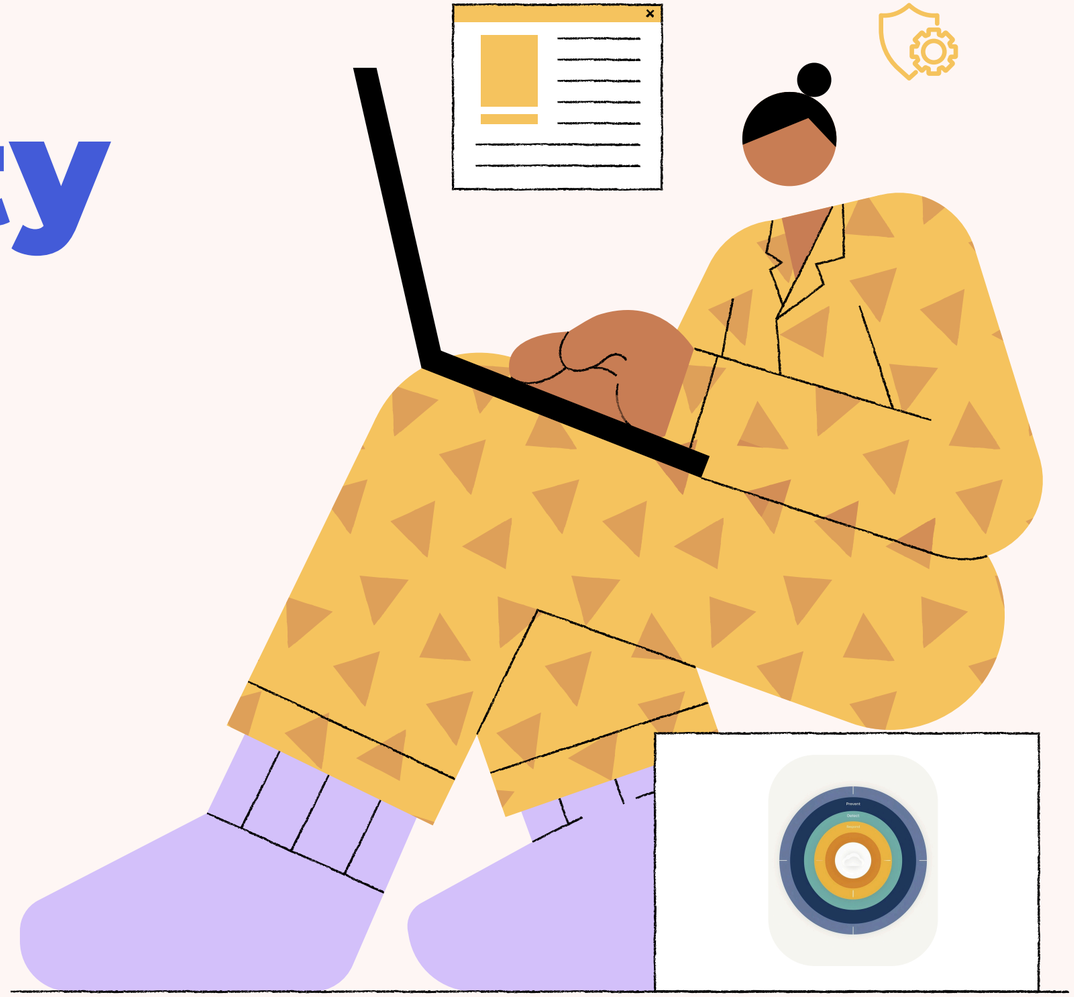
Cloud Security Engineer Roadmap



By peachycloudsecurity

https://linktr.ee/peachycloudsecurity

Peachycloud Security

What is Cloud Security?

Cloud security is the discipline of protecting data, applications, and infrastructure hosted on cloud platforms (AWS, Azure, GCP, Digital Ocean & Alibaba).

Let’s use AWS as CSP example.

The role of the Cloud Security Engineer is to design, implement, and manage security controls for these environments.

The field is crucial as global companies accelerate their migration to cloud-native and hybrid architectures.

A successful career in this domain requires a blend of security knowledge and deep cloud platform experience.

Foundations Needed

Operating Systems & Linux

Understanding OS is essential for navigating cloud environments. Familiarity with linux command line is must for enhancing troubleshooting and task automation, laying a strong foundation for security practices.

Networking

Understand host networking, firewalls, IP addressing, and DNS. This is the base layer for securing any infrastructure, cloud or otherwise.

Container Technologies

Familiarity with containerization (Docker) and orchestration (Kubernetes) is crucial as these technologies underpin modern cloud infrastructure.

Scripting Basics

Learning basic scripting in python/bash/go skills is vital for automating tasks in cloud environments. Simple scripts can streamline processes, enhance productivity, and support security by automating routine checks and actions.

Master One Cloud Provider

Answer

Learning one major provider is the key.

AWS (Amazon Web Services)

Largest market share, Focus on One excellent starting point.

Microsoft Azure

Strong integration for enterprises using Microsoft tools.

GCP (Google Cloud)

Noted for its strengths in data, AI and containers.

Statement

Familiarize yourself with core services like for AWS learn storage (S3), compute (EC2), and identity management (IAM) within your chosen cloud.

Deep Dive: Defense in Depth

Concept and Layers

Defense in Depth is a strategy that places multiple, independent security controls throughout an IT system. If one line of defense fails, another layer is there to catch the threat.

- **Network Layer:** Virtual Private Clouds (VPCs) and Network ACLs act as the outer walls.
- **Perimeter Layer:** Web Application Firewalls (WAF) and Load Balancers filter malicious traffic before it reaches the core.
- **Compute Security:** Virtual machine firewalls and host-based security tools

Practical Application

This layered approach is vital in cloud security, where the "perimeter" is often difficult to define. Assuming a breach is possible and focusing on below things:

Identity: The first layer (IAM/Least Privilege).

Data: Encryption ensures that even if an attacker penetrates the network and compute layers, the core data is unusable.

Monitoring: The final defense-logging and alerting allows you to detect and respond quickly to lateral movement inside the environment.

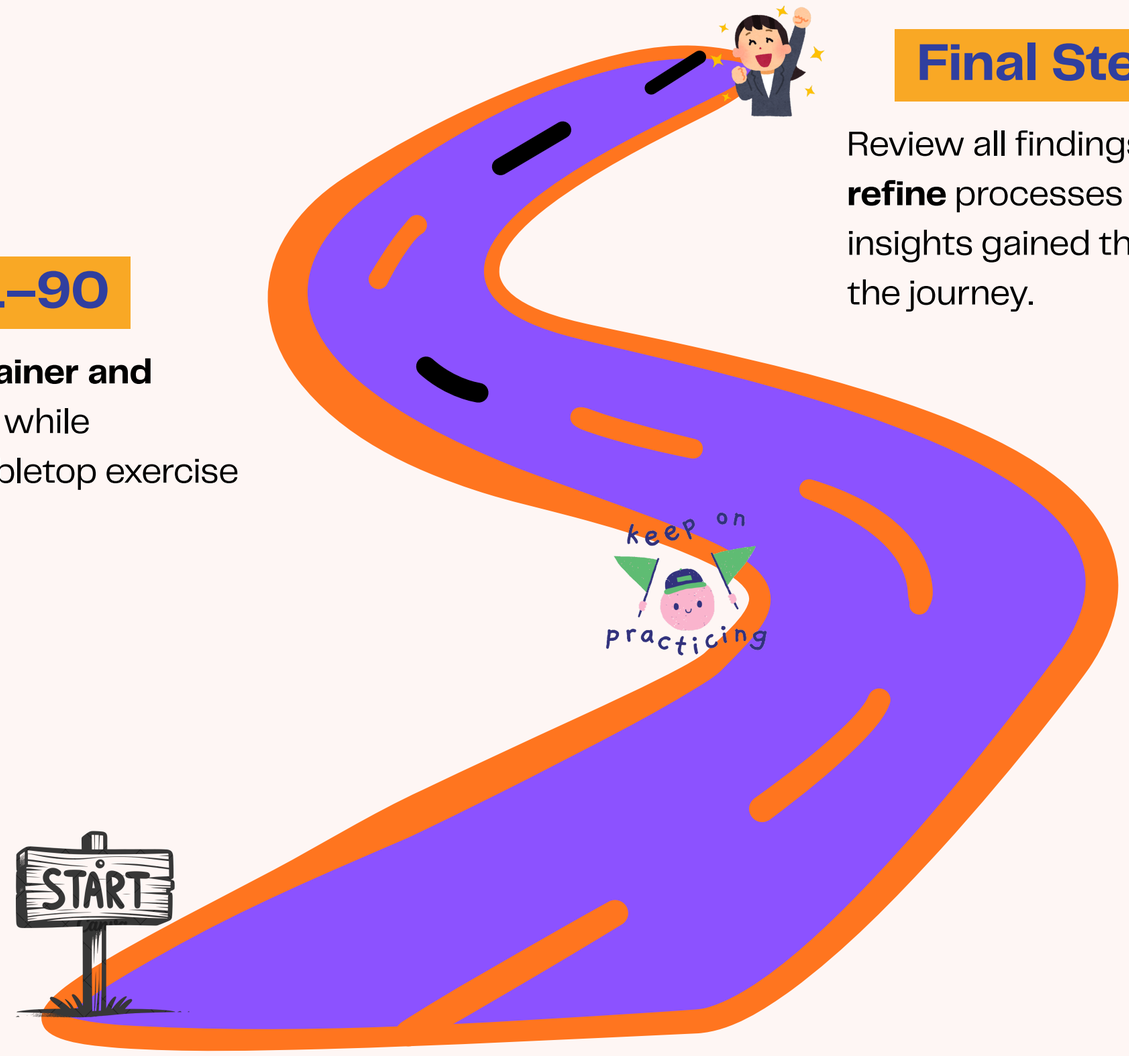
Your First 90 Days

Final Steps

Review all findings and **refine** processes based on insights gained throughout the journey.

Days 61–90

Introduce **container and cluster** policies, while conducting a tabletop exercise for refinement.

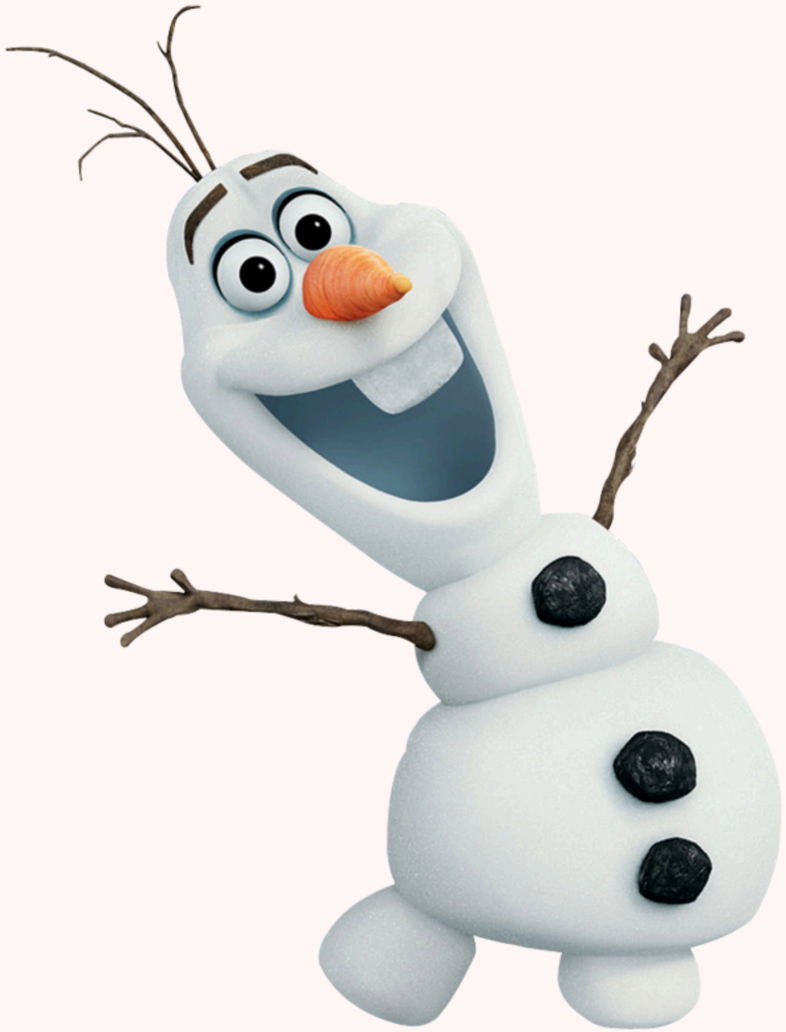


Days 31–60

Enforce **least privilege** for one workload, implementing essential policies and checks.

Days 1–30

Set up a **safe sandbox** and establish baseline guardrails for security.



Mindset and Practice

The Hacker Mindset

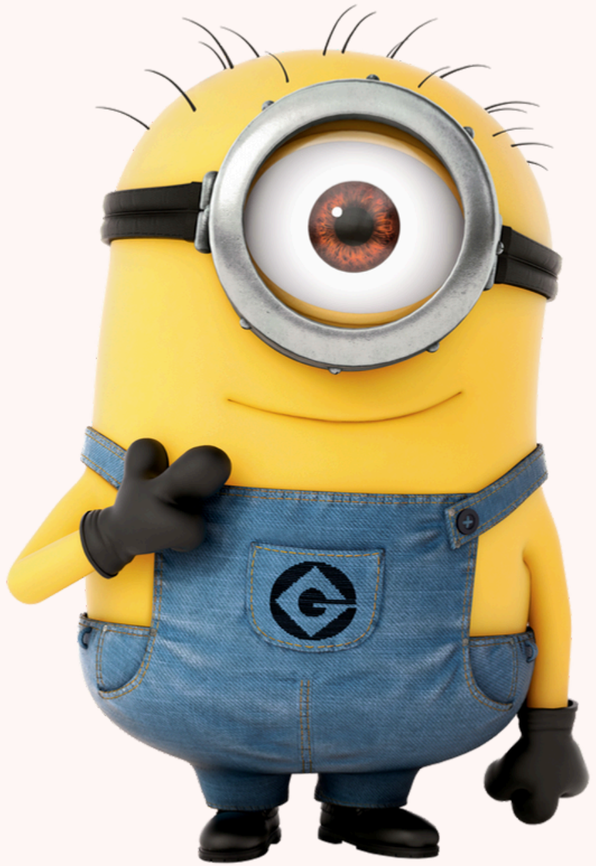
Think like a threat actor. Proactively assess the environment and question how an attacker might exploit weaknesses, especially configured identities and cloud APIs.

Automation and IaC

In a cloud environment, manual processes are inefficient. Learn scripting (Python/Bash) for custom tasks and use Infrastructure as Code (IaC) tools like Terraform to enforce consistent security standards.

Incident Response & DR

Define playbooks and automation to quickly detect, contain, and recover from security incidents (IR) or system failures (Disaster Recovery/DR).



Certifications &Motivation

The short answer is **No, but they help**. Many highly skilled engineers have fantastic careers without them because practical ability and experience.

Remember the question you are answering is:

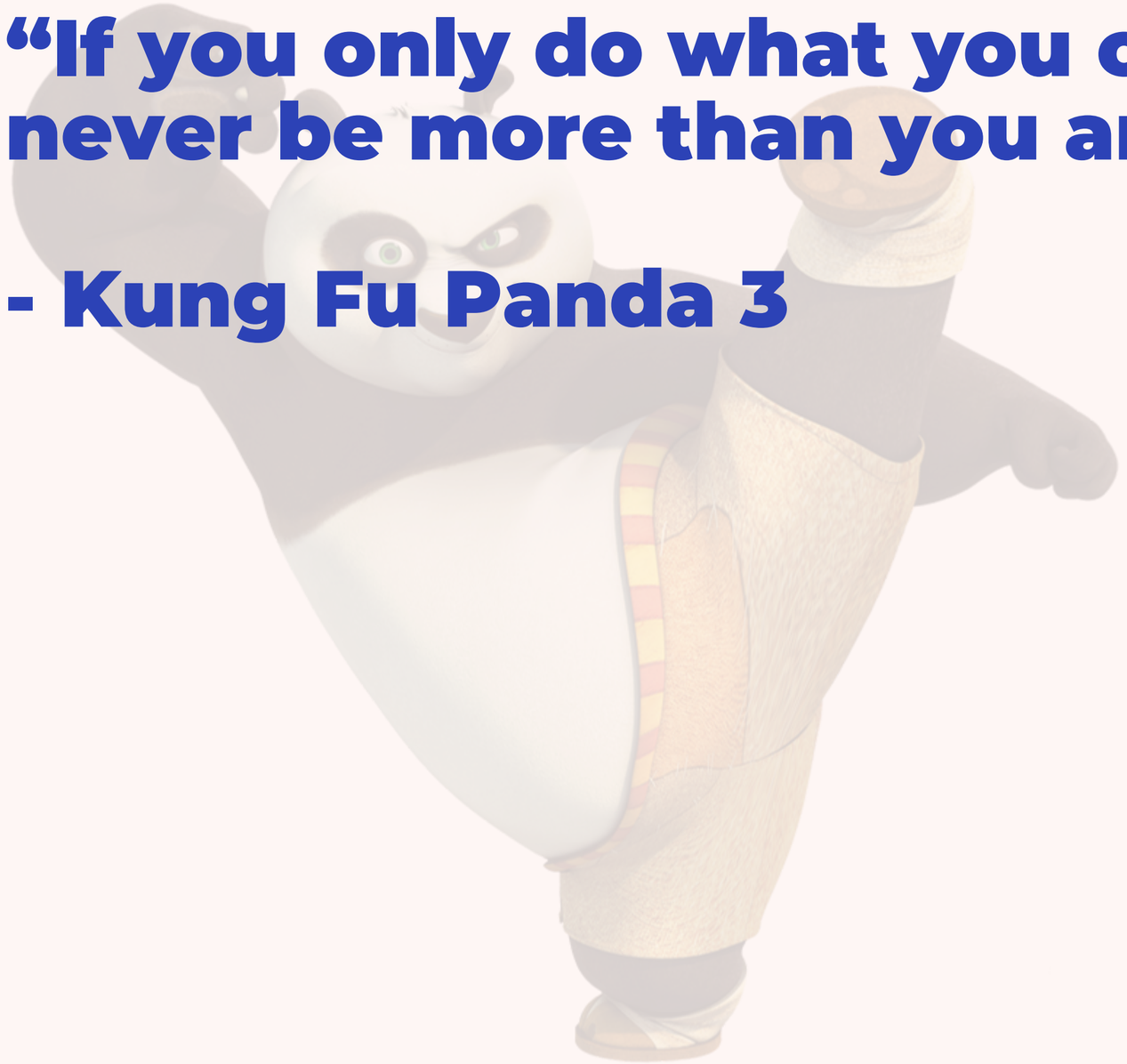
Certifications prove that one knows vocabulary and the fundamentals required however skills will be required for the job.

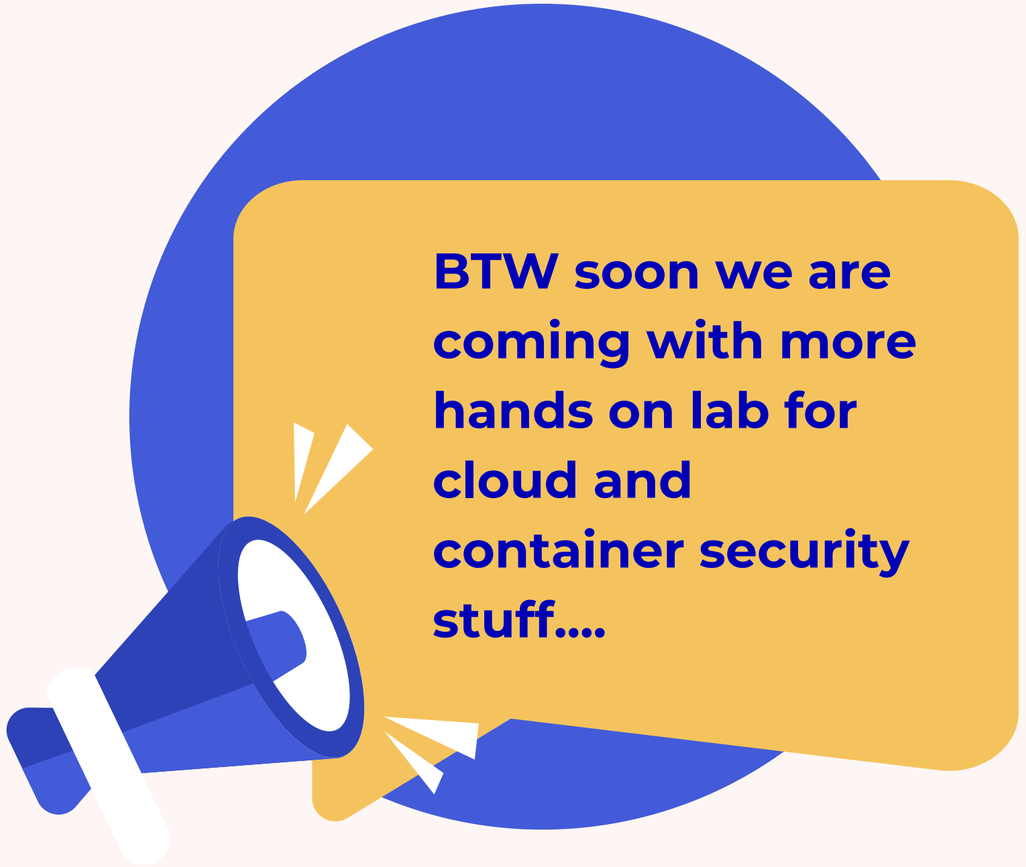
Only If you think, only then focus on **Cloud Provider Certs first** (e.g, AWS Security, Azure Security).

Excellent for opening doors and getting past initial HR screening.

“If you only do what you can do, you will never be more than you are now.”

- Kung Fu Panda 3





Connect & Follow!

Thank you for watching! Subscribe for more hands-on cloud & container security content.

Peachycloud Security

peachycloudsecurity

peachycloudsecurity

peachycloudsecurity

linktr.ee/theshukladuo