120-Day Multi-Cloud Security Engineer Daily Tracker

Goal: Master Azure + GCP Cloud Security from fundamentals → defense → automation

Time Commitment: 1–2 hrs/day

Method: Learn → Practice → Project → Document

Output: 16 hands-on projects + 1 final multi-cloud capstone

⚙️ PHASE 1 (Days 1–30): Cloud & Security Foundations

WEEK 1: Cloud Fundamentals (Days 1–7)

Day	Task	Resources
Day 1	Learn Cloud Computing models (IaaS, PaaS, SaaS)	Azure Fundamentals Doc → docs.microsoft.com/azure/architecture/guide/technology-choices/compute-decision-tree GCP: cloud.google.com/docs/overview
Day 2	Understand Shared Responsibility Models (Azure vs GCP)	Microsoft Docs & GCP Shared Responsibility whitepaper
Day 3	Explore Azure Portal & GCP Console (UI overview)	Practice: Create free accounts & explore services
Day 4	Learn Regions, Availability Zones, Resource Groups	Azure Regions link
Day 5	Learn how pricing & billing works	Azure Cost Mgmt + GCP Billing Console
Day 6	Project 1: Deploy a VM & Storage Bucket (Azure & GCP)	Practice: Create and secure both
Day 7	Document learnings (Architecture + Cost comparison)	Use Notion or Obsidian

WEEK 2: Identity & Access Management

Day	Task	Resources
Day 8	Learn Azure Entra ID & GCP IAM basics	Azure Entra Overview GCP IAM Overview
Day 9	Understand RBAC in both clouds	Create custom roles & assign
Day 10	Explore Service Accounts (GCP) & Managed Identities (Azure)	Practice enabling on a VM
Day 11	Implement MFA, Conditional Access (Azure)	Azure AD Portal
Day 12	Practice IAM Policies (GCP) – least privilege demo	Cloud Shell
Day 13	Project 2: Secure VM access using Managed Identity & Service Account	Deploy + restrict access
Day 14	Document IAM Architecture comparison (Entra vs IAM)	Draw diagram in Lucidchart

WEEK 3: Network Security

Day	Task	Resources
Day 15	Learn Virtual Network (Azure) & VPC (GCP)	Azure VNets
Day 16	Subnets, CIDR, IP planning	GCP VPC Concepts
Day 17	Configure NSG (Azure) & Firewall rules (GCP)	Hands-on
Day 18	Private Endpoints & VPC Service Controls	Deploy secure private connection
Day 19	Hub-Spoke and Peering concepts	Draw network architecture
Day 20	Project 3: Build secure network in Azure + GCP	Include private subnets
Day 21	Review + document (compare network models)	

WEEK 4: Encryption & Key Management

Day	Task	Resources
Day 22	Learn encryption in transit & at rest	Azure & GCP docs
Day 23	Explore Azure Key Vault & GCP KMS	Deploy both
Day 24	Use customer-managed keys (CMK)	Encrypt storage blob & bucket
Day 25	Learn BYOK & HSM integration concepts	Study MS & GCP models
Day 26	Configure secret rotation policy	Practice rotation via CLI
Day 27	Project 4: Encrypt Azure Storage + GCP Bucket with CMK	Verify via CLI
Day 28–30	Review + mini quiz + summary diagram	Self-assessment

📘 **Milestone:** You understand IAM, network, encryption, and foundational cloud security.

🔒 PHASE 2 (Days 31–60): Data, Compute & Application Security

WEEK 5: Compute Security

01

Day 31

Learn Azure VM Security (JIT, Disk Encryption)

Resources: Defender for Servers

02

Day 32

Learn GCE Shielded VM concepts

Resources: GCE Docs

03

Day 33

Configure JIT access & SSH lockdown

Resources: Practice

04

Day 34

Apply Disk Encryption (BitLocker, Linux)

Resources: Use CMK

05

Day 35

Project 5: Harden Azure & GCP VMs

Resources: Checklist

06

Day 36–37

Review + documentation

WEEK 6: Data Security

Day	Task	Resources
Day 38	Learn Transparent Data Encryption (Azure SQL & Cloud SQL)	Hands-on
Day 39	Enable private endpoint for SQL	Practice
Day 40	Configure access via managed identity / IAM	
Day 41	Audit & logging for database access	
Day 42–43	Project 6: Secure SQL on both clouds (Private endpoint + TDE)	
Day 44–45	Document + checkpoint	

WEEK 7: Application Security

Day	Task	Resources
Day 46	Learn App Service (Azure) & Cloud Run (GCP) security	
Day 47	Configure HTTPS & authentication	
Day 48	Learn WAF concepts (App Gateway / Cloud Armor)	
Day 49–50	Project 7: Deploy secure web app with WAF & managed identity	
Day 51	Document + compare PaaS app models	

WEEK 8: Container Security

Day	Task	Resources
Day 52	Learn AKS & GKE basics	
Day 53	Enable image scanning (Defender / Container Analysis)	
Day 54	Apply Pod Security Policies & RBAC	
Day 55–56	Project 8: Secure containerized app in AKS & GKE	
Day 57–60	Review + checkpoint	

📘 **Milestone:** You've secured compute, data, and app layers using encryption, identity, and WAFs.

🔍 PHASE 3 (Days 61–90): Monitoring, Threat Detection & Compliance

WEEK 9
Logging & Monitoring

Days 61–62: Learn Azure Monitor & Log Analytics

Days 63–64: GCP Cloud Logging & Monitoring

Days 65–66: Project 9: Build unified dashboard (VMs, DBs, Network logs)

Day 67: Document architecture

WEEK 10
Threat Detection & SIEM

Days 68–69: Learn Defender for Cloud (Azure) & SCC (GCP)

Days 70–71: Enable alerts and severity mapping

Days 72–73: Project 10: Integrate GCP logs into Azure Sentinel

Days 74–75: Document correlation queries (KQL / Chronicle Query)

WEEK 11
Compliance & Governance

Days 76–77: Learn Azure Policy & GCP Organization Policies

Day 78: Create compliance rules (CIS, NIST templates)

Days 79–80: Project 11: Apply policy baseline & evaluate Secure Score

Days 81–82: Document compliance posture report

WEEK 12
Incident Response

Days 83–84: Learn Incident Response lifecycle

Day 85: Create forensic snapshots (VMs, disks)

Days 86–87: Automate alert triage with Sentinel Playbooks

Days 88–90: Project 12: Simulate attack, perform investigation, and IR report

📘 **Milestone:** You can detect, investigate, and automate multi-cloud incidents.

⚔️ PHASE 4 (Days 91–120): Zero Trust, Automation, and Multi-Cloud Defense

WEEK 13: Zero Trust Architecture

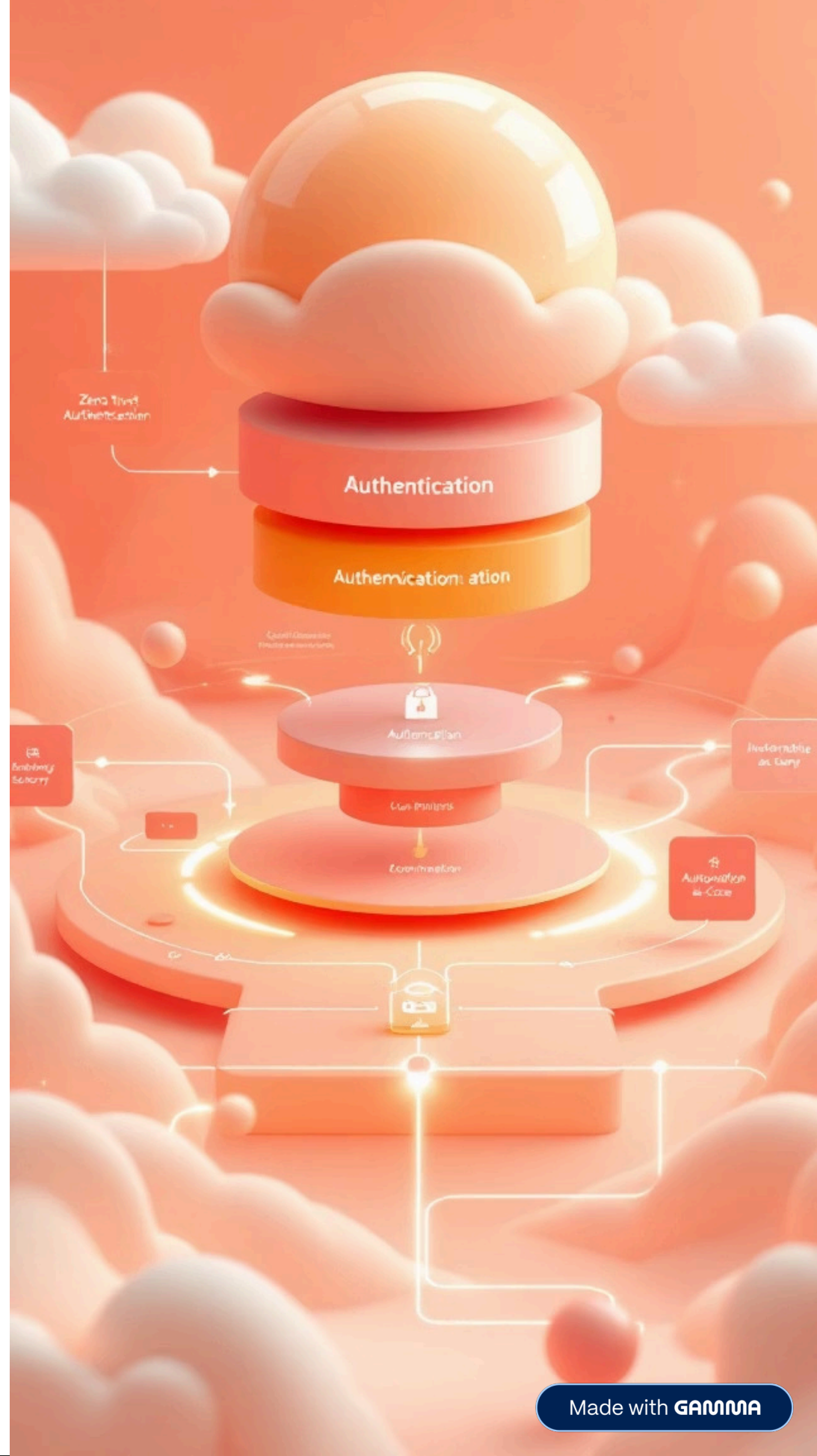
Day	Task	Resources
Day 91–92	Learn Zero Trust fundamentals	Microsoft & BeyondCorp papers
Day 93–94	Implement Conditional Access (Azure) + BeyondCorp (GCP)	
Day 95–96	Project 13: Zero Trust Access between Azure App & GCP API	

WEEK 14: DevSecOps & IaC

Day	Task	Resources
Day 97–98	Learn Terraform / Bicep basics	
Day 99–100	Scan IaC with Checkov / Snyk	
Day 101–102	Project 14: Secure IaC pipeline for Azure + GCP infra	

WEEK 15: Automation & SOAR

Day	Task	Resources
Day 103–104	Learn Logic Apps & Cloud Functions for automation	
Day 105–106	Build automation workflow for threat response	
Day 107–108	Project 15: Automated remediation for IAM misconfigurations	



WEEK 16: Capstone & Review

Day 109–114

Capstone Project: Multi-Cloud Security Operations Dashboard (Sentinel + Chronicle)

Day 115–117

Write documentation + Security Architecture Diagram

Day 118–120

Final review + Resume/Portfolio update

Include project GitHub links

Congratulations!

You are now a **Multi-Cloud Security Engineer** ready to handle Azure & GCP defense, automation, and governance end-to-end.

📘 **Final Milestone:** You are now a **Multi-Cloud Security Engineer** ready to handle Azure & GCP defense, automation, and governance end-to-end.