2026 Edition

CLOUD SECURITY ENGINEER ROADMAP

by

PWNED LABS

TABLE OF CONTENTS

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.

We 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 is different, and your 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 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.

Ubuntu

PWNCLOUDOS

https://pwncloudos.pwnedlabs.io

PWNCLOUDOS is also a good choice for students and cloud security professionals, particularly those focusing on penetration testing and security assessments. The installed tooling also aligns with our curriculum.

Your role will involve using 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. Other basic Linux OS concepts to learn are host networking (including firewalls) and the Linux file system (structure and permissions).

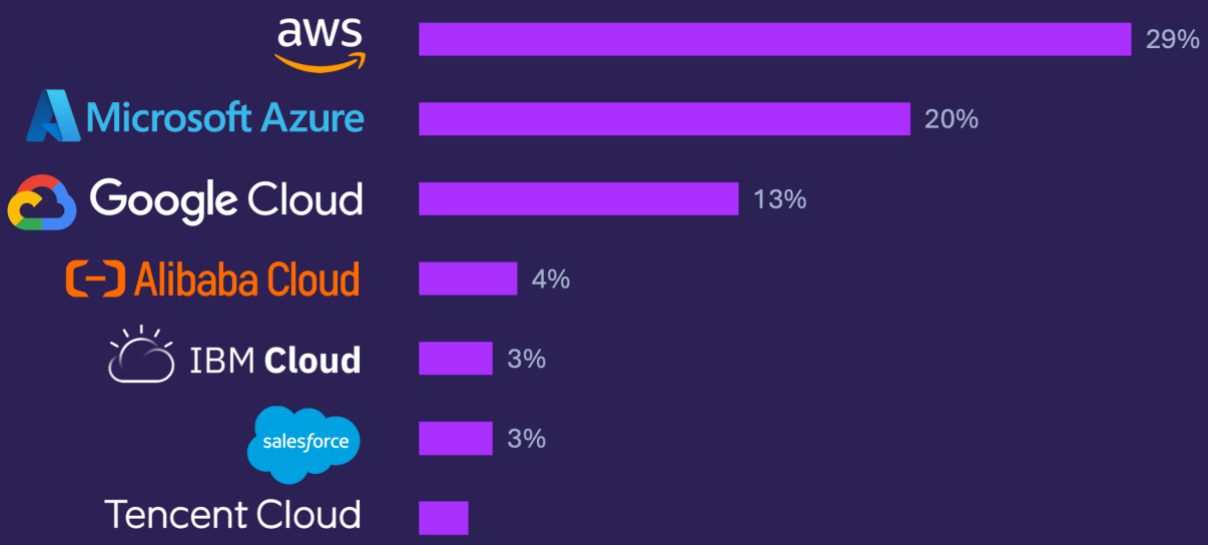
Linux's capabilities are used to support the containerization technologies that are crucial to modern cloud infrastructure. If you have some experience and understanding of container technologies such as Kubernetes and Docker this will also help your transition to cloud, including basic security concepts like image hygiene, running containers as non-root, Kubernetes RBAC and service accounts, and simple segmentation.

kubernetes docker

Hands-on: https://overthewire.org/wargames/bandit/bandit0.html

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, Q3 2025. 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)

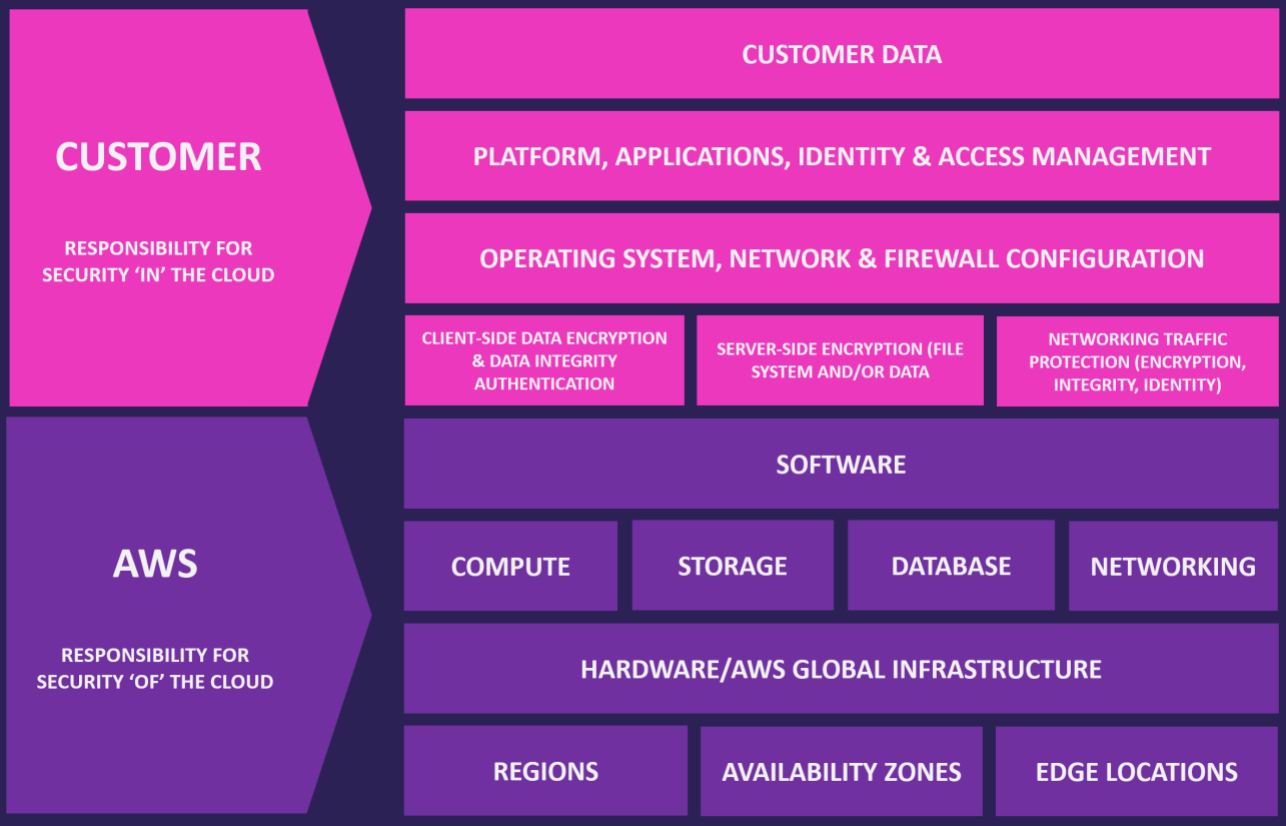
Amazon Elastic Container Service (Amazon ECS)

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

{03}

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

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.

Learn more: https://aws.amazon.com/compliance/shared-responsibility-model/

{04}

The Hacker Mindset

Threat actors approach the cloud much as they do with on-premises environments, with some important differences. With on-premises 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 a 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!

{05}

Automation and Scripting

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

You'll 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 well suited to the cloud. Python also has a 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 infrastructure as code (IaC) templates and have them consistently apply your security standards each time resources are deployed.

CI/CD is part of this. Pipelines can deploy to production and often have privileged access, so learn least privilege, approvals, safe secret handling, trusted runners, and basic build provenance.

```
null_resource.copy-web["config.php"]: Creation
null_resource.copy-web["contact_me.php"]: Creat
null_resource.copy-web["admin.php"]: Creation c
null_resource.copy-web["index.php"]: Creation co
null_resource.copy-web["home.php"]: Creation comp

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

HashiCorp Terraform

Hands-on: https://pwnedlabs.io/labs/create-custom-tooling-to-explore-aws

{06}

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.

IAM is a classic way to manage users in AWS and works well for smaller environments. For larger environments, learn and use AWS IAM Identity Center to manage access at scale using centralized workforce identity and permission sets across multiple accounts. A key benefit is reducing long-lived access keys by using short-lived role credentials, which can limit the blast radius if credentials or tokens are stolen.

IAM Identity Center 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.

{07}

Network Security

Network security is a core part of cloud security. Misconfigurations and exposed services are common, so you need strong network controls that reduce blast radius and make it harder for attackers to move laterally, even if credentials are compromised.

As part of a defense in depth approach, implement segmentation and access controls so only the required users, workloads, and services can reach each resource. To do this well, you need a strong understanding of VPC design, subnets, routing, security groups, and private connectivity patterns.

Key topics to learn:

- VPC segmentation (public vs private subnets, routing, and isolation)
- Security groups and NACLs (what they protect, and what they do not)
- Private access patterns (VPC endpoints and private connectivity)
- Egress control (restrict and monitor outbound traffic)
- DNS controls and filtering
- Edge protections (WAF and DDoS controls)
- Network telemetry (flow logs and DNS logs)

Common services to get familiar with:

- AWS WAF - Application-layer filtering
- AWS Shield - DDoS protection
- AWS Network Firewall - Traffic inspection and policy enforcement
- VPC Flow Logs - Network visibility and investigations

Hands-on: https://pwnedlabs.io/labs/reveal-hidden-risks-with-aws-security-hub

{08}

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 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 path to data exposure, often due to misconfigurations like public access or overly broad bucket policies. If buckets contain secrets like keys, tokens, or passwords, this can give threat actors a foothold in the environment. Learn S3 Block Public Access, bucket policies, and KMS encryption controls. For AWS, Amazon Macie can help you discover and audit sensitive data in S3 buckets.

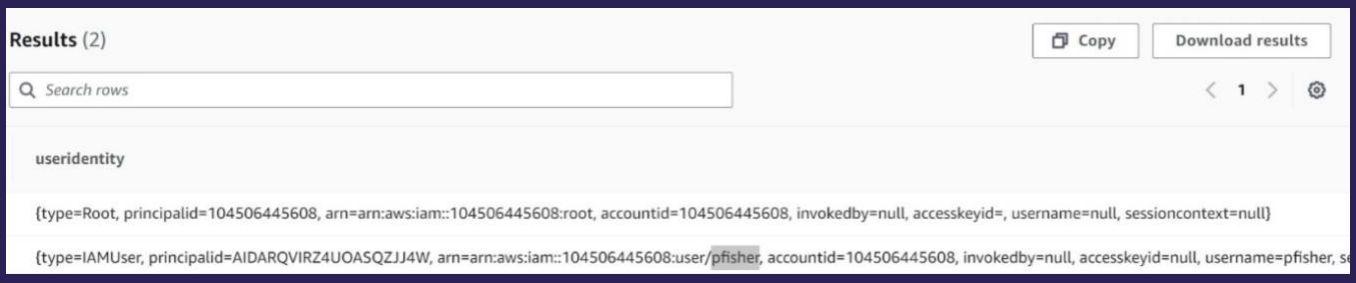
```
root@RED:~# aws macie2 get-findings --region eu-west-2 --finding-ids a9b499b2e269483ae18a91b1
dc5423eb --query 'findings[*].{Type: type, Resource: resourcesAffected.s3Bucket.name, S3Objec
t: resourcesAffected.s3Object.key}' --output table
-------------------------------------------------------------------------------------------
|                                        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 records management (control plane) API activity by default, and you can optionally enable data event logging for services like S3 and Lambda. Configure a trail to deliver logs to an S3 bucket (and optionally CloudWatch Logs) for alerting and investigations. GuardDuty analyzes CloudTrail, VPC Flow Logs, and DNS logs to produce threat findings. Security Hub (CSPM) centralizes posture checks and findings, and Inspector adds vulnerability findings. For modern, at-scale analysis, CloudTrail Lake and Amazon Security Lake support centralized querying across accounts and regions.

```
SELECT *
FROM cloudtrail_logs_aws_cloudtrail_logs_104506445608_4e45885e
WHERE eventname = 'ConsoleLogin'
AND eventTime LIKE '%2026-08-30%'
AND responseelements LIKE '%Success%'
```



Also learn ELK and Splunk for log analysis.

{10}

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 a short window of opportunity. As defenders, it's 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 and Improvement

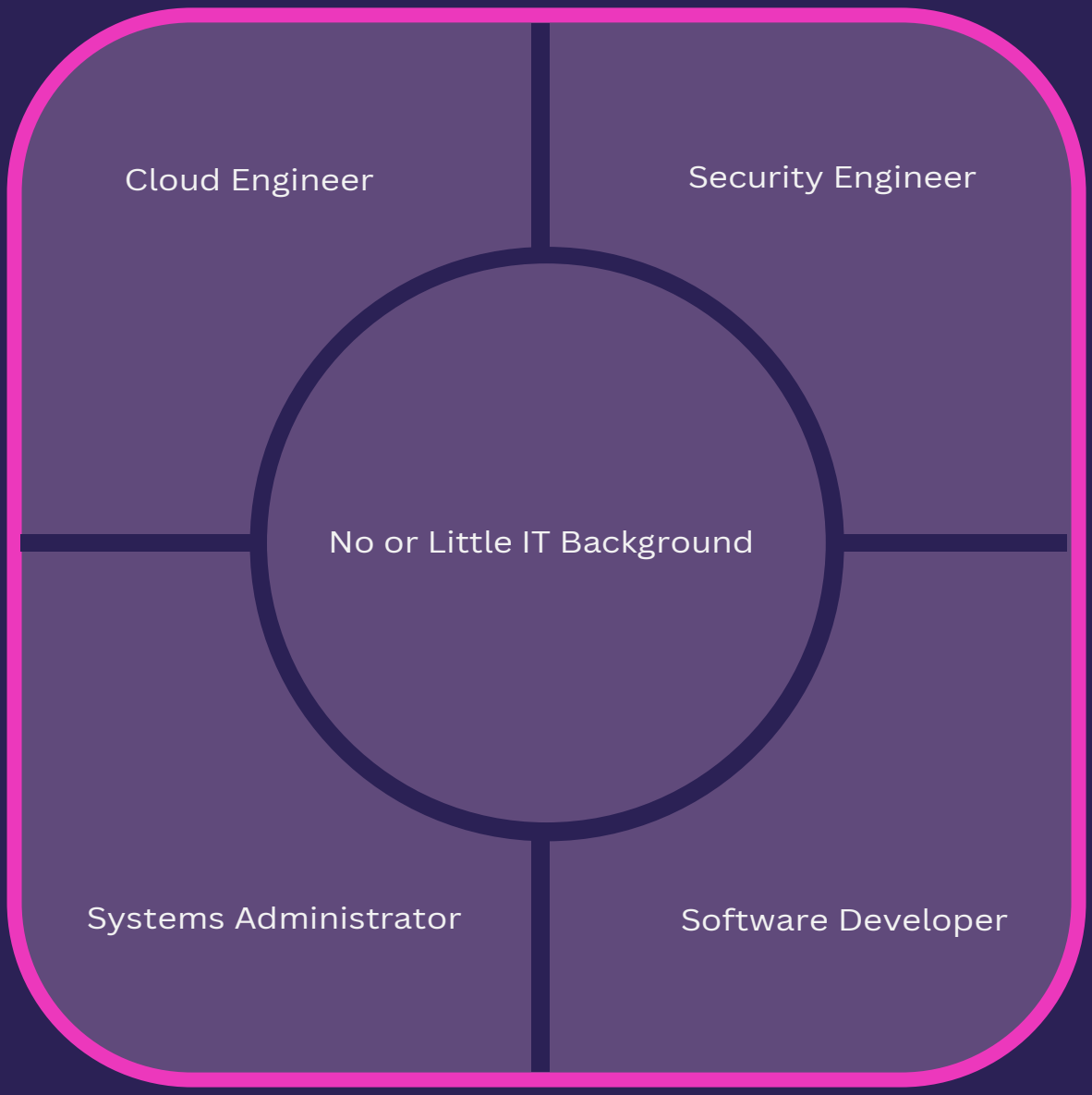
NIST Incident Response guidance (SP 800-61 Rev. 3, April 2025):
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r3.pdf

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	Warm standby	Multi-site active / active
(Recovery: Hours, Cost: $)	(Recovery: Minutes, Cost: $$)	(Recovery: Real-time, Cost: $$$)

Starting Points

Targeting a career in cloud security is the 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:

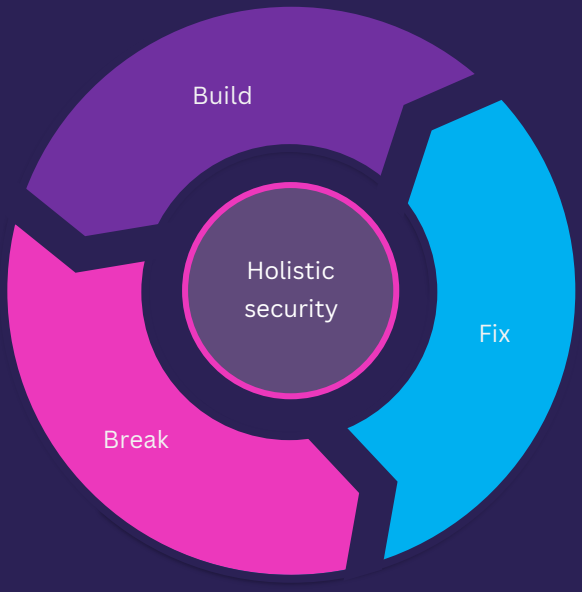
- Gain a "hacker's mindset". Thinking about how things might be attacked and exploited will allow you to implement mitigations and defenses
- Learn about specific cloud security tools used by defenders and threat actors, beyond basic cloud management

Starting as a...
Security Engineer

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

Security concepts that apply to on-premises environments apply just as well to cloud environments, with some differences. Cloud has a network and IAM perimeter, while cloud APIs used to manage and access resources are accessible from anywhere in the world. If you're familiar with raiding on-premises file shares for credentials (and then performing a DC Sync 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 will 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-premises 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 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 CloudFormation.

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

Like system administrators, you may need to gain skills in both cloud and security. However, DevOps and CI/CD should be second nature to you, so focus on pipeline hardening, secure secret handling, and build integrity! To improve your security knowledge, it's recommended to get experience with vulnerable code challenges and 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 superpower 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/

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, can 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.

PWNED LABS

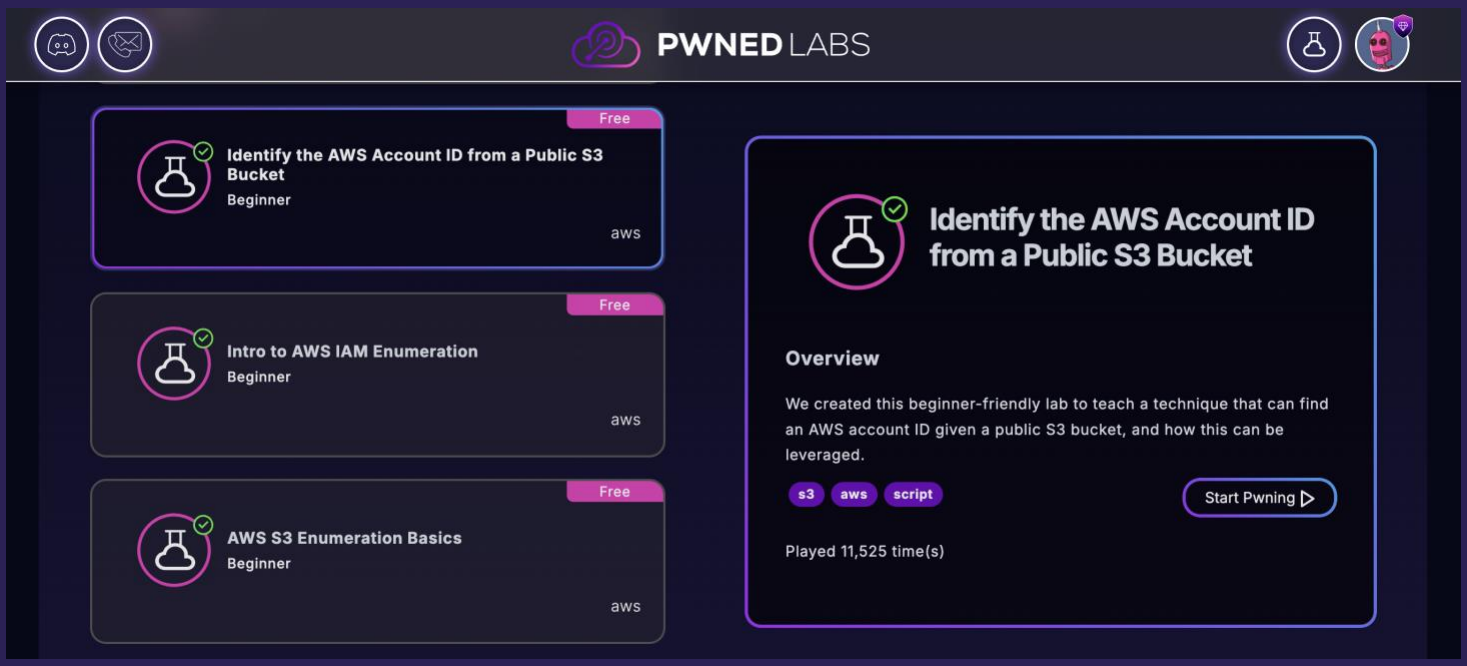
https://pwnedlabs.io

Pwned Labs 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 over 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 available, and if you want to accelerate your learning, you can join the Pwned Labs AWS Bootcamp for guided, structured upskilling with hands-on practice.

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



Good luck on your **Cloud Security journey!**

Build real cloud security skills with hands-on labs.
Join the largest cloud security community with over 40,000 practitioners

https://discord.gg/pwnedlabs

What practitioners say.

Caleb Havens

Red Team Operator & Social Engineer, NetSPI

"I've attended two training sessions delivered by Pwned Labs: one focused on Microsoft cloud environments and the other on AWS. Both sessions delivered highly relevant content in a clear, approachable manner and were paired with an excellent hands-on lab environment that reinforced key concepts and skills for attacking and defending cloud infrastructures. The training was immediately applicable to real-world work, including Red Team Operations, Social Engineering engagements, Purple Team exercises, and Cloud Penetration Tests. The techniques and insights gained continue to be referenced regularly and have proven invaluable in live operations, helping our customers identify vulnerabilities and strengthen their cloud defenses."

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

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