Making a Career in Cloud Security

Secure the cloud. The fastest-growing specialism in cybersecurity.

AUTHOR	Babashaheer
VERSION	1.0
DATE	April 2026
SERIES	Cybersecurity Career Series — Document 07 of 09
AUDIENCE	Students and cloud professionals moving into security

AWS Azure GCP

Contents

Digitally signed by Baba Shaheer Gutappa
Date: 2026.04.21 18:10:37 +01'00'

1. What Is Cloud Security — and Why Is It Different?

Cloud security is the fastest-growing specialism in cybersecurity. As organisations move their servers, data and applications from physical hardware in their own buildings to infrastructure hosted by Amazon, Microsoft and Google, the security challenges change fundamentally. The attack surface expands. The tools change. The mistakes change too.

Traditional network security assumed a clear perimeter — your building, your servers, your firewall. Cloud dissolves that perimeter entirely. An organisation's sensitive data might sit in a storage bucket that is one incorrect permission away from being publicly accessible to anyone on the internet. A misconfigured IAM role could give an attacker the ability to spin up thousands of servers and run up a £500,000 bill in 48 hours. These are not theoretical risks — they happen regularly.

> **The number one cause of cloud breaches is not hacking — it is misconfiguration.**
> Gartner predicts that through 2025, 99% of cloud security failures will be the customer's fault. The cloud is secure. How we configure it often is not.

What makes cloud security different from traditional security

Traditional / On-Premise	Cloud Security
You own the hardware — physical access controls matter	You share hardware with thousands of others — logical isolation is everything
Change is slow — new servers take weeks to deploy	Change is instant — a developer can deploy a new service in minutes
Perimeter firewall is the primary control	No perimeter — identity and IAM are the primary controls
Security team controls the environment	Developers often deploy and configure cloud resources directly
Single data centre with known IP ranges	Resources in multiple regions globally, dynamic IPs
Manual configuration changes — slower to break	Infrastructure-as-Code — a bad template replicates errors at scale

Table 1: Traditional security vs cloud security — the key differences

2. The Three Major Cloud Platforms

Cloud security is not one thing — it depends heavily on which platform your organisation uses. AWS, Azure and GCP each have their own security services, terminology, IAM models and compliance tools. Most large organisations use at least two (multi-cloud). You need to understand the differences.

AWS Amazon Web Services	Azure Microsoft Azure	GCP Google Cloud
~31%	~24%	~12%
Financial services, startups, public sector	Government, enterprise, Microsoft-heavy orgs	Tech companies, analytics, media
IAM (Identity and Access Management)	Azure Active Directory / Entra ID	Cloud IAM
Security Groups, NACLs, WAF	Azure Firewall, NSG, Application GW	VPC Firewall Rules, Cloud Armor
CloudTrail, GuardDuty, Security Hub	Microsoft Sentinel, Defender for Cloud	Chronicle, Security Command Centre
ECR, EKS, Inspector	Azure Container Registry, Defender	Artifact Registry, GKE, Security Command
AWS Security Specialty	SC-100 / AZ-500	Google PCSE
Yes — 12 months free tier	Yes — free Azure sandbox	Yes — $300 free credits

Figure 1: AWS, Azure and GCP compared across key cloud security dimensions (Synergy Research, 2024)

Which platform should you learn first?

AWS has the largest market share globally and the most job postings — start there.

If you work in a Microsoft-heavy organisation, Azure is the practical priority.

GCP is smaller but growing fast in AI/ML and analytics sectors.

3. The Shared Responsibility Model

The shared responsibility model is the most fundamental concept in cloud security. Every cloud provider publishes their version of it. Understanding it tells you exactly what the cloud provider secures — and what your organisation must secure itself.

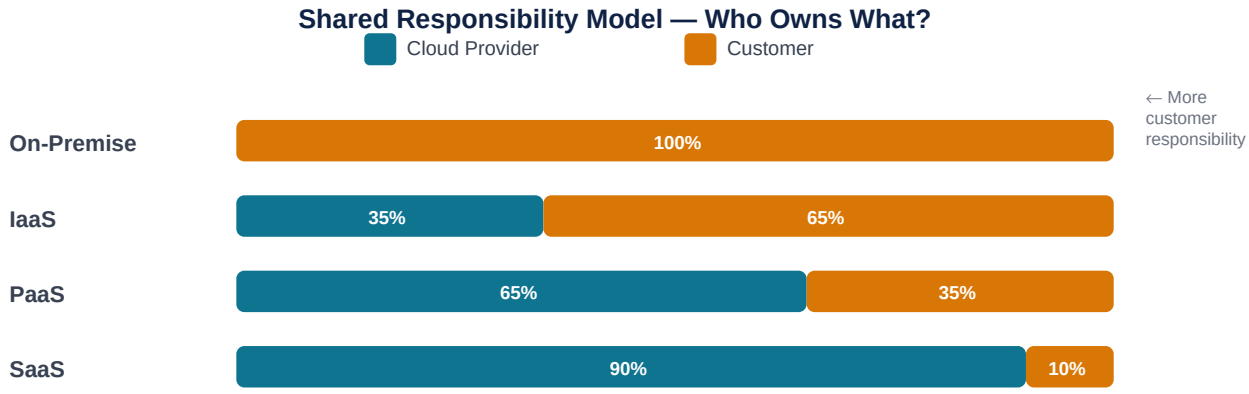


Figure 2: Shared responsibility model. As you move from IaaS to SaaS, the provider takes on more responsibility.

Service Model	Example	Provider Secures	Customer Secures
IaaS (Infrastructure as a Service)	AWS EC2, Azure VMs	Physical hardware, hypervisor, network fabric, data centre	OS, applications, data, access controls, firewall rules, patches
PaaS (Platform as a Service)	AWS RDS, Azure App Service	Hardware + OS + runtime environment	Application code, data, user access, configuration
SaaS (Software as a Service)	Microsoft 365, Salesforce, Google Workspace	Everything except data and user accounts	Your data, user access management, configuration settings

Table 2: Shared responsibility by cloud service model

The shared responsibility model does not mean 'shared blame'.
When a misconfigured S3 bucket leaks your customer data, the breach is your fault — even though AWS manages the underlying hardware. You own your configuration.

4. The Biggest Threat — Misconfiguration

Misconfiguration is consistently the leading cause of cloud security incidents. Unlike traditional hacking — which requires skill and effort — exploiting a misconfiguration often requires nothing more than knowing the right URL. Automated scanners continuously crawl the internet looking for exposed cloud resources. A newly created misconfigured bucket can be found within minutes.

Most Common Cloud Security Misconfigurations

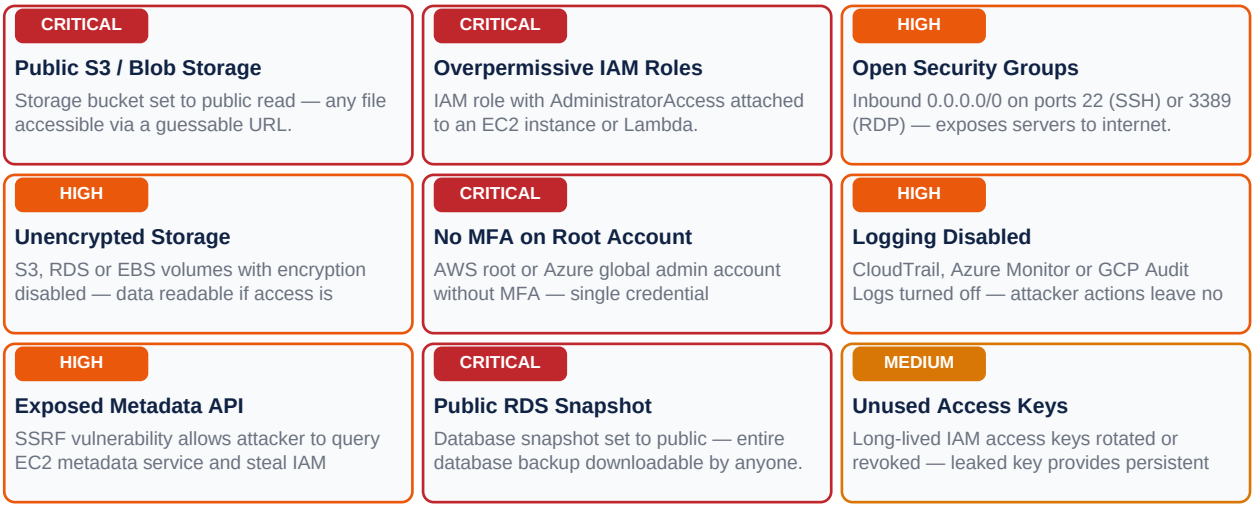


Figure 3: Most common cloud security misconfigurations by severity. Critical = breach likely if exploited.

How to find misconfigurations in your own environment:

AWS: Security Hub + Prowler (open source). Azure: Defender for Cloud + Scout Suite.

GCP: Security Command Centre. All platforms: ScoutSuite, Checkov, Trivy.

5. Identity and Access Management (IAM)

In cloud security, identity is the new perimeter. Once your infrastructure is in the cloud, there is no physical boundary to protect it. What controls who can do what is IAM — a set of policies that define permissions for users, services and applications. Getting IAM wrong is the single most common path to a serious cloud security incident.

Core IAM concepts every cloud security professional must understand

- **Principle of least privilege:** Every user, service and application should have only the minimum permissions needed to perform their function — nothing more. Most cloud environments violate this immediately because it is easier to grant broad access.
- **IAM roles vs users vs service accounts:** Human users should authenticate with identity providers (SSO). Machines and services should use roles — temporary, automatically rotated credentials. Static long-lived access keys are a persistent security risk.
- **Resource-based vs identity-based policies:** AWS attaches policies to both the resource (e.g. an S3 bucket policy) and the identity (e.g. a user's IAM policy). Both must allow the action. Understanding the intersection is essential for debugging and securing access.
- **Permission boundaries and SCPs:** Service Control Policies (AWS Organizations) and Azure Management Groups set guardrails at the organisation level — maximum permissions that cannot be exceeded even by admins. Critical for multi-account and enterprise cloud.
- **Cross-account access:** In multi-account cloud architectures, IAM roles are used to grant access across accounts. Misconfigured cross-account trust relationships are a common lateral movement path for attackers.
- **Just-in-Time (JIT) access:** Privileged access is granted temporarily, only when needed, and automatically revoked. This removes standing access that can be exploited if credentials are stolen.

Common IAM Mistake	What Happens	How to Fix
Root account used for daily tasks	If compromised, attacker has full and irreversible control	Create individual admin IAM users. Lock root account. Enable MFA on root.
Access keys in code or .env files	Developer pushes to GitHub — keys are found by automated scanner within minutes	Use IAM roles for EC2/Lambda. Use AWS Secrets Manager. Rotate and revoke old keys.
Wildcard permissions (*:*:*)	Any action on any resource — equivalent to root	Write specific resource ARNs. Use IAM Access Analyzer to identify overpermission.
No MFA enforced	Password alone is sufficient — phishing or breach = full account access	Enforce MFA for all human users via IAM policy. Use hardware tokens for high-privilege roles.
Shared credentials across services	Rotation of one credential breaks multiple services — so rotation stops happening	One IAM role per service. Automate credential rotation via Secrets Manager.

Table 3: Common IAM mistakes and how to fix them

6. Core Security Services Across AWS / Azure / GCP

Each major cloud platform provides a suite of native security services. Understanding what each one does — and the equivalent on the other platforms — is essential for any cloud security role.

Category	AWS	Azure	GCP
Threat Detection	GuardDuty	Defender for Cloud	Security Command Centre
SIEM / Log Analytics	Security Lake + OpenSearch	Microsoft Sentinel	Chronicle
Audit Logging	CloudTrail	Azure Monitor / Activity Log	Cloud Audit Logs
Config Compliance	AWS Config	Azure Policy	Config / Policy Intelligence
Secrets Management	Secrets Manager / Parameter Store	Key Vault	Secret Manager
Vulnerability Scanning	Inspector v2	Defender Vulnerability Mgmt	Artifact Analysis / Container Scanning
WAF	AWS WAF + Shield	Azure WAF + DDoS Protection	Cloud Armor
Identity Management	IAM + Identity Centre (SSO)	Entra ID (Azure AD)	Cloud Identity / IAM
Key Management	KMS (Key Management Service)	Azure Key Vault	Cloud KMS
CSPM	Security Hub	Defender for Cloud	Security Command Centre

Table 4: Equivalent native security services across the three major cloud platforms

7. Container and Serverless Security

Modern cloud applications rarely run as simple virtual machines anymore. Most are deployed using containers (Docker, Kubernetes) or serverless functions (AWS Lambda, Azure Functions). These technologies introduce their own security challenges that a cloud security professional must understand.

Container Security

- **Image scanning:** Before a container image is deployed, it should be scanned for known vulnerabilities in its OS packages and dependencies. Tools: Trivy, Snyk, Grype, AWS Inspector, Aqua Security.
- **Registry security:** Private container registries (ECR, Azure Container Registry, Artifact Registry) must be access-controlled. Publicly accessible registries with sensitive images are a common misconfiguration.
- **Runtime security:** Monitoring what containers are doing while they run — unexpected network connections, file writes, process execution. Tools: Falco (open source), Aqua, Sysdig, Prisma Cloud.
- **Kubernetes RBAC:** Kubernetes has its own role-based access control system, separate from cloud IAM. Misconfigured RBAC can allow container escape — gaining access to the underlying node or cluster.
- **Secrets in containers:** Never hardcode secrets in container images or environment variables in Dockerfiles. Use Kubernetes Secrets (or better — external secret managers like Vault or AWS Secrets Manager).

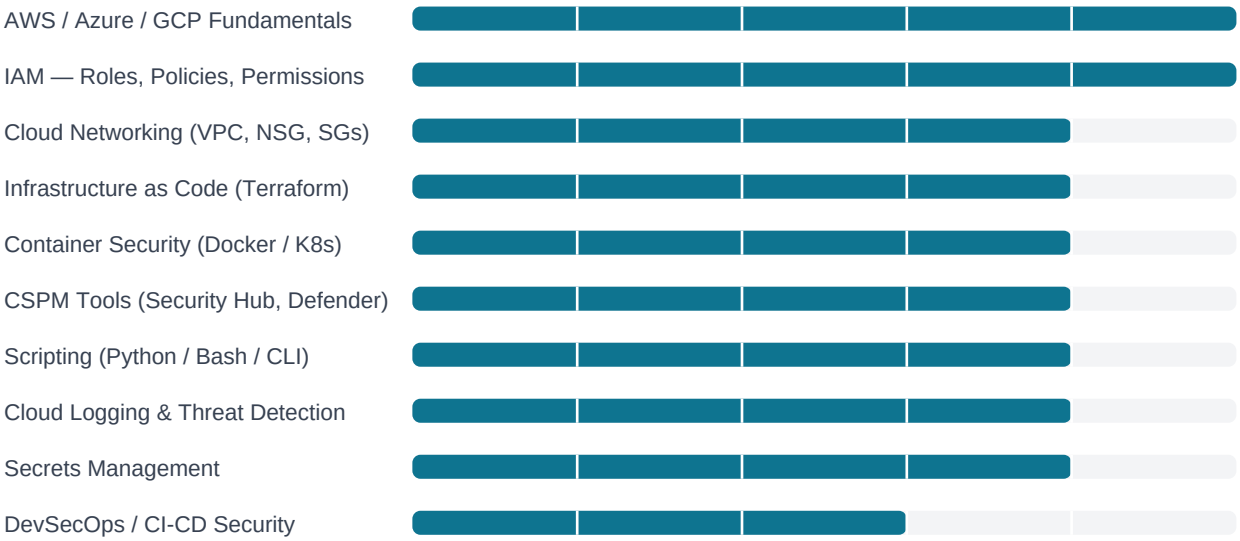
Serverless Security

Serverless functions (Lambda, Azure Functions, Cloud Functions) run your code without you managing the underlying infrastructure. The security challenges shift from server hardening to function permissions and dependency management:

- **Overpermissive function roles:** A Lambda function with AdminAccess is a common misconfiguration — if the function is compromised via injection, the attacker inherits full AWS permissions.
- **Event injection:** Serverless functions are triggered by events — API calls, queue messages, file uploads. If the event data is used unsafely (SQL injection, command injection), the function becomes an attack vector.
- **Dependency vulnerabilities:** Serverless functions include their own dependency packages. Outdated libraries with CVEs are a common entry point — use Software Composition Analysis (SCA) tools in your CI/CD pipeline.
- **Cold start timing attacks:** Function execution times can sometimes leak information about internal logic. Use constant-time comparison for security-sensitive operations.

8. Core Skills You Need to Build

Cloud security sits at the intersection of cloud engineering, DevOps and cybersecurity. The ideal cloud security professional has enough engineering background to understand how things are built — and enough security knowledge to know how they break.



The key differentiator in cloud security: infrastructure knowledge.
A cloud security engineer who can read a Terraform file, write a boto3 script, and understand VPC routing is worth significantly more than one who cannot.

9. Tools Every Cloud Security Professional Should Know

Tool	Category	What It Does	Cost
Prowler	AWS Security Audit	Open-source tool that checks hundreds of AWS configuration controls against CIS benchmarks and AWS best practices.	Free
ScoutSuite	Multi-cloud CSPM	Audits AWS, Azure and GCP configurations simultaneously. Produces an HTML report of findings categorised by severity.	Free
Trivy	Container / IaC Scanning	Scans container images, filesystems and Infrastructure-as-Code for vulnerabilities and misconfigurations.	Free
Checkov	IaC Security	Scans Terraform, CloudFormation, Kubernetes and Helm charts for security misconfigurations before deployment.	Free
CloudSploit	Cloud Misconfiguration	Automated scanning for security risks in AWS, Azure, GCP and Oracle Cloud. Good for continuous monitoring.	Free/Commercial
Pacu	AWS Exploitation	AWS penetration testing framework — offensive tool for testing IAM privilege escalation and other attack paths.	Free
Steampipe	Cloud Query Engine	SQL-based querying of cloud resources. Write queries like 'SELECT * FROM aws_s3_bucket WHERE public_access = true'.	Free
Falco	Runtime Security	Open-source runtime security for containers. Detects unexpected behaviour in running containers — new processes, file writes.	Free
AWS Security Hub	CSPM (AWS native)	Aggregates findings from GuardDuty, Inspector, Config and third-party tools. Central security dashboard for AWS.	Commercial
Microsoft Defender for Cloud	CSPM (Azure native)	Azure's native CSPM and threat protection — misconfiguration scores, recommendations and threat alerts.	Commercial
HashiCorp Vault	Secrets Management	Open-source secret management platform. Centrally store, access and rotate secrets, API keys and certificates.	Free/Commercial

Table 5: Core tools for cloud security professionals. Most are free and open-source.

10. Career Paths in Cloud Security

Cloud security is one of the highest-paid specialisms in cybersecurity. The combination of cloud engineering knowledge and security expertise is rare — and employers pay accordingly. Most cloud security professionals come from either a cloud engineering background (adding security) or a traditional security background (adding cloud knowledge).

Role	What You Do	Where You Work	UK Salary
Cloud Security Analyst	Monitor cloud security posture, review GuardDuty/Sentinel alerts, remediate findings from CSPM tools.	Financial services, tech companies	£35k–£55k
Cloud Security Engineer	Implement and maintain cloud security controls — IAM, network security, encryption, secrets management.	Enterprises, cloud-native companies	£55k–£80k
DevSecOps Engineer	Integrate security into CI/CD pipelines — SAST, DAST, SCA, IaC scanning, container scanning.	Tech companies, SaaS businesses	£55k–£80k
Cloud Security Architect	Design secure cloud architectures — multi-account strategy, Zero Trust, security guardrails at scale.	Large enterprises, consulting firms	£75k–£110k+
Penetration Tester (Cloud)	Test cloud environments for misconfigurations, IAM privilege escalation, lateral movement paths.	Consulting firms, bug bounty	£55k–£90k
CSPM / GRC Analyst	Manage cloud compliance — CIS benchmarks, SOC 2, ISO 27001 cloud controls, audit evidence.	Financial services, regulated industries	£45k–£70k
Cloud Security Consultant	Independent advisory across multiple clients — cloud security assessments, architecture review.	Self-employed, boutique firms	£600–£1,100/day

Table 6: Career paths in cloud security (Reed, 2024; CW Jobs, 2024)

11. The Learning Roadmap

Cloud security is one of the few cybersecurity disciplines where you genuinely need to understand the technology before you can secure it. Start by learning the cloud platform itself — then add the security layer.

1 **Get your AWS / Azure free account**
Sign up for AWS Free Tier or Azure free account. Spend time clicking through the console. Create an S3 bucket, an EC2 instance, an IAM user. Understand what these things are before worrying about securing them. 2–3 weeks.

2 **Learn cloud fundamentals**
AWS Cloud Practitioner or Azure Fundamentals (AZ-900) are beginner-level certs that teach you what all the services are and how they relate. Both have free study materials. AWS Skill Builder and Microsoft Learn are excellent. 4–6 weeks.

3 **Learn cloud networking**
Understand VPCs, subnets, route tables, security groups and NACLs (AWS) or VNets, NSGs and UDRs (Azure). Network misconfiguration is a common attack path. Build a multi-tier VPC with public and private subnets. 3–4 weeks.

4 **Master IAM deeply**
Spend a week doing nothing but IAM. Create users, roles, policies. Read the IAM policy evaluation logic documentation. Use IAM Access Analyzer. Practice writing least-privilege policies. This is the most important topic in cloud security. 2–3 weeks.

5 **Study cloud misconfigurations**
Run Prowler against your AWS account. Run ScoutSuite. Read every finding. Look up why each one is a risk. This is the fastest way to learn what cloud security professionals actually look for. Use flaws.cloud (free intentionally vulnerable AWS environment). Ongoing.

6 **Learn Infrastructure as Code**
Learn Terraform basics — write code that deploys cloud resources. Then run Checkov against your code to find security issues. DevSecOps is a major growth area and IaC knowledge separates junior from mid-level cloud security roles. 4–6 weeks.

7 **Get your first cloud security certification**
AWS Security Specialty or Azure AZ-500 (Security Technologies) — depending on your platform. These certifications validate real security depth and are the most recognised cloud security qualifications by hiring managers.

8 **Build hands-on evidence**
Complete TryHackMe AWS rooms, flaws.cloud, CloudGoat (Terraform-deployed vulnerable AWS environment from Rhino Security Labs). Write up your findings. Document your Prowler reports. This is your portfolio.

Timeline: cloud-platform-ready in 6 months. Security specialist in 12–18 months.
If you already work with cloud infrastructure, the security overlay takes 6–9 months.

12. Certifications That Matter

Cloud security certifications fall into two categories: vendor-neutral (applicable to any cloud) and vendor-specific (deep expertise in one platform). You need both.

Certification	Level	Provider	Focus	Why It Matters
AWS Cloud Practitioner	Beginner	AWS	Cloud fundamentals — what each service does	Foundation before any AWS security study. Required for AWS Security Specialty.
AZ-900 Azure Fundamentals	Beginner	Microsoft	Azure services overview	Same role as Cloud Practitioner but for Azure. Free exam vouchers often available.
AWS Security Specialty	Mid–Senior	AWS	IAM, encryption, monitoring, incident response in AWS	The most recognised AWS security certification. Highly valued by hiring managers.
AZ-500 Security Technologies	Mid	Microsoft	Azure security services — Defender, Sentinel, Key Vault, identity	Required for many Azure security roles in the UK, especially in Microsoft-heavy orgs.
SC-100 Cybersecurity Architect	Senior	Microsoft	Zero Trust, cloud security architecture across Microsoft stack	Senior-level cert. Required for cloud security architect roles in Azure environments.
Google PCSE	Mid	Google	Cloud security in GCP — IAM, networking, data security	Best cert for GCP security roles. Less common than AWS/Azure but growing.
CCSP — Certified Cloud Security Professional	Mid–Senior	ISC2	Vendor-neutral cloud security — architecture, data security, legal	Widely respected across industries. Good complement to a vendor-specific cert.
CKS — Certified Kubernetes Security Specialist	Mid	CNCF	Container and Kubernetes security	Best practical cert for container security. Challenging — requires CKA first.

Table 7: Cloud security certifications in order of progression

13. Case Study — The Exposed S3 Bucket

> This is a fictional case study based on one of the most common real-world cloud breach patterns.
> Exposed S3 buckets have been responsible for major real-world breaches affecting millions of people.

The Organisation

Clearview Legal Tech is a UK legal services company that recently migrated their document management system to AWS. Their development team built an application that stores client documents — contracts, NDAs, personal identity documents — in an S3 bucket. A security review was on the roadmap but had not yet happened.

Day 1 — The misconfiguration is created

09:15 — Developer deploys new S3 bucket

Marcus, a developer, creates a new S3 bucket for the client portal. He is working quickly to meet a sprint deadline. He sets the bucket ACL to 'public-read' so that the application can serve documents to authenticated users — not realising that 'public-read' means publicly readable to anyone on the internet, not just authenticated users.

The application goes live. 3,400 client documents — including passports, proof of address, signed contracts and financial statements — are now accessible via predictable URLs. No one notices. The compliance team has not

Day 23 — Discovery by an external researcher

Day 23 — Security researcher reports a finding

A security researcher running automated S3 enumeration tools discovers the bucket. They download a sample of three documents, confirm they are genuine personal data, and report the finding responsibly to Clearview Legal Tech via email.

The email reaches the operations inbox — not monitored over the weekend. It sits unread for two days. By Monday morning, the researcher has escalated to the ICO (Information Commissioner's Office) after receiving no response.

Day 25 — Incident response begins

Day 25 — ICO notification triggers internal escalation

The ICO contact triggers an urgent call to the CEO. The bucket is identified and made private within 20 minutes. CloudTrail logs are pulled to determine who accessed the bucket and when.

CloudTrail shows 847 unique IP addresses accessed at least one object over 23 days. Most are automated scanners. At least 12 appear to be manual access patterns — consistent with human browsing through documents. The scope of exfiltration cannot be determined precisely.

The cost and consequences

Cost Category	Details	Estimated Cost
Legal and regulatory advice	External law firm engaged immediately. ICO investigation management.	£65,000

Cost Category	Details	Estimated Cost
ICO fine	Personal data of 3,400 individuals exposed for 23 days. UK GDPR breach.	£95,000
Client notification	Letters, emails and credit monitoring for affected clients.	£28,000
Incident response	Forensic log analysis, breach scope assessment, remediation validation.	£40,000
Reputational damage	Three major corporate clients terminated contracts.	~£380,000
Security overhaul	Full AWS security review, GuardDuty enabled, CloudTrail expanded, IAM audit.	£55,000
TOTAL		**~£663,000**

Table 8: Estimated cost breakdown of the Clearview Legal Tech S3 breach

What should have prevented this

- Enable S3 Block Public Access at the account level — a single checkbox that prevents any bucket in the account from ever being made public
- Run Prowler or AWS Security Hub from day one — the public bucket would have appeared as a CRITICAL finding within minutes
- Implement a deployment approval process — changes to S3 bucket ACLs should require a second approver
- Enable CloudTrail and GuardDuty before migrating any personal data — logging is not optional
- Conduct a security review before go-live on any service handling personal data — not after

> **The fix would have taken 30 seconds: Block Public Access = ON.**
> **The breach cost £663,000.**
> This is why cloud security professionals exist.

14. Breaking In — Getting Your First Role

Cloud security roles are genuinely accessible if you have the right combination of cloud knowledge and security fundamentals. The most common background of people entering cloud security is cloud engineering or DevOps — they already understand the infrastructure, and they add security depth. But it is also achievable from a pure security background with deliberate cloud study.

Build visible evidence of skill

- **AWS / Azure free account lab:** Deploy intentionally vulnerable environments — CloudGoat (AWS) or XMGoat (Azure). Fix the vulnerabilities. Document your findings. Employer gold.
- **flaws.cloud and flaws2.cloud:** Free, intentionally vulnerable AWS environments. Each level teaches a real misconfiguration. Write up your solutions — this is your cloud security portfolio
- **Prowler report on your own account:** Run Prowler against your personal AWS account, remediate findings, screenshot before and after. Shows you can both identify and fix real issues
- **TryHackMe AWS rooms:** Complete the AWS-focused learning paths. Your public profile shows completion and demonstrates hands-on practice
- **GitHub with IaC and Terraform:** Put Terraform code on GitHub. Show you can deploy cloud infrastructure securely. Add Checkov to your CI pipeline and screenshot the security scan results
- **Write a blog post:** Explain a cloud misconfiguration in simple terms. 'How I found a public S3 bucket and what it could have exposed' — this kind of post gets noticed by hiring managers

Where to Look	Notes
CyberSecurityJobs.com	Search 'cloud security engineer', 'DevSecOps', 'cloud security analyst'
LinkedIn	Cloud security roles post heavily. Connect with cloud security architects and CISO contacts at tech companies
AWS / Microsoft / Google Careers	Vendor security roles — often more accessible for those with platform certs
TechJobs / Hired / Glassdoor	Good for cloud-native and startup roles where cloud security is baked in from day one
NCSC Cyber Accelerator	For early-career candidates — competitive but excellent structured programme
Consultancies (Deloitte, KPMG, Accenture)	Cloud security consulting roles — good exposure across many client environments

Table 9: Where to find cloud security roles

Interview questions to prepare for

- Explain the AWS shared responsibility model. Who is responsible for what in an EC2 deployment?
- What is an IAM role and how does it differ from an IAM user?
- An S3 bucket has been set to public. Walk me through how you would detect it and remediate it.
- What is the principle of least privilege? How would you apply it to a Lambda function?
- What tools would you use to audit the security posture of an AWS account?

- What is the metadata service on AWS EC2 and what security risk does it present?
- How does IMDSv2 protect against SSRF attacks compared to IMDSv1?
- What is a Service Control Policy (SCP) in AWS Organizations and when would you use one?

The best cloud security interview answer:
"Here is a Prowler report I ran on my own account. Here is what I found and fixed."
Real hands-on evidence consistently beats theoretical knowledge alone.

15. References

1. Amazon Web Services (2024) *AWS Security Specialty Certification.* Available at: https://aws.amazon.com/certification/certified-security-specialty/ [Accessed: 10 April 2026].
2. Checkov (2024) *Open Source IaC Security Tool.* Bridgecrew / Prisma Cloud. Available at: https://www.checkov.io [Accessed: 10 April 2026].
3. CW Jobs (2024) *Technology Salary Survey 2024.* Available at: https://www.cwjobs.co.uk/salary-checker [Accessed: 11 April 2026].
4. Flaws.cloud (2024) *Intentionally Vulnerable AWS Environment for Learning.* Available at: http://flaws.cloud [Accessed: 11 April 2026].
5. Gartner (2023) *Is the Cloud Secure?* Available at: https://www.gartner.com/en/articles/is-the-cloud-secure [Accessed: 11 April 2026].
6. Google Cloud (2024) *Professional Cloud Security Engineer Certification.* Available at: https://cloud.google.com/certification/cloud-security-engineer [Accessed: 12 April 2026].
7. ISC2 (2024) *CCSP — Certified Cloud Security Professional.* Available at: https://www.isc2.org/certifications/ccsp [Accessed: 12 April 2026].
8. Microsoft (2024) *AZ-500: Microsoft Azure Security Technologies.* Available at: https://learn.microsoft.com/en-us/certifications/azure-security-engineer/ [Accessed: 12 April 2026].
9. NIST (2020) *Zero Trust Architecture (SP 800-207).* Available at: https://doi.org/10.6028/NIST.SP.800-207 [Accessed: 13 April 2026].
10. Prowler (2024) *Open Source Cloud Security Tool.* Available at: https://prowler.pro [Accessed: 13 April 2026].
11. Reed (2024) *Cybersecurity Salary Guide UK 2024.* Available at: https://www.reed.co.uk/career-advice/cybersecurity-salary [Accessed: 13 April 2026].
12. Rhino Security Labs (2024) *CloudGoat — Vulnerable AWS Environment.* Available at: https://github.com/RhinoSecurityLabs/cloudgoat [Accessed: 14 April 2026].
13. Synergy Research Group (2024) *Cloud Infrastructure Services Market Share Q4 2023.* Available at: https://www.srgresearch.com [Accessed: 14 April 2026].

Document prepared by **Babashaheer**. Version 1.0 — April 2026. Cybersecurity Career Series — Document 07 of 09.