SOC Analyst Integrated Study Roadmap

This document provides a complete roadmap for becoming a SOC Analyst, integrating your Udemy course with free Microsoft Learn modules, certifications, and recommended software for Windows cybersecurity practice.

12-Week Integrated Study Plan

- Week 1-2: Foundations – Udemy Sections 1.1–1.6, 2.1–2.6; Microsoft SC-900 fundamentals; Set up Azure Free Account and Entra ID.
- Week 3-4: SIEM & Logs – Udemy Sections 5.1–5.7; Microsoft SC-200 Sentinel setup; Practice KQL queries; Document queries in GitHub.
- Week 5-6: Alert Handling & Investigation – Udemy Sections 6.1–6.5, 7.1–7.7; SC-200 incident triage; Create detection rules and playbooks.
- Week 7-8: Threat Intel & Playbooks – Udemy Sections 4.1–4.5, 9.1–9.8; SC-200 hunting queries; Build hunting notebooks and playbooks.
- Week 9-10: Detection Engineering & IR – Udemy Sections 10.1–10.6, 11.1–11.6; SC-200 advanced modules; Capstone attack simulation.
- Week 11-12: Portfolio & Certs – Udemy Sections 12.1–12.4; Complete SC-900, TryHackMe SOC Analyst Path, Fortinet NSE 1–3; Publish GitHub repo and demo video.

Free Certifications to Target

- Microsoft SC-900 (Security, Compliance, Identity Fundamentals) – Free learning path.
- Microsoft SC-200 learning paths – Free hands-on SOC modules.
- Fortinet NSE 1–3 – Free foundational certifications.
- TryHackMe SOC Analyst Path – Free tier available.

Recommended Software for Windows Cybersecurity Practice

- Hyper-V (built into Windows 10 Pro) or VirtualBox for virtualization.
- Splunk Free for SIEM practice.
- Microsoft Sentinel (cloud-based, via Azure).
- Microsoft Defender for Endpoint (trial).
- Wireshark for packet analysis.
- Sysinternals Suite for Windows log analysis.
- VS Code for scripting and KQL notes.
- GitHub Desktop for portfolio management.