Cybrary SOC Analyst Syllabus

Last Updated: 08-14-2018

General Information

Welcome! You have officially started your journey in becoming a Security Operations Center (SOC) Analyst. Along the way you will have the opportunity to connect with real world industry professionals to mentor you along the way. As you work through the program you will open up highly in-demand job opportunities; as well as, receive the appropriate knowledge, skills and abilities in order to earn a new job. In addition, much of the curriculum will provide you the resources to sit for, **and pass**, industry recognized certification exams.

Welcome Checklist

1. Choose Career Path relevant to current cybersecurity/IT experience
2. Find your curriculum under “My Assignments” on your home page. (Click on Cybrary logo to access)
3. Launch into your curriculum and fire up your first assignments (Start at top and work downward)
4. Need to meet your mentor? You will communicate with them and other Cybrary Insider Pro members on the community chat application Slack!
5. Look for Slack invite in your Cybrary email. If you don’t see one use the chat function on your Cybrary page (bottom right) to ask the Cybrary Customer Success team for an invite!
6. Once you have been added to Slack a member of the Cybrary team will reach out, and add you to the appropriate Career Path “Channel” to meet your mentors!

Expectations and Goals

We have found that the students who are most successful in the program spend at least 30 minutes on learning a day. This includes time for engaging with your mentor and your community. Communicating difficult concepts is a learned skill and our community provides a risk free for you to test that skill. In addition our community will show you some of the learnings they have gotten in the past as they have gone through their journey.

Your time is extremely valuable and so if there is a concept you already know do not hesitate to skip that portion of the curriculum. This syllabus is meant as a guide for a completely new person to the field.

The structure for the content is course, lab, assessment. By using the materials concurrently it will provide you with a surrounding experience that will both enhance your chances of passing the certification exam and give you the experience you need for the actual job role.

SOC Analysts are highly sought after in the cyber security industry, and this program will prepare you to confidently apply for this job role and start a new career in cyber security.

Lead Mentors	**Names in Slack:** **@Mark Nibert** **@Shane Markley**
Function	**Provide guidance on:** ● Career goals/planning, ● Cybersecurity industry knowledge, ● How to get into a cybersecurity work role, what a “day in the life” is like, ● Career path content questions, ● All other topics around cybersecurity/IT
Assistant Mentors	**Names in Slack:** @Joseph White / @Lori P / @nunoramao / @analyze
Function	**Provide Guidance on:** ● General career path related questions ● Common navigation problems ● Tell you where to go for specific technical issues ● Share experience with the industry
Schedule a Meeting	Mark Nibert: https://calendly.com/marknibert ---weekly calls, Sunday 12pm EST Shane Markley: https://calendly.com/shane-markley Weekly calls, Tuesday 12pm EST

Office Location & Hours	EST +7, Manama, Bahrain EST -3, Las Vegas, Nevada
Certifications You Will Be Prepared For	CompTIA Server+ CompTIA Network+ CompTIA Security+ CompTIA Linux+ Ec-Council CEH CompTIA CySA+ CompTIA CASP

Cybrary Insider Pro FAQ sheet located at bottom of document.

The courses listed below are listed in order for a reason. Each course will build upon itself from easier to more difficult. You will go over information gathering, enumeration, post exploitation and other key elements of penetration testing.

LIVE courses

Log in and check out our LIVE Soc Analyst page to locate new and upcoming course related to your career path! SOC Analyst

Course Schedule

Cybrary's SOC Analyst Career Path			
Entry SOC Analyst			
Steps	**Topic**	**Length (approx.)**	**Format**
Step 1	Meet your Mentor Session (via Slack Community). Connect with classmates starting with you.	1	Slack Community Chat
Step 2	CompTIA Linux+ (LX0-103 (modules 1-3))	4	On Demand Video Course
Step 3	CompTIA Linux+ Part 1 Virtual Lab (LX0-103)	20	Hands On Virtual Lab
Step 4	Practice Questions for the CompTIA Linux+ Part 1 (LX0-103)	3	Practice Test
Step 5	CompTIA Linux+ Part 1 Practice Test	1.5	Practice Test

	(LX0-103)		
Step 6	**Lab1:** Performing Incident Response in a Windows Environment **Lab 2:** Use pfTop to Analyze Network Traffic **Lab 3:** Identifying System Vulnerabilities with OpenVAS Using PowerShell to Analyze a System **Lab 4:** Using Snort and Wireshark to Analyze Traffic **Lab 5:** Denial of Service PCAP Analysis **Lab 6:** Manual Vulnerability Assessment **Lab 7:** Vulnerability Scan Analysis	30-45 minutes a day of labs	Hands On Virtual Labs to develop real world experience
Step 7	CompTIA Linux+ Part 2 (Module 4)LX0-104)	2	On Demand Video Course
Step 8	CompTIA Linux+ Part 2 Virtual Lab (LX0-104)	20	Hands On Virtual Lab
Step 9	Practice Questions for the CompTIA Linux+ Part 2 (LX0-104)	3	Practice Test
Step 10	CompTIA Linux+ Part 2 Practice Test (LX0-104)	N/A	Practice Test
Step 11	CompTIA Server+ Virtual Lab	20	Hands On Virtual Lab
Step 12	Practice Questions for the CompTIA Server+	3	Practice Test
Step 13	CompTIA SK0-004: Server+ Practice Test	1.5	Practice Test
Step 14	Virtualization Management	20	On Demand Video

			Course
Step 15	CompTIA Network+	32	On Demand Video Course
Step 16	CompTIA Network+ Virtual Lab (N10-007)	20	Hands On Virtual Lab
Step 17	Practice Questions for the CompTIA Network+ (N10-007)	3	Practice Test
Step 18	Full CompTIA Network+ Practice Test	1.5	Practice Test
Step 19	Peripheral Devices and Connectors	2	On Demand Video Course
Step 20	Review and Curriculum Spill Over	N/A	Review
Step 21	Resume and Job Prep Session (w/ Mentor)	N/A	Job Preparation

When you are ready, continue on to

Junior SOC Analyst

Week	Topic	Length (approx.)	Format
Step 1	Meet your Mentor Session (via Slack Community)	1	Slack Community Chat
Step 2	CompTIA Security+ (SY0-501)	10	On Demand Video Course
Step 3	CompTIA Security+ Virtual Lab (SY0-501)	20	Hands On Virtual Lab
Step 4	Practice Questions for the CompTIA Security+ (SY0-501)	3	Practice Test
Step 5	CompTIA Security+ Practice Test (SY0-501)	N/A	Practice Test
Step 6	Intro to Cyber Threat Intelligence	4	On Demand Video Course

Step 7	Security Assessment & Testing	2	On Demand Video Course
Step 8	Fundamental Vulnerability Management	2	On Demand Video Course
Step 9	**Lab 1:** Applying Filters to TCPDump and Wireshark Memory Extraction and Analysis **Lab 2:** Parse Files Out of Network Traffic Recover from SQL Injection Attack **Lab 3:** Threat Designation Vulnerability Analysis/Protection **Lab 4:** Vulnerability Identification and Remediation Creating Recommendations Based on Vulnerability Assessments **Lab 5:** Centralized Monitoring	N/A	Hands On Virtual Labs to develop real world experience
Step 10	Penetration Testing and Ethical Hacking	14	On Demand Video Course
Step 11	Certified Ethical Hacker (CEH) Virtual Lab	5	Hands On Virtual Lab
Step 12	Log Analysis	2	Hands On Virtual Lab
Step 13	Conduct Log Analysis and Cross Examination for False Positives	2	Hands On Virtual Lab
Step 14	Performing an Initial Attack Analysis	2	Hands On Virtual Lab
Step 15	Review and Curriculum Spill Over	N/A	Review

Step 16	Resume and Job Prep Session (w/ Mentor)	N/A	Job Preparation
When you are ready, continue on to Senior SOC Analyst			
Step 1	Meet your Mentor Session (via Slack Community)	1	Slack Community Chat
Step 2	Web App Security Fundamentals	2	On Demand Video Course
Step 3	Asset Security	1	On Demand Video Course
Step 4	Introduction to Wireshark Virtual Lab	5	Hands On Virtual Lab
Step 5	Computer and Hacking Forensics	7	On Demand Video Course
Step 6	Computer Forensics and Investigations Virtual Lab	5	Hands On Virtual Lab
Step 7	IDS/IPS	2	On Demand Video Course
Step 8	CompTIA Advanced Security Practitioner (CASP)	11	On Demand Video Course
Step 9	CompTIA Advanced Security Practitioner (CASP)	5	Hands On Virtual Lab
Step 10	Practice Questions for the CompTIA Advanced Security Practitioner (CASP)	3	Practice Test
Step 11	CompTIA Advanced Security Practitioner (CASP) Practice Test	3	Practice Test
Step 12	CompTIA CySA+ Threat Management	2	On Demand Video Course
Step 13	CompTIA CySA+ Virtual Lab	5	Hands On Virtual Lab

Step 14	Practice Questions for the CompTIA CySA+	3	Practice Test
Step 15	CompTIA CySA+ Practice Test	3	Practice Test
Step 16	Advanced Cyber Threat Intelligence	3	On Demand Video Course
Step 17	Nessus Fundamentals	2	On Demand Video Course
Step 18	**Lab 1:** Dynamic Malware Analysis Capstone Identify Rootkit and DLL Injection Activity Image Forensics Capstone **Lab 2:** Analyze and Classify Malware Identify Whether High-Risk Systems Were Affected **Lab 3:** Analyze Structured Exception Handler Buffer Overflow Exploit Check for Indicators of Other Attack Activity (Debug PE File) **Lab 4:** Comprehensive Threat Response Cybersecurity Testing with Core Impact	N/A	Hands On Virtual Labs to develop real world experience
Step 19	Review and Curriculum Spill Over	N/A	Review
Step 20	Resume and Job Prep Session (w/ Mentor)	N/A	Job Preparation

Additional Log Analysis Training

[Routergods Wireshark Playlist]

Hak5 Wireshark Playlist

Cybrary Insider Pro FAQ:

GENERAL
What is the training format of Cybrary?
All of the training through Cybrary is on-demand and available 24/7:

- On-demand Video-Based Courses
- Virtual Hands On Labs
- Capture the Flag Assessments
- Monthly Live Webcasts
- Monthly Live Course

What is the benefit of Cybrary over other training providers?
Cybrary provides you premium access to innovative, experiential learning and skill assessment technology. Over 300 tools are available for purchase in the catalog via the Cybrary Vendor network. The Cybrary platform is an ecosystem, which brings together the learner and the employer. This partnership allows the individual to develop a deep understanding of a company, their services or products, and build the skills needed to advance their career.

Are there any LIVE training courses?
We offer live training courses for certification prep and NICE cybersecurity workforce education! See the LIVE tab on the Cybrary site for additional information! (Episodes will be recorded and posted some time after they are recorded for those who were not able to join in). We primarily use the 24/7 on-demand video-based training format to provide the flexibility of self-paced learning. This option also allows learners to go back through any training modules to help them retain information through repetition.

How do I get added to a Career Path channel?
When you chose a Career Path, you will receive a welcome message with instructions on how to proceed. Please reach out to @Sam from our Customer Success Team for further assistance.

Which is the best Career Path for me?
Check out the following two links for guiding on choosing a Career Path:

- https://www.cybrary.it/course-paths/
- https://www.cybrary.it/cyber-security-jobs/

CompTIA's Career Path Roadmap might also help with you decision on how you want to progress through training. As always, feel free to reach out to any of the Mentors or Customer Success team for additional guidance.

Can I change Career Paths once I start one?
Of course! We want your learning experience to be exactly what you are looking for. If you start a career path that you are not comfortable with, just let @Sam and/or @Megan from our Customer Success Team know and they will get you moved over.

How do I access my assignments?
Your assignments are located under your home tab on Cybrary.it under "My assignments":

Your assignments are listed from top to bottom base on the syllabus for each career path. If any of the assignment hyperlinks are broken, please make sure to bring this to the attention of the Mentors/Customer Success Team so it can be corrected. In the meantime, you can also search for a specific assignment under the courses catalog - **https://www.cybrary.it/catalog/.**

Do I have to follow all of my assignments in the exact order?
The assignments list and syllabus are there for guidance purposes on the best way to progress through a career path, but they do not need to be followed exactly how they are listed.

What is the deadline for assignments?
While we provide guidance on how to progress through the various Career Paths, there are no hard deadlines for assignments. Cybrary's teaching format is meant to be self-paced so learners are able to go through the program as slow or as fast as they chose. We encourage people to use Cybrary as a continuous learning tool as content is consistently being updated which is very much needed in our ever changing industry.

Will there be any Final Projects?
Yes! We are currently developing this part of the program and we will be releasing some beta Final Projects for testing.

Is there a mobile version of Cybrary?
Yes! There is a Cybrary.it app currently available for Android. We are still working on usability testing on this app as well as providing it for different formats.

Who are my mentors?
@Mark Nibert and @Shane Markley are the three Senior Mentors for all Career Paths. There are also a handful of Assistant Mentors assigned to each channel for additional assistance. Assistant Mentors are also very active in the *public_chat* channel and will typically have "Assistant Mentor" description in their Slack profile. @gina is the Mentor to reach out to for job placement assistance, resume building, and interview skills.

Where can I find additional help with the CTF Exercises?
There is minimal help we can offer with the CTF Exercises/Assessments as those scores are tracked. We are able to offer general guidance, but not give too much information on how to answer the questions. If there are any technical issues with the CTF Exercises or HOLs, please report this to support@practice-labs.com and also notify your Mentors so they have visibility on the problems that are occurring. If you are not getting a timely response from the Labs Support Team, please notify @Sam and/or @Megan from our Customer Success Team for escalation assistance.

What is the best certification for me to start with?
We will be doing a more detailed overview for specific certifications in the near future. Our monthly live webinars also go into detail for certifications based on the specific Career Path that is being covered. CompTIA's IT Certification Roadmap is also a great resource.

How do I become an Assistant Mentor?
Mentoring gives you the extraordinary opportunity to facilitate a protege's personal and professional growth by sharing knowledge you learned through your experience. While the primary intent of your mentoring role is to challenge the protege to think in new and different ways, the protege is not the only one who gains from the arrangement. As a mentor, there are various ways you can benefit as well:

- Enhance your skills. The experience you gain by mentoring someone can facilitate your own professional growth, making you more of an asset to your organization/industry. Mentoring allows you to strengthen your coaching and leadership skills by working with individuals from different backgrounds and with different personality types.

- Develop and retain talent in your organization. Your role as a mentor can contribute to the success of your entire organization. As a Cybersecurity professional, you know the importance of developing and retaining good employees.
- Create a legacy. By becoming a mentor, you create a legacy that has a lasting impact on your protege and the Cybersecurity field.
- Opportunity to be promoted to a Junior Mentor for future cohorts.

Reach out to @Mark Nibert and @Shane Markley for additional information.

Can I "test out" of any of my assignments?
If you have direct work experience or hold a current certification in a subject you may skip the content and move to the next subject. The purpose of the career path is to ensure you have all the Knowledge/skills/abilities associated with the program. If you already have them there is no need to duplicate efforts.

Will any of the Career Paths prepare me to take any certifications?
Each career path has certification courses, these courses will prepare you to take the certification it is teaching. If you feel like you need more training or other resources please reach out to the mentors to get supplemental material. This material may be on Cybrary but they can also make recommendations on things to use outside of Cybrary to help you obtain that certification.

I am having trouble with <insert lab, course, assessment, CTF? How do I find help?
Our first recommendation is to post any questions you have in the cohort channel. If no one responds you can also try the public chat. The assistant mentors and career mentors are also here to help if those options do not work. Please remember that investigation and research is a large part of the learning process and only becomes more prominent as you move forward in your career.

TECHNICAL ISSUES

How do I troubleshoot general access issues with Labs?
First, always clear cache, cookies and allow all pop-ups. If it is a potential access issue or glitch with the lab, it might be a good idea to restart the individual VMs

or log out and back into the lab environment. If you are able to recreate the issue in the lab, then the problem might be with the actual lab itself and the issue should be submitted. They can be contacted via the Help and Support tab within the labs or by emailing support@practice-labs.com. It is always a good idea to post something to your channel to see if anyone else is experiencing any issues and so that the Mentors and Customer Success staff have knowledge that this is occurring. There is usually a way to find a workaround, but if not, feel free to skip over that particular exercise and continue forward for now so they do not get too far behind.

How do I troubleshoot issues with VMs not starting?
It is a good idea to try logging out and back into the lab environment to see if the issue still exists. It is also a good idea to test from a different OS or computer if this option is available. This will help to further troubleshoot the issue.

What do I do if I have issues with the CTF Assignments?
There is minimal help we can offer with the CTF Exercises/Assessments as those scores are tracked. We are able to offer general guidance, but not give too much information on how to answer the questions.

ADMINISTRATIVE QUESTIONS
Whom do I contact in regards to Accounting/Billing questions?
The Cybrary Customer Success Team can assist you with any questions regarding billing/account in the chat icon on the Cybrary.it website. We have access to your account information here so the process is as quick and seamless as possible.

Whom do I provide general feedback to?
Feedback is always encouraged and appreciated. The Cybrary Team logs all feedback through the chat icon on your Cybrary.it website.

JOB PLACEMENT
Hiring managers are looking for cyber experience and I don't have any. What should I do?
This is an age-old issue that many new and transitioning job seekers face. We encourage you to keep persisting in seeking experience. Everyone starts somewhere and, odds are, someone will give you your "big break" at some point.
Additionally, here are a few ways to potentially acquire non-traditional experience: take part in free hackathons and CTFs; join a Meetup that focuses on IT and Cyber issues (although this won't provide experience, it will show industry involvement and may be a

good place to network); consider doing volunteer work in your area of interest (if you can afford to do so).

How do I add my Cybrary courses/career path to my resume?
We often recommend adding your courses/career path to the “Education” section on your resume. Keep in mind that if you’ve not yet completed your courses or career path, you might write something like this:

Does my resume need to be one page?
The short answer: No. Why? These days, job seekers (especially cyber and IT) have many skills, certs, accomplishments, educational components, and experience they should include on their resume; this info does not often fit on one page. Also, remember that your resume may be loaded into a database, in which case the number of pages is not relevant. Be aware, though, that you should aim to keep the MS Word version of resume to three pages max.

How can I improve my interview skills?
Reading, researching, and practice can all help. Read articles (and watch free videos) on how to be a better interviewee. Research the companies with whom you have interviews. Learn everything you can about them. Practice interviewing with a friend or the career mentor at Cybrary (via Skype).