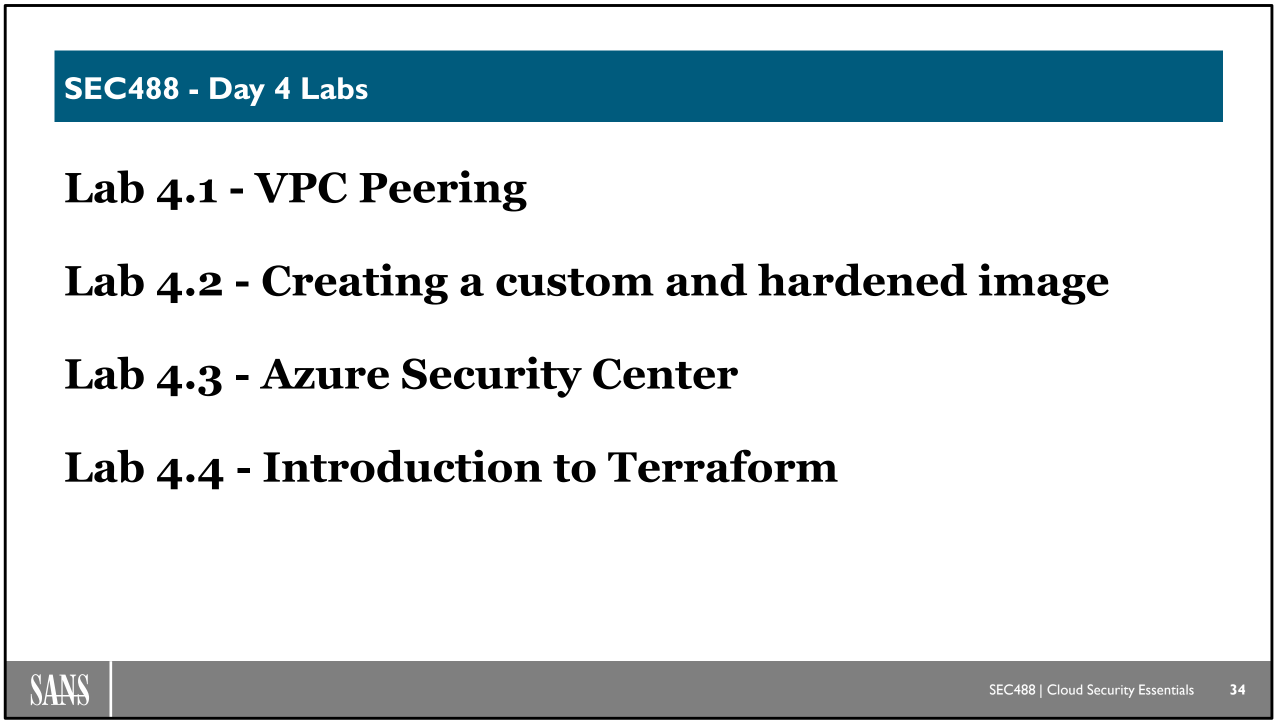
Image: https://docs.aws.amazon.com/vpc/latest/peering/what-is-vpc-peering.html

AWS VPC Peering Considerations

- **Monitor VPC Peering for Account IDs that aren’t owned by Organization**
- If VPC Peering is intended, plan CIDR range allocation.
  - VPC Peering does not support overlapping CIDR blocks
- Each VPC must have its own VPC Peer
  - Transitive Trust is not supported:



If an organization is looking to peer VPCs as part of the ‘big picture architecture’ then it should be reviewed carefully for what constitutes an ‘invalid peer’ and what is unsupported. Image: https://docs.aws.amazon.com/vpc/latest/peering/invalid-peering-configurations.html



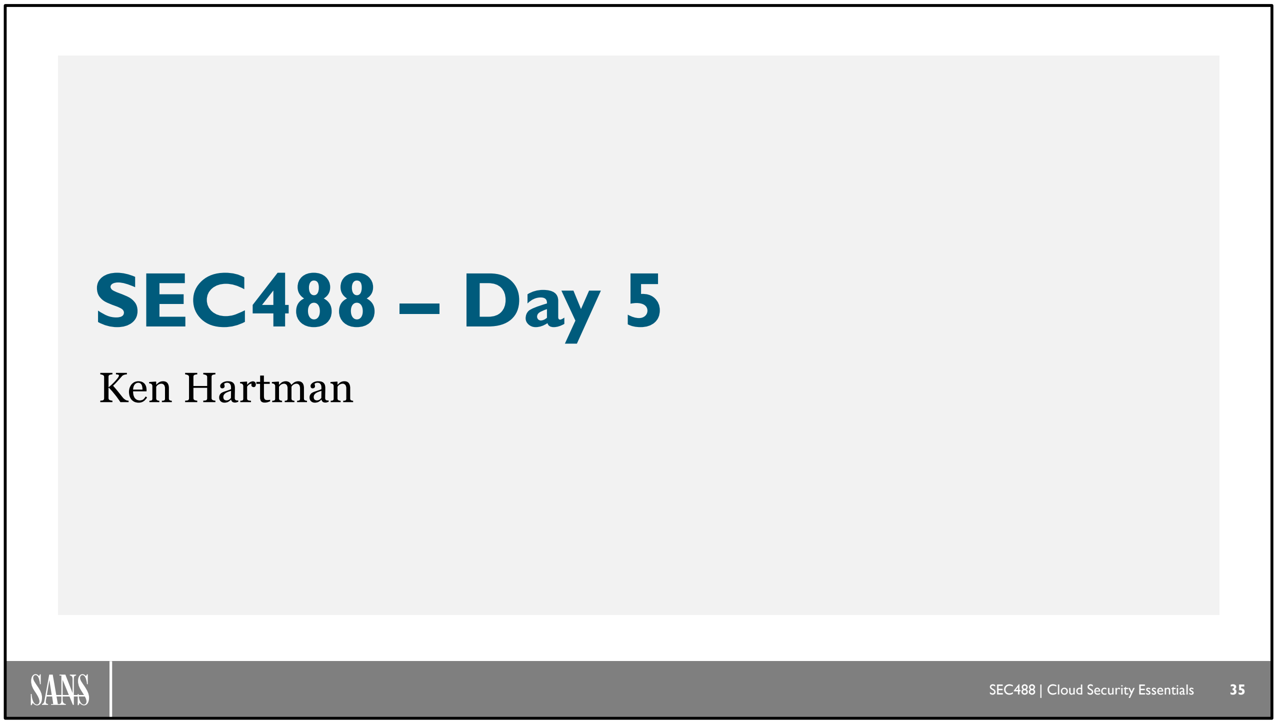
SEC488 - Day 4 Labs

Lab 4.1 - VPC Peering

Lab 4.2 - Creating a custom and hardened image

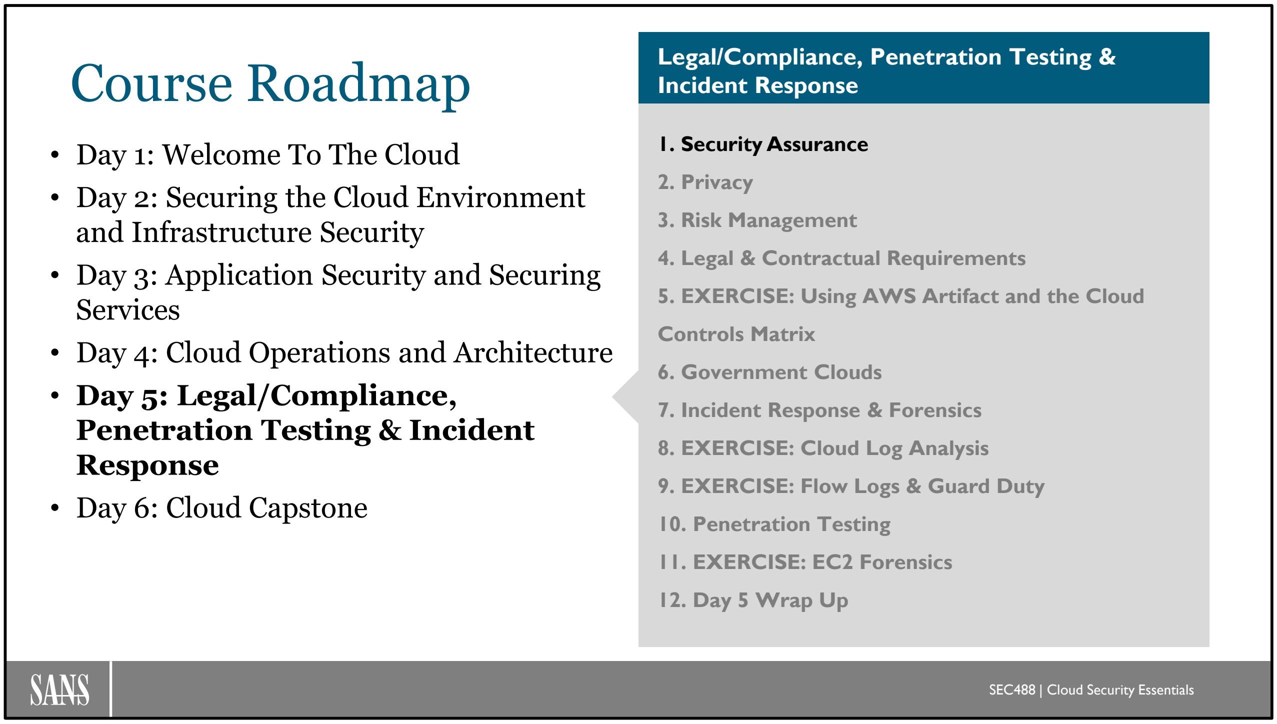
Lab 4.3 - Azure Security Center

Lab 4.4 - Introduction to Terraform



SEC488 – Day 5

Ken Hartman



Course Roadmap

- Day 1: Welcome To The Cloud
- Day 2: Securing the Cloud Environment and Infrastructure Security
- Day 3: Application Security and Securing Services
- Day 4: Cloud Operations and Architecture
- **Day 5: Legal/Compliance, Penetration Testing & Incident Response**
- Day 6: Cloud Capstone

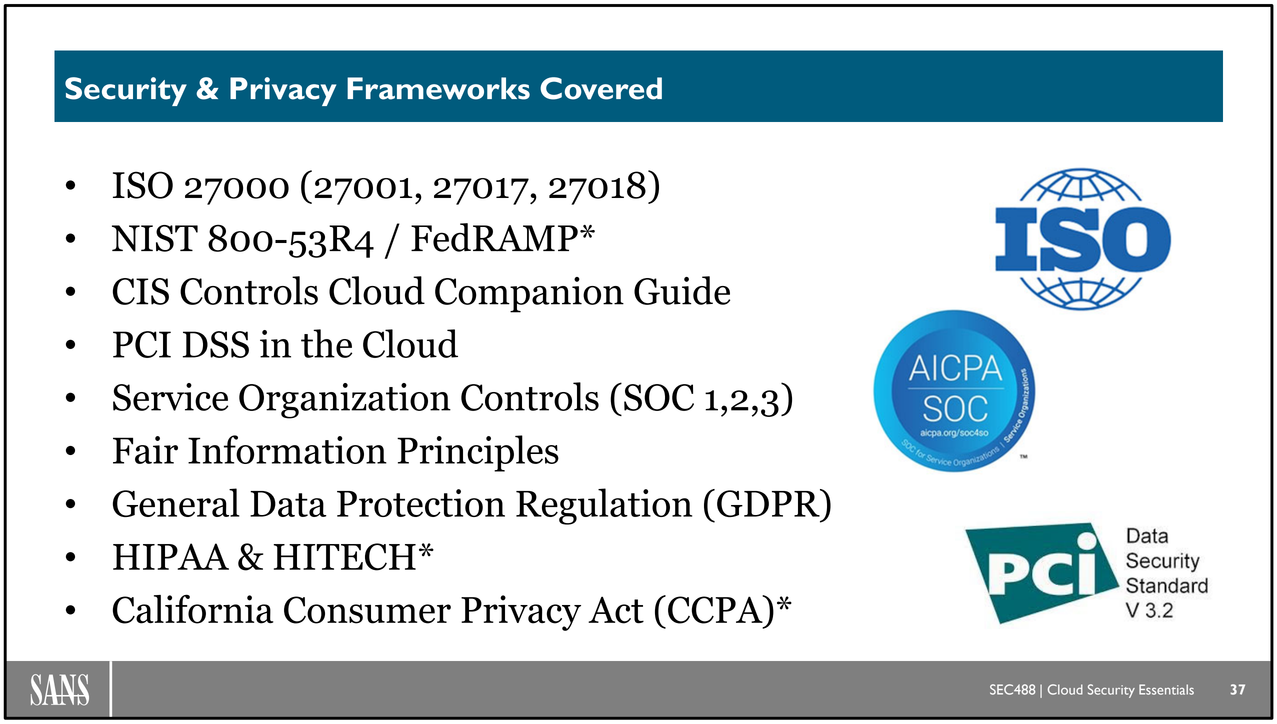
Legal/Compliance, Penetration Testing & Incident Response

1. Security Assurance
2. Privacy
3. Risk Management
4. Legal & Contractual Requirements
5. EXERCISE: Using AWS Artifact and the Cloud Controls Matrix
6. Government Clouds
7. Incident Response & Forensics
8. EXERCISE: Cloud Log Analysis
9. EXERCISE: Flow Logs & Guard Duty
10. Penetration Testing
11. EXERCISE: EC2 Forensics
12. Day 5 Wrap Up

Throughout the week of instruction, we discuss security controls that work in concert to secure your cloud environments. Sometimes it's the cloud service provider that's responsible for the security control and other times it's your responsibility, as the cloud customer. As we've emphasized, it's of critical importance to make sure that the appropriate security controls are in place and maintained by the proper owner. Day Five is focused on making sure that those controls are in place, operational, and effective.

Depending on the industry that your organization is in and the requirements of your customers, you may have to provide and attestation of security assurance. Typically, this will take the form of a third-party audit report which may, in turn, rely on an audit report produced by the cloud service provider.

These third-party audit reports and contractual guarantees, along with documentation published by the cloud service providers may be all that is available to us as a cloud customer to use as part of our pre-engagement due diligence. This information may be all that we have to make a very important risk decision — and that decision is *"can we trust this cloud service provider?"*

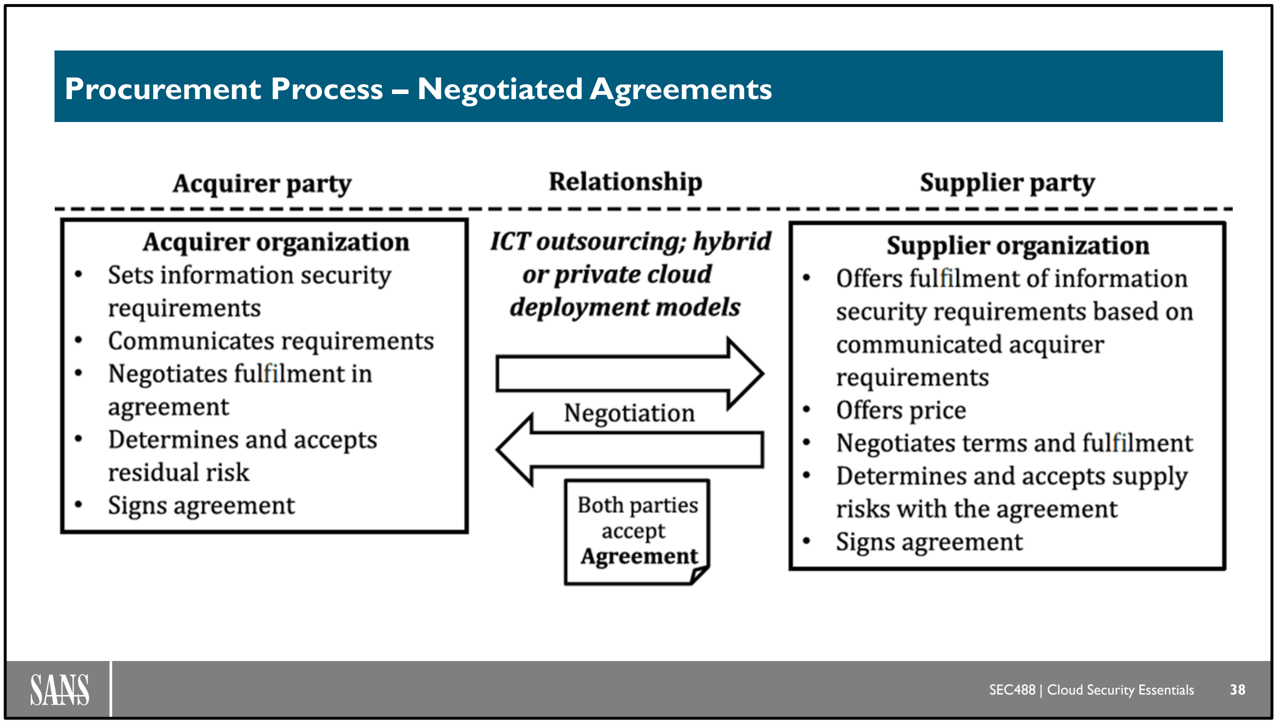


Security & Privacy Frameworks Covered

- ISO 27000 (27001, 27017, 27018)
- NIST 800-53R4 / FedRAMP*
- CIS Controls Cloud Companion Guide
- PCI DSS in the Cloud
- Service Organization Controls (SOC 1,2,3)
- Fair Information Principles
- General Data Protection Regulation (GDPR)
- HIPAA & HITECH*
- California Consumer Privacy Act (CCPA)*

ISO
AICPA
SOC
aicpa.org/soc4so
SOC for Service Organizations | Service Organizations
PCi
Data
Security
Standard
V 3.2
SANS

While it is certainly true that "just because you're compliant doesn't mean you are secure" but I can certainly guarantee you that if you are not compliant then you are not secure! In Day Five, we teach you how to leverage your compliance frameworks to drive your security agenda and have the confidence that the appropriate security controls are in place to meet your organization's legal, compliance, privacy, and security requirements.



Procurement Process – Negotiated Agreements

Acquirer party | **Relationship** | **Supplier party**

Acquirer organization

- Sets information security requirements
- Communicates requirements
- Negotiates fulfilment in agreement
- Determines and accepts residual risk
- Signs agreement

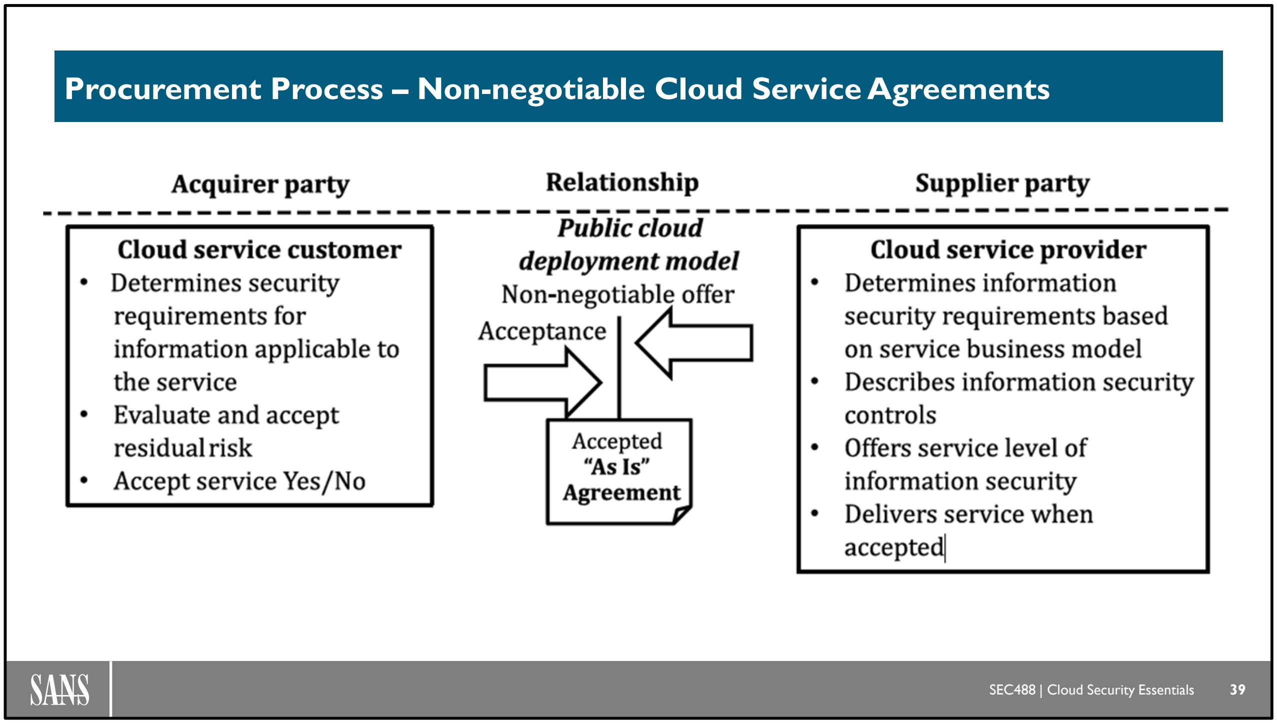
ICT outsourcing; hybrid or private cloud deployment models

Supplier organization

- Offers fulfilment of information security requirements based on communicated acquirer requirements
- Offers price
- Negotiates terms and fulfilment
- Determines and accepts supply risks with the agreement
- Signs agreement

Typically, in the traditional IT procurement process, contracts are negotiated between the buyer and the seller. Proactive security managers are able to inject their security requirements early in the process, often at the request for proposal stage.

[1] ISO/IEC 27036-4:2016 Information technology — Security techniques — Information security for supplier relationships — Part 4: Guidelines for security of cloud services.
https://www.iso.org/standard/59689.html



Procurement Process – Non-negotiable Cloud Service Agreements

Acquirer party

Relationship

Supplier party

Cloud service customer

- Determines security requirements for information applicable to the service
- Evaluate and accept residual risk
- Accept service Yes/No

Public cloud deployment model

Non-negotiable offer

Acceptance

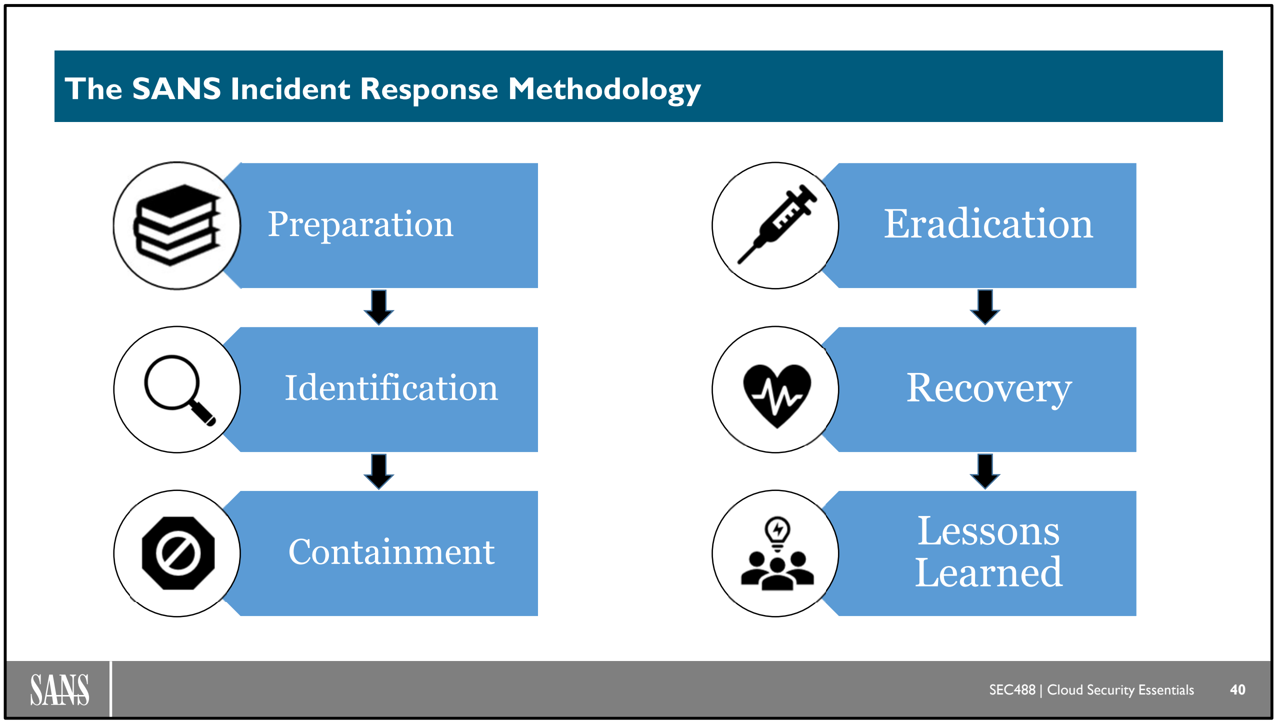
Accepted **"As Is" Agreement**

Cloud service provider

- Determines information security requirements based on service business model
- Describes information security controls
- Offers service level of information security
- Delivers service when accepted

However, that may not be the case with certain cloud service providers. Their service may be offered on a "take it or leave it" basis. That is generally the case with the large cloud service providers (AWS, Azure, GCP, etc.) because they have hundreds of thousands of customers and customizing contracts does not scale well. For the most part, it's based on the negotiating power of the cloud customer relative to the cloud service provider. There are notable counter-examples, like the US Department of Defense JEDI Contract, but that is because the DoD brought wheelbarrows of cash to Amazon and Azure, with Azure ultimately winning the contract (for now, however it still disputed).

[1] ISO/IEC 27036-4:2016 Information technology — Security techniques — Information security for supplier relationships — Part 4: Guidelines for security of cloud services.
https://www.iso.org/standard/59689.html



The SANS Incident Response Methodology

Preparation

Identification

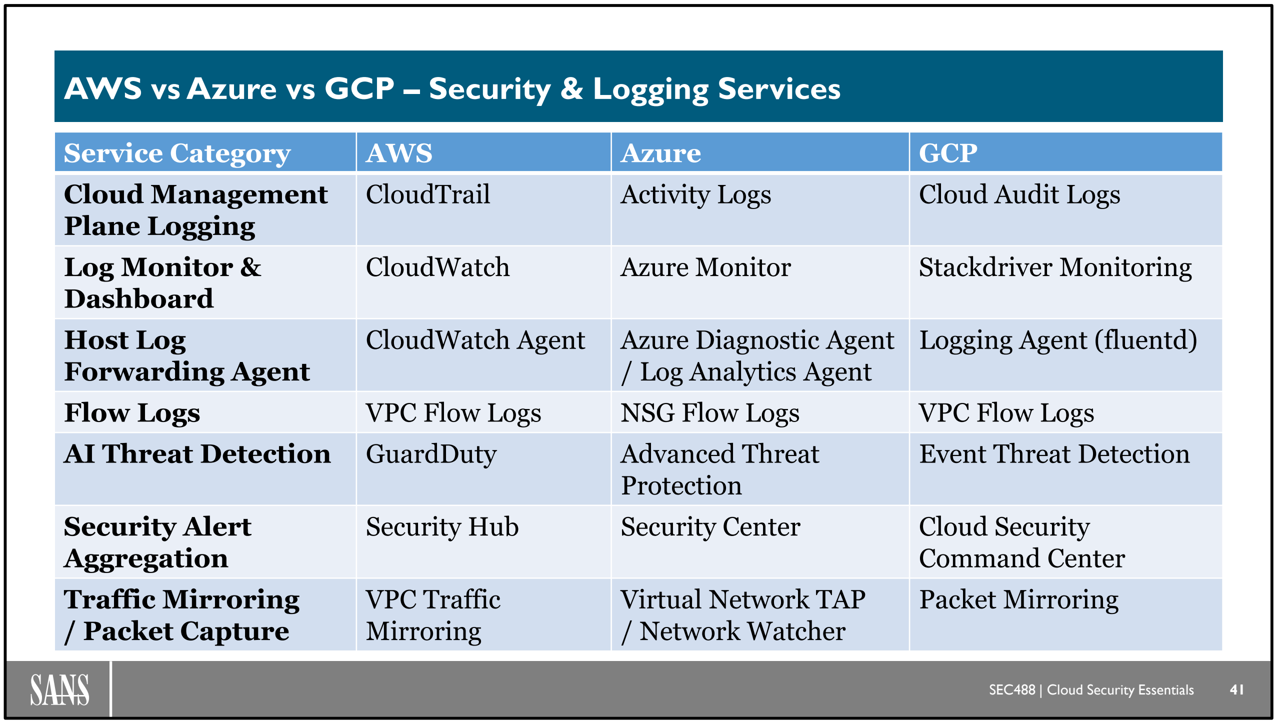
Containment

Eradication

Recovery

Lessons Learned

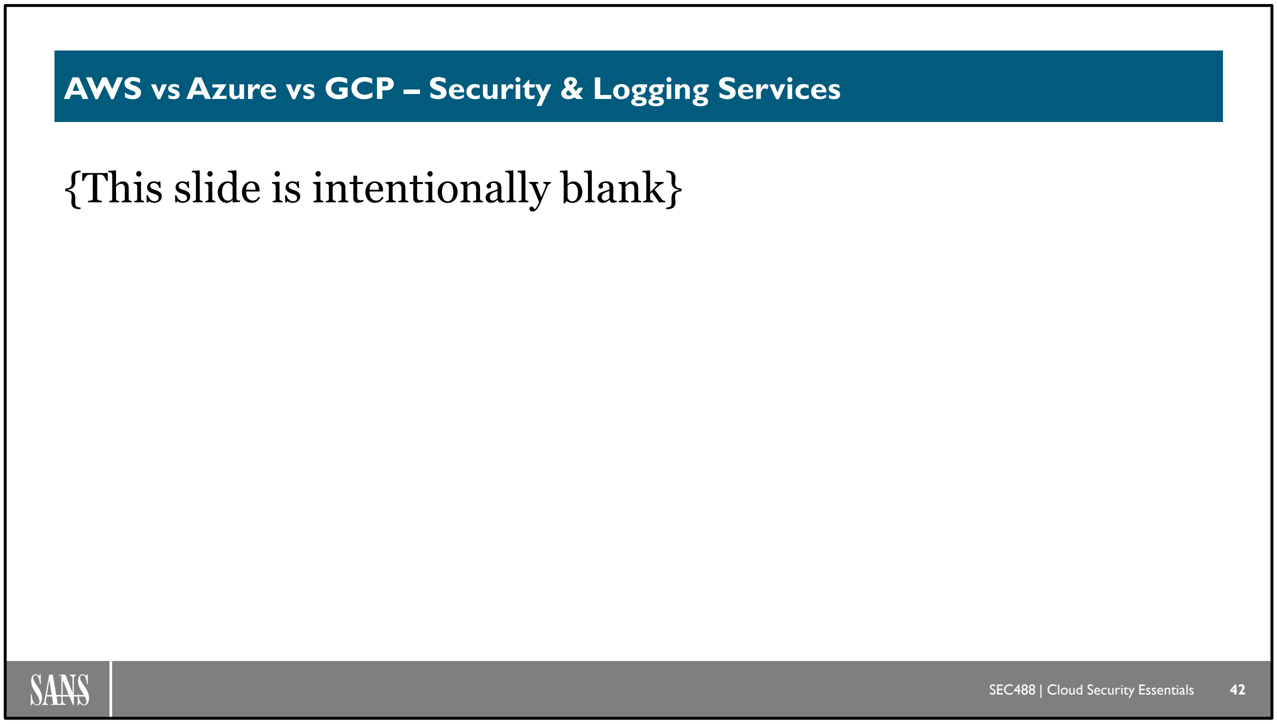
On Day Five, we also talk about incident response in the cloud with a focus on how it differs from on premises. Note that SANS has a complete course on Cloud Incident Handling in the works, so our focus is simply what your organization should consider when moving to the cloud.



AWS vs Azure vs GCP – Security & Logging Services

Service Category	AWS	Azure	GCP
Cloud Management Plane Logging	CloudTrail	Activity Logs	Cloud Audit Logs
Log Monitor & Dashboard	CloudWatch	Azure Monitor	Stackdriver Monitoring
Host Log Forwarding Agent	CloudWatch Agent	Azure Diagnostic Agent / Log Analytics Agent	Logging Agent (fluentd)
Flow Logs	VPC Flow Logs	NSG Flow Logs	VPC Flow Logs
AI Threat Detection	GuardDuty	Advanced Threat Protection	Event Threat Detection
Security Alert Aggregation	Security Hub	Security Center	Cloud Security Command Center
Traffic Mirroring / Packet Capture	VPC Traffic Mirroring	Virtual Network TAP / Network Watcher	Packet Mirroring

One distinct advantage of working with the large cloud service providers are the cloud native security services. This includes capabilities that log every activity taken in the Cloud Management Plane (basically every change made to the cloud environment itself), cloud native logging and analytics capabilities, as well as Threat Detection services that leverage artificial intelligence and third-party data feeds.



AWS vs Azure vs GCP – Security & Logging Services

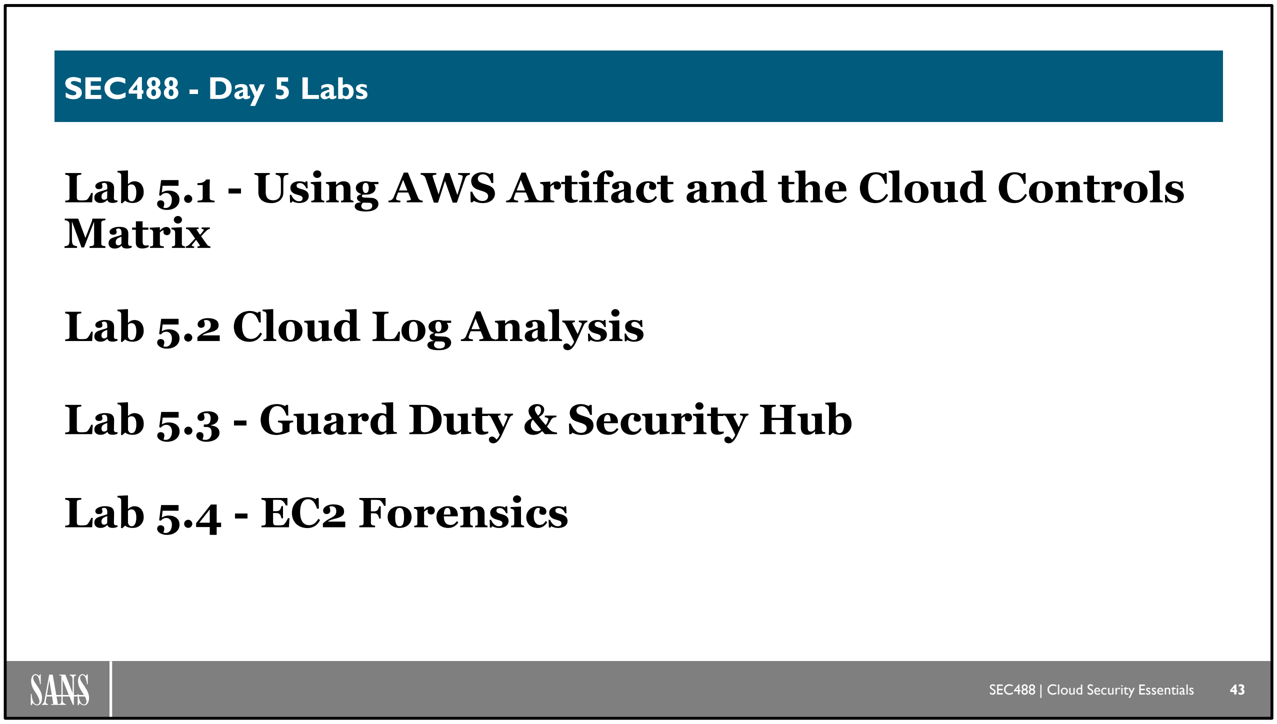
{This slide is intentionally blank}

AWS

- CloudTrail: https://aws.amazon.com/cloudtrail/
- CloudWatch: https://aws.amazon.com/cloudwatch/
- CloudWatch Agent: https://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/Install-CloudWatch-Agent.html
- VPC Flow Logs: https://docs.aws.amazon.com/vpc/latest/userguide/flow-logs.html
- GuardDuty: https://aws.amazon.com/guardduty/
- Security Hub: https://aws.amazon.com/security-hub/
- VPC Traffic Mirroring: https://aws.amazon.com/blogs/aws/new-vpc-traffic-mirroring/

Azure

- Activity Logs: https://docs.microsoft.com/en-us/azure/azure-resource-manager/management/view-activity-logs
- Azure Monitor: https://azure.microsoft.com/en-us/services/monitor/
- Azure Diagnostic Agent / Log Analytics Agent: https://docs.microsoft.com/en-us/azure/azure-monitor/platform/agents-overview
- NSG Flow Logs: https://docs.microsoft.com/en-us/azure/network-watcher/network-watcher-nsg-flow-logging-overview
- Advanced Threat Protection: https://azure.microsoft.com/en-us/features/azure-advanced-threat-protection/
- Security Center: https://azure.microsoft.com/en-us/services/security-center/



SEC488 - Day 5 Labs

Lab 5.1 - Using AWS Artifact and the Cloud Controls Matrix

Lab 5.2 Cloud Log Analysis

Lab 5.3 - Guard Duty & Security Hub

Lab 5.4 - EC2 Forensics

Day Five has four different labs. In the first lab, we use AWS Artifact in the Cloud Controls Matrix to perform a high-level review of the proposed system to identify any compliance issues. This is a realistic request commonly made of cloud security engineers. Understanding how to do this can prevent your organization from wasting valuable time and resources during the initial stages of a new cloud deployment.

Lab Two provide some fantastic hands-on experience analyzing logs generated by an actual cloud deployment in AWS. (SEC545 Cloud Security Architecture & Operations shows how to configure and optimize these logs.)

In Lab Three we show you how to use AWS GuardDuty to monitor your AWS accounts and how to use Security Hub to aggregate the output from several cloud native and third-party security tools.

Lab Four shows you how digital forensics can be performed on virtual hard drives in the cloud, using AWS Elastic Compute Cloud EBS volumes as an example. In this lab, we attach a volume created from a snapshot of a compromised virtual machine to a SIFT Workstation and perform some preliminary file system forensics. (Note that SANS has a Cloud Forensics course in development as well.)
Our objective for day five is not to fully equip you to be a cloud DFIR expert, but to give you an appreciation of additional skills to consider when moving to the cloud.

Concluding Thoughts

Hopefully as result of listening to this webcast, you have a much greater sense of What to Do When Moving to the Cloud. We also hope that this has piqued your interest in taking SECSEC488: Cloud Security Essentials. Stay tuned for announcements from SANS as to when this will be available.

I know that we are all very excited to bring this course to the security community.