SOC Analyst — Threat Detection Specialist — Security Automation

github.com/Omar671

6-MONTH PLAN FOR SOC ANALYST (4 HOURS/DAY)

MONTH 1-2: FOUNDATION & CERTIFICATIONS

Target Certifications:

- **CompTIA Security+** (Weeks 1-6)
- **Microsoft SC-900** (Weeks 3-4)
- **AWS Cloud Practitioner** (Weeks 5-8)

Weekly Breakdown:

Week 1-8: Security+ Intensive

- **Daily:** Professor Messer videos + Dion practice tests
- **Lab:** Setup SOC Home Lab with Wazuh
- **GitHub:** Create "security-plus-notes" repository

Week 3-9: Microsoft Security Stack

- **Daily:** Microsoft Learn modules for SC-900
- **Lab:** Azure Sentinel trial setup
- **GitHub:** "azure-sentinel-queries" - KQL queries

Week 5-12: Cloud Security Foundation

- **Daily:** AWS Cloud Practitioner course
- **Lab:** AWS Free Tier - Security Hub + GuardDuty
- **GitHub:** "cloud-security-basics" documentation

Week 7-24: Practical Application

- **Certification Exams:** Schedule all 3 certifications (keep studying if you think you won't pass the exam, There are more weeks ahead)
- **GitHub:** "certification-projects" showcase
- **LinkedIn:** Update headline with certifications
- **Applications:** applying..

MONTH 3-4: SOC SPECIALIZATION

Core Projects:

- **Enterprise SIEM Implementation**
- **Threat Detection Automation**
- **Incident Response Framework**

Weekly Breakdown:

Week 9-10: SIEM Mastery

- **Project:** "soc-home-lab-advanced" - Elastic Stack + Wazuh
- **Skills:** lot of detection rules, dashboard creation
- **GitHub:** Document entire setup with detection rules

Week 11-12: Threat Hunting

- **Project:** "threat-hunting-platform" - Python + MITRE ATT&CK
-
- **Skills:** Proactive threat detection, TTP mapping
- **GitHub:** Create hunting playbooks and scripts
- **Practice:** TryHackMe SOC Level 2 path completion

Week 13-14: Automation & SOAR

- **Project:** "soc-automation-framework" - Python
- **Skills:** API integration, alert enrichment, auto-response

- **GitHub:** automation scripts for common SOC tasks

Week 15-16: Incident Response

- **Project:** "incident-response-playbooks" - NIST framework
- **Skills:** Digital forensics, evidence collection, reporting
- **GitHub:** Create IR runbooks for different attack scenarios

MONTH 5-6: ADVANCED SPECIALIZATION & JOB HUNT

Advanced Projects:

- **Cloud SOC Implementation**
- **AI-Powered Security Tools**
- **Multi-Platform Detection**

Weekly Breakdown:

Week 17-18: Cloud SOC

- **Project:** "cloud-soc-monitoring" - AWS + Azure + GCP
- **Skills:** Cloud trail analysis, CSPM, cloud threat detection
- **GitHub:** Multi-cloud detection rules and scripts

Week 19-20: AI & Machine Learning

- **Project:** "ai-threat-detection" - Anomaly detection ML models
- **Skills:** Python ML libraries, behavioral analytics
- **GitHub:** Jupyter notebooks with security ML examples

Week 21-22: Portfolio Polish

- **GitHub:** Clean all repositories, add professional READMEs
- **LinkedIn:** Optimize profile with projects and certifications
- **Resume:** Tailor for international remote positions

Week 23-24: Intensive Job Search

- **Applications:** 5 quality applications per day
- **Interviews:** Practice technical interviews daily
- **Networking:** Leverage LinkedIn for referrals
- **Final Touch:** Create personal website/portfolio

GITHUB PORTFOLIO PROJECTS

Essential SOC Projects:

1. SOC Home Lab Complete

- **Tech:** Wazuh, Elastic Stack, TheHive, Cortex
- **Features:** detection rules, automated alerting
- **Docs:** Complete setup guide and use cases

2. Threat Intelligence Platform

- **Tech:** Python, MISP, AlienVault OTX, AbuseCH
- **Features:** IOC aggregation, automated enrichment
- **Docs:** API integration examples and dashboards

3. Security Automation Framework

- **Tech:** Python, Flask, Docker, multiple security APIs
- **Features:** Auto-triage, enrichment, response actions
- **Docs:** Installation guide and use case examples

4. Cloud Security Monitoring

- **Tech:** AWS CloudFormation, Azure ARM, Terraform
- **Features:** Multi-cloud detection, compliance monitoring
- **Docs:** Infrastructure as code templates

5. Incident Response Simulator

- **Tech:** Python, Vagrant, VirtualBox
- **Features:** Mock incident scenarios, evidence collection
- **Docs:** IR playbooks and forensic procedures

INTERNATIONAL JOB SEARCH STRATEGY

Target Companies:

- **MSSPs:** CrowdStrike, Palo Alto, Arctic Wolf
- **Tech:** GitLab, Shopify, Zapier (remote-first)
- **Startups:** Security startups on AngelList
- **Consulting:** Deloitte, EY, PwC (remote divisions)

Application Process:

- **Week 1-8:** Build foundation - no applications
- **Week 9-16:** Selective applications (5/week)
- **Week 17-24:** Aggressive applications (5/day)
- **Focus:** Quality over quantity - tailor each application

🚀 6-MONTH MASTER PLAN EXECUTION

Follow this roadmap rigorously + Adapt based on market feedback + Don't STOPPP