APPSEC engineer

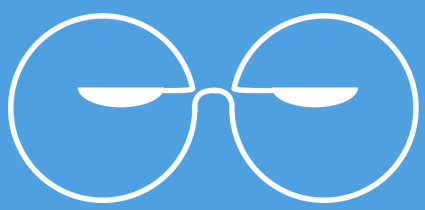
by

Cloud Security Careers

A BEGINNER'S GUIDE

CONTENTS

INTRODUCTION



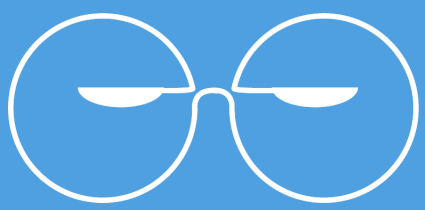
In 1776, a struggling Scottish engineer put the final touches on a machine he'd been labouring on for the past ten years of his life. When he released it to the public later that year, the world's first modern steam engine took 18th century London by storm, and setting the stage for the greatest era of technological advancement and commercial growth Great Britain had ever seen. James Watt had just unleashed the Industrial Revolution onto the world.

It wouldn't be inaccurate to say that cloud computing has had a comparable impact on the people's lives as the Industrial Revolution, particularly in the last decade. It's what kept the global economy from totally imploding during the Covid-19 pandemic, and it's the foundation on which thousands of new technologies and businesses are being built.

But the dominance of cloud is also what makes it vulnerable to security attacks on a daily basis. According to a report, over 94% of companies have adopted cloud technology. Of those, a staggering 81% have reported at least one security incident in 2022. Businesses are slowly coming to grips with the fact that they simply can't afford to build on the cloud without considering security.

This ebook is meant as a guide for newcomers in the cloud security job market, who are looking to join an exciting young industry that's set to dominate all aspects of our lives in the years to come. You'll learn why becoming a cloud security professional is a great idea, and what you need to know about this career path. You'll also understand what skills you'll need to get hired and excel at your job, and how you can acquire those skills online.

WHY CHOOSE A CAREER IN CLOUD SECURITY?



Cloud security is at the confluence of the two fastest growing sectors in tech: cloud (which businesses need to scale their operations) and security (which they need to gain customer trust). At a time when companies are adopting the cloud at record rates, they're also acknowledging the need to build secure software that doesn't put their entire business at risk.

This makes it an ideal choice for a career in 2023 and beyond, particularly if you've previously had a technical role on a product team. Cloud security is by no means an entry-level role as we'll see in this ebook, but it's quickly becoming a point of focus for forward-thinking engineering teams. The primacy of cloud technology, combined with the increasing awareness around secure application development, is driving a steep demand for skilled cloud security talent in the post-pandemic economy.

Get ready for massive industry growth

One of the markers of a promising career path is to see how quickly the industry is growing. Are businesses innovating? Are consumers impacted by the technology? Are traditional business models changing over time?

As we've seen, cloud has already proven itself as more than capable of satisfying all of these requirements, arguably having had the biggest impact of any new technology in the 2010s. It's gone far beyond the 'disruptive' phase in tech to being downright essential to the survival of hundreds of thousands (if not millions) of businesses globally.

It should be no surprise, then, that the need to secure cloud infrastructure is more important than ever. Online systems post-Covid have seen an alarming rise in cyberattacks, pointing to a distinct need for skilled security professionals in the cloud space.

Cloud security spending is already seeing staggering growth, and is expected to increase from USD $33 billion in 2022 to over USD $106 billion by 2029. As more employers prioritise going all-in on cloud, employment opportunities for cloud security will only grow more lucrative.

Even today, the demand for skilled cloud security professionals is far outstripping supply.

We're seeing a crippling skills shortage

While the cloud and cloud security markets are seeing dizzying levels of expansion, the number of high-skill workers is nowhere close to meeting the demand. In fact, a 2022 survey showed that nearly 40% of technologists across various industries say one of their largest skills gaps is in cloud security.

It's gotten so serious that some pundits believe it could actually hold back cloud adoption if it's not resolved soon. But while all that might sound scary to an employer, this situation is favourable to people like you who are considering shifting careers to cloud security.

In fact, as the second-fastest growing skill area in security, tech professionals have already got the memo. We're going to see a rise in the number of workers taking up cloud security roles, with a projected 5-year growth of 115%.

In 2023 and beyond, these are the skills that will determine how valued you are at any company you choose to work at.

A way to avoid being laid off

Perhaps the bleakest reminder of how fast the tech industry moves were the sweeping layoffs that shook some of the biggest tech companies in 2022 and early 2023. Many of the workers who lost their jobs in this period were junior-level professionals, or those who lacked skills in emerging areas of software technology.

Cloud remains one of the most important skills in this regard. Going into 2023, IT leaders find cloud and cybersecurity roles the hardest to find skilled talent for. Regardless of which side of a layoff you're on, upskilling in cloud security can help you weather periods of uncertainty in tech.

If you're worried about getting laid off from your job, bolstering your skill set with cloud security can help with both horizontal and vertical mobility at your workplace. Conversely, if you've been laid off recently and are looking to get back in the job market, a fresh new set of skills will be impossible to miss on your resume.

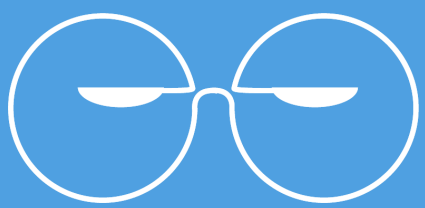
Make one of the top salaries in tech

If you're going to be in one of the most high-demand roles in all of tech, you deserve to be paid like it. As of early 2023, the average cloud security engineer in the US makes nearly $150,000 a year. In fact, compensation across many security roles is on average higher than other technical roles on the product team.

Another important factor is how fast your career moves up. A developer with 3–4 years of experience would be considered junior-mid level, while a security engineer with the same experience would be considered senior.

The sheer lack of security talent out there means that as a skilled cloud security professional, you'll be highly valued in the tech space right now.

WHAT DOES A CLOUD SECURITY ENGINEER DO?



Before we get into the roles and responsibilities of a cloud security engineer, it's important to note that this isn't an entry-level security role. Even a junior-level engineer needs to have had at least a few years of experience working in cloud environments and performing security tasks.

"[Cloud security] definitely cannot be your first job," says Infosec skills author Joseph South, "because cloud security spans just about every single domain in security. They're deploying tools, working with clients...they really need to have those skills and experience before they're going into the cloud."

If you're a security professional, or a member of the engineering team looking to shift careers to cloud security, you need to be familiar with the cloud systems you'll be interfacing with in your new role.

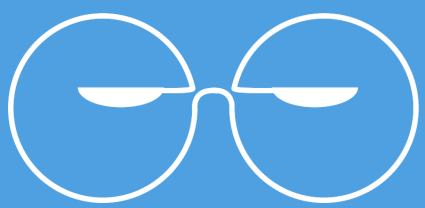
Roles and responsibilities of a Cloud Security Engineer

To understand what the day-to-day responsibilities of a cloud security engineer look like, it helps to break it up into three experience levels: junior, senior, and lead cloud security engineers.

At the junior level (which is definitely not a junior role in security overall), cloud security engineers spend most of their time responding to alerts from various tools the team has set up across the cloud infrastructure. This includes security scanners, assessment tools, and monitoring systems for whatever cloud provider the organisation is using.The senior level engineer is actually implementing these tools and systems. They are responsible for setting up, configuring, and deploying these various tools in the cloud, conducting security assessments and audits, and ensuring compliance with relevant security standards. They're also in charge of things like access control policies and monitoring the cloud environment.

A lead cloud security engineer has a more 'big picture' role on the team. They're the ones identifying critical security gaps in the organisation's cloud environment, and exploring viable solutions to fill those gaps (keeping in mind factors like time and budget). The lead is also driving the overall direction of the cloud security team and collaboration with the developers, architects, etc.

WHAT SKILLS DOES A CLOUD SECURITY ENGINEER NEED?



Cloud security is one of those disciplines that requires a cross-section of skills across a variety of fields, from application security, to DevSecOps, to cryptography, to network security architecture. This isn't to say that every engineer's skill sets are the same — the broad nature of cloud means your skills will specifically need to adapt to your organisation's tech stack. For instance, if your company relies on containers and Kubernetes, you'd need to develop your skills in that field.

1. Knowledge of different cloud providers & services

Although all the top cloud providers do more or less similar things, the *way* they do it is very different. AWS, for example, has over 200 services to manage everything from access control to monitoring to container orchestration. Competitors like Azure and GCP offer similar services, but they operate on different principles and have unique features. As a cloud security engineer, you'll need to be familiar with many of these services, the security controls they offer, and how they affect your application.

It's important to note that you shouldn't just focus on the security services like AWS IAM or GCP Secret Manager. Even a storage service like Amazon S3 offers a host of security configurations that help you safely store data. Given the interdependence of all these cloud services, it's vital to understand how they collectively influence the security posture of your cloud environment.

2. Programming and scripting

A cloud security engineer isn't expected to be a coding wizard, but you get a lot out of relatively basic scripting skills.

Security automation is the most prominent use case for this. It's pretty much impossible to rely purely on manual testing today, with cloud environments growing in complexity and teams rapidly releasing software, sometimes multiple times a day.

Security testing, result aggregation, and even reporting can often be integrated right into the CI/CD pipeline with the help of automation scripts. The security team can not only free up hours of bandwidth by automating security processes, but security won't be a frustrating bottleneck for engineering if they both move at the same pace.

A less tangible—but no less important—factor is the collaboration between security and engineering teams. Developers and security engineers famously don't get along for a number of reasons, chief among them the fact that they don't 'speak each other's language'. Security folks complain that developers don't fix the bugs they find, while developers find it hard to understand security reports and replicate bugs.

Learning to code can give you a deeper appreciation for the constraints the engineering team faces in building and fixing apps, while also making it easier for you to communicate your security findings to developers in a way they understand.

"The more you understand code and how to develop software," says Brian Levine, Director of Product Security at Elastic, "the more it permeates into every aspect of your role [as a security engineer]. If you understand the code, you'll be able to sit down with the developer and explain to them why something is a vulnerability, instead of leaving it to them to figure it out."

3. Identity and access management (IAM) controls

The biggest source of vulnerabilities in a cloud environment come from security misconfigurations. These range from insecure secrets management, lack of input validation—or perhaps most importantly—identity and access management controls. Cloud providers like AWS offer a dizzying number of IAM configs, and as the size of your team grows, managing all the users, IAM identities, and third-party services only becomes more challenging.

You'll be expected to implement features like MFA and federated access across your organisation's infrastructure, monitor the cloud environment for suspicious activity, manage permissions and access policies, and follow IAM best practices. Effective IAM controls can significantly reduce the number of threat vectors to your web applications.

4. Logging and monitoring

Most major cloud providers offer tools and services to monitor your cloud environments for malicious activity and log real-time metrics for your perusal. Monitoring is an essential step for security because it offers a look into how real-world users interact with your app and what threats can emerge from unexpected avenues.

Crucially, monitoring services also let you set up alerts that can be triggered when certain conditions are met. For example, if a user is calling a particular API too many times in a short span of time, the system can instantly send you an alert, allowing you to respond before the API is overloaded.

Over time, the metrics you collect from monitoring will help you further improve security controls across the cloud environment, since you now have the data to identify threat scenarios before they actually become a problem for your team.

5. DevSecOps

Cloud environments offer an unprecedented level of freedom and customisability in how apps are architected and built. But this freedom is a double-edged sword: it also leaves more room for mistakes than ever before. In order to deal with this increased complexity, product teams need a 'playbook' — a list of processes that can be applied across the entire system without manual intervention.

That's what DevSecOps lets you do. By breaking down silos between roles—security, engineering, DevOps—DevSecOps lets you integrate security processes right into the software cycle without slowing or disrupting the pace of development.

As a cloud security engineer, you'll be expected to work with the rest of the product team to seamlessly incorporate security testing, reporting, and audits into the DevOps pipeline.

Security automation, as we saw earlier, plays a key part in enabling faster, more regular security testing. This is the central pillar of DevSecOps, and when your team is releasing software at a rapid pace, this is the only way to ensure new builds are tested and fixed before going to production.

But in order for DevSecOps to be effective, it needs a high degree of communication between teams. Real-time knowledge sharing is how everyone stays on the same page while moving from one build to the next, and lets you accommodate for any sudden changes of plan. Which brings us to the next skill...

6. Communication

Soft skills might seem rather obvious, but they're often overlooked in favour of technical skills. In the role of a cloud security engineer, you'll be interfacing with people in various other disciplines, working with them to formulate security protocols and integrate tools into the pipeline. It's important to be able to clearly explain what you're doing and how your work will affect your team members' workflow.

For example, if you're automating security scans for dynamic security testing, you'll need to work with the developers on your team to integrate it into the CI/CD pipeline, set up plugins and APIs, and customise the scan to your security needs. You'll even need to consider how to prioritise and report the results to the developer for swift remediation.

For this to work, you need to understand the pain points of the developers, the constraints they face, and work towards a solution together. Without clear, frequent communication between you and your colleagues, that will be impossible.

Be friendly and personable with your team members, learn about what they go through every day, and build your network by supporting colleagues that need help.

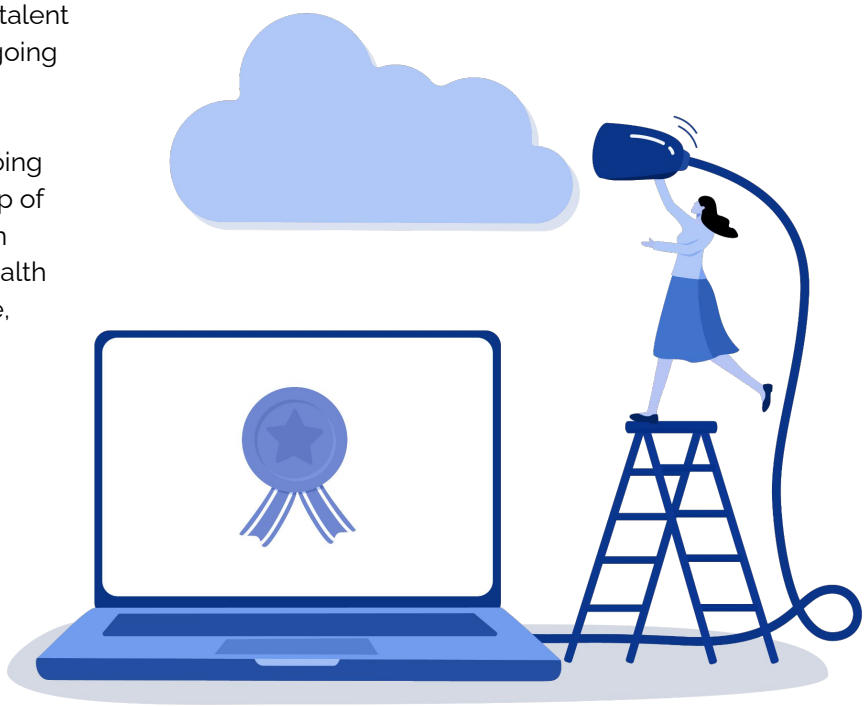
Product teams are not the siloed, assembly-line software factories they used to be. Today, successful teams value communication and interdependence more than ever.

Bonus skill: Containers and Kubernetes

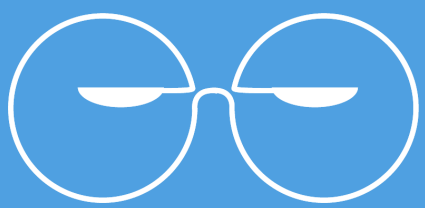
What exactly does 'bonus skill' mean? Containers and Kubernetes security skills aren't something a cloud security engineer typically starts off with, but this is an area you'll almost certainly encounter in the very near future. A 2021 survey reported that 96% of companies are either using or evaluating Kubernetes technology.

Containers and Kubernetes are closely tied to cloud-native infrastructure, allowing organisations to massively scale up their cloud operations with very little overhead. It's practically irrefutable that this upward trend is only just beginning, and skilled talent in this space is going to become very valuable going into 2023.

This is cutting-edge technology that's rapidly going mainstream, and you have a chance to be on top of this wave. A cloud security engineer with skills in container and Kubernetes security will find a wealth of opportunities at some of the top tech, finance, medical, or business firms in the world.



HOW DO YOU GET CLOUD SECURITY SKILLS?



Here's the problem with security training content: there's plenty of it out there, but it's all scattered across hundreds of different websites, ebooks, courses, etc. Not to mention, quality remains a serious issue. Fortunately, the three biggest cloud providers in the world—AWS, Azure, and Google Cloud—all offer free and paid courses for their respective cloud platforms.

But these trainings have some drawbacks: they're mostly text or video-based lessons, with very few (if any) hands-on exercises. They also rarely get new content or updates, and the information if often out of date/obsolete.

Here's a list of some of the best cloud security training programs you can find right now (paid and free):

1. AppSecEngineer

With AppSecEngineer, all your security learning is in one place. Our cloud security training features the Big Three: AWS, Azure and GCP. We've got courses in identity & access management (IAM), cloud storage, network security, secrets management, logging & monitoring, and more.

But what sets us apart is our focus on hands-on learning: every single lesson is taught with hands-on labs and cyber-ranges. We like to minimise distractions and focus on building skills fast.

With over 200+ hours of content in cloud security alone, there's a huge variety in the kind of learning we offer:

- Video lessons
- Hands-on labs (practical exercises)
- Playgrounds (sandbox-style environments)
- Challenges (solve real-world security issues)

This is a comprehensive deep-dive into every aspect of cloud security, and is designed for both for beginner cloud security engineers, and experienced pros looking to update their skills
We're also the only AppSec training provider who adds new content every two weeks. .

That means you're getting new cloud security courses, Playgrounds, and Challenges twice a month.

2. AWS

As the largest provider of cloud services in the world, it stands to reason that AWS has a pretty large library of learning material for newbies. AWS offers a number of free, self-paced learning options where you can start learning.

These are mostly in the form of text-based digital trainings, with some video lessons, but few hands-on labs. You can train for a certification exam at the end of the learning plan.

For a full list of training content, you can check out this Ramp-Up Guide.

3. Azure

Microsoft offers a range short courses in Azure security, covering various aspects of the subject. These are self-paced courses with no video content, and each course is relatively short and easy to complete. However, the lack of hands-on labs means you won't be able to get real-world experience of working on Azure cloud systems.

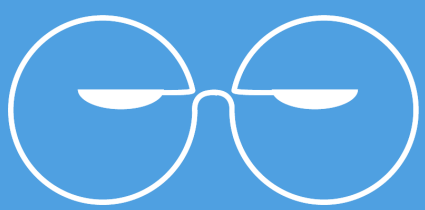
They also have an Azure security certification which you can train for in this course.

4. GCP

Google Cloud has a security engineer learning path that showcases 11 courses covering different aspects of GCP security. Most of these are either text or video-based lessons, which are free, but the few hands-on labs need to be purchased in order to get access.

They also have a network engineer learning path which has some security-related courses.

YOUR CLOUD SECURITY CAREER BEGINS WITH APPSECENGINEER



Choosing a new career is one of the toughest decisions you can make as it is. Add to that the confusion and difficulty of learning skills that employers actually want, and you get a bunch of beginners who have no idea where to even start.

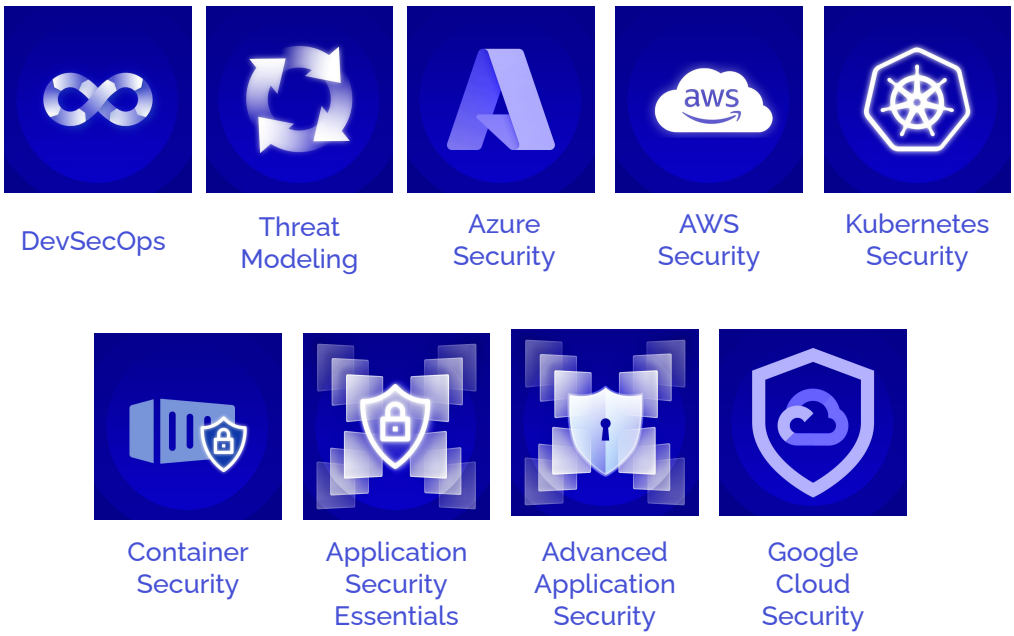
AppSecEngineer is designed from the ground-up to be the beginning, middle, and end of a security engineer's journey. In fact, we have courses meant for every single role on a product team, right from security, to developers, to DevOps, to architects.

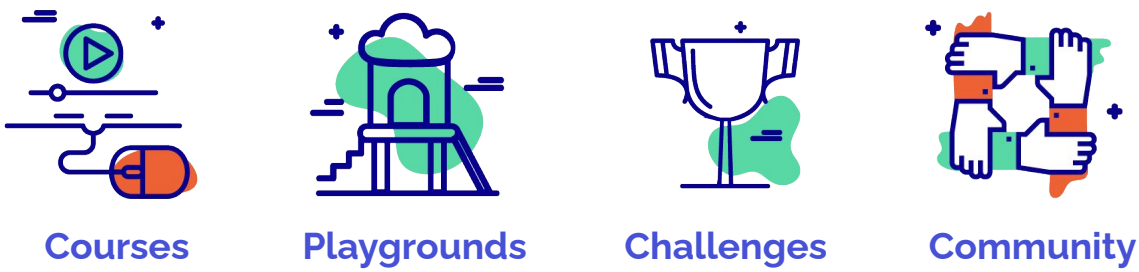
From DevSecOps and advanced application security, to containers, Kubernetes, and cloud security, every course features video lessons accompanied by hands-on labs.

With the addition of Playgrounds (sandbox-style environments to learn secure coding), and Challenges (solving real-world security issues), we have 1000+ hours of learning here, with more content on the way.

If you're serious about a career in cloud security, there's no better way to start learning than with AppSecEngineer. We offer by far the best value of any security training provider in the world, and it only gets better as we add new content every month.

Explore our catalogue of courses and start learning with AppSecEngineer now:





800+ Labs, 100+ Challenges and counting...

Beginner's AWS security learning roadmap