



SOC Analyst Level: 3

Course Schedule

Step	Topic	Length(Hours)	Format
Step 1	Meet your mentor	1	Community Chat
Step 2	Soc Analyst 3 Assessment	0.5	Assessment
Step 3	CASP+	35	Course
Step 4	OWASP	12	Course
Step 5	Check for Indicators of Other Attack Activity (Debug PE File)	1.5	Lab
Step 6	Analyze SQL Injection Attack	1	Lab
Step 7	Analyze Various Data Sources to Confirm Suspected Infection	1	Lab
Step 8	Analyze and Classify Malware	1	Lab
Step 9	Analyze Malicious Activity in Memory Using Volatility	1	Lab
Step 10	Analyze Structured Exception Handler Buffer Overflow Exploit	0.5	Lab
Step 11	Microsoft Baseline Security Analyzer	1	Lab
Step 12	Use pfTop to Analyze Network Traffic	1	Lab
Step 13	Using Powershell to Analyze a system	1	Lab
Step 14	WebApp Attack PCAP Analysis	1	Lab
Step 15	Threat Designation	1	Lab
Step 16	Intro to Malware and Reverse Engineering	9	Course
Step 17	BSWJ Series WinDBG	0.5	Course
Step 18	BSWJ Series OllyDBG	0.5	Course
Step 19	Manually Analyze Malicious PDF Documents	1	Lab
Step 20	Manually Analyze Malicious PDF Documents Part 2	1	Lab

Step 21	BSWJ Series binwalk	0.5	Course
Step 22	Denial of Service PCAP Analysis	1	Lab
Step 23	RootKit	1	Lab
Step 24	Recover from SQL Injection Attack	1	Lab
Step 25	Recover from Web-Based Flashpack Incident	1	Lab
Step 26	Respond to Cyber Espionage against overseas corporate assets in Taiwan	1	Lab
Step 27	Post Incident Service Restoration	1	Lab
Step 28	Fundamentals of Risk Policies and Security Controls	1	Course
Step 29	SOC Analyst Assessment Level 1	1	Assessment
Step 30	SOC Analyst Assessment Level 2	1	Assessment
Step 31	Comprehensive Threat Response	2	Lab
Step 32	Resume and Job Prep Session	3.5	Course
Step 33	Review	1	One to One

