Here’s a **detailed execution plan** for your project while ensuring you have **5 free hours daily**. I’ll break it down into **weekly goals** and **daily schedules** for maximum efficiency.

**📅 Project Execution Plan (4 Weeks)**

**💡 Goal:** Complete AWS & Azure security setup, logging, automation, and pentesting.  
**⏳ Daily Workload:** ~5 hours/day

**🟢 Week 1: IAM, Policies & S3 Bucket Setup (AWS & Azure)**

📌 **Objective:** Configure IAM roles, policies & secure cloud storage

**Day 1: AWS IAM & Azure RBAC Setup**

✅ Define IAM users, groups, roles in **AWS IAM**  
✅ Configure Azure **Role-Based Access Control (RBAC)**  
✅ Set up **least privilege access policies** for both

**Day 2: Secure AWS S3 & Azure Blob Storage**

✅ Create **AWS S3 bucket & Azure Blob Storage**  
✅ Define IAM policies for S3 bucket access  
✅ Configure **encryption (AWS KMS & Azure SSE)**

**Day 3: Enabling Logging & Monitoring**

✅ Enable **CloudTrail** log **Monitor & Activity Logs**  
✅ Store logs secure s in AWS  
✅ Enable **Azure** ly in S3/Azure Storage

**Day 4: Threat Detection Setup**

✅ Set up **AWS GuardDuty** for anomaly detection  
✅ Configure **Azure Defender for Cloud**  
✅ Enable **alerting on suspicious activities**

**Day 5: Validation & Review**

✅ Test IAM permissions  
✅ Verify logs are collected  
✅ Identify gaps for improvement

**🟢 Week 2: Logging, SIEM & Security Automation**

📌 **Objective:** Centralized logging, SIEM integration & automated threat detection

**Day 6: AWS CloudTrail & Azure Log Analytics Setup**

✅ Enable **AWS CloudTrail for API activity logs**  
✅ Configure **Azure Log Analytics Workspace**  
✅ Route logs from AWS → Azure Monitor

**Day 7: Integrating Logs with Splunk (SIEM)**

✅ Connect **AWS CloudTrail logs to Splunk**  
✅ Configure **Azure Sentinel (SIEM) for monitoring**  
✅ Define **log retention & filtering**

**Day 8: Setting Up Alerts & Incident Response Automation**

✅ Create **AWS CloudWatch Alarms**  
✅ Configure **Azure Monitor Alerts**  
✅ Automate incident responses with **Azure Logic Apps & AWS Lambda**

**Day 9: Advanced Threat Detection**

✅ Enable **GuardDuty & Azure Security Center**  
✅ Define **custom threat detection rules**  
✅ Simulate threats to test detection capabilities

**Day 10: Testing & Review**

✅ Validate **SIEM dashboards & alerts**  
✅ Optimize log retention policies  
✅ Identify false positives & fine-tune alerts

**🟢 Week 3: SOAR (Security Orchestration, Automation & Response)**

📌 **Objective:** Automate security responses & implement incident response

**Day 11: Setup Free SOAR Tool (Shuffle / Wazuh / TheHive)**

✅ Deploy **a free SOAR tool**  
✅ Connect it with **Splunk & Azure Sentinel**  
✅ Create security playbooks

**Day 12: Automate AWS & Azure Incident Response**

✅ Configure **AWS Step Functions** for auto-remediation  
✅ Use **Azure Logic Apps** to automate threat response  
✅ Trigger automated actions for **failed login attempts, unauthorized access**

**Day 13: Simulate Cyber Attacks & Measure Response**

✅ Use **Atomic Red Team** to simulate attacks  
✅ Validate **incident response workflows**  
✅ Improve **alert thresholds & automation**

**Day 14: Implement Web Application Firewall (WAF) & DDoS Protection**

✅ Deploy **AWS WAF** & **Azure Web Application Firewall**  
✅ Configure **DDoS mitigation (AWS Shield / Azure DDoS Protection)**  
✅ Test application security

**Day 15: Final Review of Security Automation**

✅ Ensure **automated response playbooks are working**  
✅ Optimize **response time & accuracy**  
✅ Document **findings & improvements**

**🟢 Week 4: Penetration Testing & Project Finalization**

📌 **Objective:** Test security defenses & finalize documentation

**Day 16: AWS & Azure Penetration Testing Setup**

✅ Get **Pentest Approval from AWS/Azure**  
✅ Use **Nmap, Nessus, Burp Suite, Metasploit** for scanning  
✅ Identify **vulnerabilities in IAM & Network Security Groups**

**Day 17: Exploit Simulation & Risk Assessment**

✅ Run **Common Vulnerabilities Exploits (CVE) scans**  
✅ Test for **SQL Injection, XSS & SSRF vulnerabilities**  
✅ Analyze **risk & impact of identified threats**

**Day 18: AWS & Azure Security Posture Review**

✅ Compare findings with **AWS Security Hub & Azure Defender**  
✅ Implement **remediation steps** for security flaws  
✅ Fine-tune **network rules & firewall settings**

**Day 19: Documentation & Report Writing**

✅ Document **security configurations & findings**  
✅ Summarize **threat detection strategies & improvements**  
✅ Prepare **a final project presentation**

**Day 20: Final Review & Deployment Check**

✅ Perform a **security audit**  
✅ Ensure **all logs, alerts & SOAR automation are working**  
✅ Submit the final **project report & findings**

**📌 Daily Work Schedule (Sample)**

| **Time Slot** | **Task** |
| --- | --- |
| **9:00 AM - 10:30 AM** | Configuration & Setup |
| **10:30 AM - 11:00 AM** | Testing & Validation |
| **11:00 AM - 12:30 PM** | Debugging & Refinement |
| **12:30 PM - 1:00 PM** | Documentation |
| **1:00 PM - 2:00 PM** | Research & Review |

**🎯 Key Outcomes**

✅ **Secure IAM & Storage Policies**  
✅ **Centralized Logging with SIEM (Splunk & Azure Sentinel)**  
✅ **Automated Threat Detection & Response (SOAR)**  
✅ **Network Hardening & Security Best Practices**  
✅ **Pentesting & Incident Simulation**  
✅ **Final Documentation & Security Report**

This **plan keeps you on track** while allowing **5 hours of free time per day**.  
⚡ **Do you want a more detailed breakdown for any specific area?**