Career Path Syllabus: Become a SOC Analyst 1

Last Updated: November 2021

Career Path Description

A Security Operations Center Analyst (SOC Analyst) stands as a front line of defense against the ever-present cyber threats faced by organizations today. A SOC team ensures an organization’s digital assets remain secure and protected from unauthorized access by monitoring and responding to massive amounts of data in record time. In this role, you will protect your organization’s infrastructure by monitoring data to identify suspicious activity, then mitigating risks before a breach occurs. Cybrary's Become a SOC Analyst - Level 1 career path will equip you to break into the field with skills aligned to the US National Institute of Standards and Technology's Cyber Defense Analyst NICE work role.

Career Path Expectations and Goals

We have found the learners who are most successful in the program spend at least 30 minutes on learning a day. Your time is extremely valuable, so if there is a concept you already know, do not hesitate to skip that portion of the curriculum. The purpose of the career path is to ensure you have the knowledge/skills/abilities needed for the role. If you already have them, there is no need to duplicate efforts.

Career Paths can contain courses, labs, and assessments. Using these materials concurrently provides you with both instructional and hands-on experience that will enhance your chances of passing potential certification exams and give you the experience you need for the actual job role.

We also encourage you to engage with the mentors and other learners in the Cybrary Insider Pro (CIP) Slack Community. The CIP community members will share the insights they have acquired as they have gone through their journey. In addition, communicating difficult concepts is a learned skill and our community provides a risk-free environment for you to test that skill.

Career Path Outline

Important note: This syllabus presents Cybrary's suggested way to progress through the career path, but syllabus items do not need to be completed in the order they are listed. You have the freedom to complete items in any order.

Become a SOC Analyst - Level 1	Content Type	Difficulty	Duration (Hours)
Welcome to the SOC Analyst Level 1 Career Path	Course	Beginner	0.03
Kali Linux Fundamentals	Course	Beginner	2.1
Command Line Basics	Course	Beginner	5.5
Incident Response Procedures, Forensics, and Forensic Analysis Lab	Lab	Intermediate	1.5
Linux Attack and Response Lab	Lab	Intermediate	1.5
How to use BinWalk (BSWJ)	Course	Intermediate	0.1
Malware Threats	Course	Intermediate	4.5
Host Data Integrity Baselining	Lab	Intermediate	1
Attacks and Persistence for Incident Handlers	Course	Intermediate	0.5
Cybersecurity Kill Chain	Course	Beginner	1.75
Post Exploitation Hacking	Course	Advanced	7.75
Scanning, Enumeration, and Vulnerabilities	Course	Beginner	9
Creating Recommendations Based on Vulnerability Assessments	Lab	Intermediate	1
OWASP	Course	Intermediate	12.1
Sniffing	Course	Beginner	14.25
Deep Dive in Packet Analysis - Using Wireshark and Network Miner Lab	Lab	Advanced	1.5
Applying Filters to TCPDump and Wireshark	Lab	Intermediate	1
Use Wireshark to Intercept Network Traffic	Lab	Intermediate	1
Identify Non-Secure Network Traffic	Lab	Beginner	0.75
Parse Files Out of Network Traffic	Lab	Intermediate	1
Intro to Splunk	Course	Beginner	2.5

Log Analysis in Linux and Splunk Lab	Lab	Advanced	1.5
Log Event Reports	Lab	Intermediate	1
Event Log Collection	Lab	Intermediate	1
Log Correlation	Lab	Intermediate	0.75
Log Correlation & Analysis to Identify Potential IOC	Lab	Intermediate	1
Identifying Web Attacks Through Logs	Course	Beginner	2.25
Log Analysis	Lab	Intermediate	1.5
Centralized Monitoring	Lab	Intermediate	1
Creating SIEM Reports with Splunk	Lab	Intermediate	1
Intro to Python	Course	Beginner	3
Intro to PowerShell Scripting	Course	Beginner	1.75
Using PowerShell to Analyze a System	Lab	Intermediate	1
CompTIA Security+ (SY0-601)	Course	Beginner	8

Total titles: 34

Total learning hours: 95