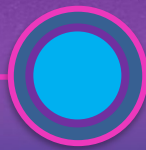


2024 Edition

CLOUD SECURITY ENGINEER ROADMAP



by



PWNED LABS
UNLOCK YOUR CYBER POWER

Customized for **Cloud Career Journeys**
<https://cloudcareerjourneys.com/>



TABLE OF CONTENTS

START

CLOUD SECURITY ENGINEER ROADMAP

- 01 - Linux and Containers
- 02 - Learn One Cloud Provider
- 03 - Cloud Security Principles
- 04 - The Hacker Mindset
- 05 - Automation and Scripting
- 06 - Identity and Access Management (IAM)
- 07 - Network Security
- 08 - Data Encryption, Keys and Storage
- 09 - Logging and Monitoring
- 10 - Incident Response and DR

STARTING POINTS

- Cloud Engineer
- Security Engineer
- Systems Administrator
- Software Developer
- No or Little IT Background

RECAP AND RESOURCES

- Recap – Cloud Security Engineer Roadmap
- Pwned Labs Resources
- Good Luck!

Start

Welcome! This roadmap is intended to be a step-by-step path that I would take to becoming a cloud security engineer today, if I was embarking on this exciting journey.

I will keep this roadmap updated with feedback from all who pass through here, and look to make this a useful resource for people looking to start a rewarding and fun career as a cloud security engineer.

Let's just start by saying – there is no one correct route to getting started in cybersecurity and cloud security. Every path and story are different, and this unique path will be a positive differentiator in your career.

This roadmap has sections that provide individual guidance on transitioning to cloud security based on five common starting points:

- Cloud Engineer
- Security Engineer
- Systems Administrator
- Software Developer
- No or Little IT Background

Let's jump in!

Cloud Security Engineer Roadmap

This roadmap aligns at a high level with the expected knowledge areas for a cloud security engineer, and is intended for people who are new to cloud security and who aspire to perform a cloud security engineering role.

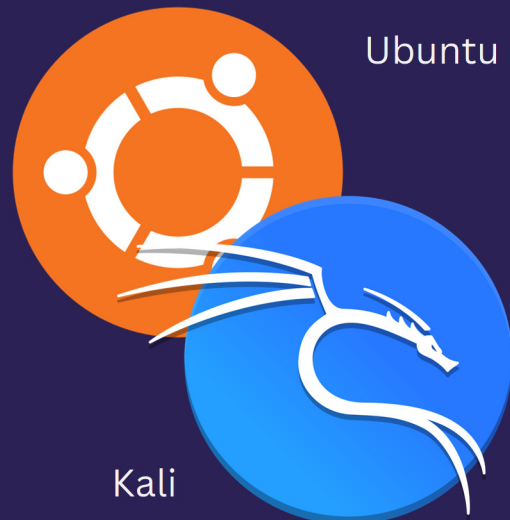
To help you get a job as a cloud security engineer it is important to:

- Learn the foundations well
- Build, break and fix in the cloud!
- Reinforce theoretical learning through practice
- Demonstrate continuous learning (it doesn't stop!)

Linux and Containers

As a cloud security engineer, you will frequently use the Linux command-line to perform tasks, due to its customizability and great support for cloud, security and DevOps tooling.

Ubuntu is a solid choice of Linux distro given its ease of use and large community.



Kali Linux is also a good choice for cloud security professionals, particularly those focusing on penetration testing and security assessments. Your role will involve using automated scripts to improve security at cloud-scale, as well as troubleshooting and investigating cloud services, so you need to be familiar with Linux shell commands. Some other basic Linux OS concepts that you need to be familiar with are host networking (including security features like firewalls) and the Linux file system (structure and permissions).

Linux's capabilities are used to support the containerization technologies that are crucial to modern cloud infrastructure. If you have some experience and understanding of container technologies such as Kubernetes and Docker this will also help your transition to cloud.



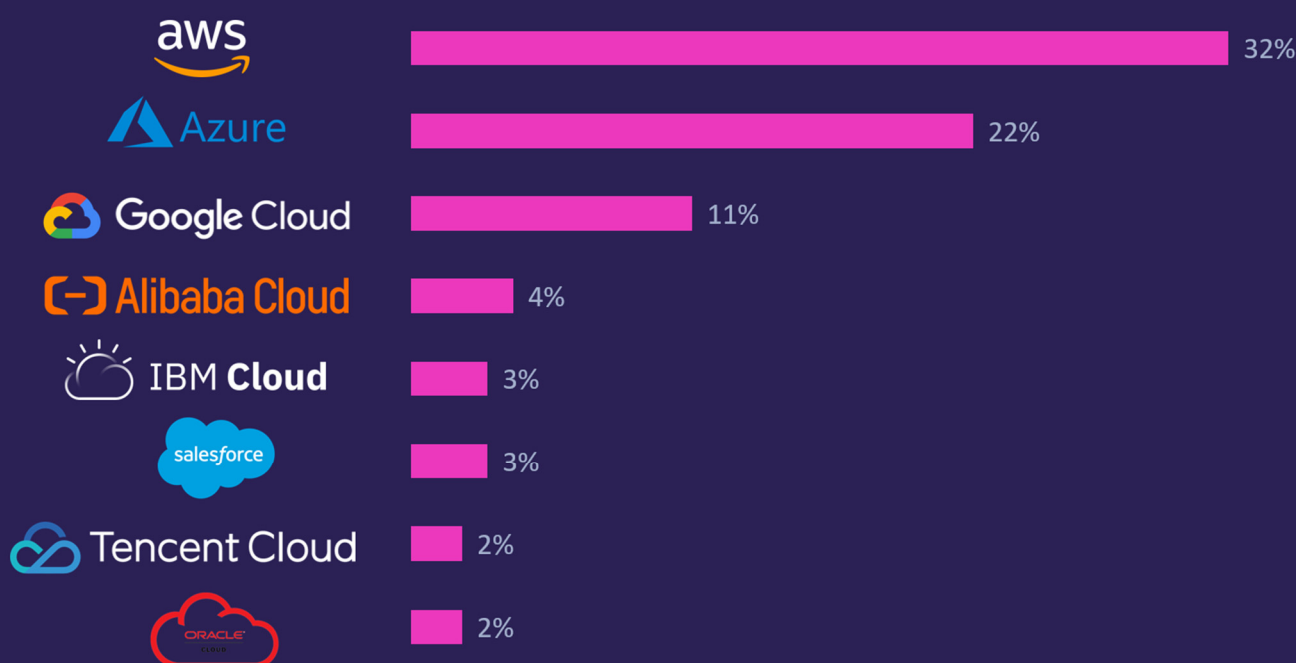
kubernetes



docker

Focus on One Cloud

Migration to the cloud is accelerating, with companies increasingly adopting hybrid cloud architectures. If you are starting a company today, it's very likely that you will be cloud-native from the beginning.



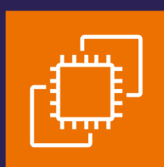
Worldwide IaaS & PaaS Market Share, Q2 2023. Adapted from:

<https://www.statista.com/chart/18819/worldwide-market-share-of-leading-cloud-infrastructure-service-providers/>

Learning one cloud provider is like learning a programming language, once you know one it becomes much easier to learn others! For AWS, here are some key services to get familiar with and learn the security implications of:



AWS Identity and Access Management (IAM)



Amazon Elastic Compute Cloud (Amazon EC2)



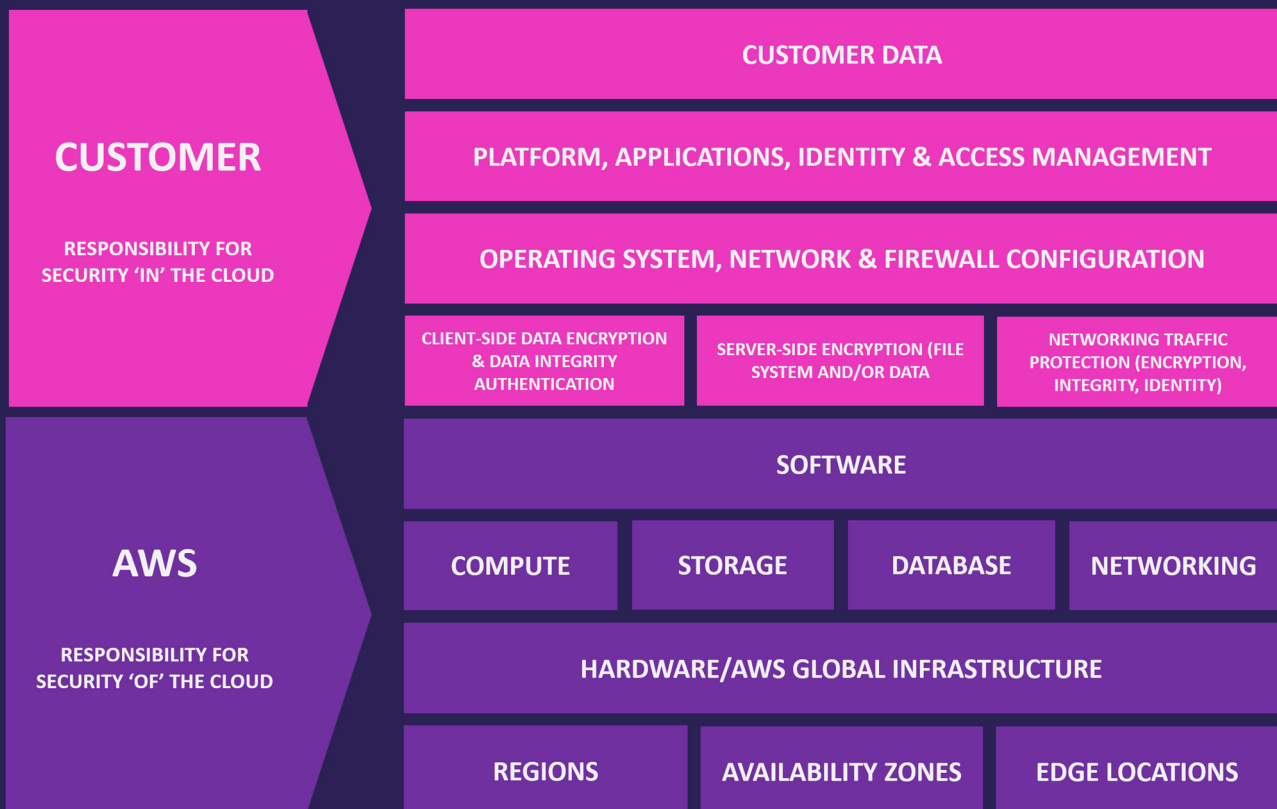
Amazon Simple Storage Service (Amazon S3)



Amazon Elastic Container Service (Amazon ECS)

Cloud Security Principles

The Shared Responsibility Model is a very important concept. AWS is responsible for “Security of the Cloud” - protecting the infrastructure that runs and underpins all of the services offered in the AWS Cloud. The customer has responsibility for “Security in the Cloud” – ensuring security when performing configuration and management tasks.

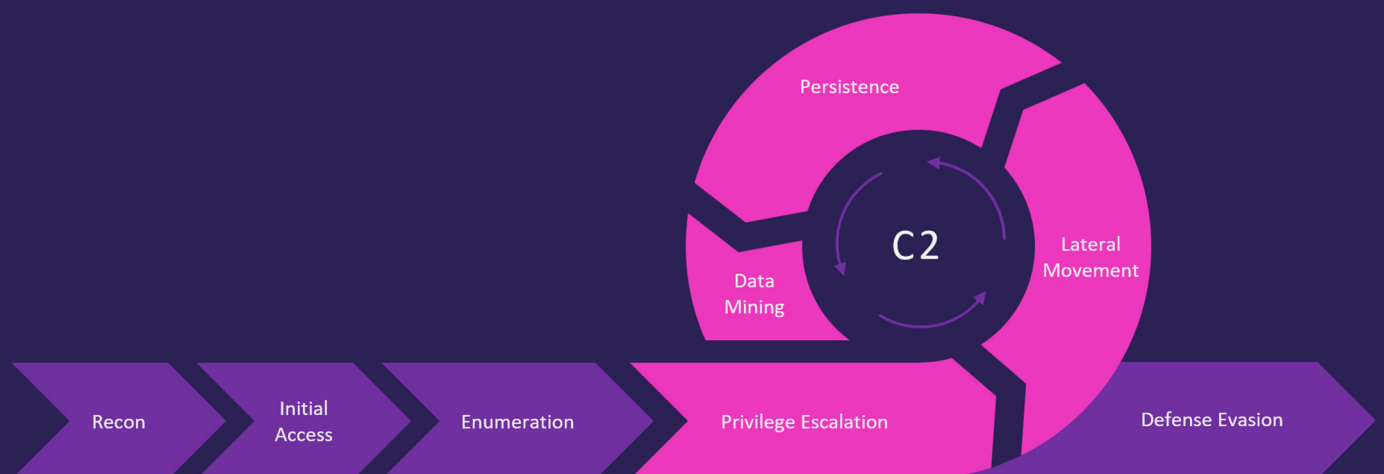


AWS Shared Responsibility Model, Q1 2024. Adapted from:
<https://aws.amazon.com/compliance/shared-responsibility-model/>

Another key principle is Defense in Depth. This is a layered approach to security, ensuring that if one layer fails, others are in place to provide protection. The principle of Least Privilege is also very important, ensuring that identities or services in the cloud have only the minimum level of access or permissions necessary to perform their functions.

The Hacker Mindset

Threat actors approach the cloud much as they do with on-premise environments, with some important differences. With on-premise networks you need to consider the security of your perimeter to prevent being breached. With perimeterless cloud environments, you need to consider the strength of your configured identities (IAM users and roles) that can interact with cloud APIs.



The Cloud Kill Chain

Just as thinking like defender makes red teamers better able to evade defenses (and provide better advice to clients on improving their security posture), thinking like a hacker allows blue teamers to better anticipate potential security weaknesses.

Proactively and continuously assessing the security of your environment and questioning how an attacker might exploit it will result in a much-improved security posture that is more resilient against [ransomware](#) and crypto-mining. Purple teaming FTW!

Automation and Scripting

In a dynamic and expansive cloud environment, manual processes are not only inefficient but also prone to error.

You will use scripting languages like Bash, Python and PowerShell to create custom security tasks for monitoring, alerts, and incident response – tailored to your specific cloud environment.



These cross-platform scripting languages are easier to learn compared to other languages and are suited to the cloud. Python also has rich ecosystem of libraries and frameworks, which is very beneficial in cloud security. Libraries like Boto3 for AWS enable easy interaction with cloud services.

Using automation tools such as Terraform, you can define resources once in the infrastructure as code (IaC) templates, and have them consistently apply your security standards each time the resources are deployed.

```
null_resource.copy-web["config.php"]: Creation complete
null_resource.copy-web["contact_me.php"]: Creation complete
null_resource.copy-web["admin.php"]: Creation complete
null_resource.copy-web["index.php"]: Creation complete
null_resource.copy-web["home.php"]: Creation complete
```

```
Apply complete! Resources: 49 added, 0 changed, 0 destroyed
```



Identity and Access Management (IAM)

IAM is the cornerstone of cloud security. In the cloud, where resources are potentially accessible from anywhere, controlling who has access to what becomes paramount. With effective IAM, you will help ensure the security of your cloud environment.



Identity and Access Management

Apply fine-grained permissions to services and resources



Who

Workforce users and workloads with IAM



Can access

Permissions with IAM policies or RBAC



What

Resources within your cloud environment

IAM is a classic way to manage users in AWS, and is good for smaller environments. It's also good to learn and use AWS IAM Identity Center, so you can manage IAM at scale. IAM Identity Center supports key rotation, which means that even if a threat actor gains access to credentials, they will only be valid for a short period of time, potentially reducing the damage that can be done.

It allows collections of permissions to be assigned to users and groups and used across multiple accounts. This makes permissions management more efficient and reduces the risk of errors or inconsistencies.

Network Security

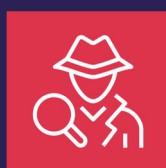
Vulnerability management and network security are a key aspect of cloud security. Misconfigurations can occur and vulnerabilities may be found in deployed services. Regular auditing and penetration testing is recommended, as well as maintaining a risk register to work on prioritizing and addressing risks.

As part of a defense in depth approach, network controls should be implemented so that only those users and resources that need to use the resource are granted access at the network layer. So that even if IAM user credentials are compromised, a threat actor wouldn't be able to do much damage. It's very important to understand what a Virtual Private Cloud (VPC) is and how they are used to isolate resources.

Another important skill is being able to integrate AWS services with other AWS security services and also third-party tools and services such as CloudFlare, and evaluate the benefits of each option.



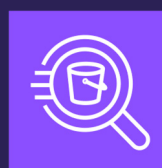
Some important AWS security services to get familiar with are:



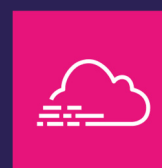
Amazon Detective –
Investigate Events



Amazon Macie –
Securing S3



Amazon Athena –
Find Anomalies



AWS CloudTrail –
Capture Activity

Data Security

The crown jewels for a company are usually some form of data. As a cloud security engineer, you will need to ensure that sensitive data is encrypted in transit and also at rest. You will need to choose the appropriate encryption, key management and storage solution based on legislation, business requirements and risk appetite. It's recommended to gain familiarity with AWS KMS, a key management solution that allows you to centrally manage the encryption keys that control access to your data.



AWS Key Management Service
(AWS KMS)

Storage services such as buckets are a common way that threat actors gain sensitive data, as they can be misconfigured for public access or contain a mix of public and sensitive data. If the data includes credentials such as keys, tokens or passwords, this could result in threat actors getting a foothold in the environment. For AWS, Amazon Macie can help you to audit and secure your deployed S3 buckets.

```
root@RED:~# aws macie2 get-findings --region eu-west-2 --finding-ids a9b499b2e269483ae18a91b1dc5423eb --query 'findings[*].{Type: type, Resource: resourcesAffected.s3Bucket.name, S3Object: resourcesAffected.s3Object.key}' --output table
```

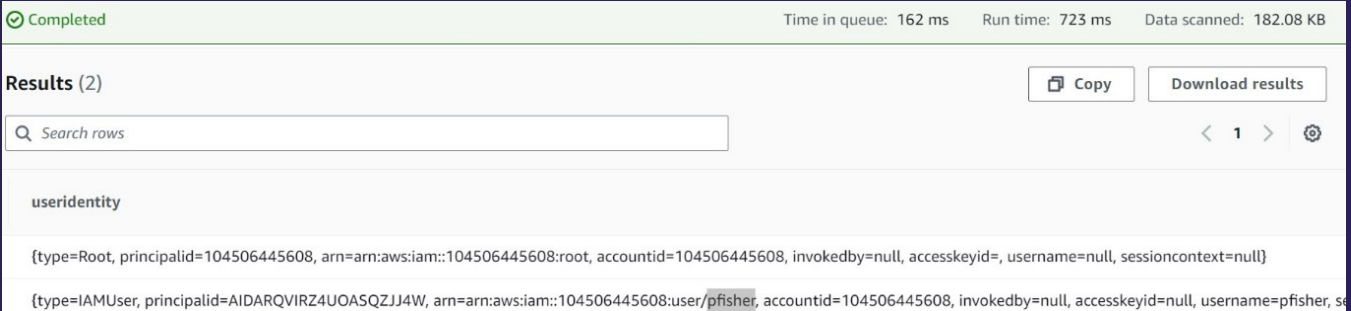
| GetFindings | | |
|-----------------|-------------------------------|------------------------------------|
| Resource | S3Object | Type |
| hlogistics-beta | SystemTrackingPackagesTest.py | SensitiveData:S3Object/Credentials |

Logging and Monitoring

Being able to “hear a pin drop” and understand when abnormal behavior is occurring in your environment is crucial. This relies on collecting the right data, and then creating specific detection rules. Good detection rules will let you know when something is up, without generating too many alerts, which can result in “alert fatigue”.

In AWS, CloudTrail allows you to log events that occur on both the control (management) and data planes, and save the results to an S3 bucket. CloudWatch can then be configured to alert on anomalies, while the Amazon Athena interactive query service makes it easy to analyze data directly from Amazon S3 using standard SQL queries.

```
SELECT *
FROM cloudtrail_logs_aws_cloudtrail_logs_104506445608_4e45885e
WHERE eventname = 'ConsoleLogin'
AND eventTime LIKE '%2023-08-30%'
AND responseelements LIKE '%Success%'
```



The screenshot shows the Amazon Athena console interface. At the top, it indicates the query is 'Completed' with a green checkmark. Performance metrics are shown: 'Time in queue: 162 ms', 'Run time: 723 ms', and 'Data scanned: 182.08 KB'. Below this, there are buttons for 'Copy' and 'Download results'. A search bar labeled 'Search rows' is present. The results are displayed in a table with a header 'useridentity' and two rows of JSON data. The first row shows a root user, and the second row shows an IAM user named 'pfisher'.

Other popular log analysis tools to get familiar with are ELK stack and Splunk.



Incident Response and DR

Quickly and effectively responding to security incidents will reduce the amount of damage caused by threat actors. In the cloud, which has very well-defined APIs and offensive tooling created for it, potential intrusions can result in exfiltration of company secrets and destruction of infrastructure in even short windows of opportunity. As defenders, it's really important to define incident response playbooks and automation, and be able to respond and contain the threat as quickly as events unfold.

Step 1 - Preparation

Step 2 - Detection and Analysis

Step 3 - Containment, Eradication & Recovery

Step 4 - Post-Incident Activity

NIST Incident Response Steps, 2024

<https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf>

Disaster Recovery in the cloud involves planning and implementing strategies to recover data and resume business operations quickly after a disaster. This could be due to natural disasters, technical failures, or cyberattacks. This includes identifying critical systems and data, and outlining recovery procedures from backups.

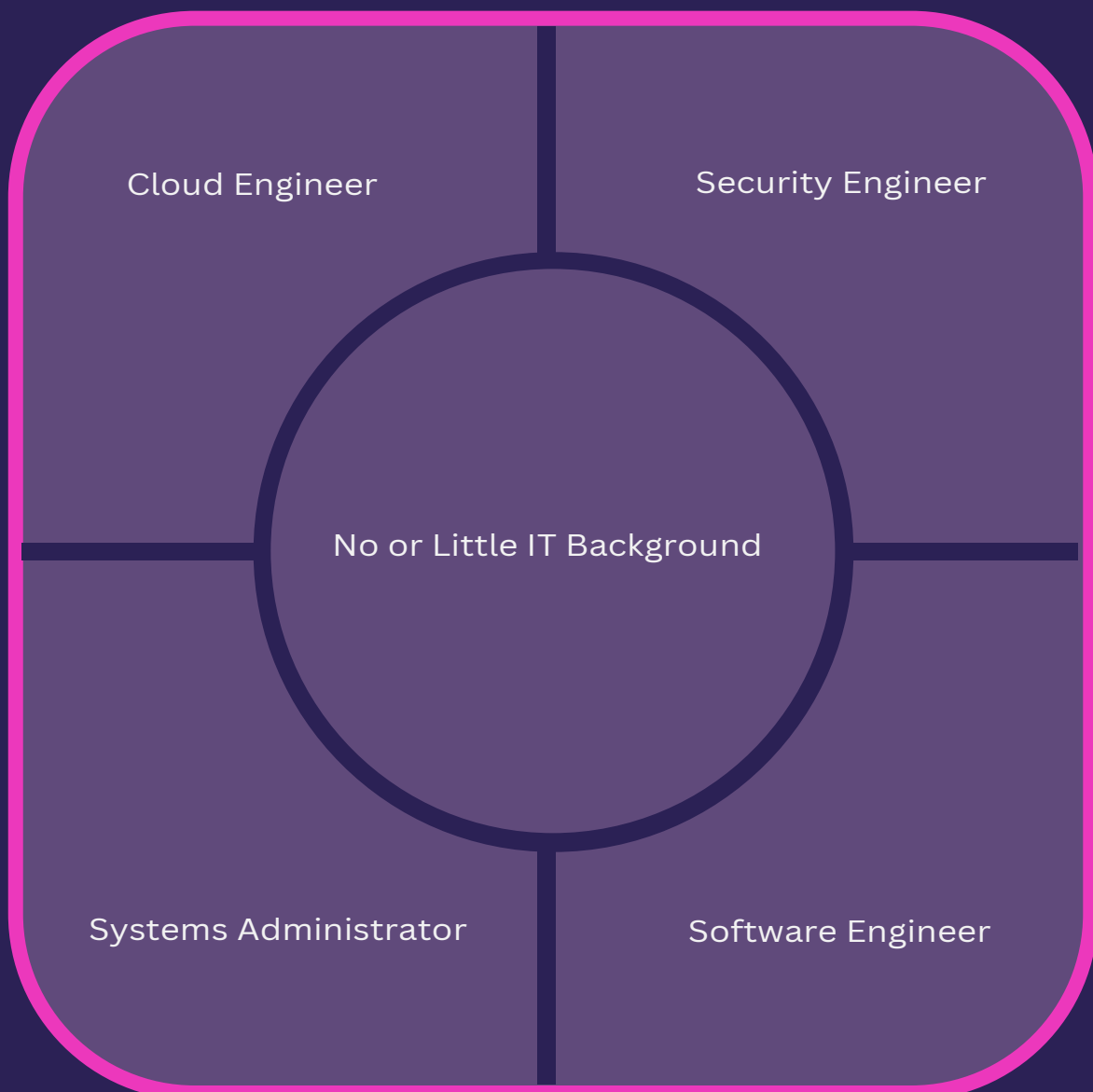
Backup & Restore
(Recovery: Hours, Cost: \$)

Warm standby
(Recovery: Minutes, Cost: \$\$)

Multi-site active/active
(Recovery: Real-time, Cost: \$\$\$)

Starting Points

Targeting a career in cloud security is the ultimate goal, and we each have different backgrounds as we start on this journey. In this section we provide individual advice for common starting points on how you can leverage your existing skills to get hired in a cloud security engineering role.





Starting as a... **Cloud Engineer**

Your skills in cloud engineering will be very useful in cloud security! Automation and Scripting (e.g., using Python, Terraform) are valuable for implementing security automation. Your networking knowledge and experience in VPCs and connectivity will help you design and implement network security controls.

Along with security engineers, this is one of the easier roles to transition to a cloud security engineer role. As a cloud engineer you will also be aware of some common mistakes, misconfigurations and bad practices that can be made in cloud environments (maybe even you made some yourself), which gives you a great start towards protecting the cloud.

Threat actors are currently exploiting native cloud platform and identity management tools to obtain administrative rights, allowing them to shift laterally between different cloud environments, as well as using cloud as part of their offensive infrastructure. Your existing cloud expertise gives you a head start in identifying offensive tradecraft as you know where to look and what doesn't look right.

Skills you need to learn to transition to cloud security:

- Gain a “hacker mindset”. Thinking about how things might be attacked and exploited will allow you to implement mitigations and defenses
- Learn about specific cloud security tools used by defenders and threat actors, beyond basic cloud management

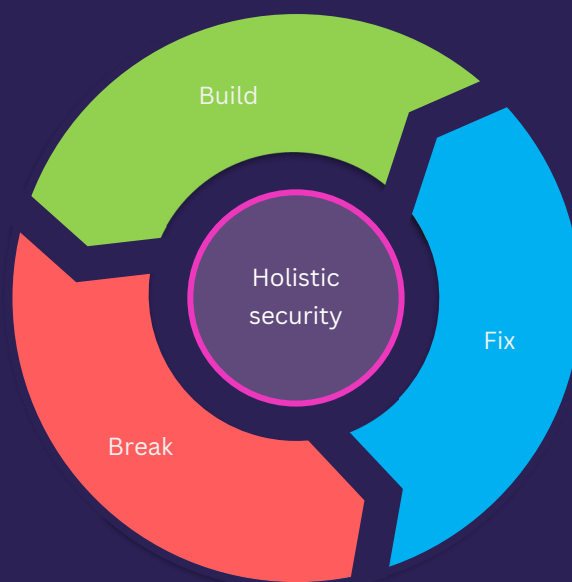


Starting as a... Security Engineer

You already know security and how to defend on-premise environments. Along with cloud engineers, you may have an easier transition to become a cloud security engineer.

Security concepts that apply to on-premise environments apply just as well to cloud environments, with some differences. Cloud is perimeterless and cloud APIs to interact with your resources are accessible from anywhere in the world. If you're familiar with raiding on-premise file shares for credentials (and then performing a DCSync attack), you should know that storage buckets in the cloud often allow for lateral and vertical movement as well!

A “purple team” approach of build, break and fix will allow you to quickly adapt to the cloud. You will be able to bootstrap your skills much faster by playing your offensive and defensive skillsets off each other. By building in the cloud using infrastructure as code, you be able to provide better security advice to devops and cloud engineers.



Starting as a... **Systems Administrator**

Depending on your experience you may already have some security knowledge – especially if you’ve worked for smaller companies that often don’t have dedicated security personnel. You probably also are familiar with the security mistakes of end-users, and have ideas about designing secure systems that don’t rely on users making good trust decisions.

Many people have the assumption that they can just lift and shift existing on-premise workloads, processes and data to the cloud, where it will be secure by default. In reality, the default settings are often insecure and support weaker security settings for backwards compatibility. As a sysadmin, you know many of the security mistakes that are made in on-prem enterprise environments, and many of these also translate to the cloud...

You have an advantage as a skilled builder and eat documentation for breakfast! Building in the cloud should be no problem for you, given the really good public documentation. You may be experienced with VMware and local storage solutions, so you’ll need to learn how to deploy infrastructure in the cloud as code using Terraform, Ansible or Cloud Formation.

Once you’re familiar with building in the cloud, you need to develop your security knowledge by reading, watching, researching and creating vulnerable scenarios on your own, as well as using labs and CTFs from training providers.

GET PWNING! 

Starting as a... Software Developer

As a software developer, you're already familiar with software development workflows and release pipelines in CI/CD. Additionally, your coding ability means you can easily learn infrastructure as code and review the security of deployed code. Some of the best security people are previous software developers and sysadmins!

Traditionally, security has been an afterthought in the SDLC (Software Development Lifecycle), with security controls added at the end of the development process. It can take a lot of time to fix the issues and security bugs at this stage, making sure that no other vulnerabilities are introduced, and performing QA to make sure that the software still works as expected. These retrospective fixes are expensive, and can result in downtime and breaches. As a cloud security engineer, you can champion a "shift left" methodology of testing and checking code quality earlier in the SDLC.



The cost to companies of resolving security issues further through the development lifecycle

Similar to system administrators, you may need to gain skills in both cloud and security. However, DevOps and Ci/CD should be second nature to you! To improve your security knowledge, it's recommended to get experience with vulnerable code challenges and also real-life cloud security labs.

Starting with...

No or Little IT Background

With practice and perseverance, it's possible to go from any background to cloud security, whether in IT or not. For example, as a physics teacher you may be very technical and analytically minded, and these qualities will be a super power in your cloud security journey!

Although it is possible to train for a cloud security role without prior IT, cloud or security experience, cloud security is not really an entry-level profession, meaning that there are foundations that you will need to learn first.

1 Get familiar with Linux

Set up and play with Linux. Then work your way through the OvertheWire Bandit wargame to get practice with Linux shell commands

<https://overthewire.org/wargames/bandit/bandit0.html>

2 Pass the AWS Certified Cloud Practitioner exam

Learn AWS with no prior IT or cloud experience

<https://explore.skillbuilder.aws/learn/course/external/view/elearning/11458/aws-cloud-quest-cloud-practitioner>



3 Get real experience with cloud security

Get hands-on with beginner-friendly cloud security labs that provide real-world experience

<https://pwnedlabs.io>



Summary

Cloud Security Engineer

Roadmap

This roadmap is not prescriptive, but is a foundation and guideline for your own roadmap into cloud security! Cloud security is an exciting and fast-growing area, with many job opportunities. With desire and determination, nothing is impossible!

If you have a good understanding of Linux, have experience with deploying workloads in the cloud, are able to use infrastructure as code, and have hands-on experience with real-world cloud security scenarios, you'll be in a great position to land a cloud security engineer role.





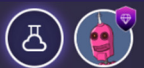
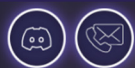
<https://pwnedlabs.io>

Pwned Labs Academy is the place to get real-world experience and kickstart your cloud security career.

Whether you're a total beginner or you're currently studying for an AWS security certification, Pwned Labs has 30 free hands-on cloud security scenarios providing you with job-ready skills.

It's important to us that cloud security is accessible to all. Premium labs are also available, for those who wish to further accelerate their learning.

Start today and get hands-on with labs that cover the topics introduced in this roadmap!



Beginner



Free



Intro to AWS IAM Enumeration
Beginner



Free



AWS S3 Enumeration Basics
Beginner



Free



Azure Blob Container to Initial Access
Beginner



Intro to AWS IAM Enumeration

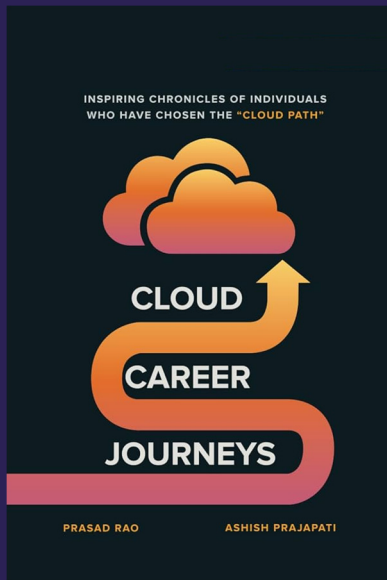
Overview

We created this beginner-friendly lab to give an introduction to the AWS CLI as well as IAM user, role, group, and policy enumeration. This lab is good for red and blue looking to gain familiarity with AWS cloud!

aws iam

Play Lab ▶

Played 300 time(s)



Exclusive offer for
Cloud Career Journeys
readers

CCJBOOK

<https://cloudcareerjourneys.com/>

15% off Pwned Labs Pro

Real-World Cloud Security Labs

Go from Zero to Hero with our byte-sized content.



GET PWNING!

Good luck on your Cloud Security journey!

Got feedback or want to discuss your journey
into cloud security? Let's connect!

<https://www.linkedin.com/in/ian-austin/>

